Microsoft

Introduction to Microsoft security solutions

Learning Path Agenda

- Describe Microsoft Security Copilot.
- Describe core infrastructure security services in Azure.
- Describe security management capabilities of Azure.
- Describe capabilities of Microsoft Sentinel.
- Describe threat protection with Microsoft Defender XDR.

Module 1: Describe Microsoft Security Copilot

Module 1 introduction

In this module, you will get acquainted with Microsoft Security Copilot. You are introduced to some basic terminology, how Microsoft Security Copilot processes prompts, the elements of an effective prompt, and how to enable the solution.

Learning objectives

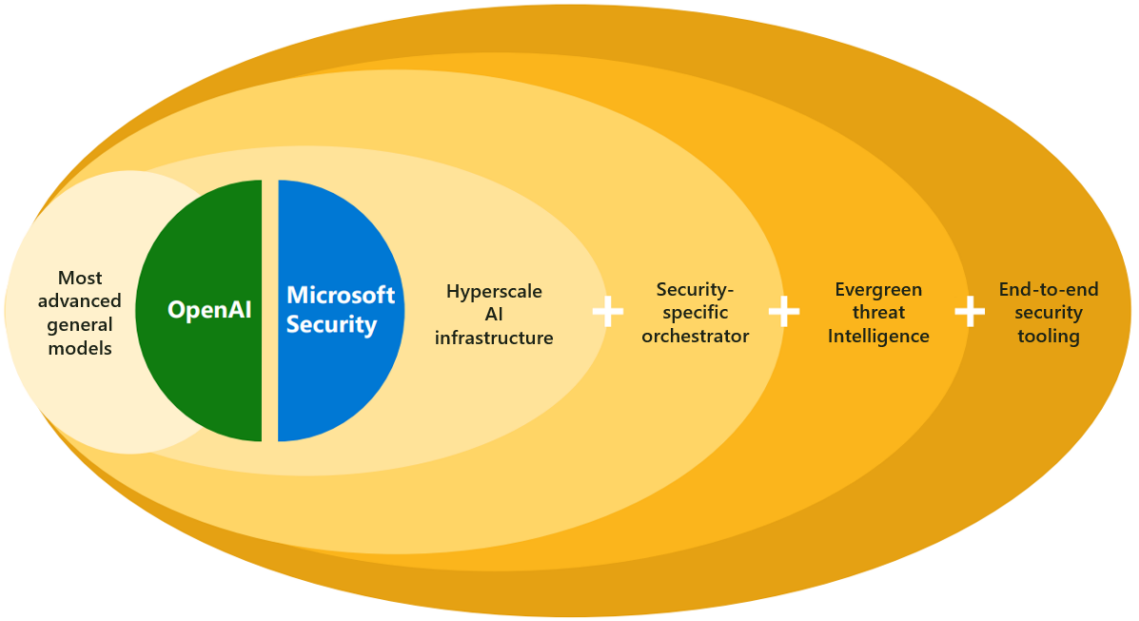
By the end of this module, you'll be able to:

- Describe what Microsoft Security Copilot is.
- Describe the terminology of Microsoft Security Copilot.
- Describe how Microsoft Security Copilot processes prompt requests.
- Describe the elements of an effective prompt
- Describe how to enable Microsoft Security Copilot.

Describe what 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.

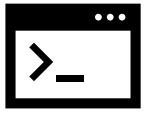
- Copilot combines powerful LLMs with a security-specific model from Microsoft.
- Copilot integrates with Microsoft and non-Microsoft sources.
- Copilot learns at machine speed to help analysts identify and respond to emerging threats.
- Enterprise data is protected by comprehensive enterprise compliance and security controls.



Describe Microsoft Security Copilot – Use cases

Incident summarization. Distil complex security alerts into concise actional summaries.

Impact analysis. Assess the potential impact of security incidents to enable quicker response times and streamlined decision-making.

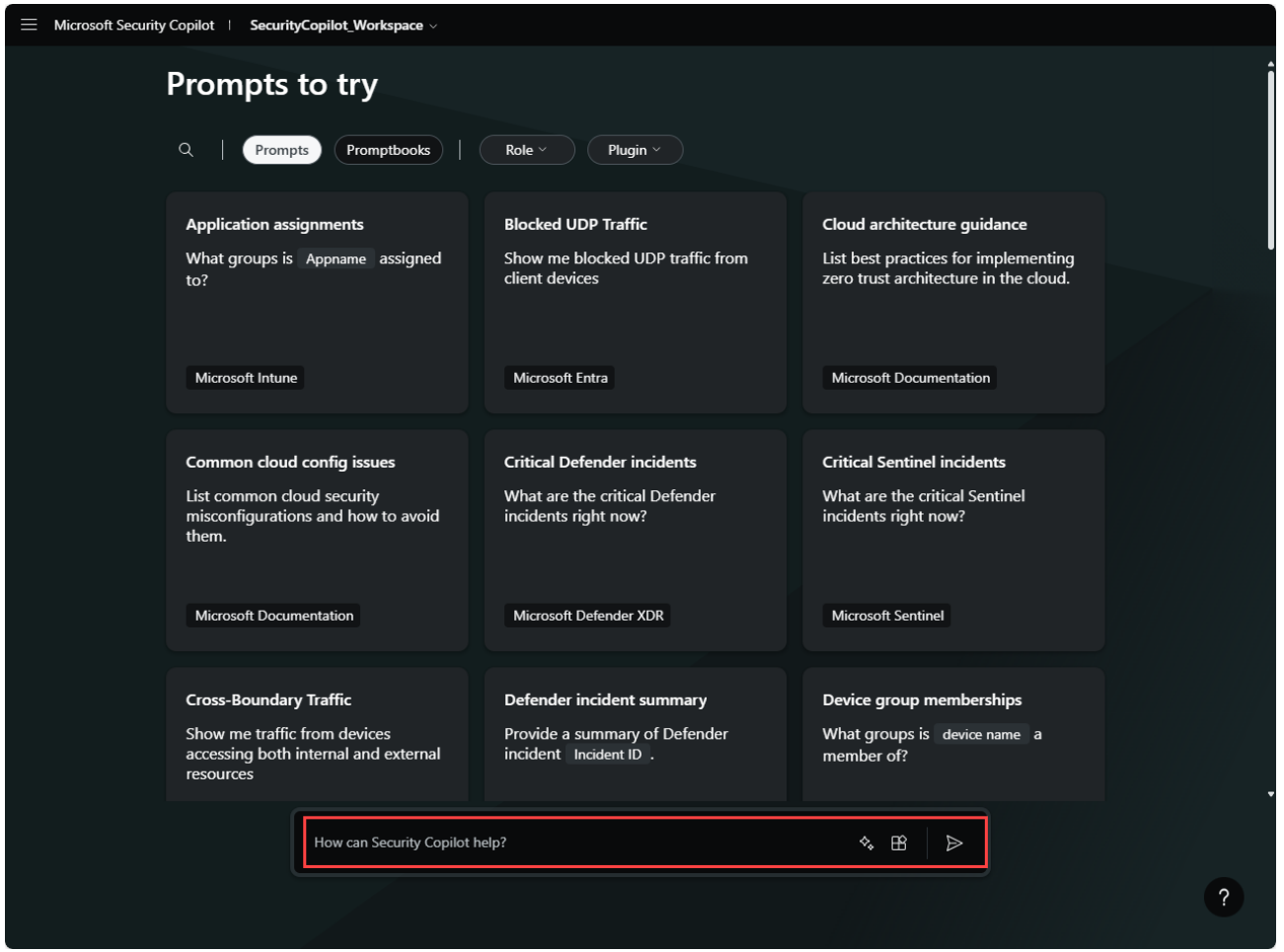


Reverse engineering of scripts. Analyze complex command line scripts and translate them into natural language with clear explanations of actions.

Guided responses. Actionable step-by-step guidance for incident response, including directions for triage, investigation, containment, and remediation.

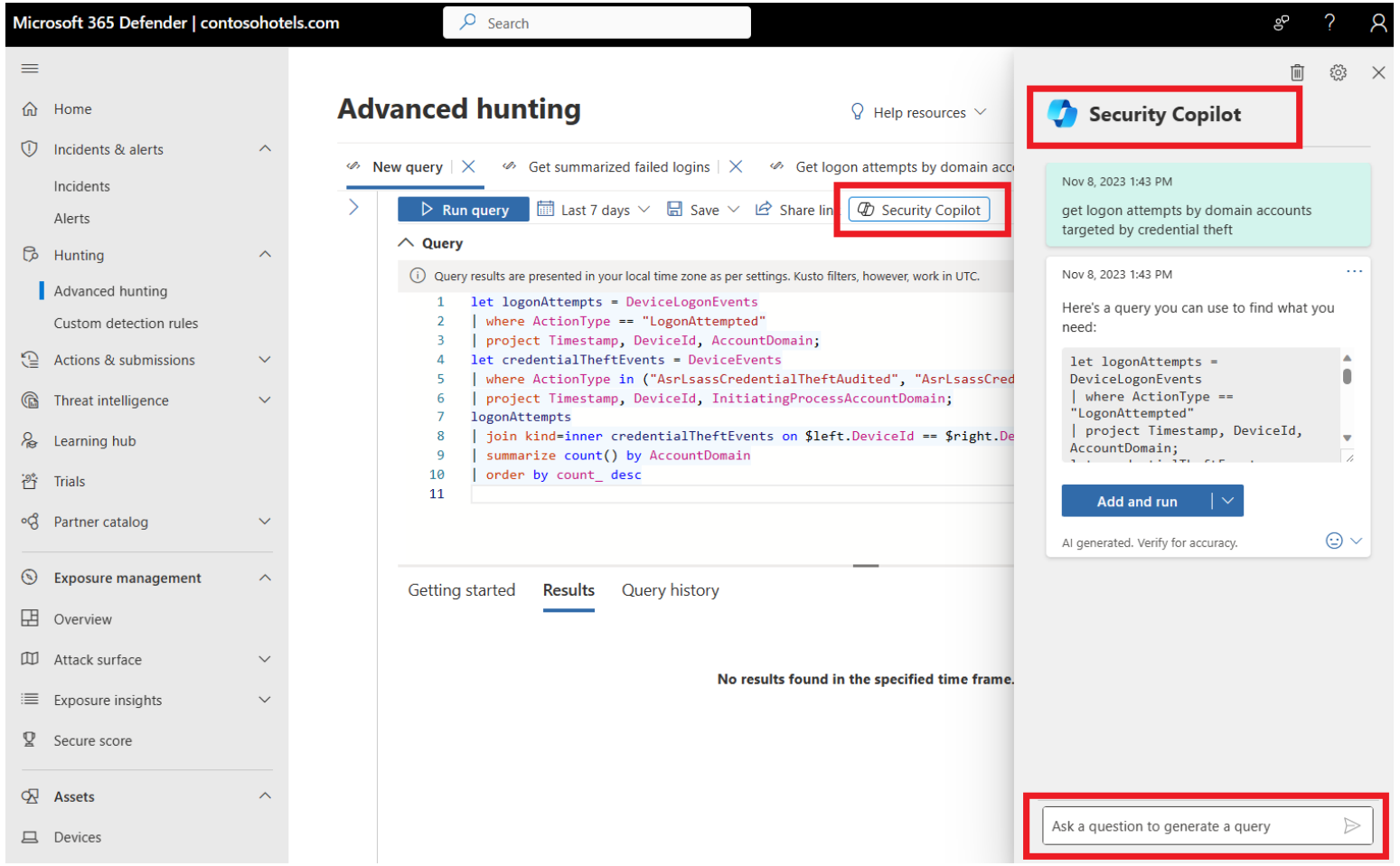
Describe Microsoft Security Copilot - Standalone experience

- Copilot through a dedicated site.
- Users make requests in natural language and receive response outputs as text, images, or documents.



Describe Microsoft Security Copilot – Embedded experience

- Some Microsoft products embed Copilot directly inside their user interface.

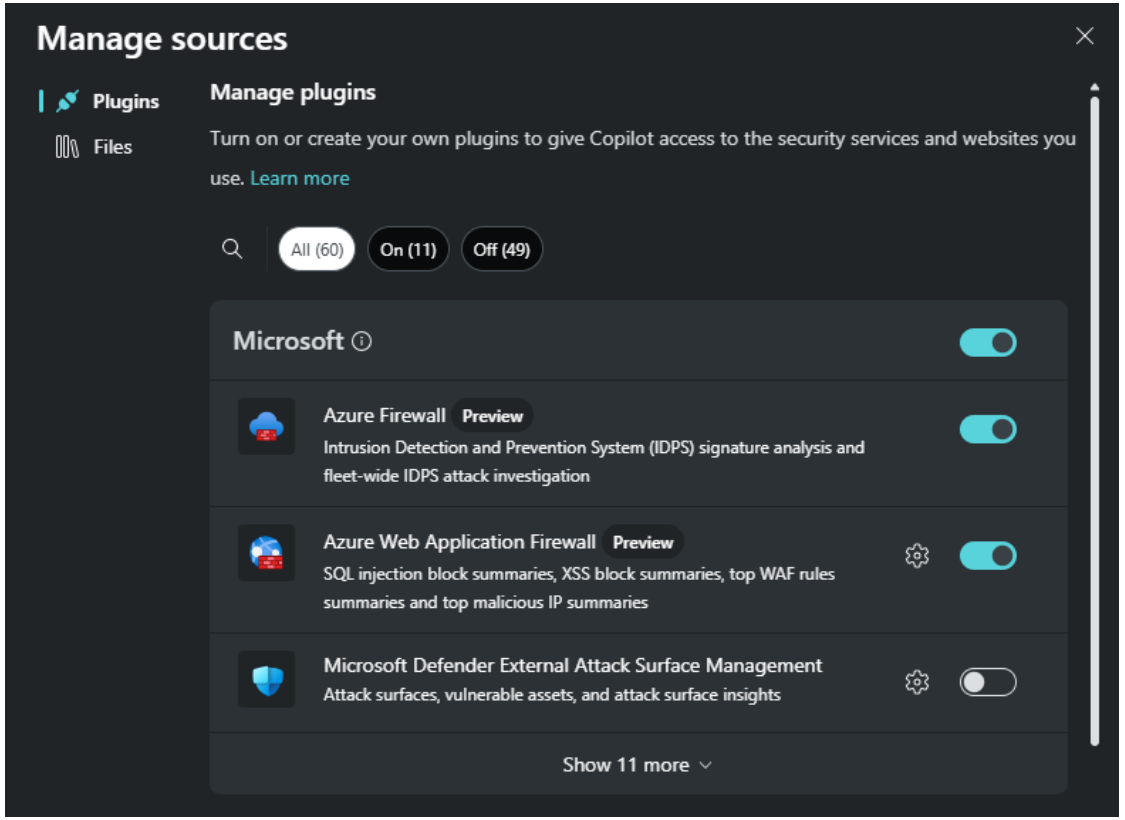


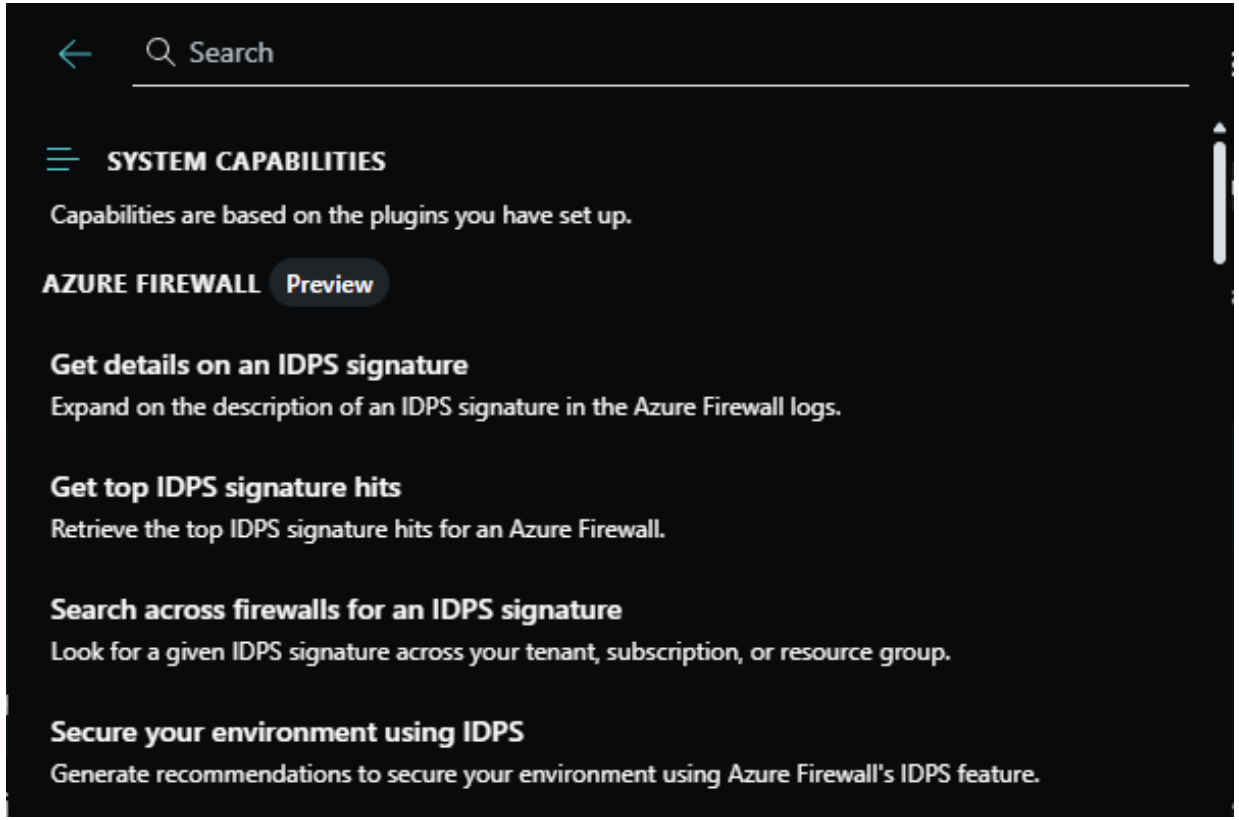
Describe the terminology of Microsoft Security Copilot

- **Session**: a particular conversation within Microsoft Security Copilot.
- **Prompt**: a specific user statement or question within a session.
- **Capability**: a function Microsoft Security Copilot uses to solve part of a problem.
- **Plugin**: A collection of capabilities by a particular resource, like Microsoft Intune.
- **Workspace**: Copilot workspaces are separate Copilot work environments within the tenant in which your Copilot instance is operating.
- **Agents**: 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**: Used to compose skills together, to answer a user's prompt.

The prompt bar, used to enter prompts.

Example: plugins and capabilities

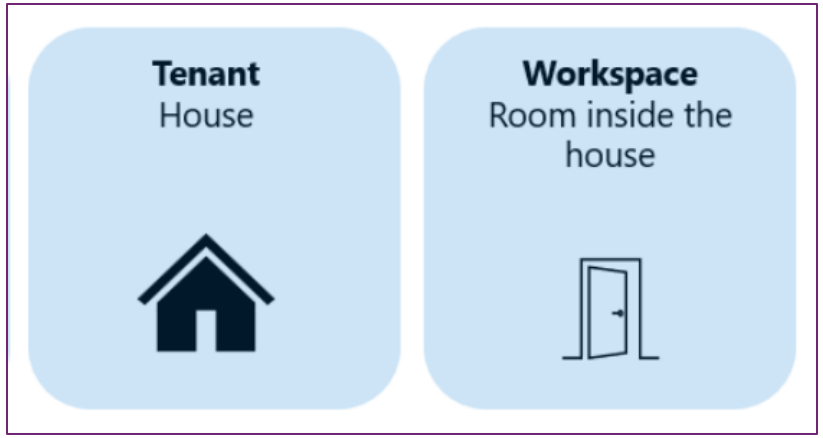


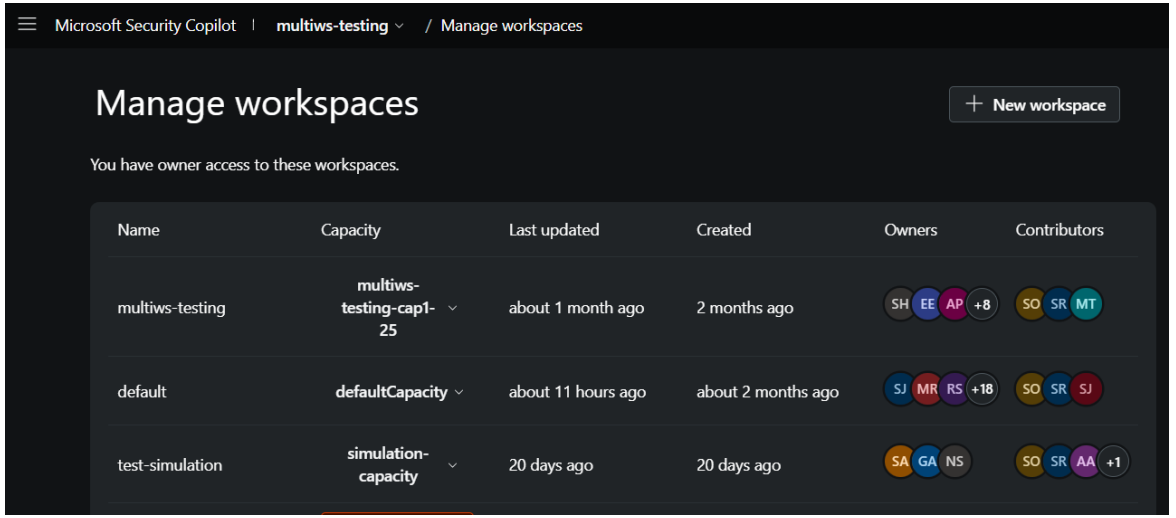


Copilot workspaces

Benefits of Copilot workspaces:

- Set up individual workspaces to address specific team needs.
- Manage and map costs based on team needs and budgets.
- Ensure critical workflows aren't disrupted by throttling.
- Store session data according to geo-specific regulations.
- Set up and manage specific plugins, promptbooks, and files for specific team needs.
- Experiment with custom plugins and promptbooks before organization-wide deployment.

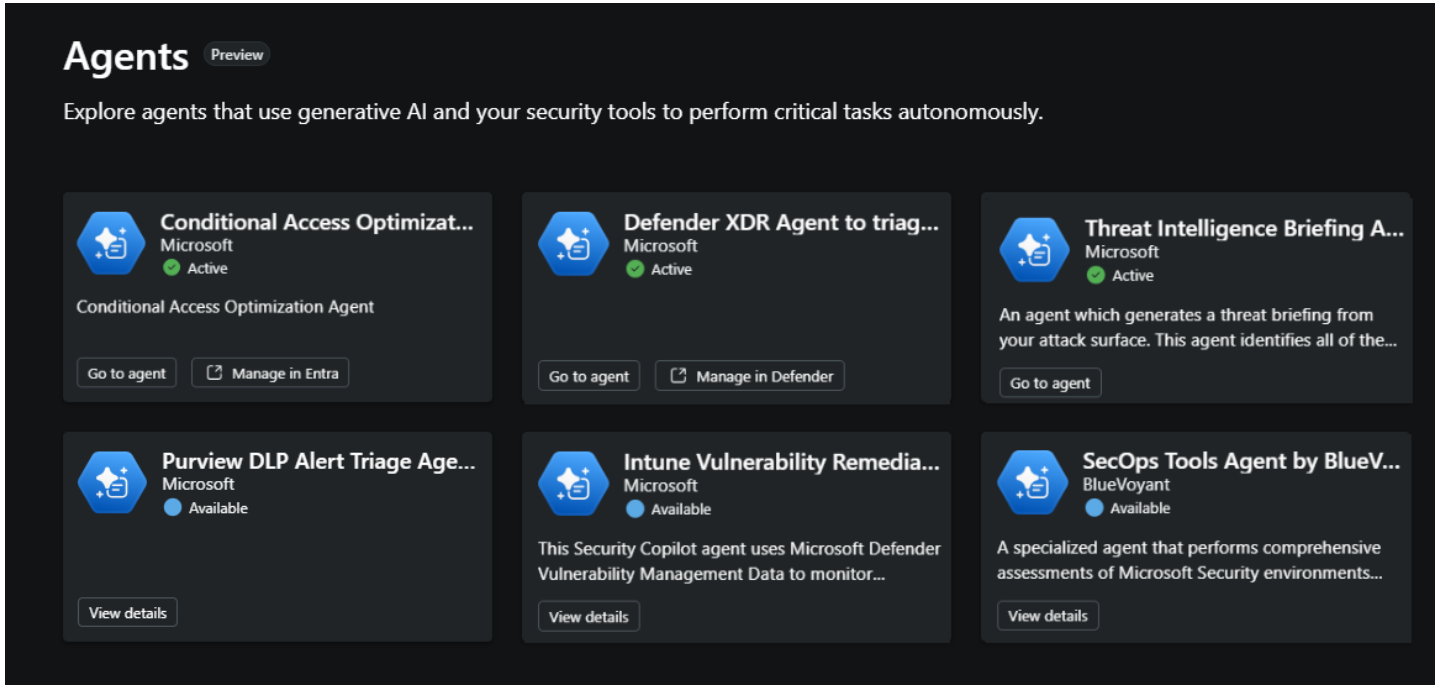




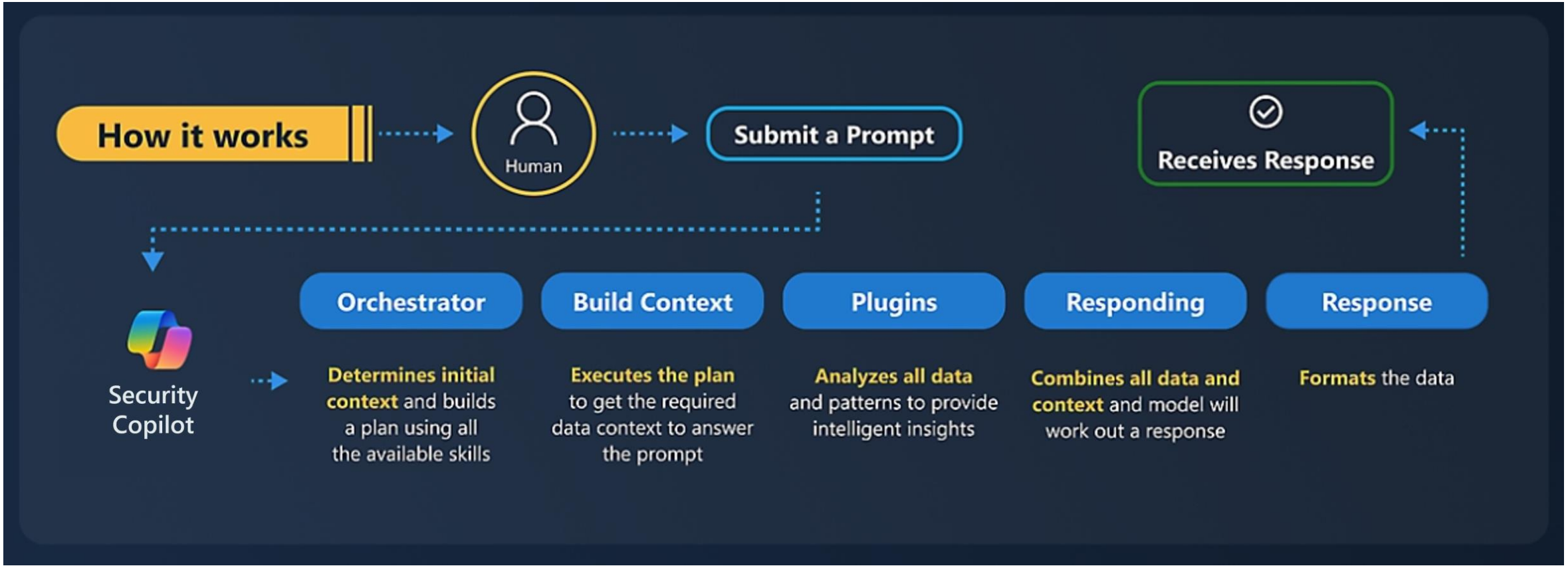
Describe Microsoft Security Copilot agents

AI-powered assistants built into Microsoft Security Copilot

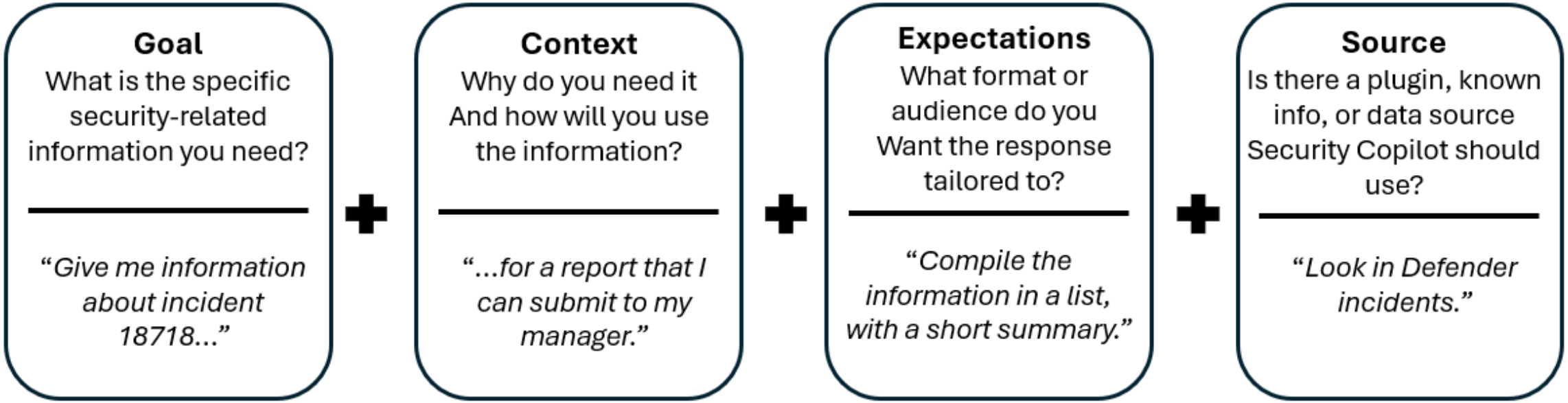
- Automate repetitive tasks, reduce manual workloads, and optimize security operations.
- Agents learn based on feedback and keep you in control on the actions it takes.
- Agents are available in the standalone and embedded experiences.
- Integrate seamlessly with Microsoft Security solutions and the broader supported partner ecosystem.
- Utilize security compute units (SCUs) to operate.



Describe how Microsoft Security Copilot processes prompt requests



Describe the elements of an effective prompt



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. Role assignments

Demo

Explore the standalone experience of Microsoft Security Copilot

Module 2: Describe the core infrastructure security services in Azure

Module 2 introduction

After completing this module, you should be able to:

1. Describe Azure security capabilities for protecting your network.
2. Describe Azure Bastion.
3. Describe Azure Key Vault.

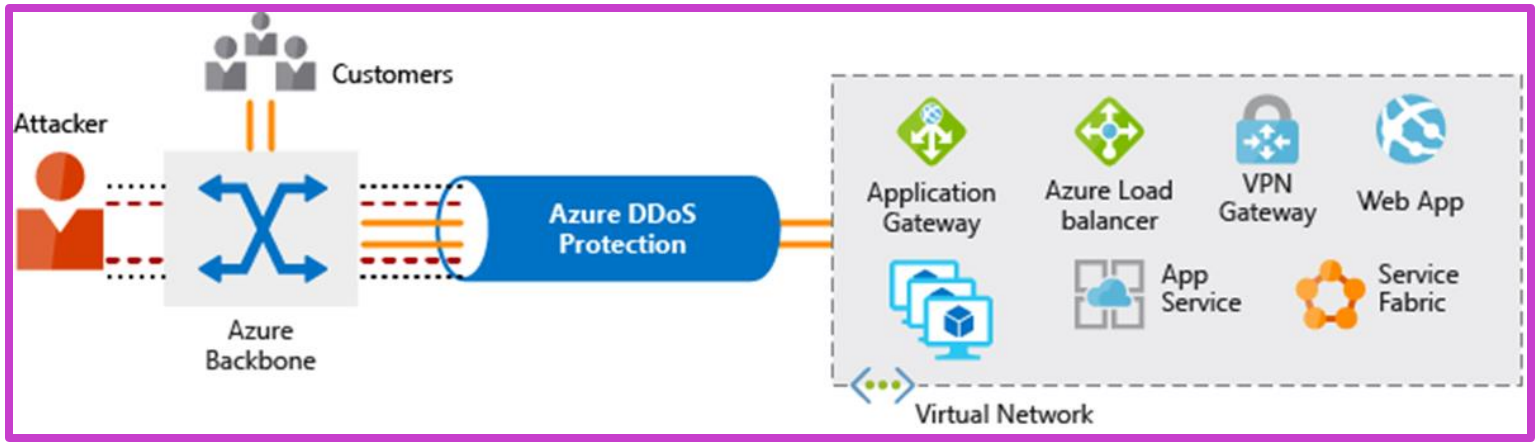
Azure DDoS Protection

Distributed Denial of Service (DDoS)

- Attacks that makes resources unresponsive.

Azure DDoS protection

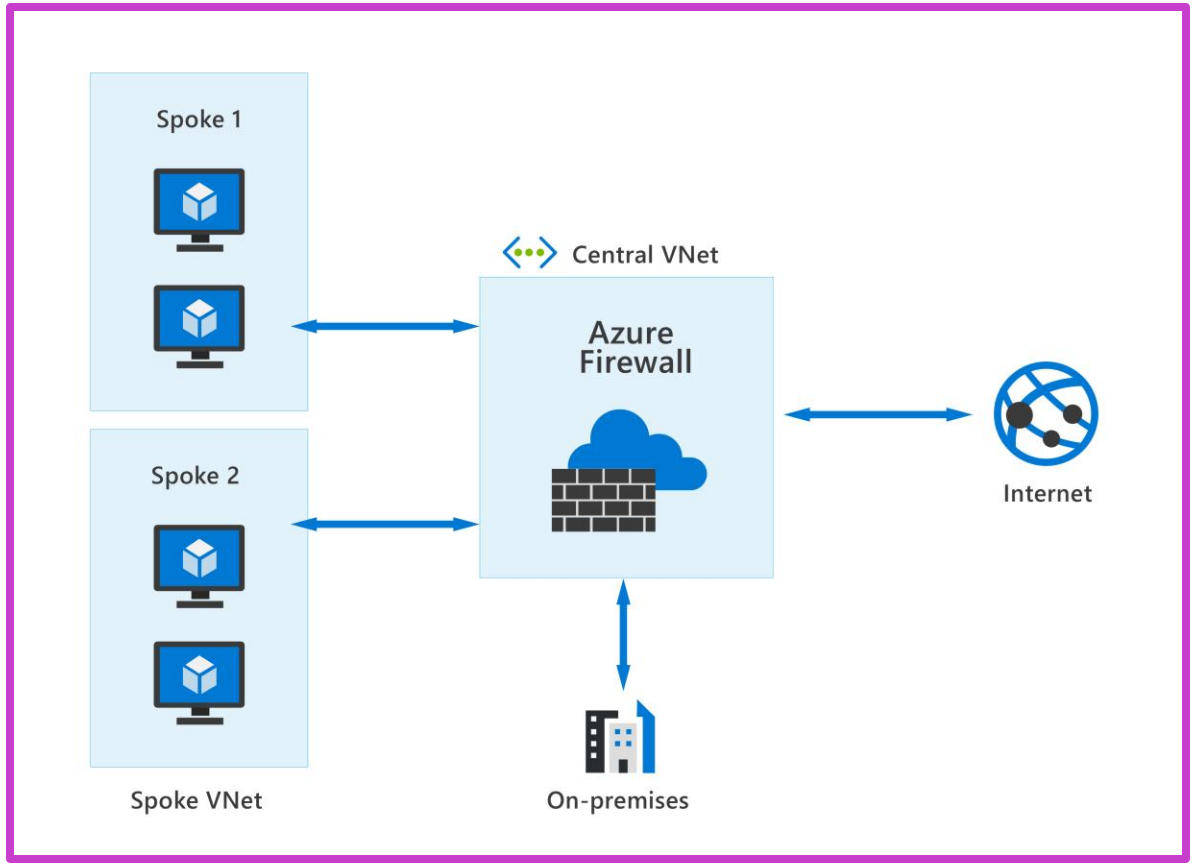
- Analyzes network traffic and discards anything that looks like a DDoS attack.
- Always-on traffic monitoring.
- Adaptive real-time tuning.
- DDoS Protection telemetry, monitoring, and alerting.



Azure Firewall

Azure Firewall protects your Azure Virtual Network (VNet) resources from attackers.

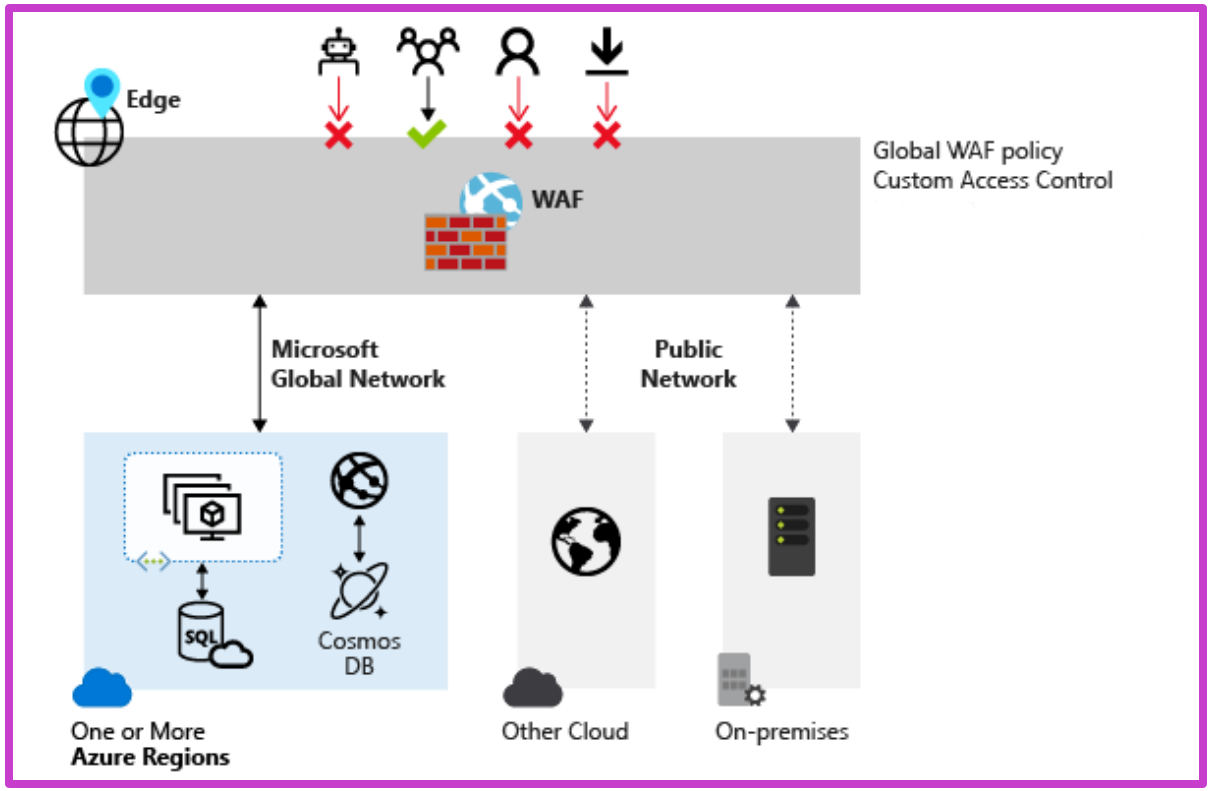
- Create *allow* or *deny* network filtering rules.
- Use Microsoft Threat Intelligence feed to alert or filter traffic from/to known malicious IP addresses and domains.
- All outbound virtual network traffic IP addresses are translated to the Azure Firewall public IP to make it harder for attackers to target internal network devices.
- Integration with Microsoft Security Copilot
- And much more…



Web Application Firewall

Centralized protection of your web applications from common exploits and vulnerabilities.

- Protection against threats and intrusions.
- Protects web applications DDoS attacks.
- Patching a known vulnerability in one place.
- Integration with Microsoft Security Copilot
- And more…



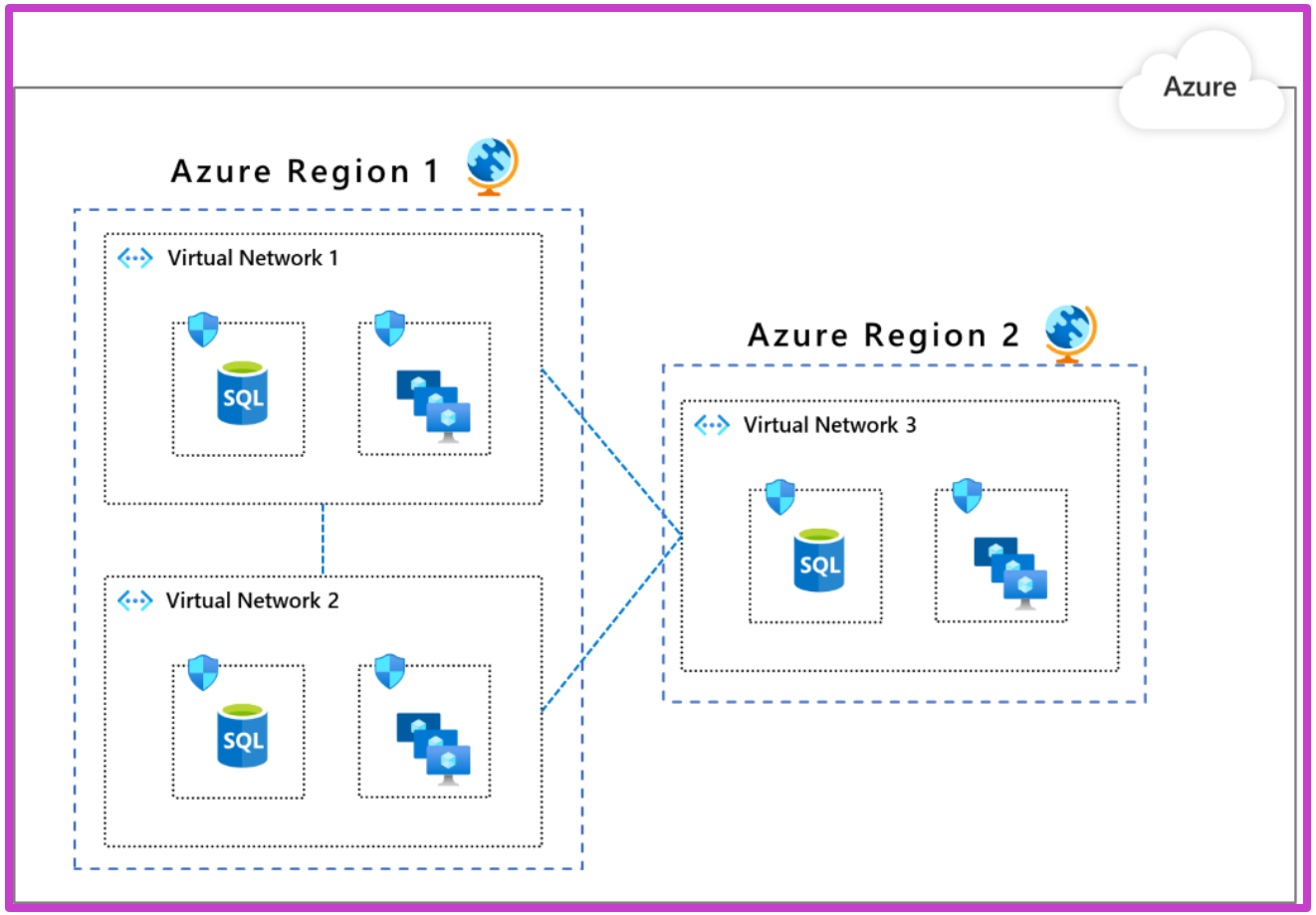
Network segmentation and Azure VNet

Reasons for network segmentation

- The ability to group related assets.
- Isolation of resources.
- Governance policies set by the organization.

Azure Virtual Network (VNet)

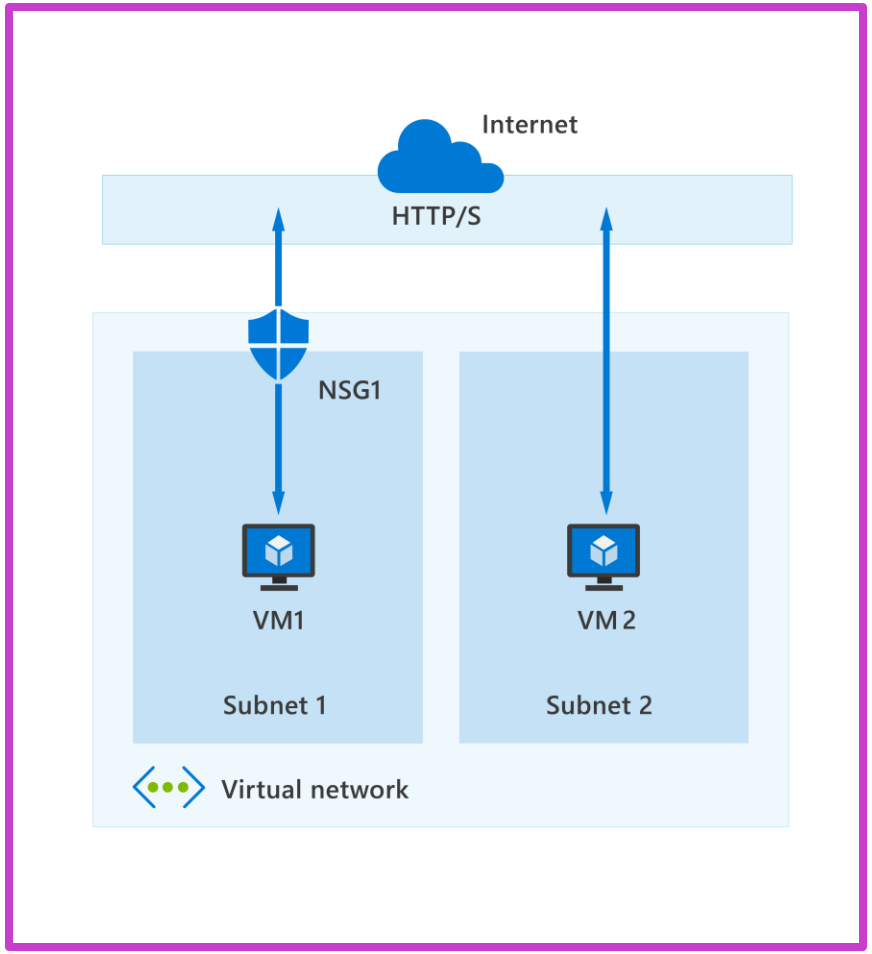
- Network level containment of resources with no traffic allowed across VNets or inbound to VNet.
- Communication needs to be explicitly provisioned.
- Control how resources in a VNet communicate with other resources, the internet, and on-premises networks.



Azure network security groups (NSGs)

Filter network traffic between Azure resources in an Azure virtual network.

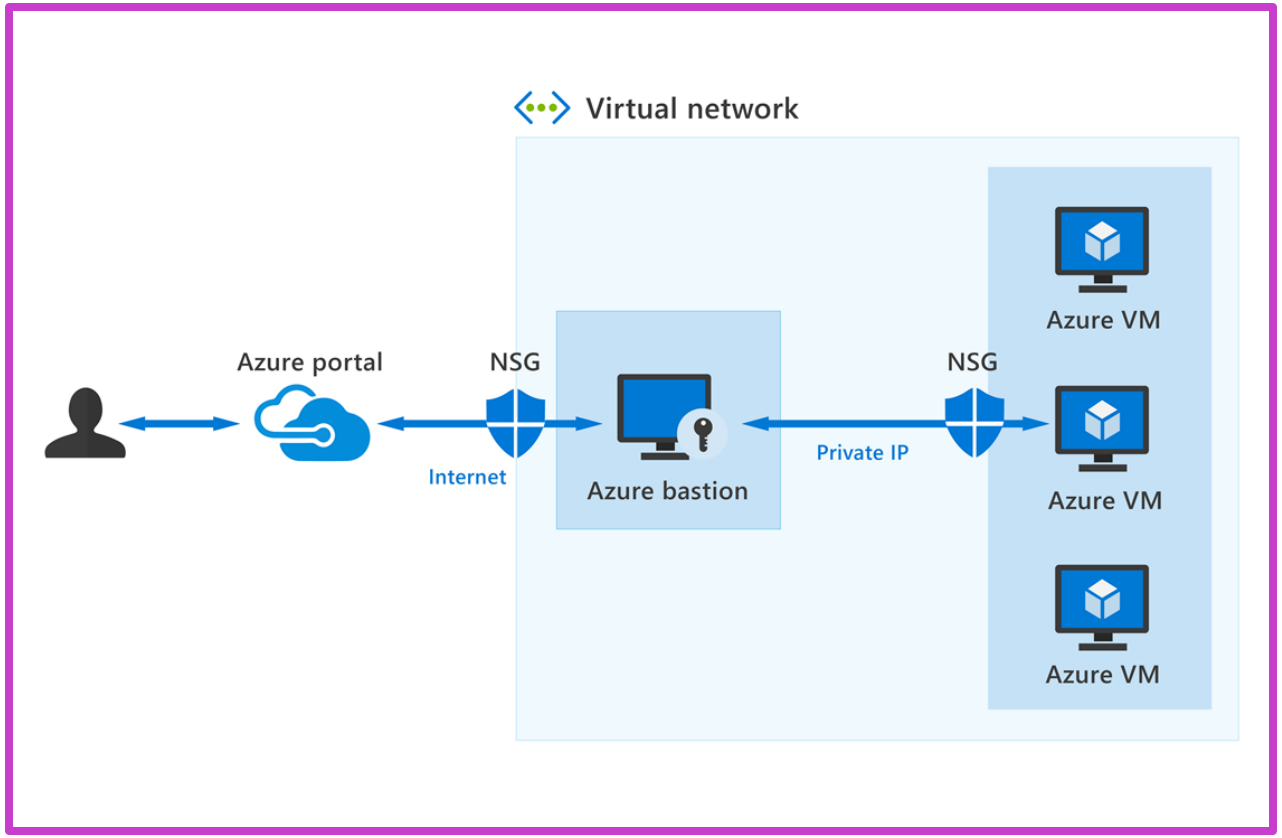
- An NSG is made up of inbound and outbound security rules that allow or deny traffic.
- An NSG can contain many rules, the rules are processed based on their assigned priority.
- When an NSG is created, it includes default inbound and outbound rules.
- You can't remove the default rules, but you can override them by creating new rules with higher priorities.



Secure remote access to VMs: Azure Bastion

Azure Bastion – secure connectivity to your VMs from the Azure portal.

- RDP and SSH directly in the Azure portal.
- Traverse the corporate firewalls securely.
- No public IP required on Azure VM.
- No need to manage NSGs.
- Protection against port scanning.
- Protect against zero-day exploits.

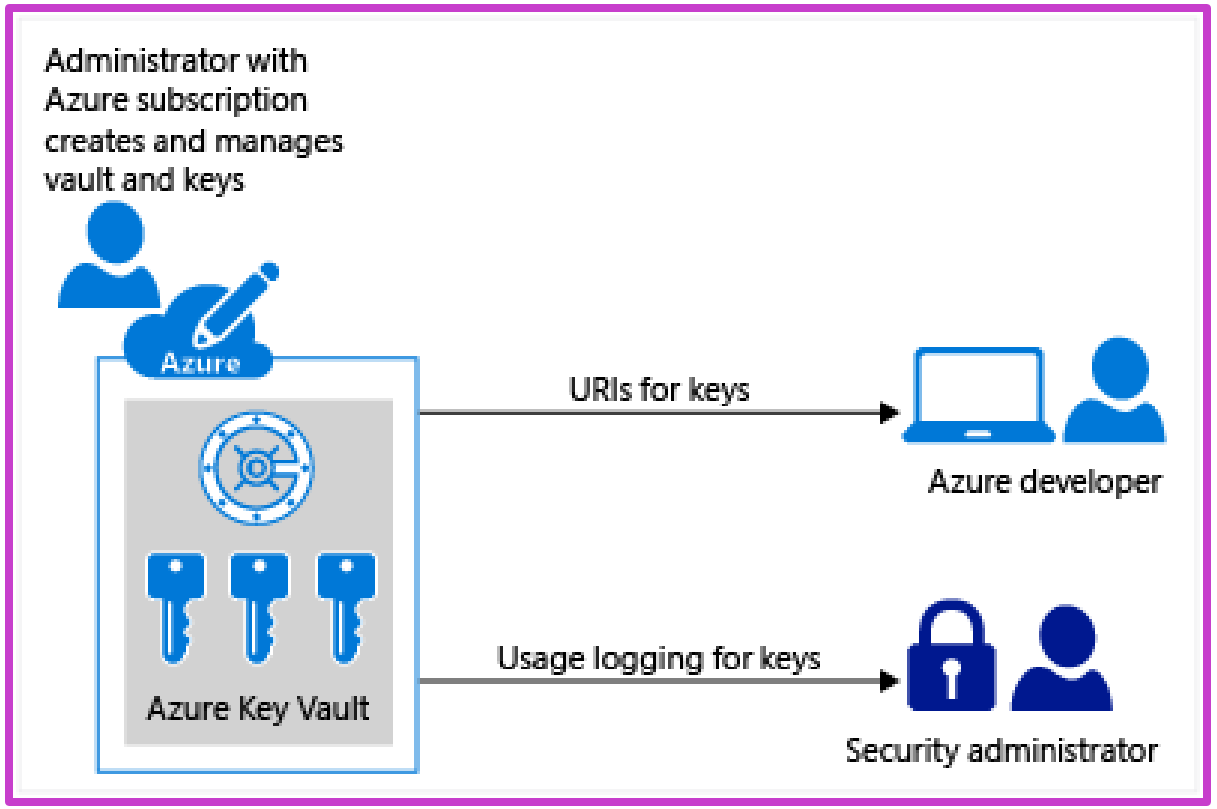


Azure Key Vault

A cloud service for securely storing and accessing secrets such as API keys, passwords, certificates, or cryptographic keys.

Key Vault benefits

- Centralize application secrets.
- Securely store secrets and keys.
- Monitor access and use.
- Simplified administration of application secrets.
- Two tiers
  - Standard: SW-based encryption.
  - Premium: HW security module (HSM) protected keys.



Module 3: Describe security management capabilities of Azure

Module 3 introduction

After completing this module, you should be able to:

1. Describe Microsoft Defender for Cloud.
2. Describe how security policies and initiatives improve cloud security posture.
3. Describe how the three pillars of Microsoft Defender for Cloud protect against cyberthreats and vulnerabilities.

Microsoft Defender for Cloud

A cloud-native application protection platform (CNAPP) with a set of security measures and practices designed to protect cloud-based applications from various cyberthreats and vulnerabilities.

Cloud security posture management (CSPM)

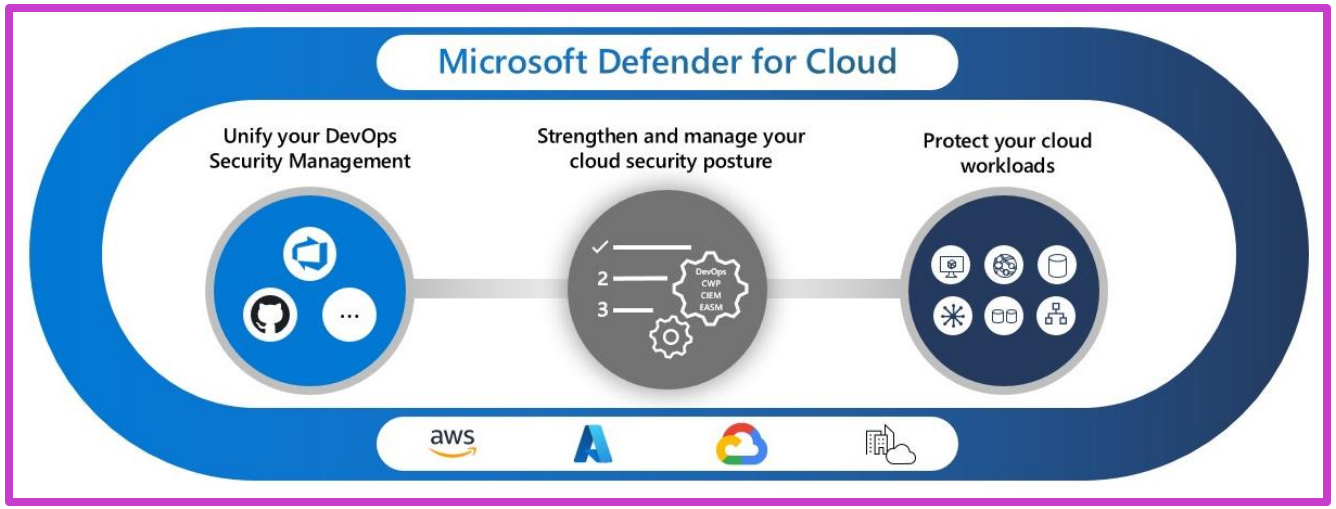
Surfaces actions that you can take to prevent breaches.

Cloud workload protection platform (CWPP)

Specific protections for servers, containers, storage, databases, and other workloads.

Development security operations (DevSecOps)

Unifies security management at the code level across multicloud and multiple-pipeline environments.



Describe how security policies and initiatives improve cloud security posture

Security initiatives

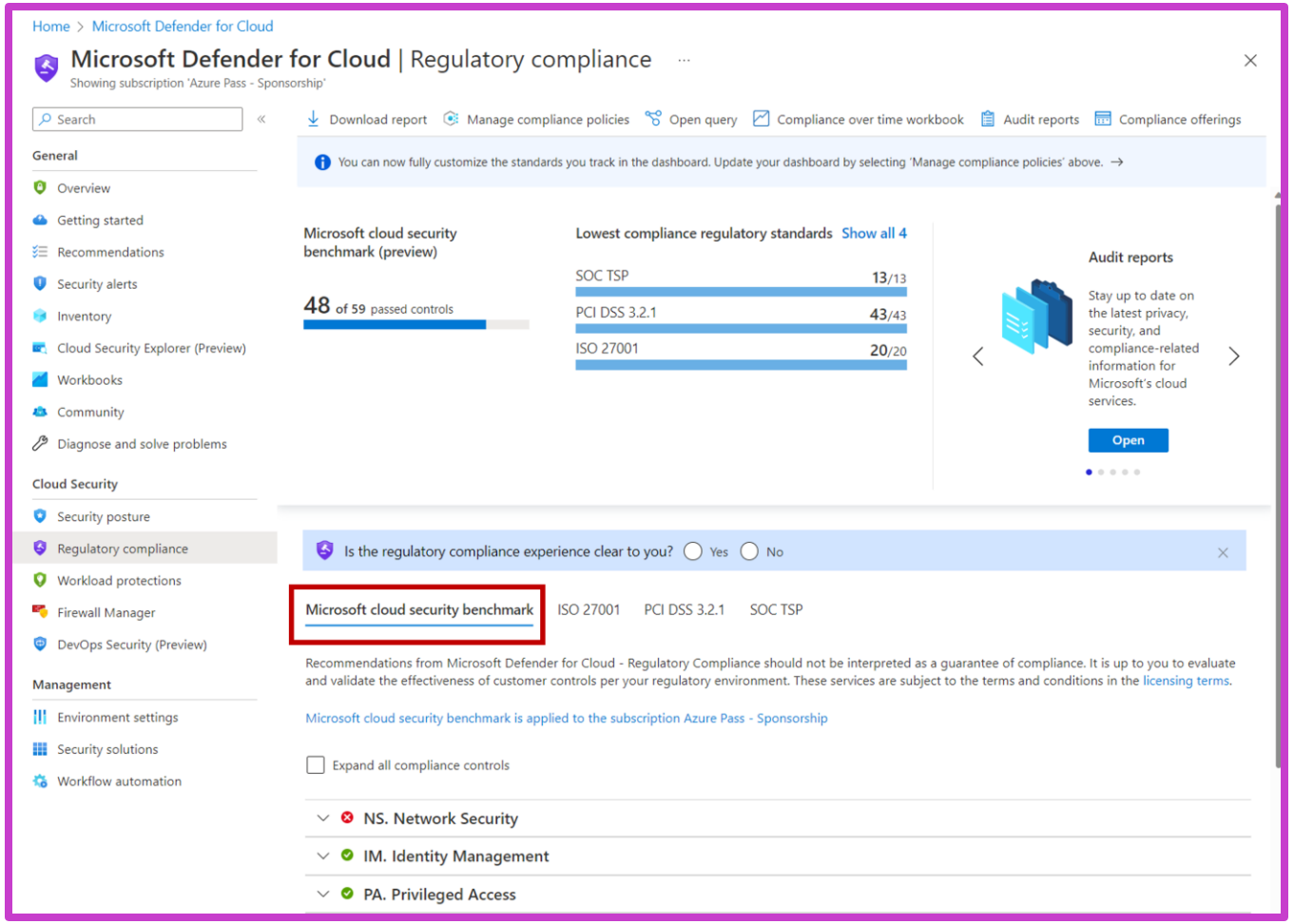
- A collection of policies.
- Assigned to resources, subscriptions, and so on.

Microsoft cloud security benchmark (MCSB)

- Default security initiative in Defender for Cloud.
- Provides best practices and recommendations to improve the security of workloads, data, and services on Azure and other clouds.

Microsoft Defender for Cloud

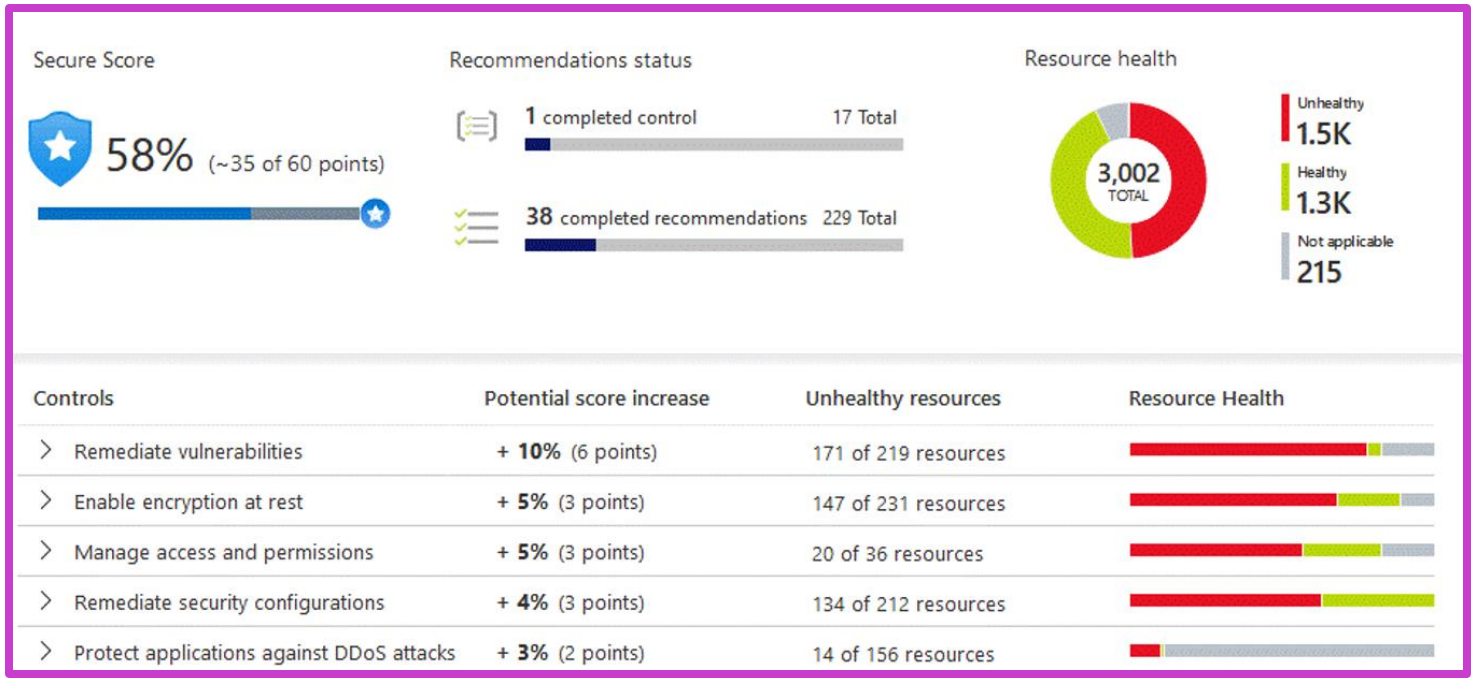
- Continually assesses your environment against MCSB and other security initiatives.



Cloud Security Posture Management (CSPM)

Visibility and recommendations

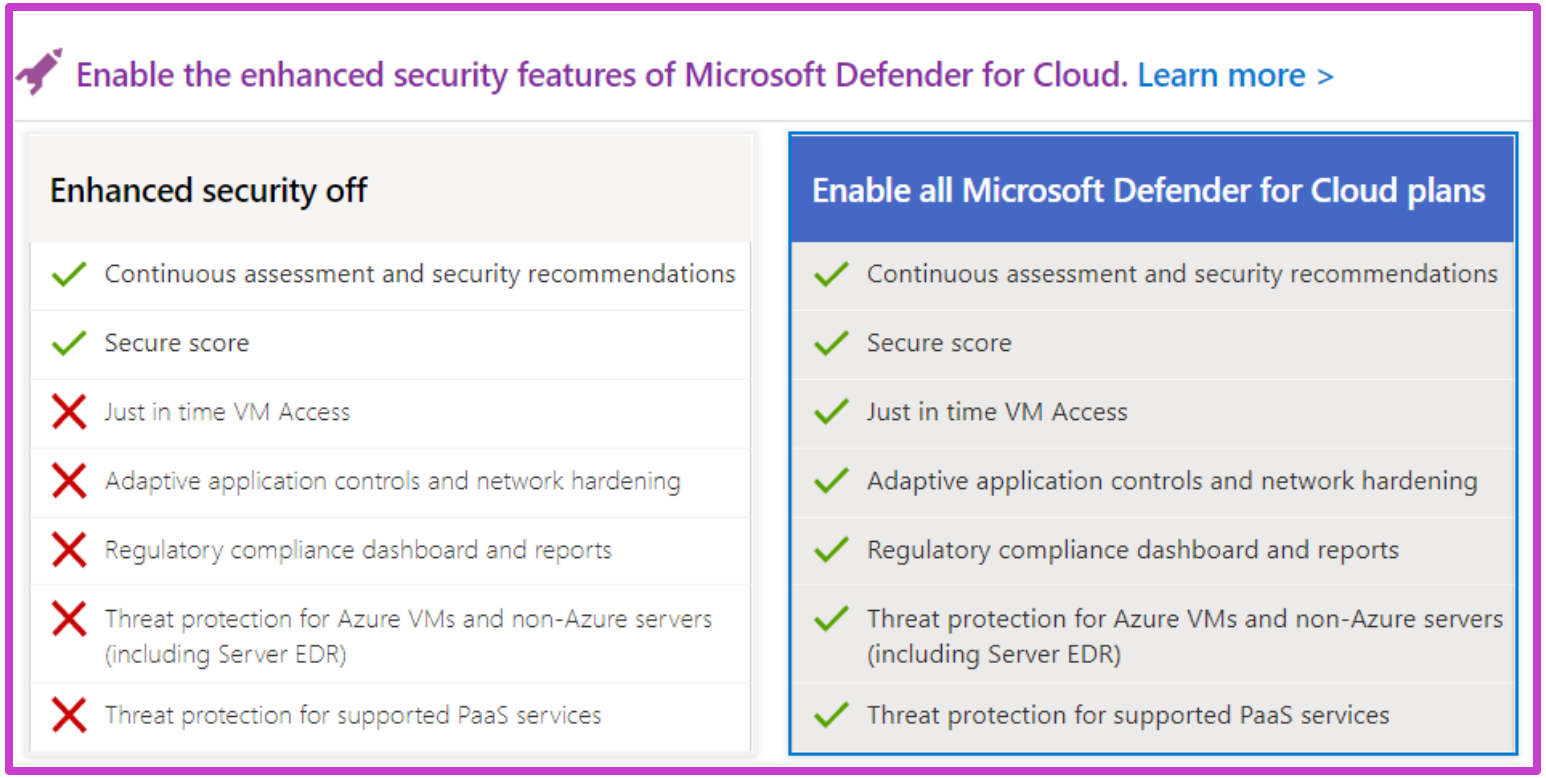
- Continually assesses your resources, subscriptions, and organization for security issues.
- Aggregates all the findings into a single secure score.
- Hardening recommendations on any identified security misconfigurations and weaknesses.
- Visibility and recommendations across your multicloud environment.
- Embeds capabilities of Microsoft Security Copilot on the recommendations page.



Cloud workload protection platform (CWPP)

CWPP plans offer enhanced security features for your workloads.

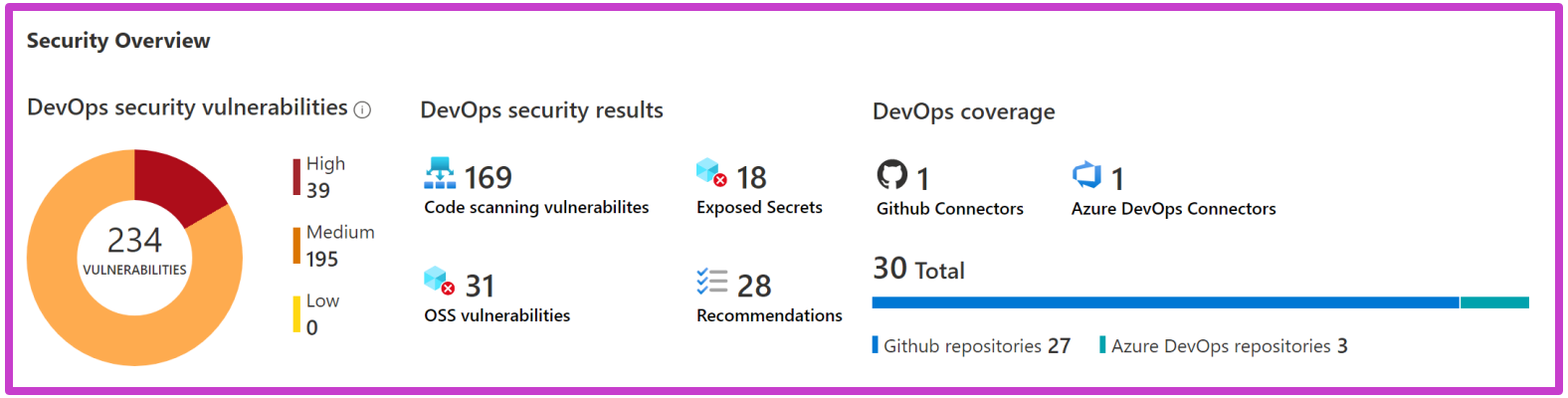
- Endpoint detection and response
- Vulnerability scanning
- Multicloud security
- Hybrid security
- Threat protection alerts
- Access and application controls



Development security operations (DevSecOps)

Empowers security teams to manage DevOps security across multipipeline environments.

- Unified visibility into DevOps security posture.
- Strengthen configurations of cloud resources in the development life cycle.
- Prioritize remediation of critical issues in code.



Demo
Microsoft Defender for Cloud

Module 4: Describe the security capabilities of Microsoft Sentinel

Module 4 introduction

After completing this module, you should be able to:

1. Describe the security concepts for SIEM and SOAR.
2. Describe how Microsoft Sentinel provides threat detection and mitigation.
3. Describe Microsoft Security Copilot integration with Microsoft Sentinel.

SIEM and SOAR

Security incident and event management (SIEM)

- Collects data from across the whole digital estate.
- Analyzes and looks for correlations or anomalies.
- Generates alerts and incidents.

Security orchestration automated response (SOAR)

- Takes alerts from many sources, such as SIEM systems.
- Triggers action-driven automated workflows and processes.
- Runs security tasks that mitigate the issue.

Microsoft Sentinel threat detection and mitigation

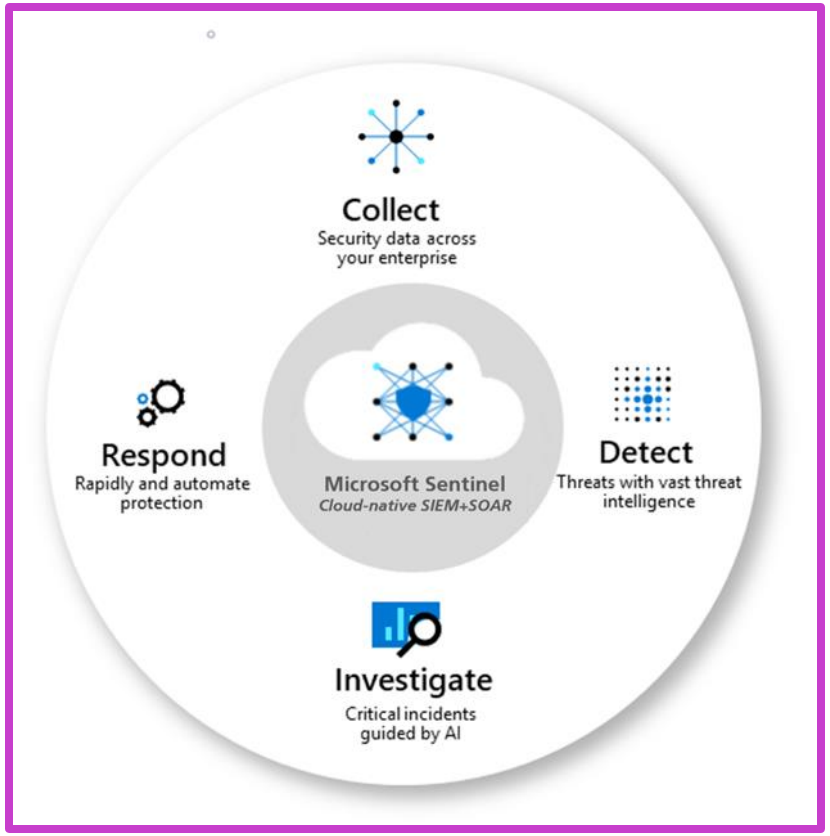
Collect data at scale across all users, devices, applications, and infrastructure, both on-premises and in multiple clouds.

Detect previously uncovered threats and minimize false positives using analytics and unparalleled threat intelligence.

Investigate threats with 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.

Microsoft Sentinel can now be accessed from the Microsoft Defender portal, which delivers Microsoft's unified security operations platform.



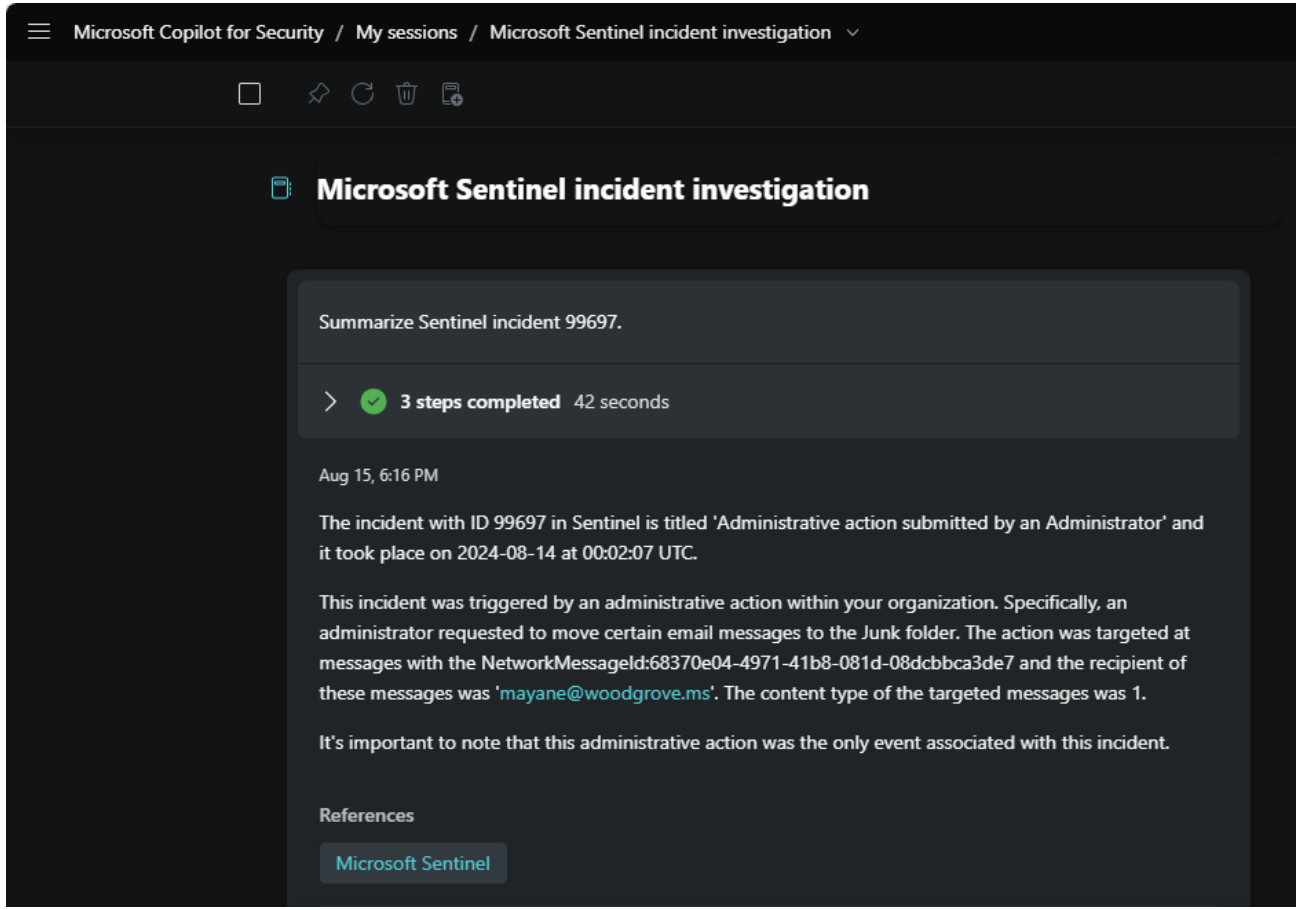
Microsoft Security Copilot integration with Microsoft Sentinel

Copilot plugins:

- Microsoft Sentinel
- Natural language to KQL for Microsoft Sentinel

Copilot integration supported through:

- Standalone experience
- Embedded experience in the Microsoft Defender Portal



Demo
Microsoft Sentinel

Module 5: Describe threat protection with Microsoft Defender XDR

Module 5 introduction

After completing this module, you should be able to:

1. Describe the Microsoft Defender XDR service.
2. Describe how Microsoft Defender XDR provides integrated protection against sophisticated attacks.
3. Describe and explore the Microsoft Defender portal.
4. Describe Microsoft Defender for Copilot integration with Microsoft Defender XDR.

Microsoft Defender XDR

An enterprise defense suite that natively coordinates detection, prevention, investigation, and response across your environment to provide integrated protection against sophisticated attacks.

The Defender includes:

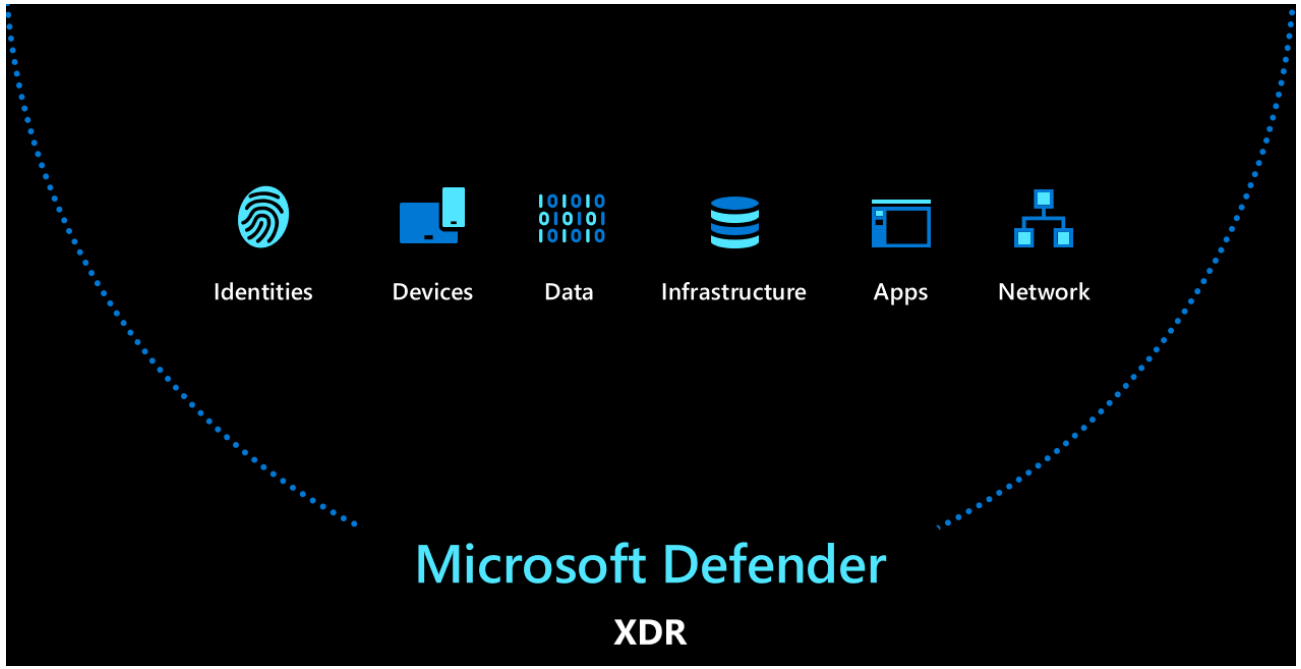
- Microsoft Defender for Endpoint
- Microsoft Defender for Office 365
- Microsoft Defender for Identity
- Microsoft Defender for Cloud Apps
- Microsoft Defender Vulnerability Management

Microsoft Defender XDR portal

- Delivers a unified security operations platform.
- Includes information and insights from Defender XDR, Microsoft Sentinel, and more.

Integration with Microsoft Security Copilot:

- Enabled through plugins
- Standalone and embedded experiences.



Microsoft Defender for Office 365

Seamless integration into your Office 365 subscription that provides protection against threats that arrive in email, links, attachments, or collaboration tools.

Prevent and detect

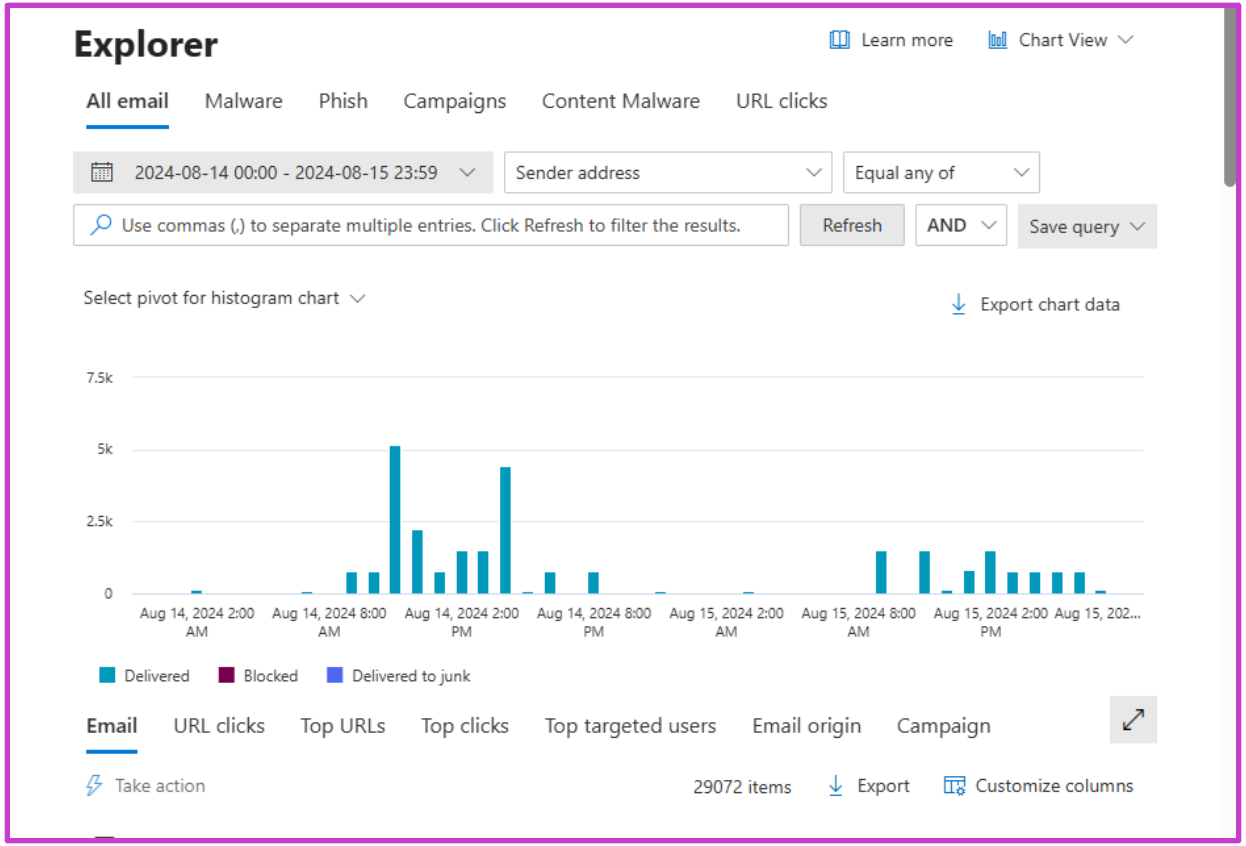
- Policies for anti-malware, anti-spam, anti-phishing
- Safe attachments
- Attack simulation training
- More…

Investigate

- Audit log search
- Message trace
- Explorer
- More..

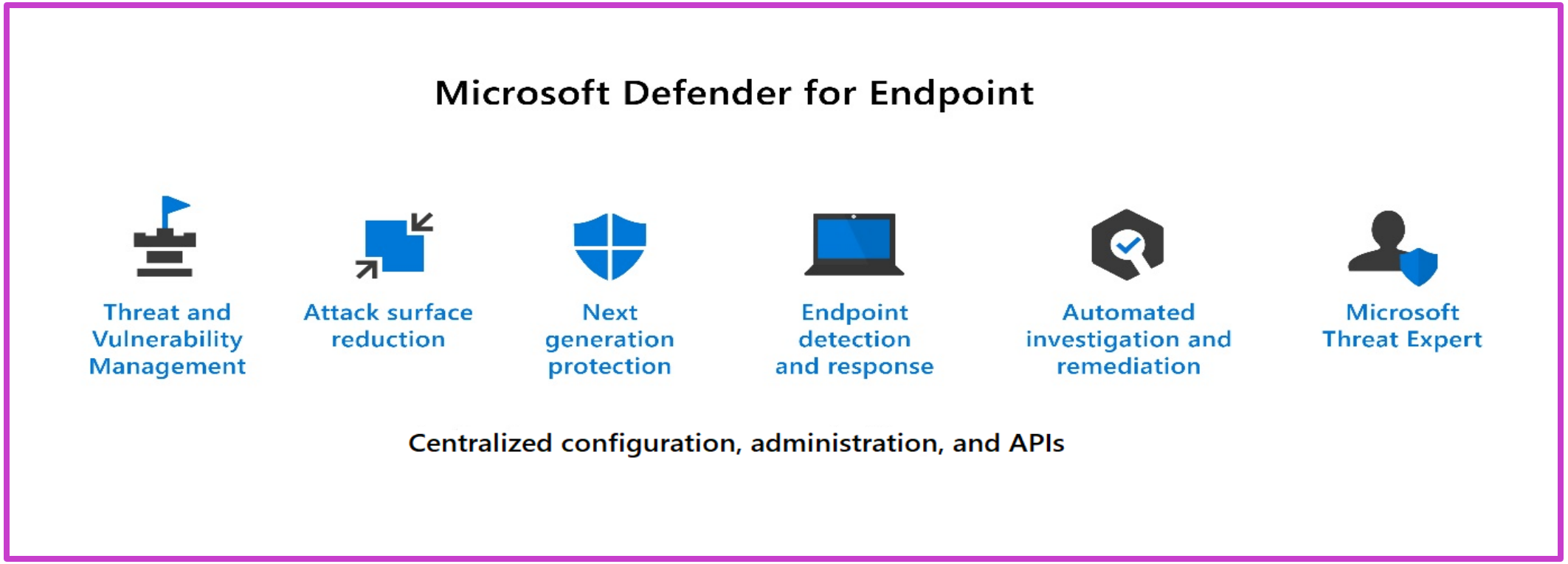
Respond

- Zero-hour auto purge (ZAP)
- Automated investigation and response
- More…



Microsoft Defender for Endpoint

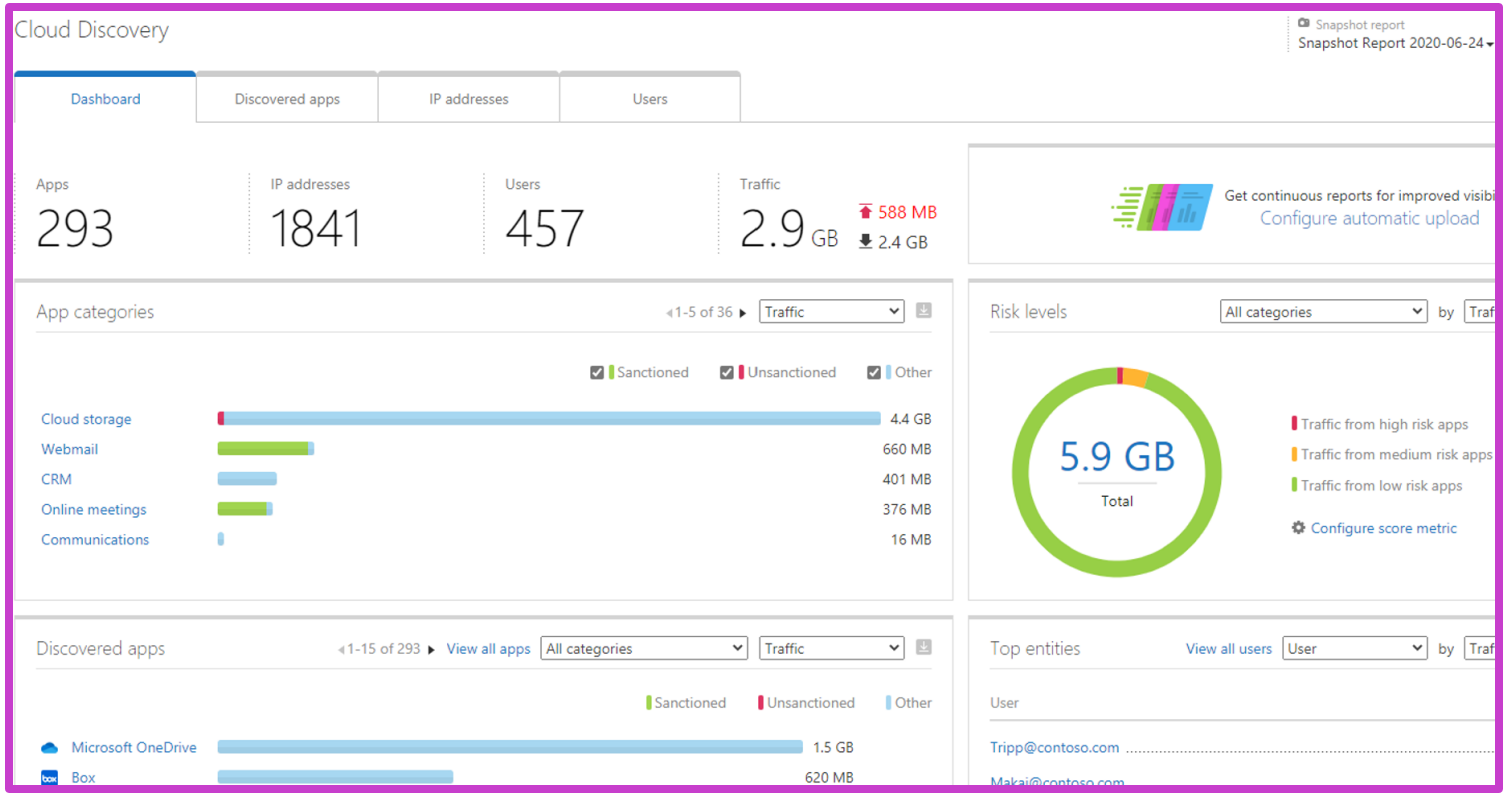
Microsoft Defender for Endpoint is a platform designed to help enterprise networks protect endpoints.



Microsoft Defender for Cloud Apps

Provides rich visibility to your cloud services, control over data travel, and sophisticated analytics to identify and combat cyberthreats across all your Microsoft and third-party cloud services.

- Discover SaaS applications
- Information protection
- SaaS Security Posture Management (SSPM)
- Advanced threat protection
- App-to-app protection with app governance

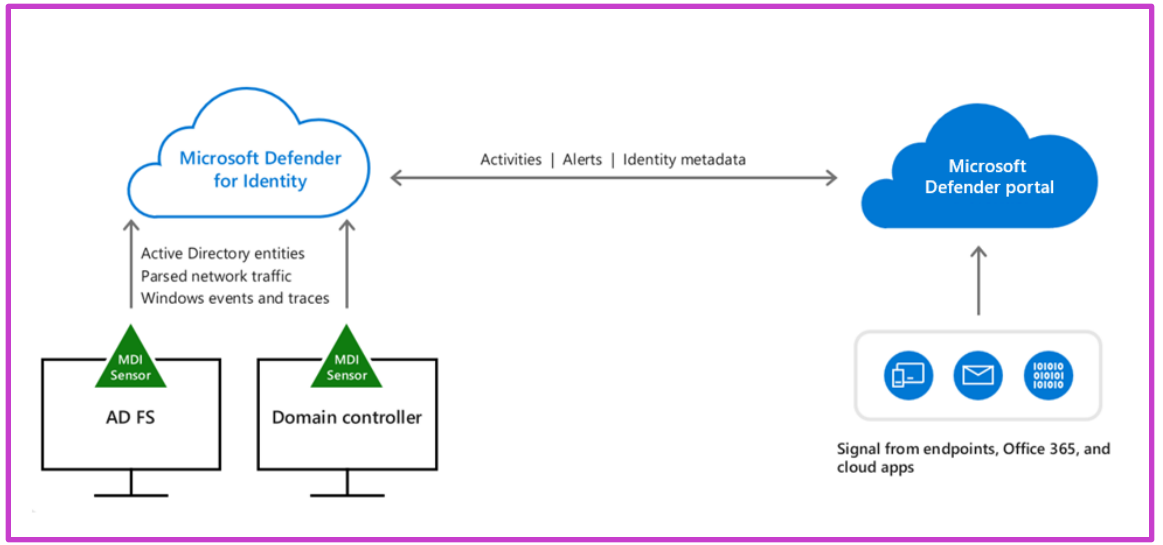


Demo
Microsoft Defender for Cloud Apps

Microsoft Defender for Identity

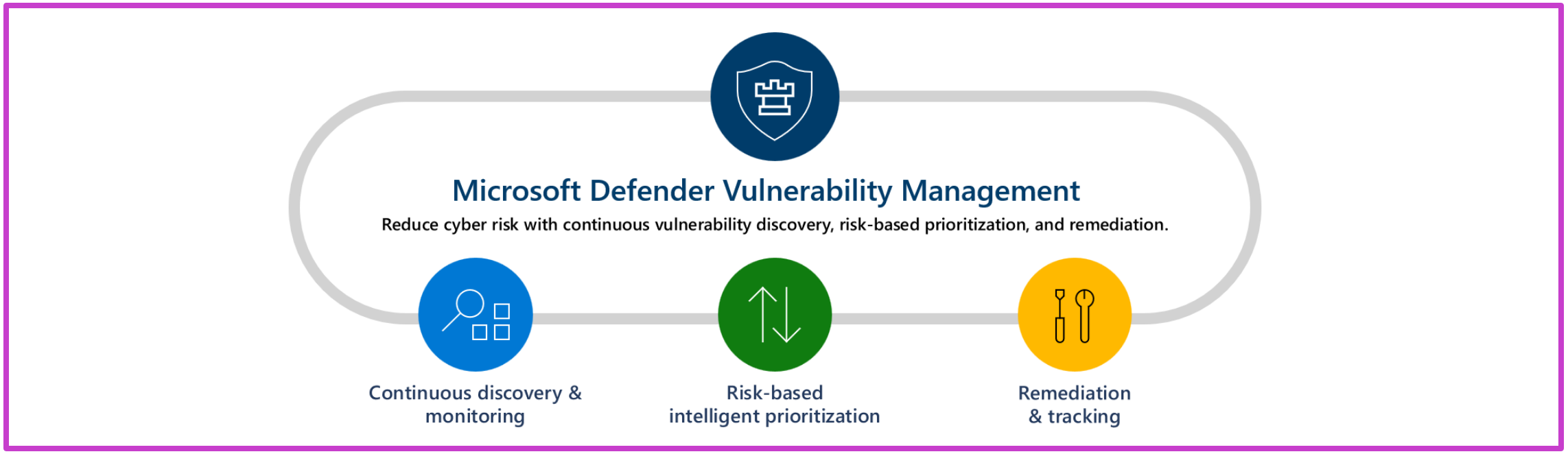
A cloud-based security solution that uses signals from your on-premises identity infrastructure servers to detect threats, like privilege escalation or high-risk lateral movement, and reports on easily exploited identity issues.

- Software-based sensors installed on your on-premises identity infrastructure servers send signals to the Microsoft Defender for Identity service.
- Defender for Identity uses signals to provide identity threat detection and response (ITDR) that enables security pros to:
  - Proactively assess your identity posture
  - Detect threats, using real-time analytics and data intelligence
  - Investigate alerts and user activities
  - Remediate actions
- The Microsoft Defender portal provides security teams a unified security operations platform for investigating and responding to attacks.



Microsoft Defender Vulernability Management

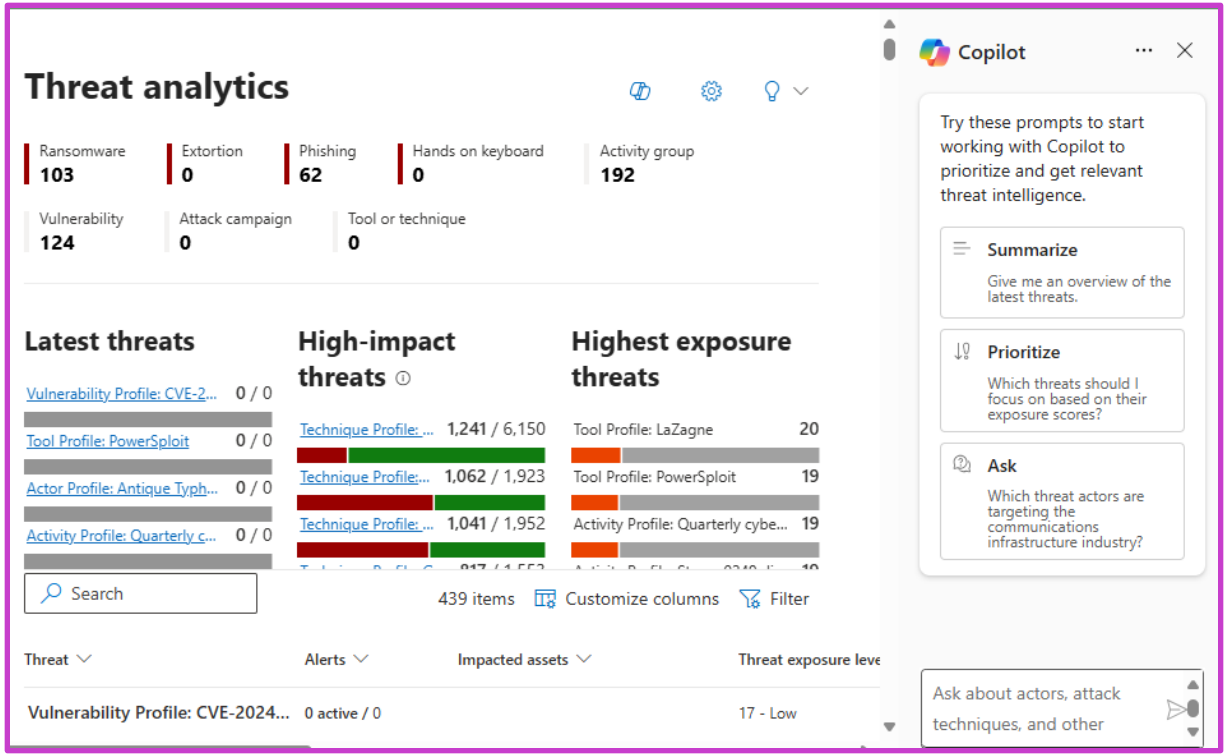
Delivers asset visibility, intelligent assessments, and built-in remediation tools for Windows, macOS, Linux, Android, iOS, and network devices.



Microsoft Defender Threat Intelligence

Aggregates and enriches critical threat intelligence data sources and is integrated with Microsoft Security Copilot to help security analyst as they triage, investigate, and remediate vulnerabilities in their organization.

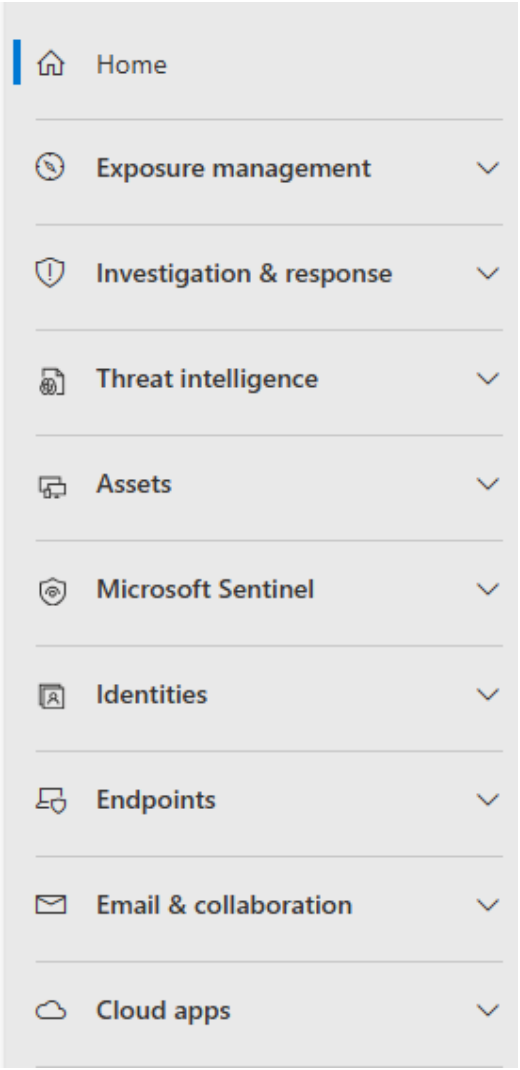
- Threat analytics - Understand how emerging threats impact your organization's environment.
- Intel profiles - A definitive source of Microsoft's shareable knowledge on tracked threat actors, malicious tools, and vulnerabilities.
- Intel explorer - Where analysts can quickly scan new featured articles and perform search for intelligence gathering.
- Intel projects – Users can create projects that organize indicators of compromise (IOCs) from an investigation and contain associated artifacts and a detailed history.



Microsoft Defender portal

The Microsoft Defender portal delivers a unified security operations platform

- The best of SIEM, XDR, posture management, and threat intelligence with advanced generative AI as a single platform.
- Combines protection, detection, investigation, and response to threats across your entire organization and all its components, in one place.

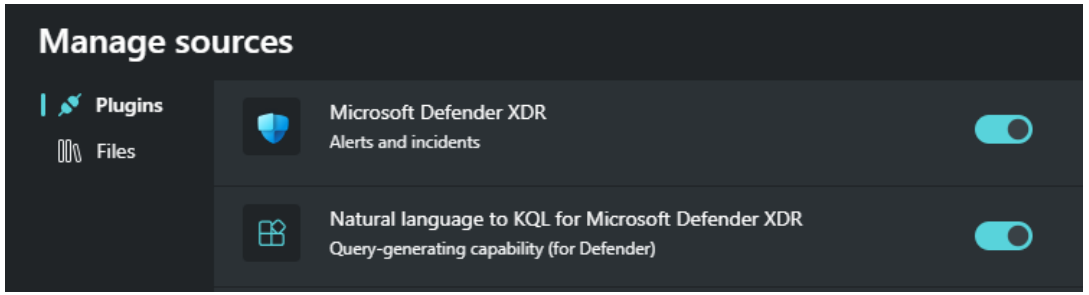


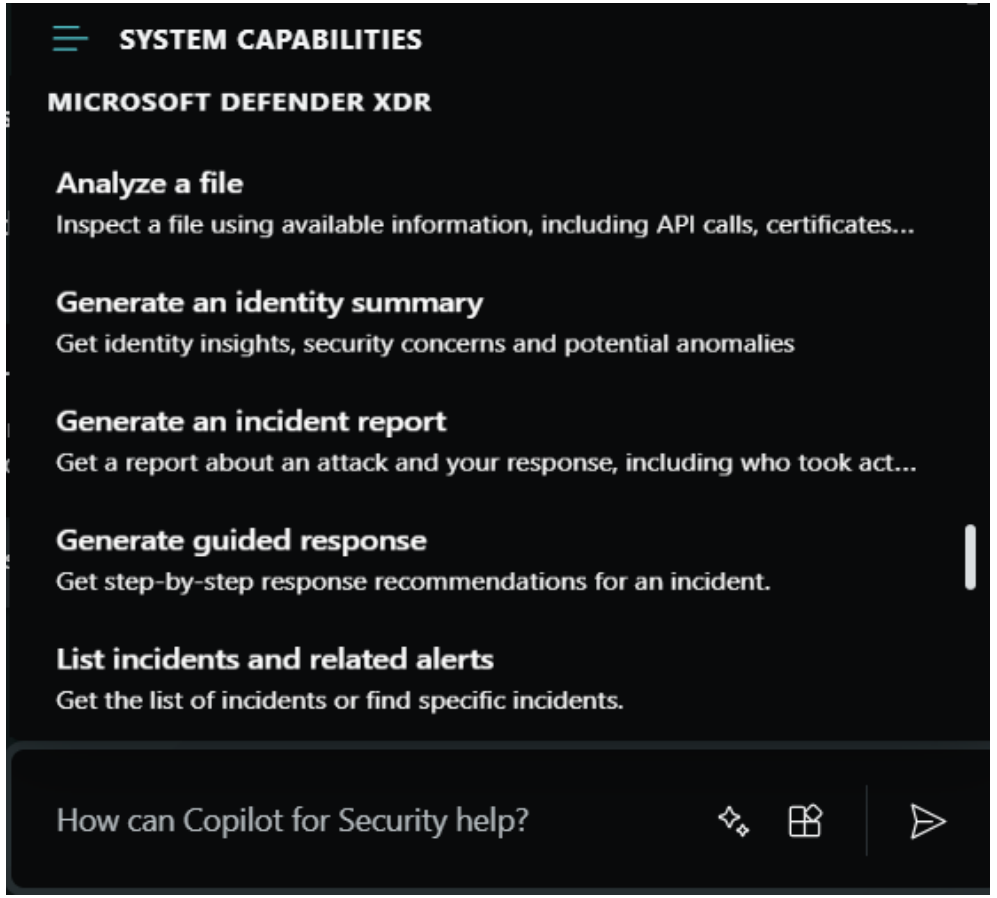
Copilot integration with Microsoft Defender XDR

Copilot integration is experienced through the standalone and embedded experiences.

Standalone experience:

- Enable plugins to support integration with Microsoft Defender XDR
- System capabilities serve as built-in prompts.
- Use built-in Defender incident investigation promptbook or create your own.



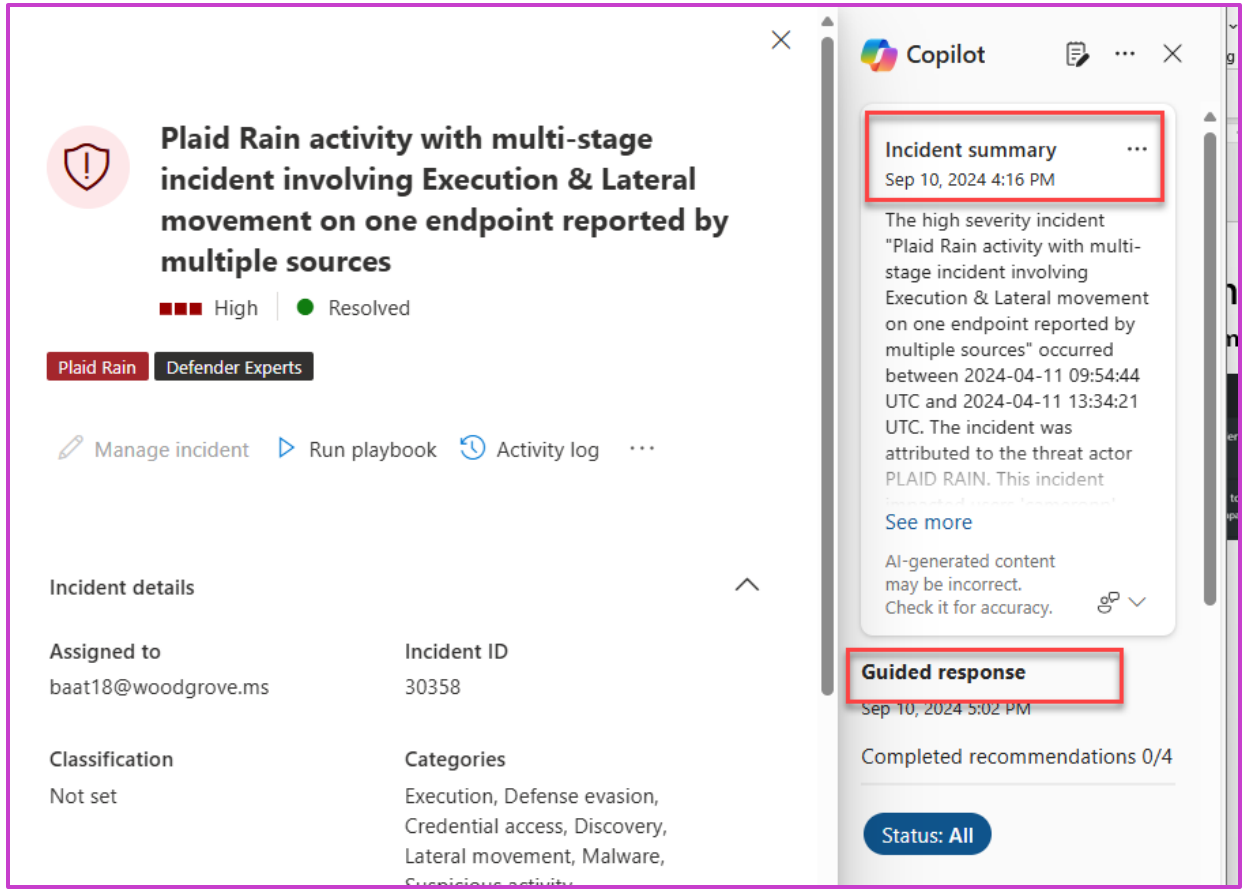


Copilot integration with Microsoft Defender XDR (con't)

Copilot integration is experienced through the standalone and embedded experiences.

Embedded experience:

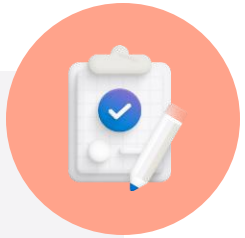
- Summarize incidents
- Guided responses
- Script analysis
- Natural language to KQL query
- Incident reports
- Analyze files
- Device summaries
- Identity summaries



Demo

The Microsoft Defender XDR portal

Learning Path Summary



Describe the capabilities of Microsoft security solutions.

In this learning path, you have:

- Learned about Microsoft Security Copilot.
- Learned about the core infrastructure security services in Azure.
- Learned about the security management capabilities of Azure.
- Learned about the security capabilities of Microsoft Sentinel.
- Learned about the threat protection with Microsoft Defender XDR.

Knowledge check

What are the steps required to onboard organizations and users to Microsoft Security Copilot?

A. Enable Copilot plugins and procure Microsoft Entra Premium 1 licensing.
B. Procure Microsoft Entra Premium 1 licensing.
C. Provision SCUs, set up the default environment, and assign role permissions.

How can application developers benefit from using Azure Key Vault?

A. To test and debug their application code.
B. To register their application with Azure.
C. To securely store and retrieve application secrets

Microsoft Defender for Cloud covers three pillars of cloud security. Which pillar provides visibility to help you understand your current security situation and provides hardening recommendations?

A. Cloud security posture management (CSPM)
B. Cloud workload protection (CWP)
C. Microsoft Cloud security benchmark

Knowledge check continued

As the lead admin, it's important to convince your team to start using Microsoft Sentinel. You've put together a presentation. What are the four security operation areas of Microsoft?

A. Collect, Detect, Investigate, and Redirect.
B. Collect, Detect, Investigate, and Respond.
C. Collect, Detect, Investigate, and Repair.

A lead admin for an organization is looking to protect against malicious threats posed by email messages, links (URLs), and collaboration tools. Which solution from the Microsoft Defender XDR suite is best suited for this purpose?

A. Microsoft Defender for Office 365.
B. Microsoft Defender for Endpoint.
C. Microsoft Defender for Identity.