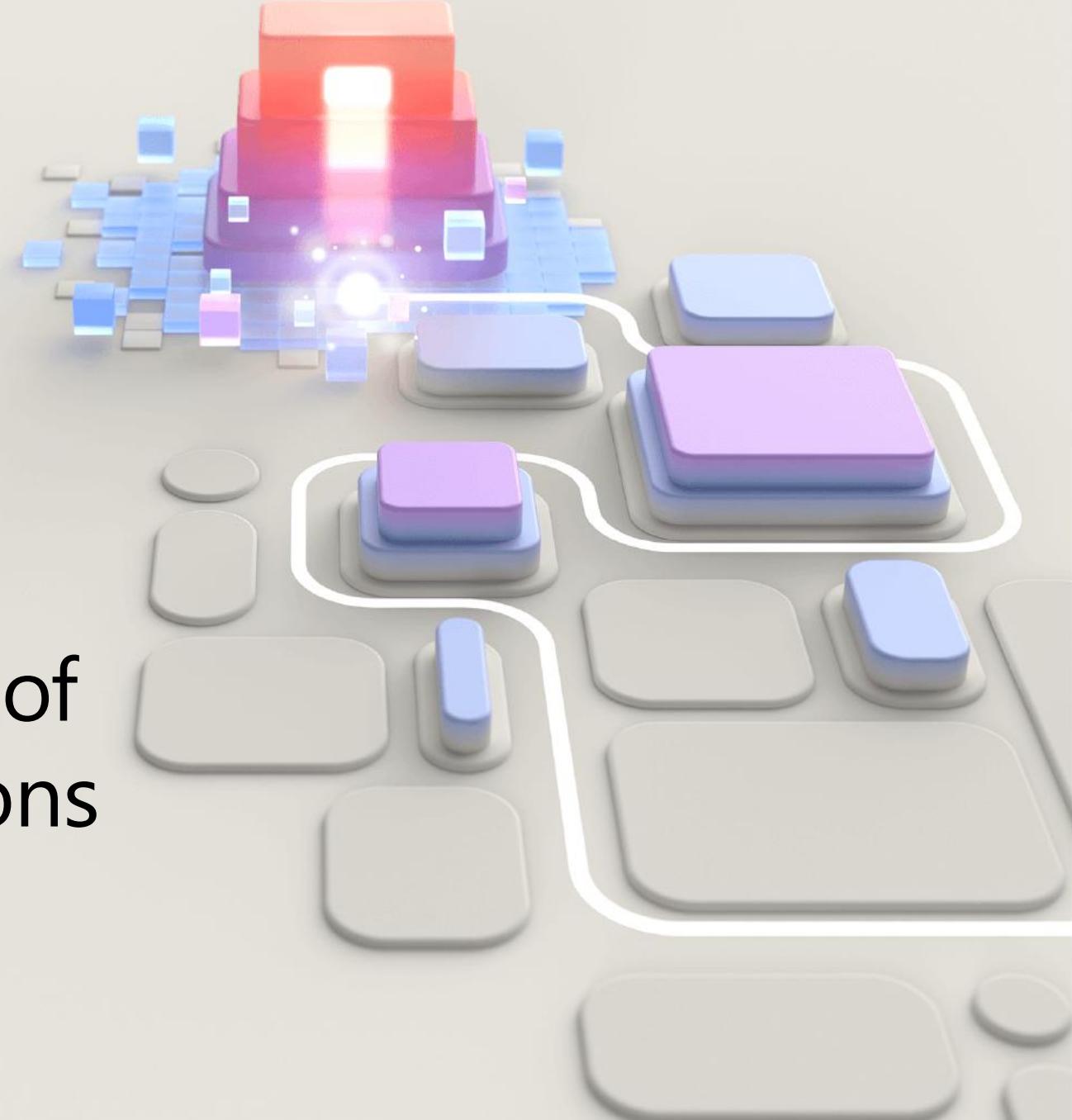


SC-900

Learning path 3:

Describe the capabilities of
Microsoft security solutions



SC-900 Course Agenda

- Learning Path 1 Describe the concepts of Security, Compliance, and Identity
- Learning Path 2 Describe the capabilities of Microsoft Entra ID
- Learning Path 3 Describe the capabilities of Microsoft Security Solutions
- Learning Path 4 Describe the capabilities of Microsoft Compliance Solutions
 Purview

Lab 6 Monate

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. **SIEM**
- Describe threat protection with Microsoft Defender XDR.

Defender Cloud

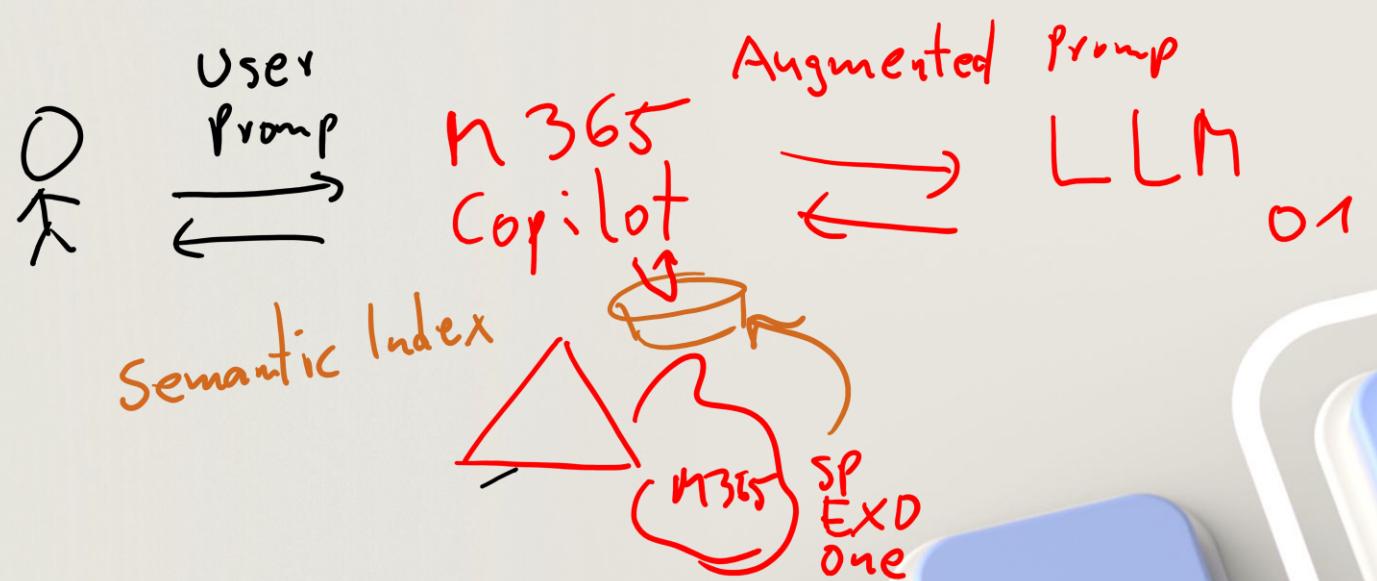
Azure

Splunk

Def EIP

Def O365

Def Cloud Apps



Module 1:

Describe Microsoft Security Copilot

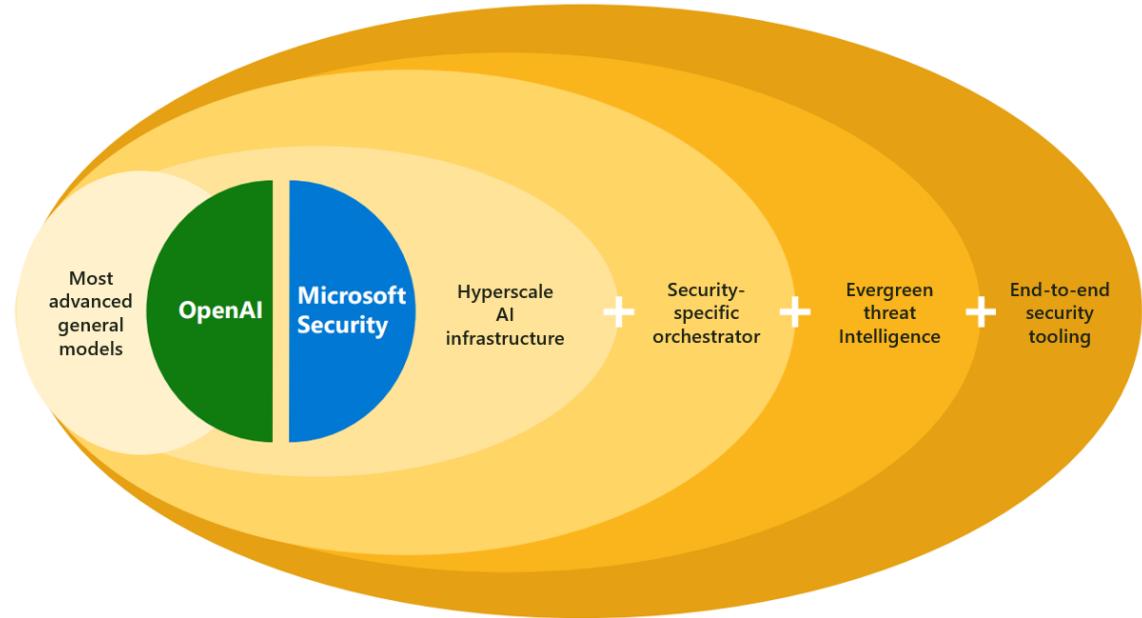
NLP

A2
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.

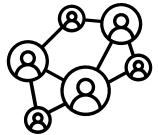
- Copilot combines powerful LLMs with a security-specific model from Microsoft.
- Copilot integrates with Microsoft and non-Microsoft sources.
- Copilot learns at machine speed to help analysts identify and respond to emerging threats.
- Enterprise data is protected by comprehensive enterprise compliance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



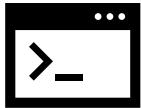
Describe Microsoft Security Copilot – Use cases



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.



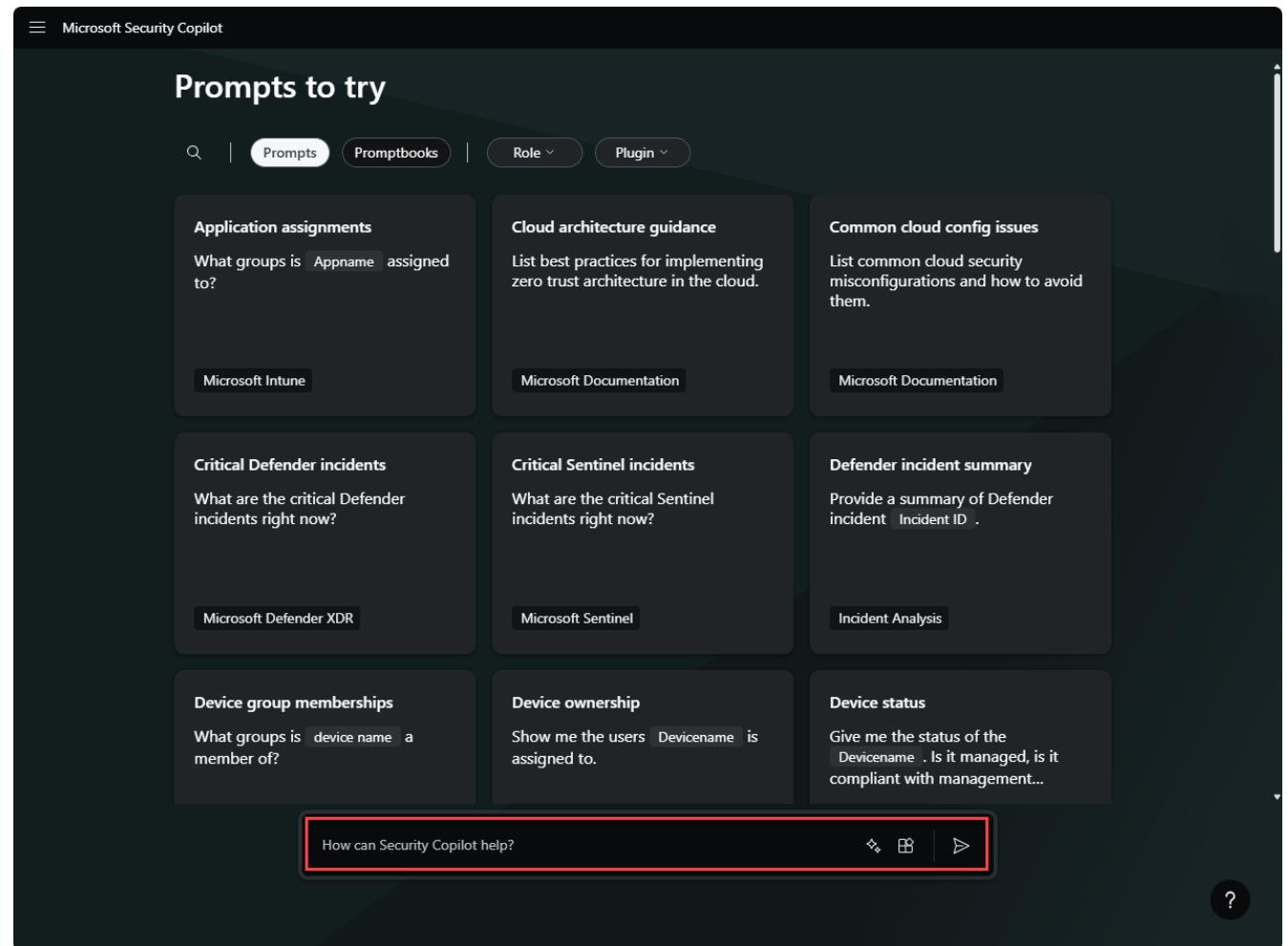
Reverse engineering of scripts. Analyze complex command line scripts and translate them into natural language with clear explanations of actions.



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.

The screenshot shows the Microsoft 365 Defender interface for 'contosohotels.com'. The left sidebar includes sections like Home, Incidents & alerts, Hunting (Advanced hunting selected), Threat intelligence, Learning hub, Trials, Partner catalog, Exposure management, Overview, Attack surface, Exposure insights, Secure score, Assets, and Devices. The main area is titled 'Advanced hunting' and displays a Kusto Query Language (KQL) query:

```
1 let logonAttempts = DeviceLogonEvents  
2 | where ActionType == "LogonAttempted"  
3 | project Timestamp, DeviceId, AccountDomain;  
4 let credentialTheftEvents = DeviceEvents  
5 | where ActionType in ("AsrlsassCredentialTheftAudited", "AsrlsassCred  
6 | project Timestamp, DeviceId, InitiatingProcessAccountDomain;  
7 logonAttempts  
8 | join kind=inner credentialTheftEvents on $left.DeviceId == $right.De  
9 | summarize count() by AccountDomain  
10 | order by count_ desc  
11
```

A red box highlights the 'Security Copilot' button in the top right of the query editor. Another red box highlights the 'Ask a question to generate a query' input field at the bottom right. The text 'KQL' is handwritten in red over the query results area. The right side of the screen shows a sidebar with a recent query result from November 8, 2023, and a generated KQL script.

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.
- **Orchestrator:** Used to compose skills together, to answer a user's prompt.



The prompt bar, used to enter prompts.

Agent mit Skills
Semantic Kernel

Example: plugins and capabilities

Manage sources

Plugins Manage plugins

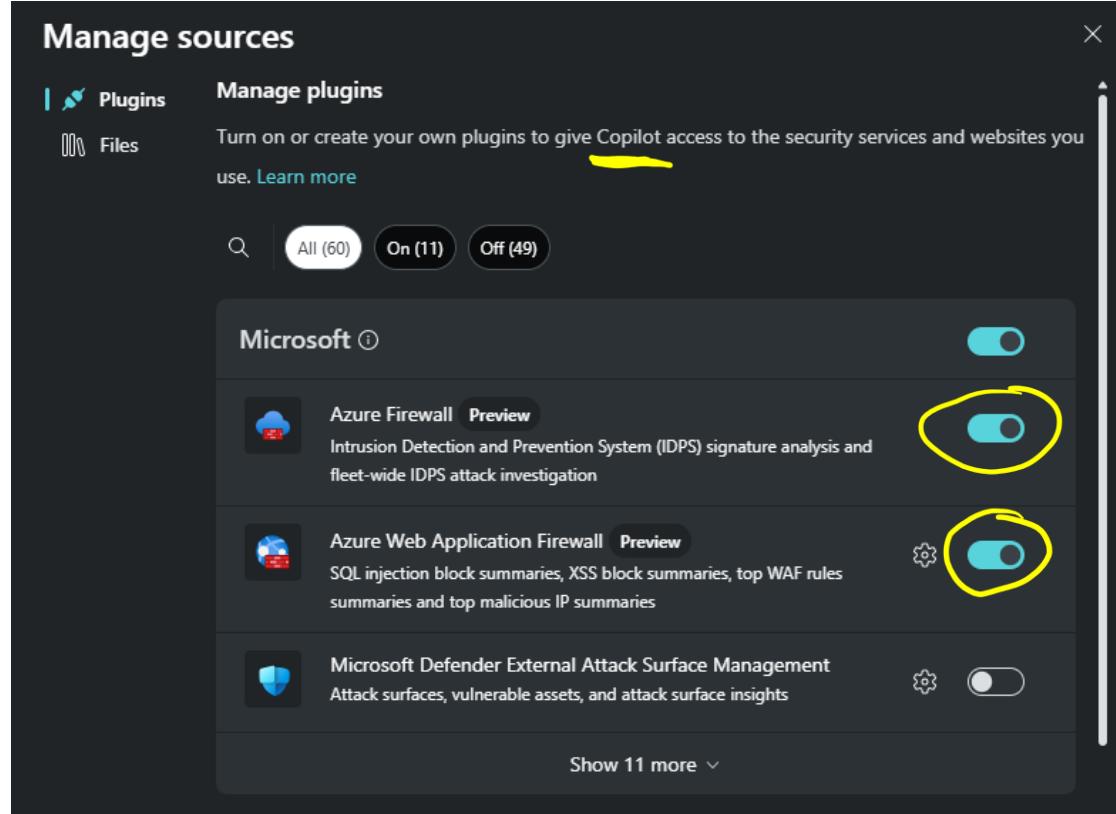
Turn on or create your own plugins to give Copilot access to the security services and websites you use. [Learn more](#)

All (60) On (11) Off (49)

Microsoft

Service	Status
Azure Firewall <small>Preview</small>	<input checked="" type="checkbox"/>
Azure Web Application Firewall <small>Preview</small>	<input checked="" type="checkbox"/>
Microsoft Defender External Attack Surface Management	<input type="checkbox"/>

Show 11 more ▾



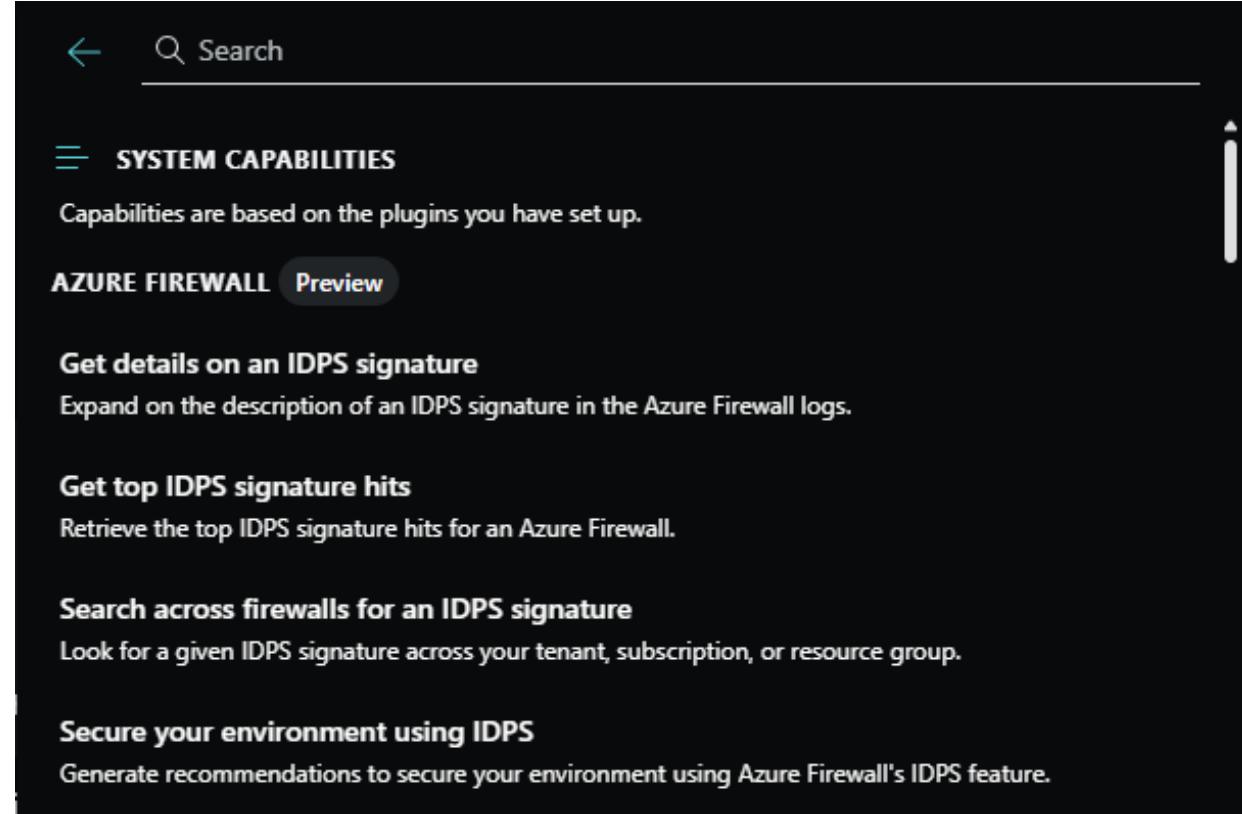
← Search

SYSTEM CAPABILITIES

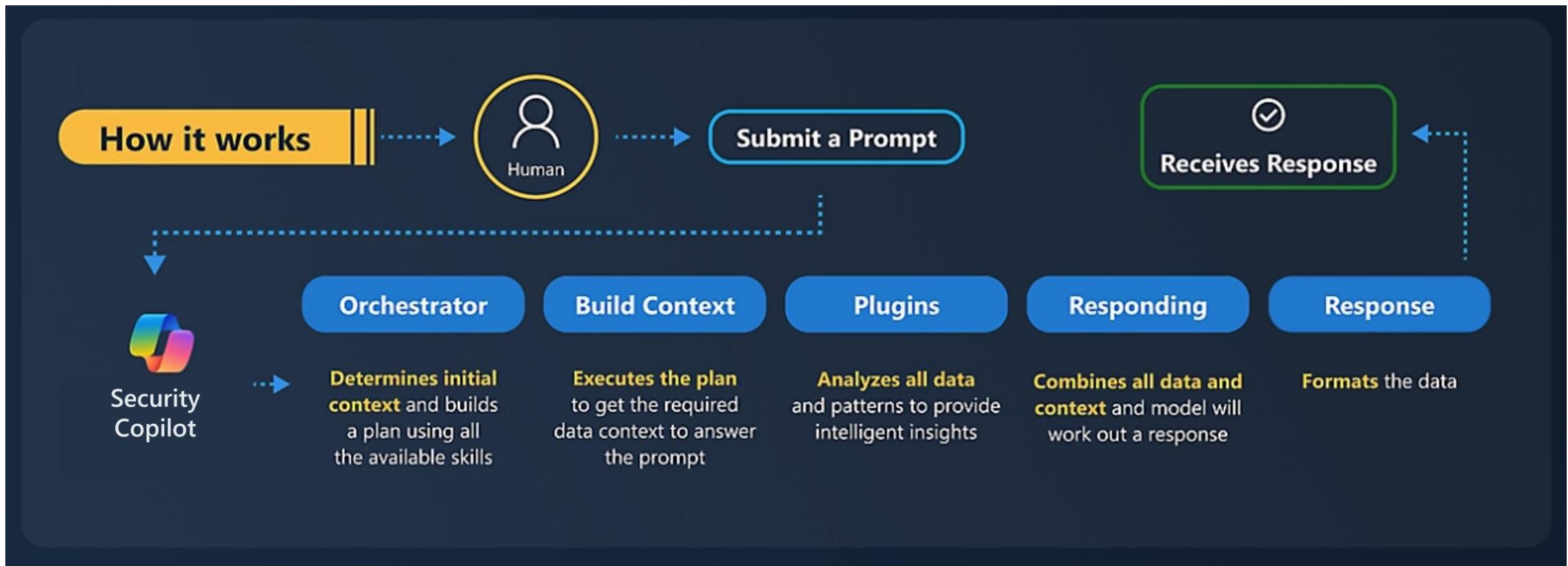
Capabilities are based on the plugins you have set up.

AZURE FIREWALL Preview

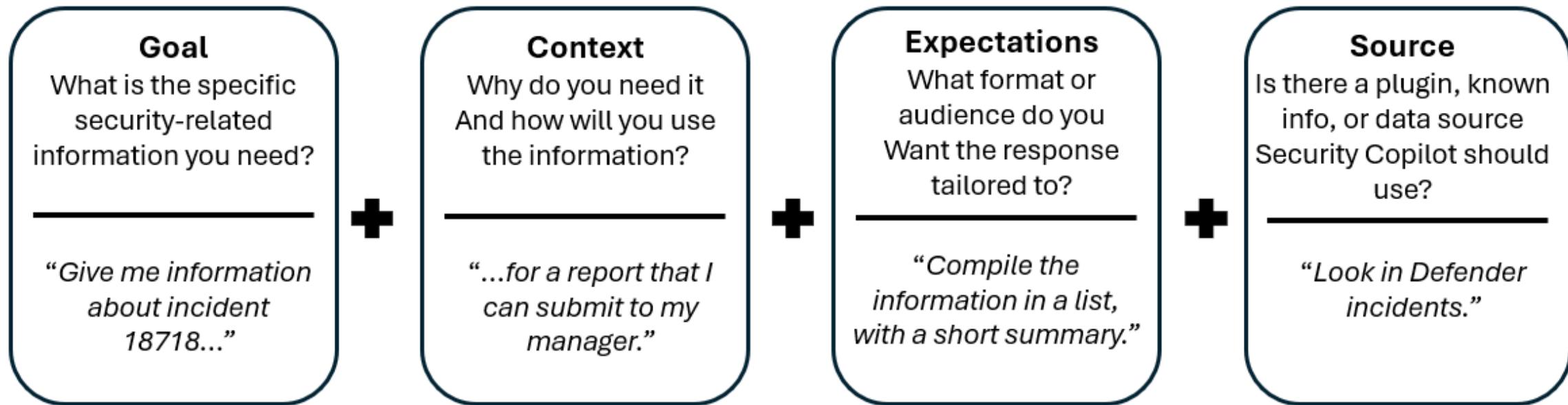
- Get details on an IDPS signature**
Expand on the description of an IDPS signature in the Azure Firewall logs.
- Get top IDPS signature hits**
Retrieve the top IDPS signature hits for an Azure Firewall.
- Search across firewalls for an IDPS signature**
Look for a given IDPS signature across your tenant, subscription, or resource group.
- Secure your environment using IDPS**
Generate recommendations to secure your environment using Azure Firewall's IDPS feature.



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

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.

Jump Server

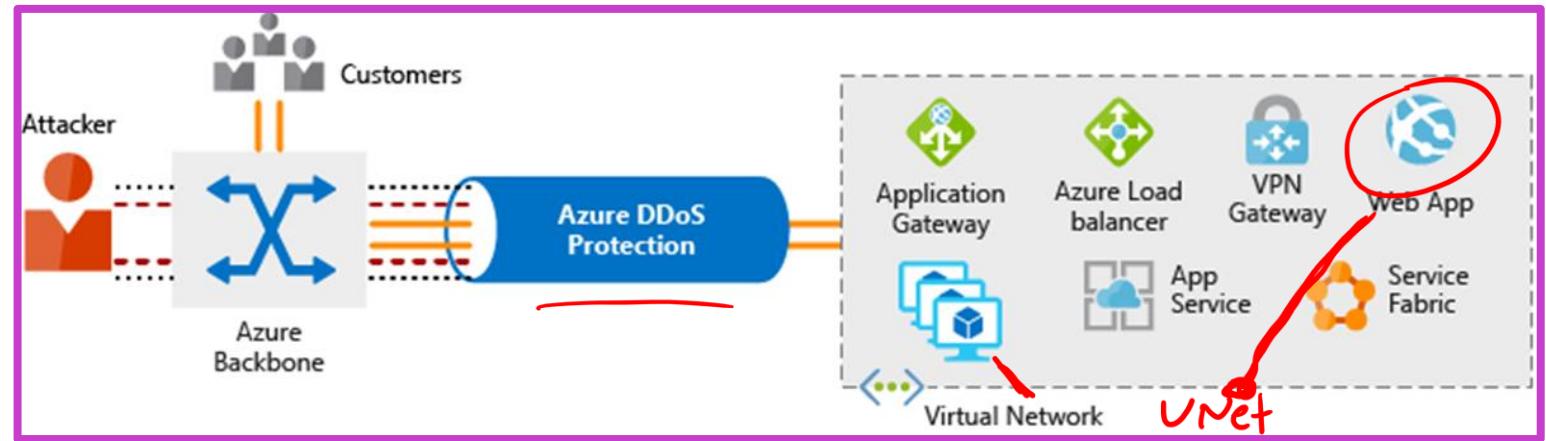
Azure DDoS Protection

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.

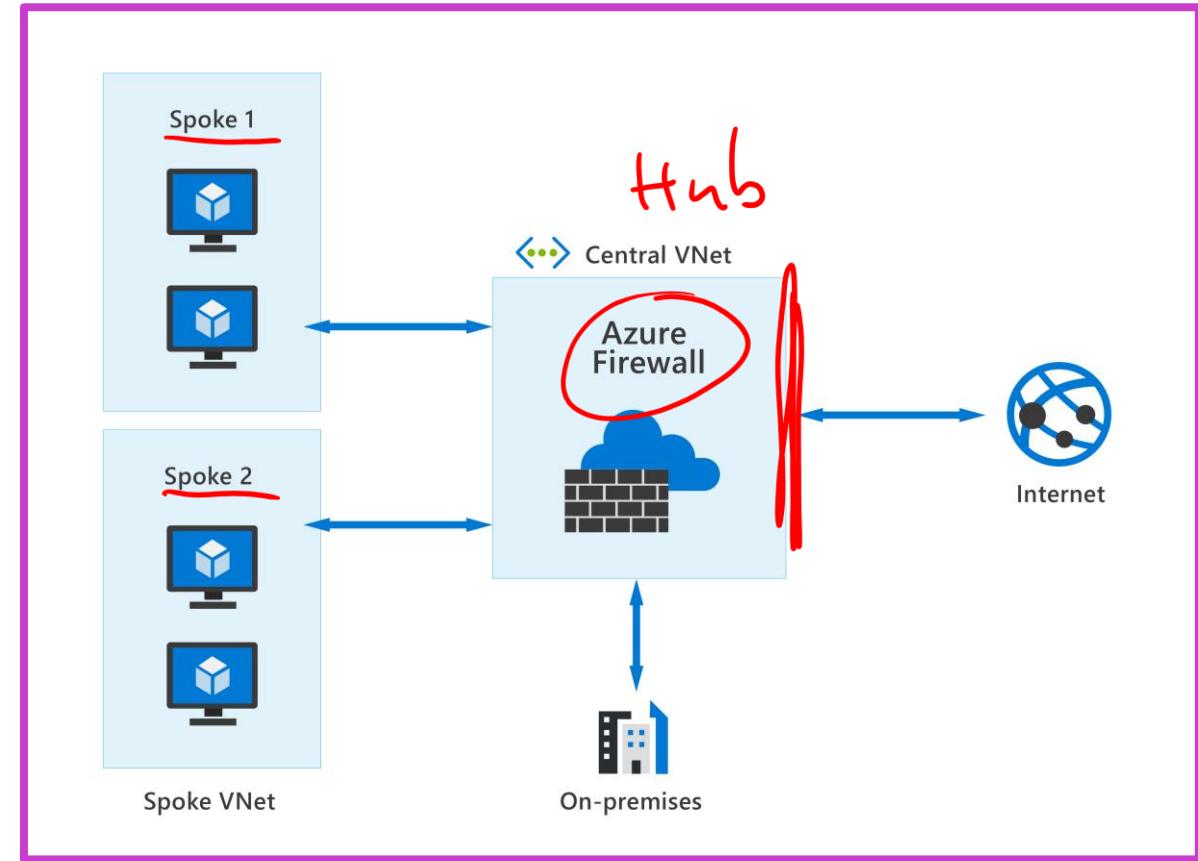


TCP / IP
IPv6

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...

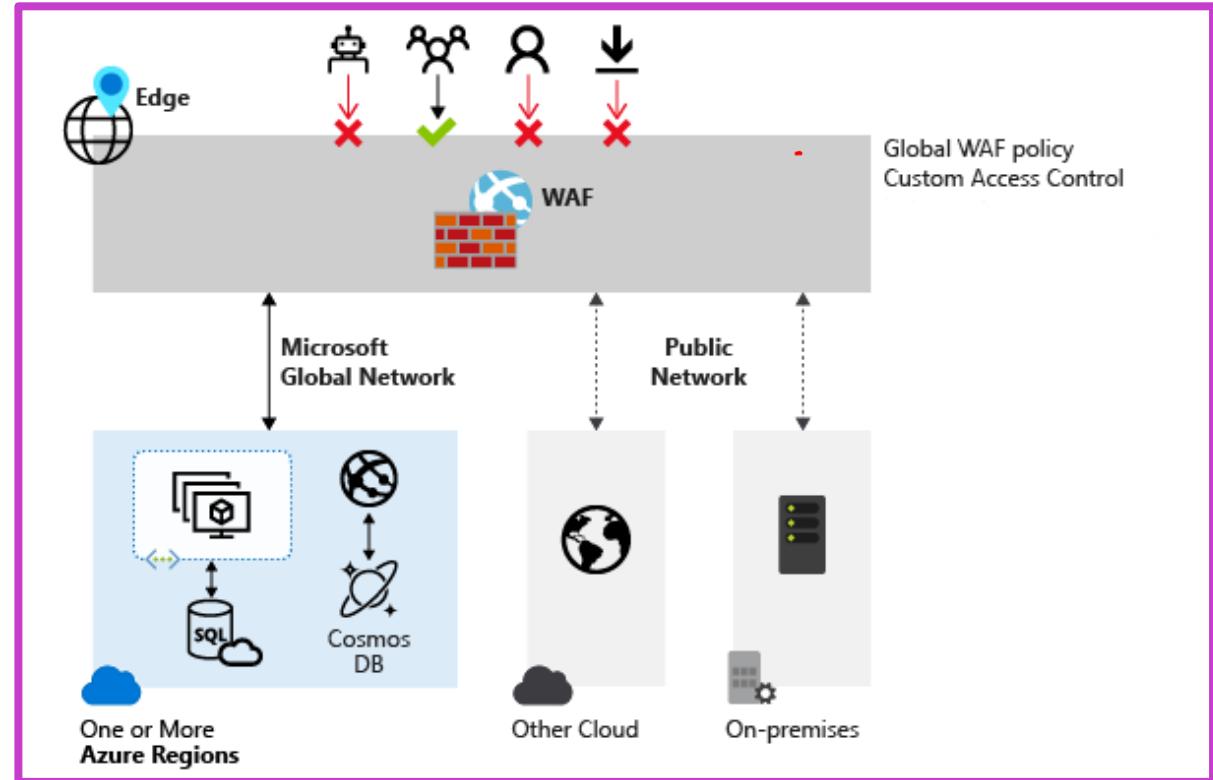


Web Application Firewall

App. GW
WAF
Front Door

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...



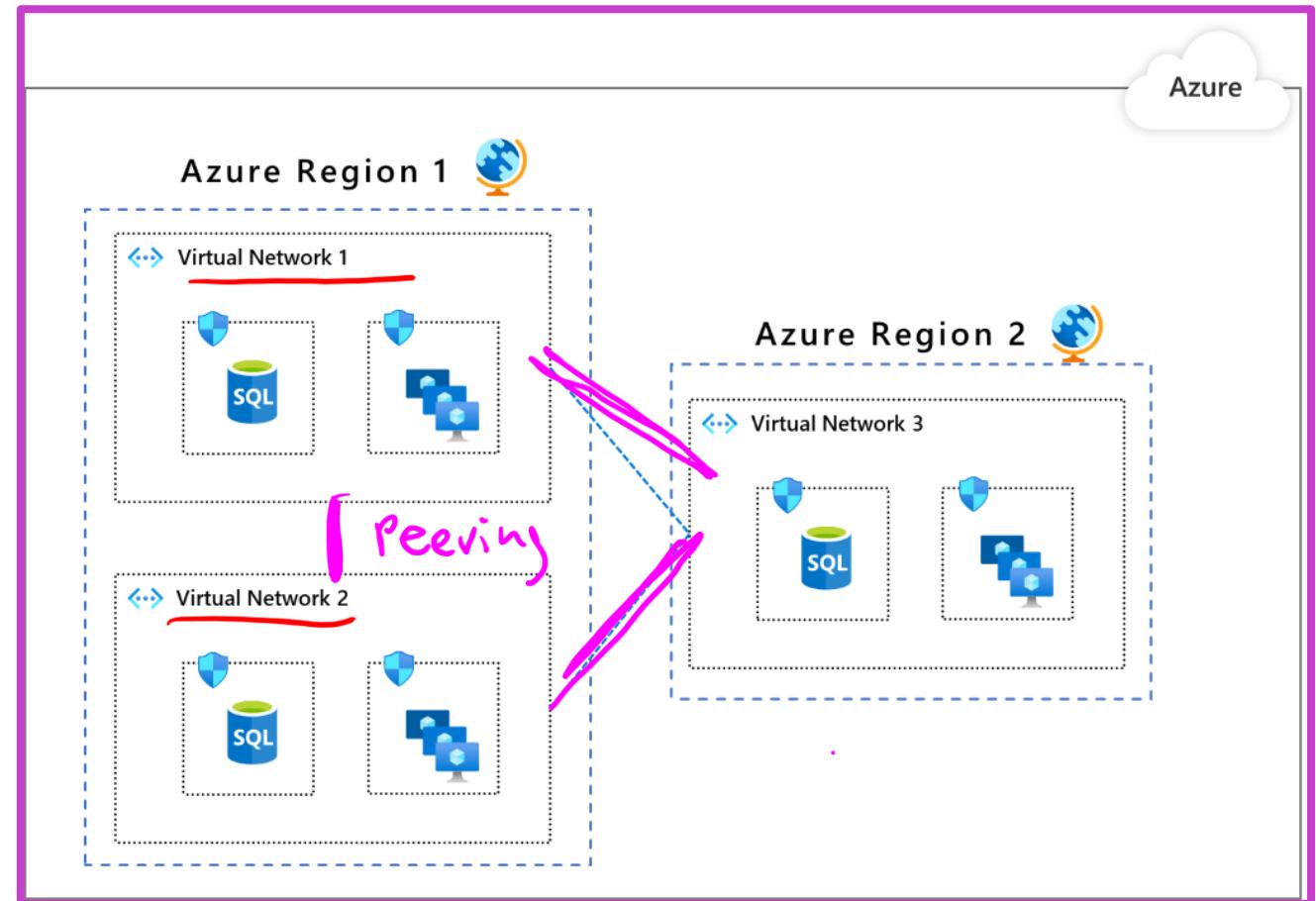
Network segmentation and Azure VNet

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.

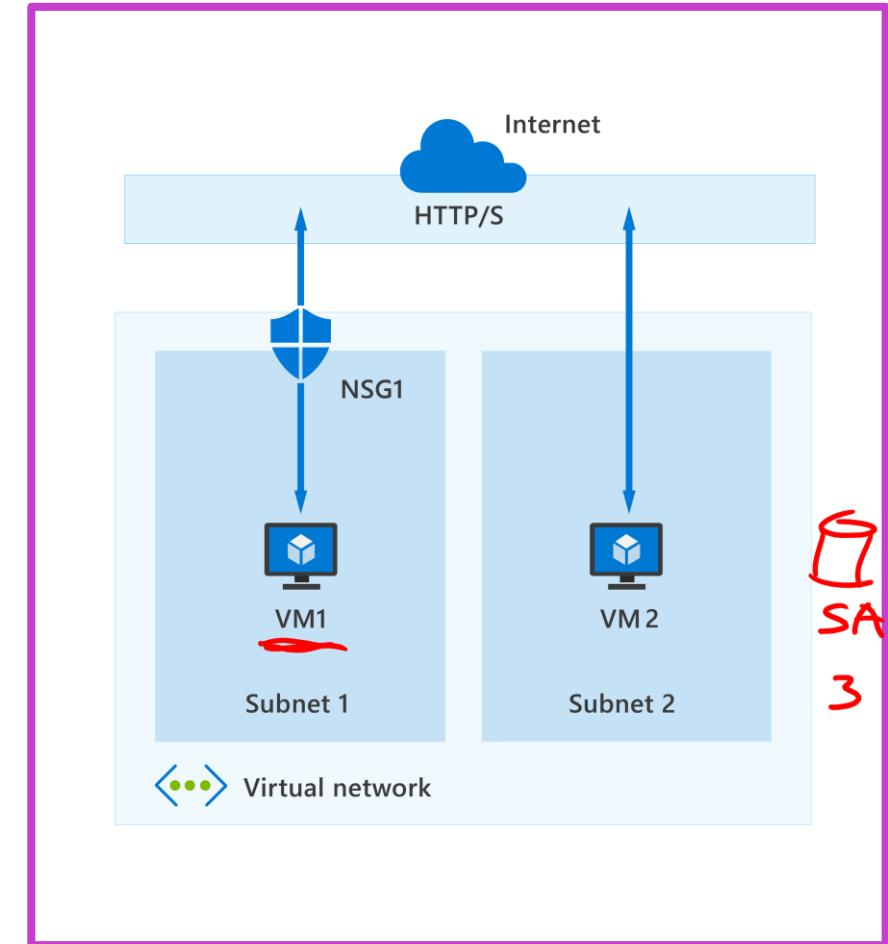


DE

Azure network security groups (NSGs)

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

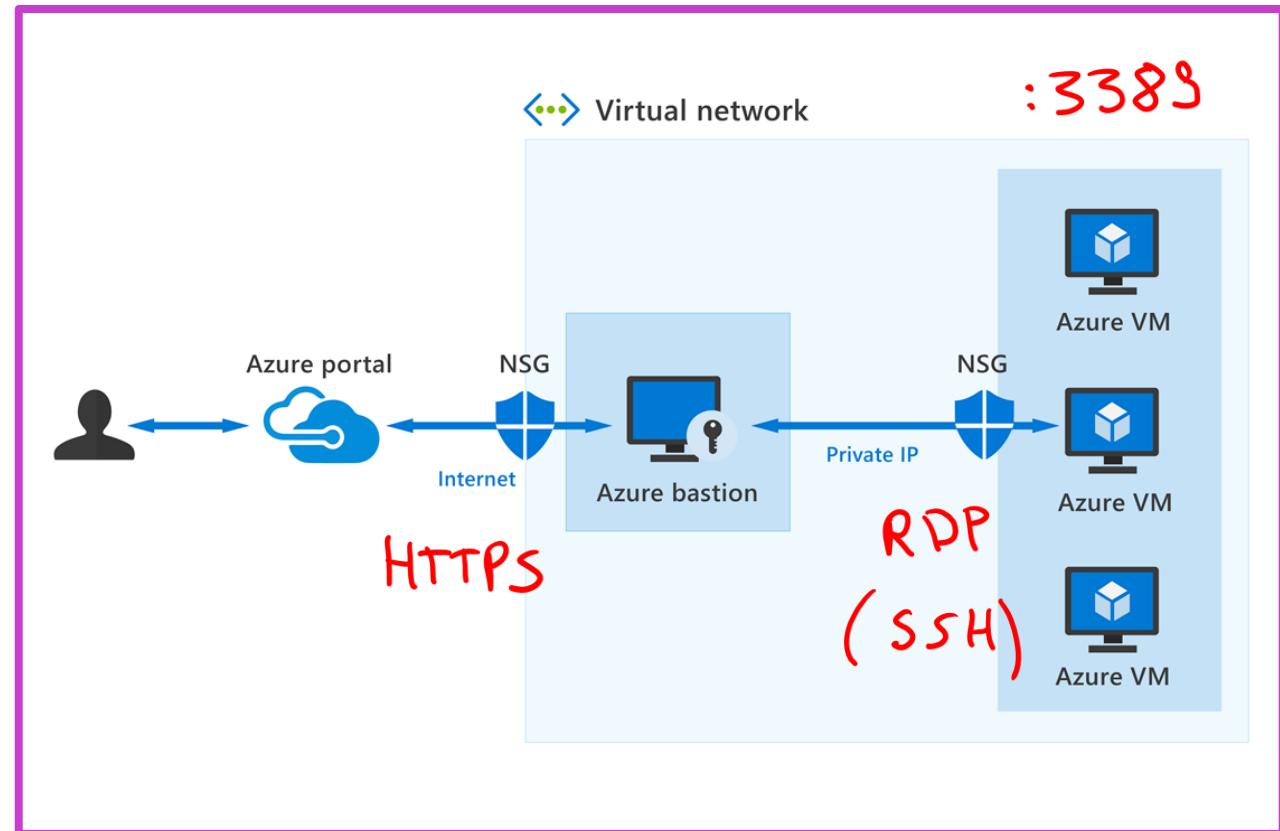
- An NSG is made up of inbound and outbound security rules that allow or deny traffic.
- An NSG can contain many rules, the rules are processed based on their assigned priority.
- When an NSG is created, it includes default inbound and outbound rules.
- You can't remove the default rules, but you can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

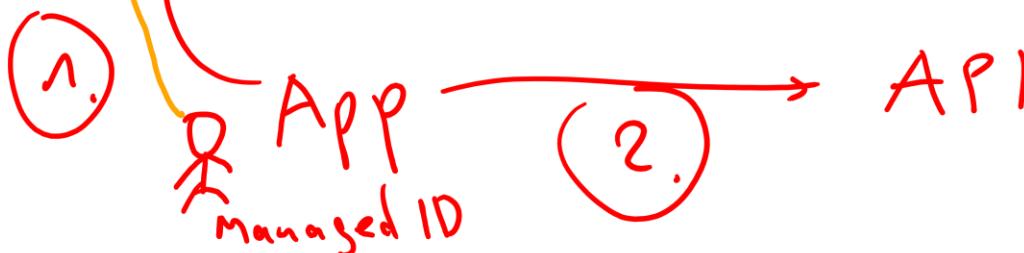
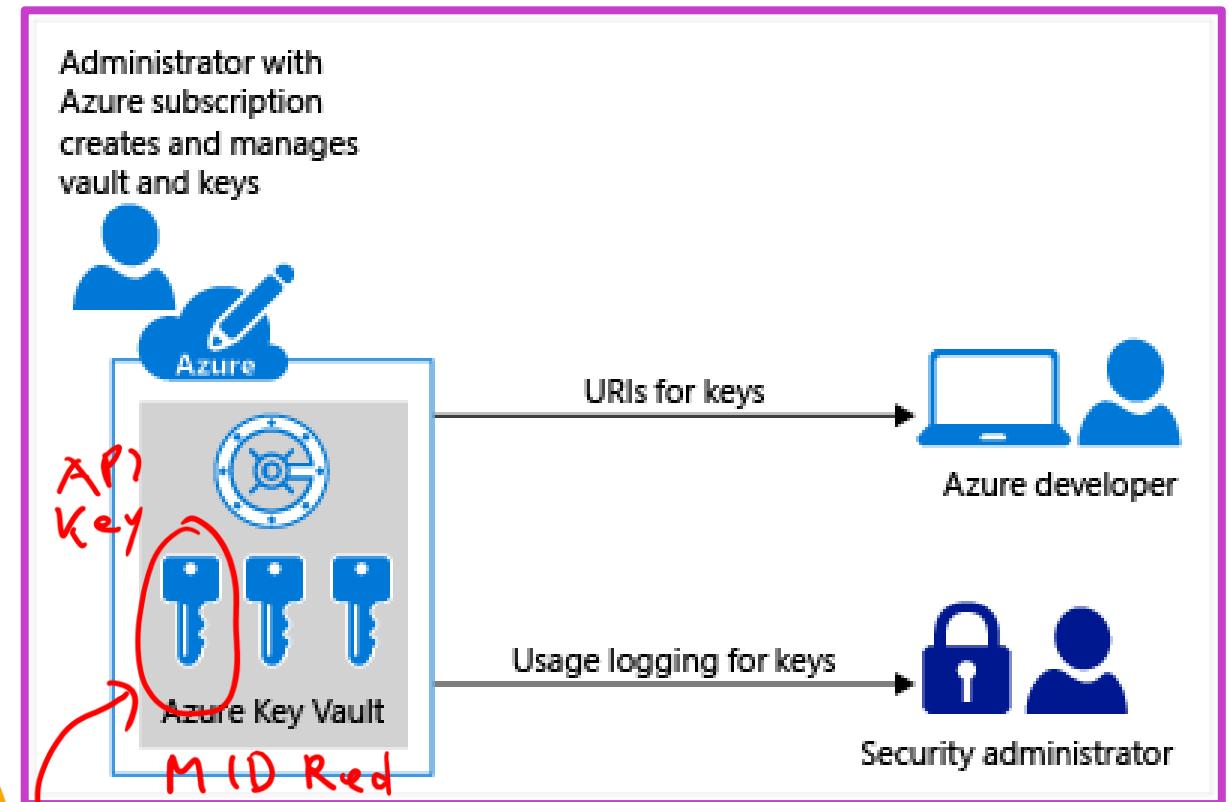


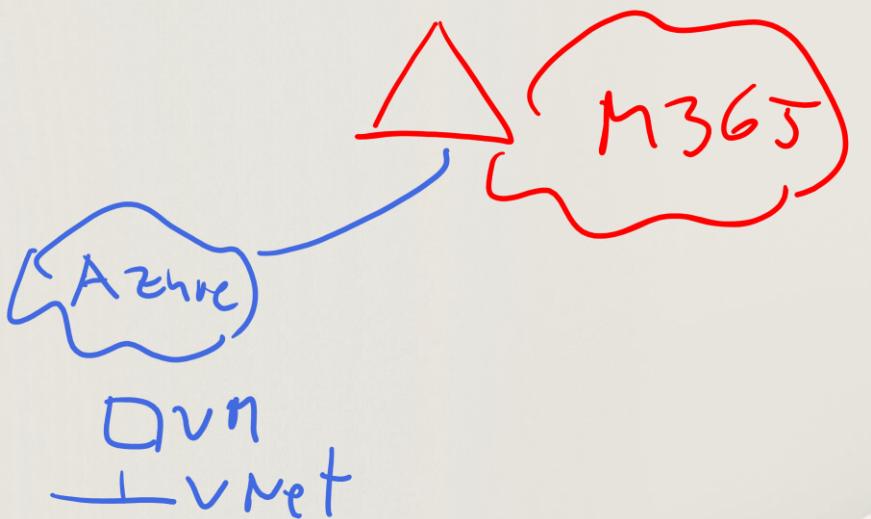
Azure Key Vault

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

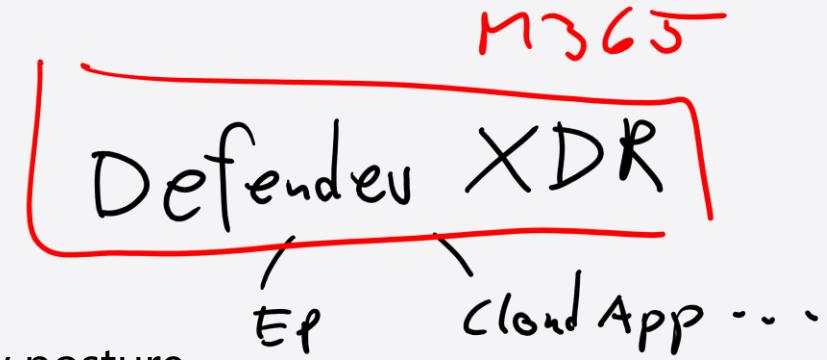
Module 3 introduction

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.



Azure



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.

Free

42%

Cloud security posture management (CSPM)

Surfaces actions that you can take to prevent breaches.

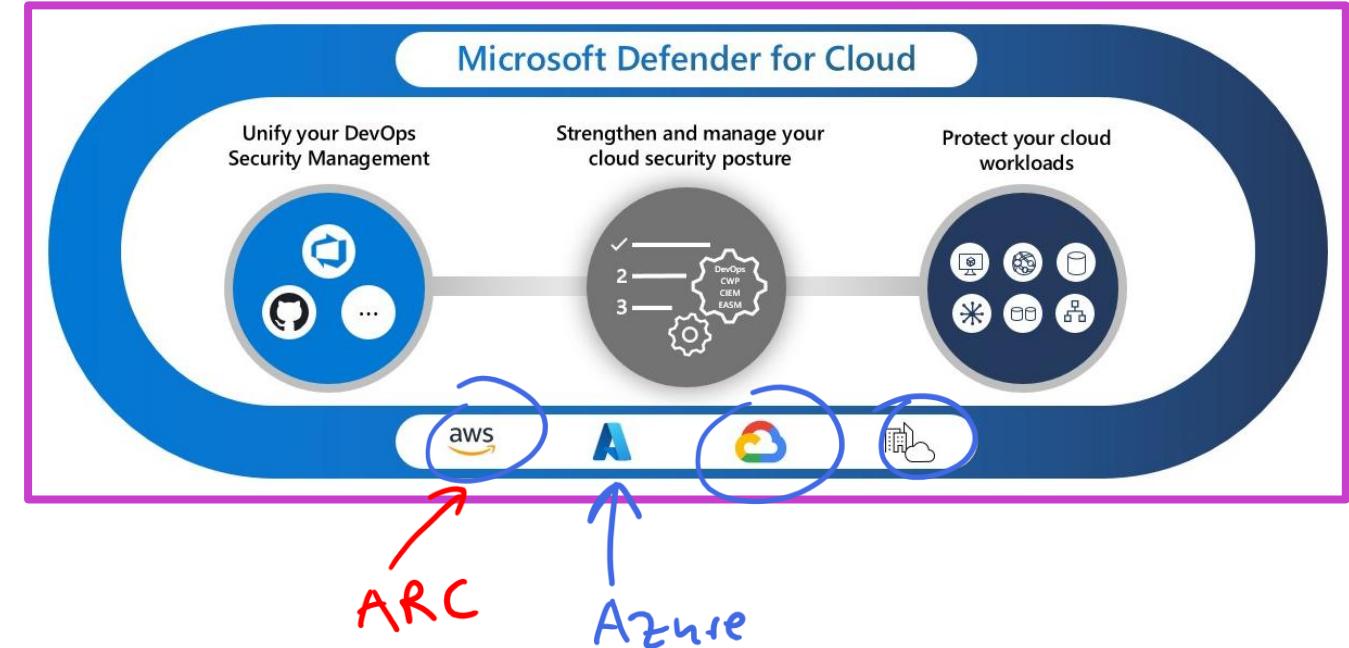
Recommendation

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

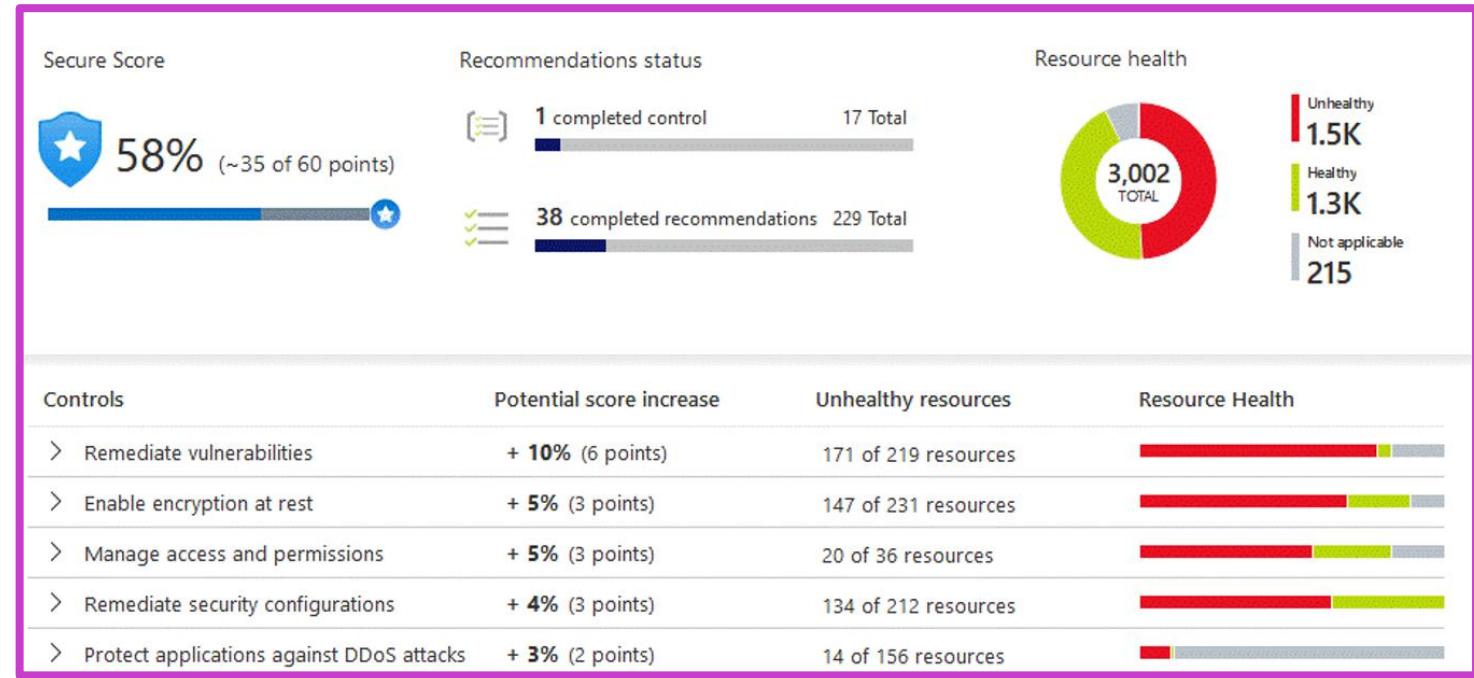
- Continually assesses your environment against MCSB and other security initiatives.

The screenshot shows the Microsoft Defender for Cloud Regulatory compliance dashboard. On the left, there's a sidebar with categories like General, Cloud Security, and Management. The 'Regulatory compliance' section is currently selected. In the main area, there's a heading 'Microsoft cloud security benchmark (preview)' with a red box around it. Below it, a progress bar shows '48 of 59 passed controls'. To the right, there's a chart titled 'Lowest compliance regulatory standards' showing results for SOC TSP, PCI DSS 3.2.1, and ISO 27001. Further down, there's a survey question 'Is the regulatory compliance experience clear to you?' with 'Yes' and 'No' options. A red box highlights the 'Microsoft cloud security benchmark' link. At the bottom, there's a section for 'NS. Network Security', 'IM. Identity Management', and 'PA. Privileged Access' with green checkmarks. A red box also highlights the 'Expand all compliance controls' checkbox.

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

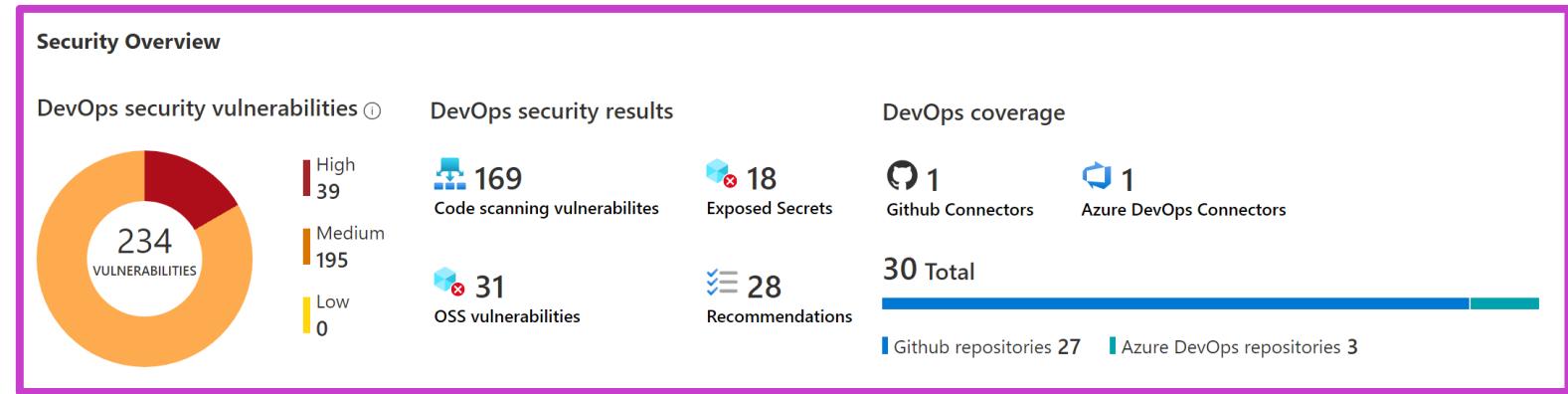
 Enable the enhanced security features of Microsoft Defender for Cloud. [Learn more >](#)

Enhanced security off	Enable all Microsoft Defender for Cloud plans
✓ Continuous assessment and security recommendations	✓ Continuous assessment and security recommendations
✓ Secure score	✓ Secure score
✗ Just in time VM Access	✓ Just in time VM Access
✗ Adaptive application controls and network hardening	✓ Adaptive application controls and network hardening
✗ Regulatory compliance dashboard and reports	✓ Regulatory compliance dashboard and reports
✗ Threat protection for Azure VMs and non-Azure servers (including Server EDR)	✓ Threat protection for Azure VMs and non-Azure servers (including Server EDR)
✗ Threat protection for supported PaaS services	✓ Threat protection for supported PaaS services

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.



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.

Sentinel SIEM and SOAR

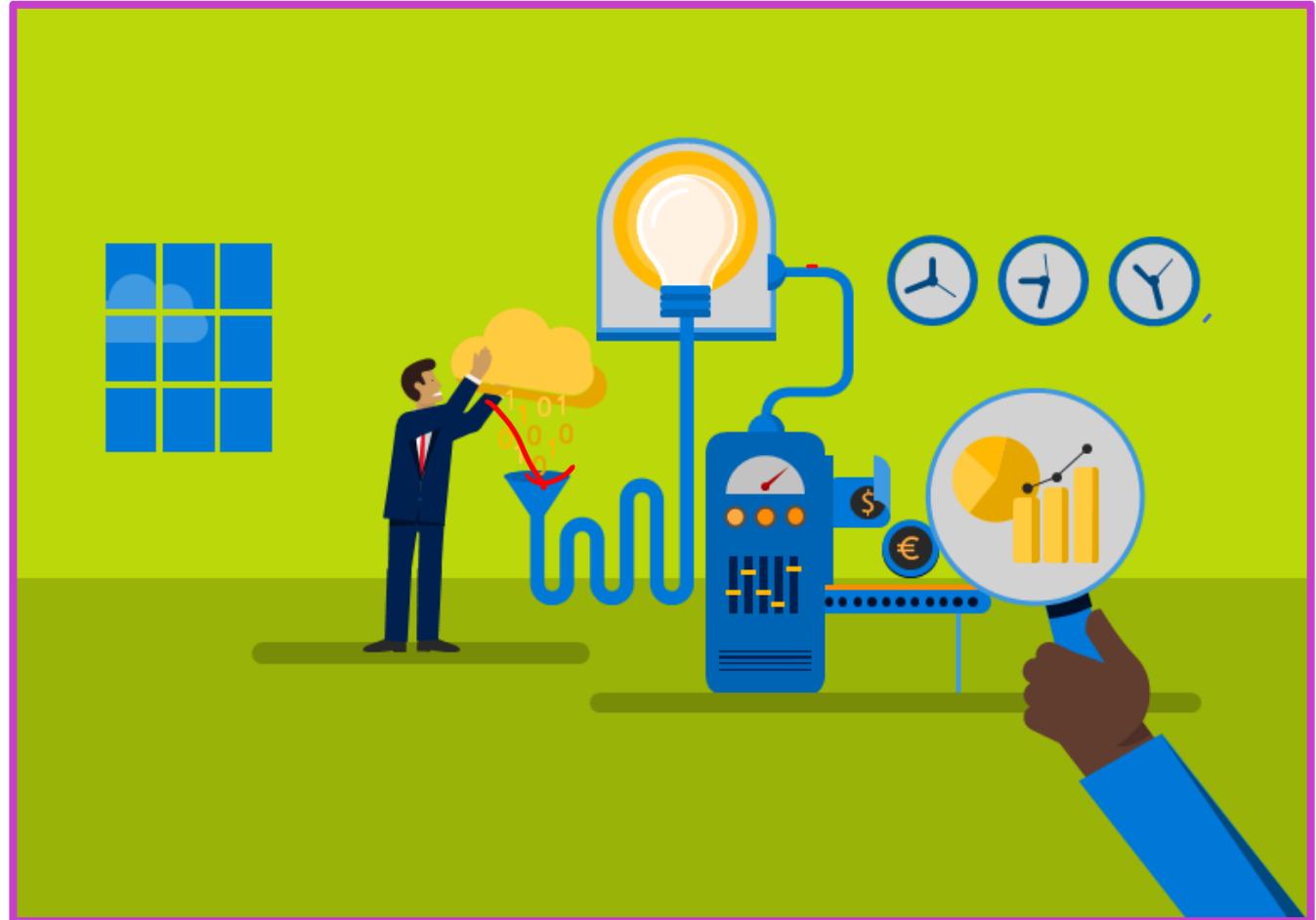


Security incident and event management (SIEM)

- 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

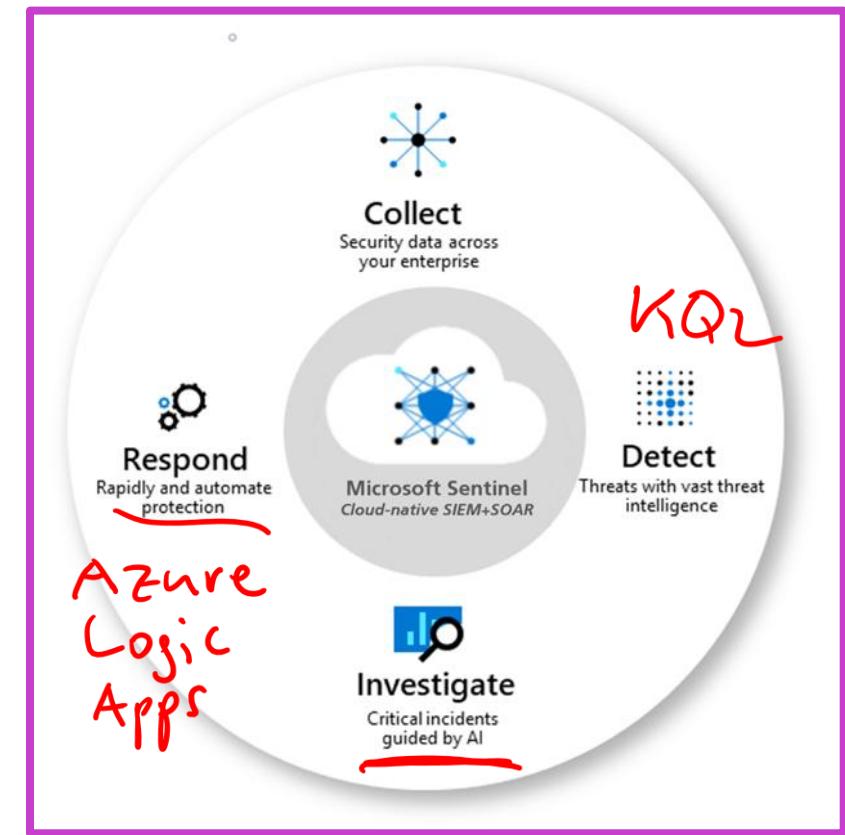
Collect data at scale across all users, devices, applications, and infrastructure, both on-premises and in multiple clouds.

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

The screenshot shows a dark-themed user interface for Microsoft Copilot for Security. At the top, there's a navigation bar with the text "Microsoft Copilot for Security / My sessions / Microsoft Sentinel incident investigation". Below the navigation are several small icons. The main area has a title "Microsoft Sentinel incident investigation" with a sub-section "Summarize Sentinel incident 99697". A progress bar indicates "3 steps completed" in 42 seconds. The summary text details an incident from Aug 15, 6:16 PM, with ID 99697, titled "Administrative action submitted by an Administrator", which occurred on 2024-08-14 at 00:02:07 UTC. It describes an administrator moving email messages to the Junk folder, targeting NetworkMessageId:68370e04-4971-41b8-081d-08dcbbca3de7 with recipient mayane@woodgrove.ms and content type 1. A note states that this was the only event associated with the incident. At the bottom, there are "References" and a "Microsoft Sentinel" button.

Module 5: Describe threat protection with Microsoft Defender XDR

Module 5 introduction

After completing this module, you should be able to:

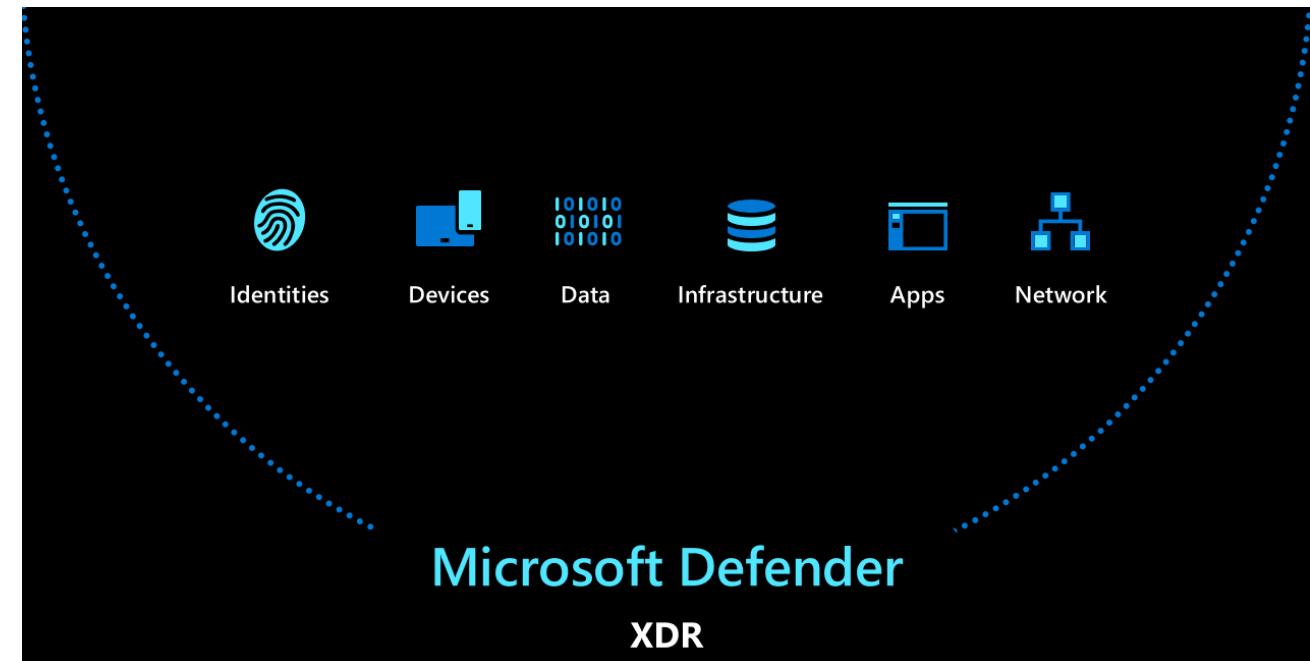
- 1** Describe the Microsoft Defender XDR service.
- 2** Describe how Microsoft Defender XDR provides integrated protection against sophisticated attacks.
- 3** Describe and explore the Microsoft Defender portal.
- 4** Describe Microsoft Defender for Copilot integration with Microsoft Defender XDR.

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

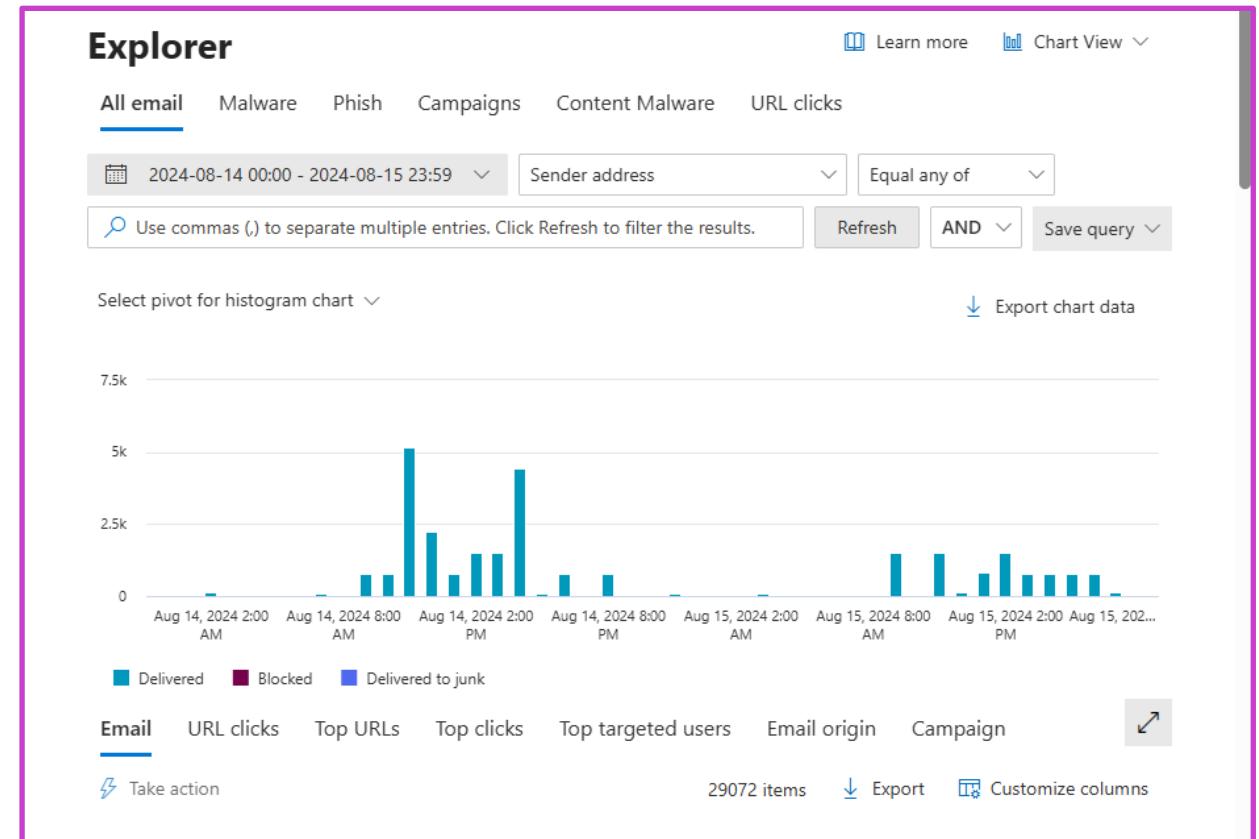
- Policies for anti-malware, anti-spam, anti-phishing |
- Safe attachments |
- Attack simulation training |
- More...

Investigate

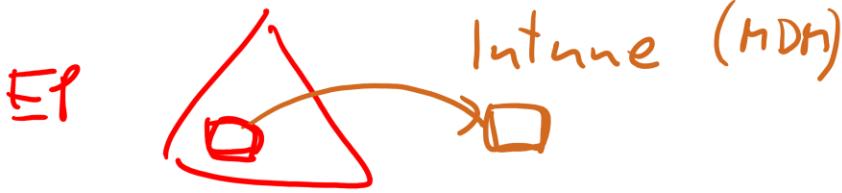
- Audit log search
- Message trace
- Explorer
- More..

Respond

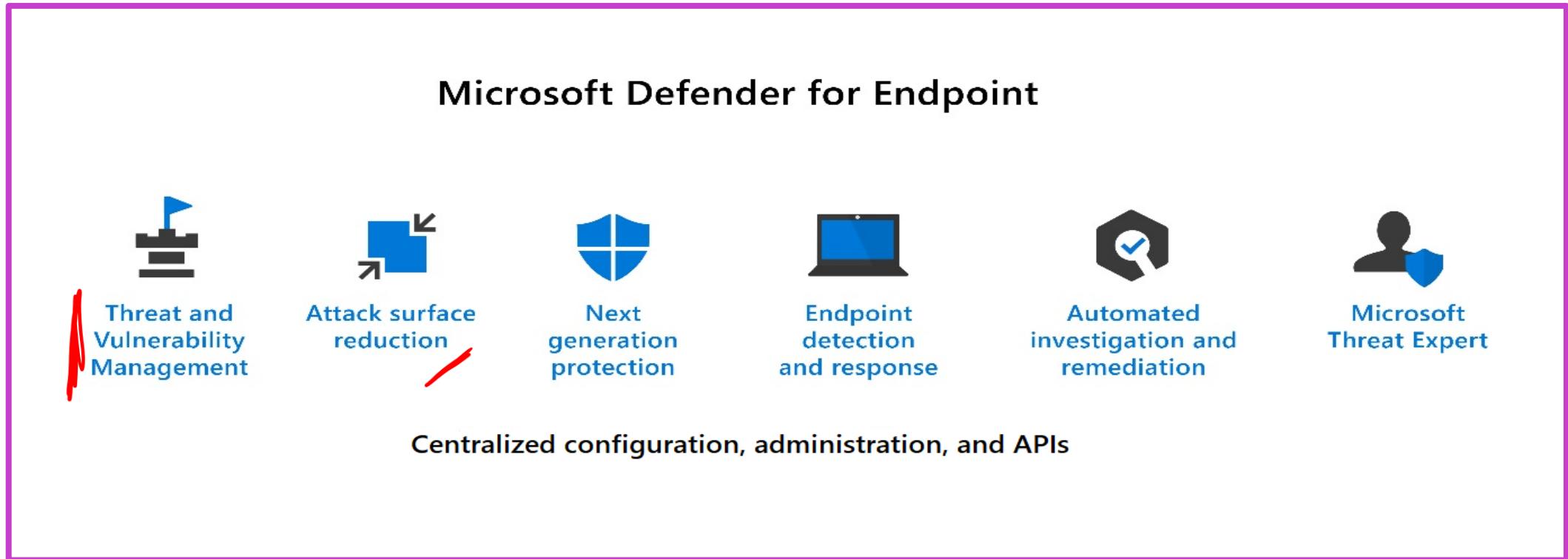
- Zero-hour auto purge (ZAP)
- Automated investigation and response
- More...



Microsoft Defender for Endpoint



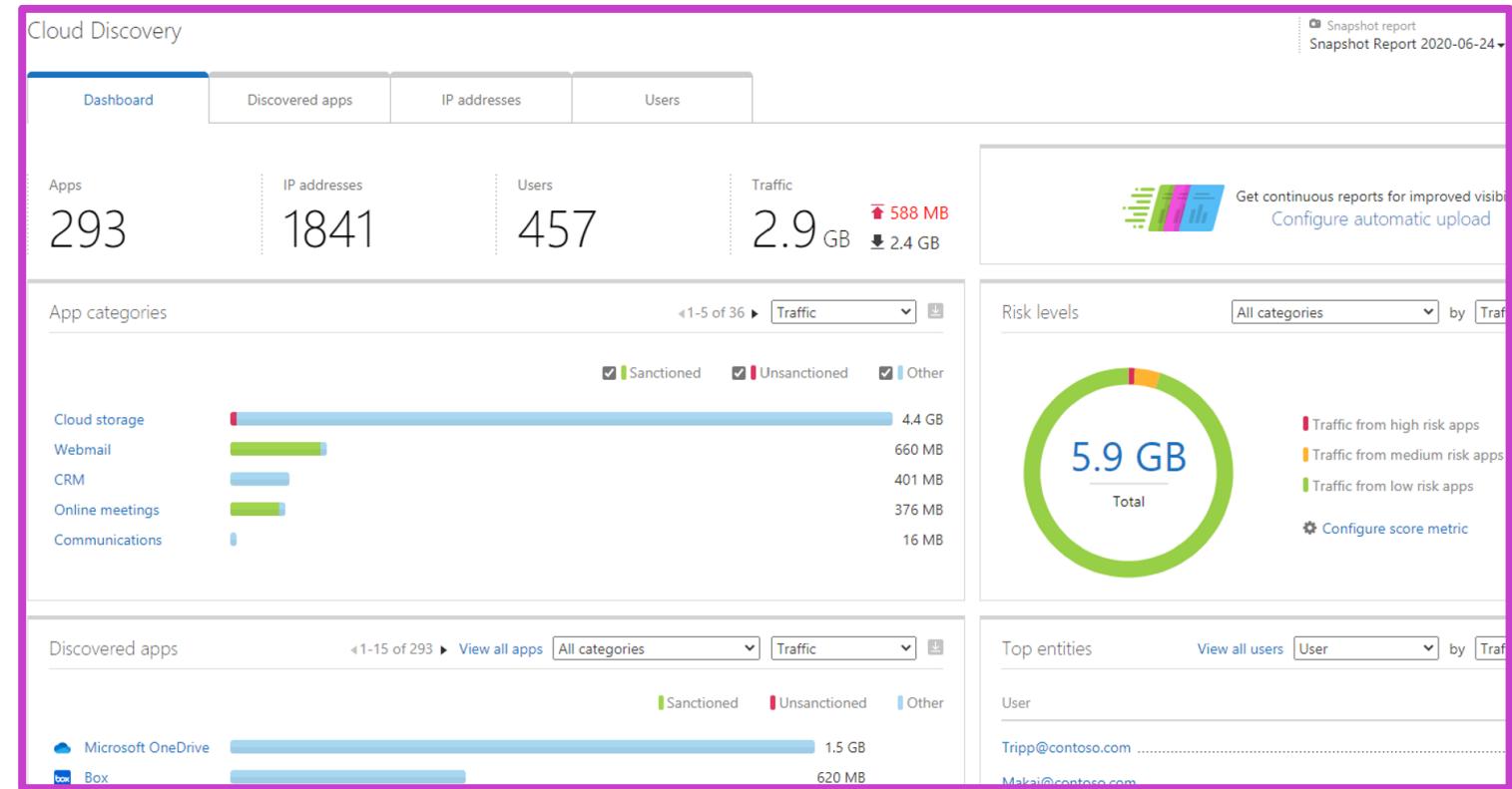
Microsoft Defender for Endpoint is a platform designed to help enterprise networks protect endpoints.



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.

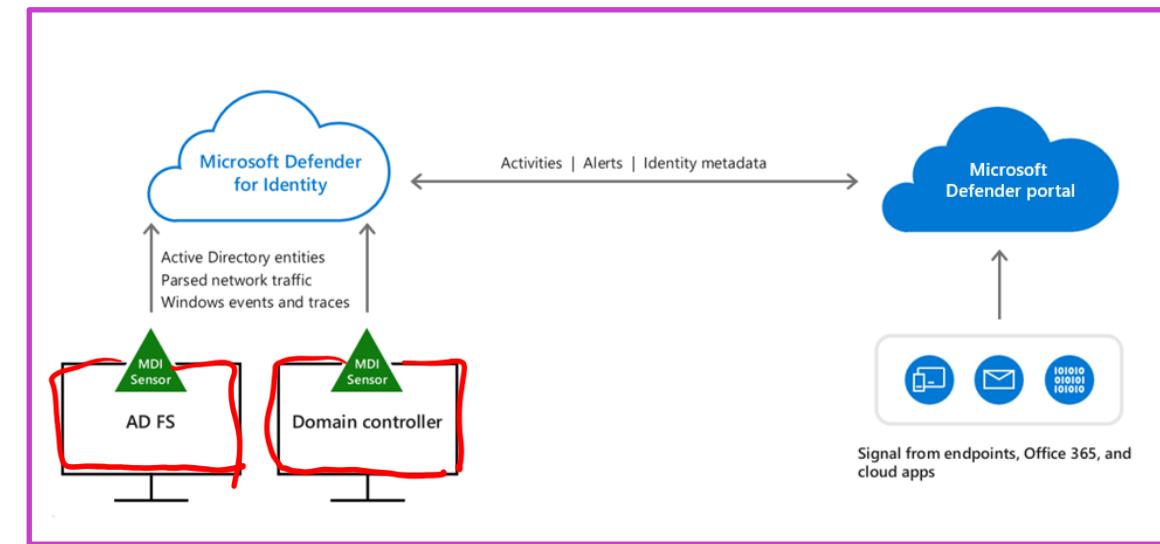
- Discover SaaS applications
- Information protection
- SaaS Security Posture Management (SSPM)
- Advanced threat protection
- App-to-app protection with app governance



Microsoft Defender for Identity

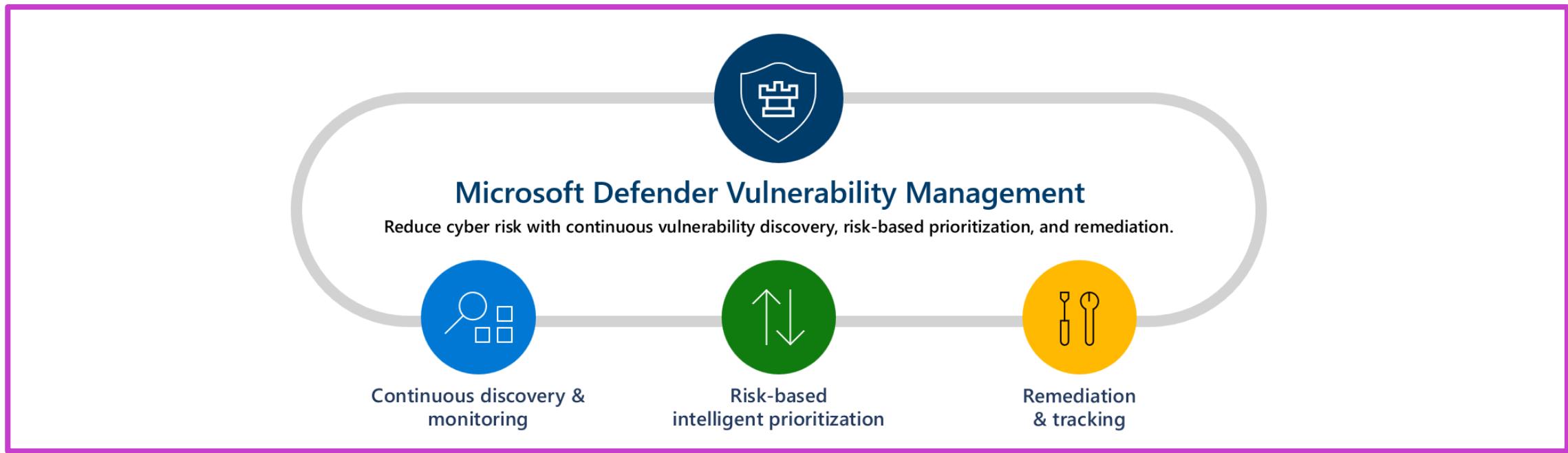
A cloud-based security solution that uses signals from your on-premises identity infrastructure servers to detect threats, like privilege escalation or high-risk lateral movement, and reports on easily exploited identity issues.

- 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 Vulnerability Management

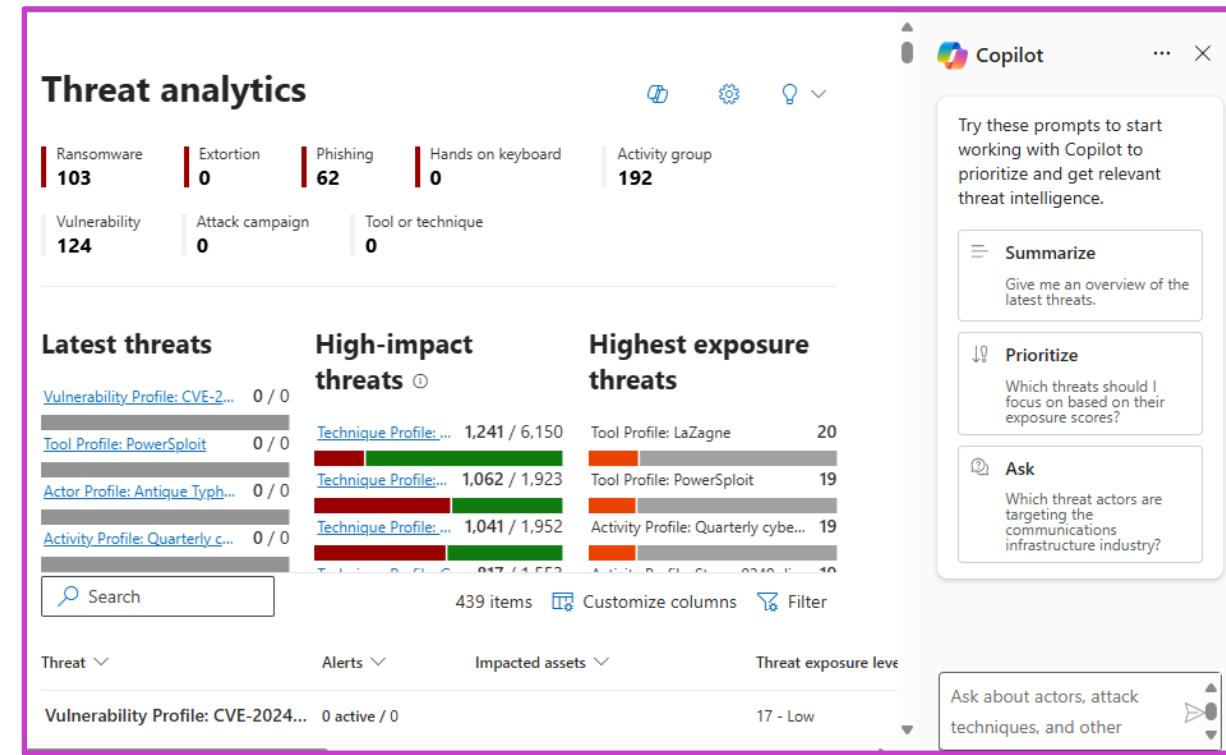
Delivers asset visibility, intelligent assessments, and built-in remediation tools for Windows, macOS, Linux, Android, iOS, and network devices.



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.

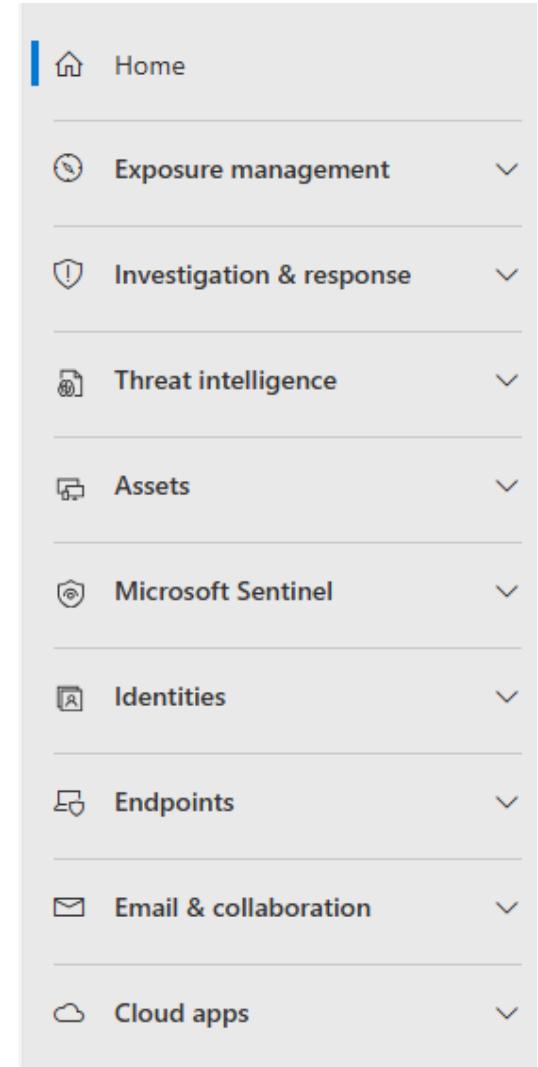
- Threat analytics - Understand how emerging threats impact your organization's environment.
- Intel profiles - A definitive source of Microsoft's shareable knowledge on tracked threat actors, malicious tools, and vulnerabilities.
- Intel explorer - Where analysts can quickly scan new featured articles 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.

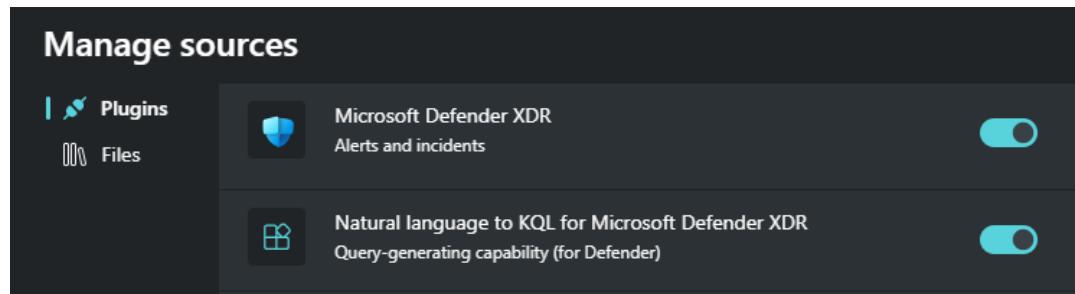


Copilot integration with Microsoft Defender XDR

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.



≡ SYSTEM CAPABILITIES

MICROSOFT DEFENDER XDR

Analyze a file
Inspect a file using available information, including API calls, certificates...

Generate an identity summary
Get identity insights, security concerns and potential anomalies

Generate an incident report
Get a report about an attack and your response, including who took act...

Generate guided response
Get step-by-step response recommendations for an incident.

List incidents and related alerts
Get the list of incidents or find specific incidents.

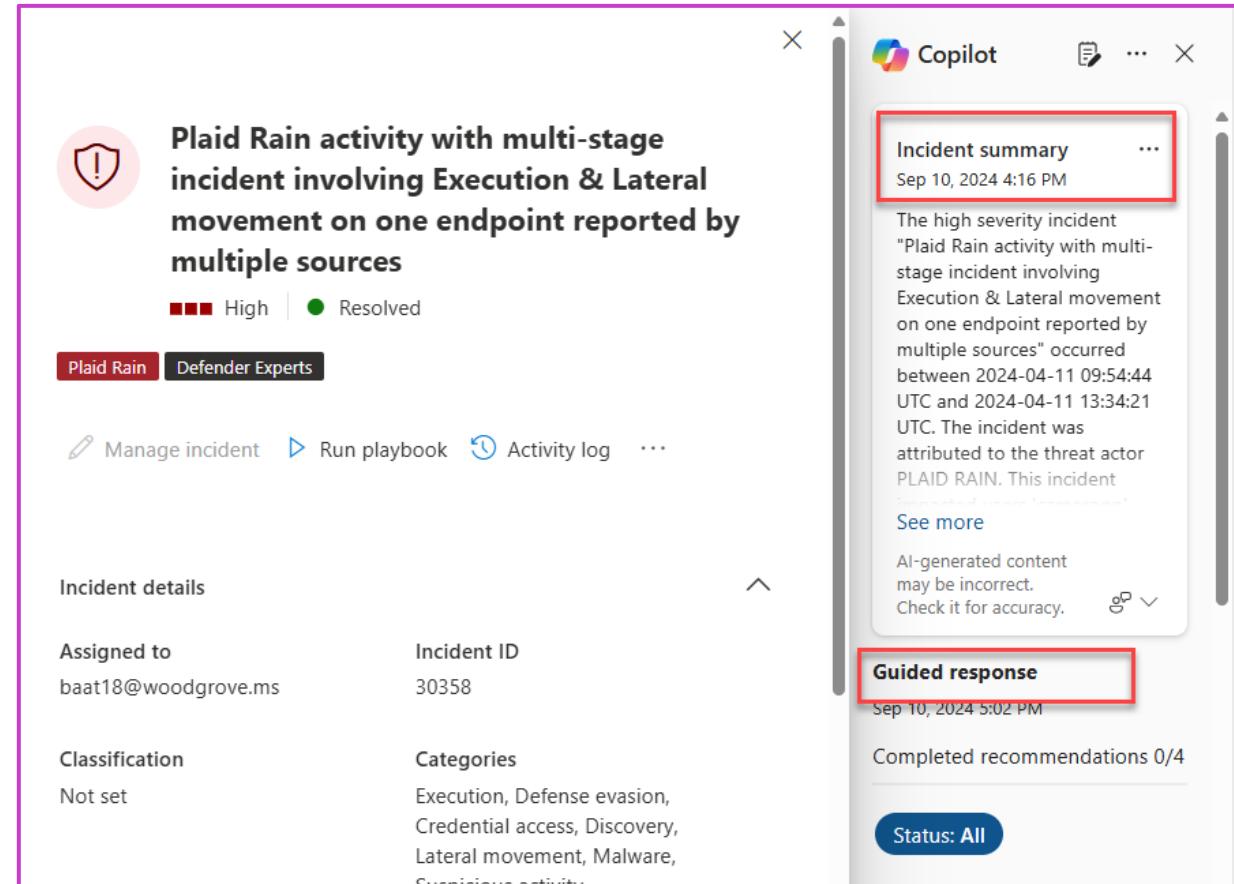
How can Copilot for Security help? ✖️ ✖️ ✖️

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



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.

