



Microsoft Learn Spark possibility



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

Learning Path Agenda



- 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 the core infrastructure security services in Azure



Module 1 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.

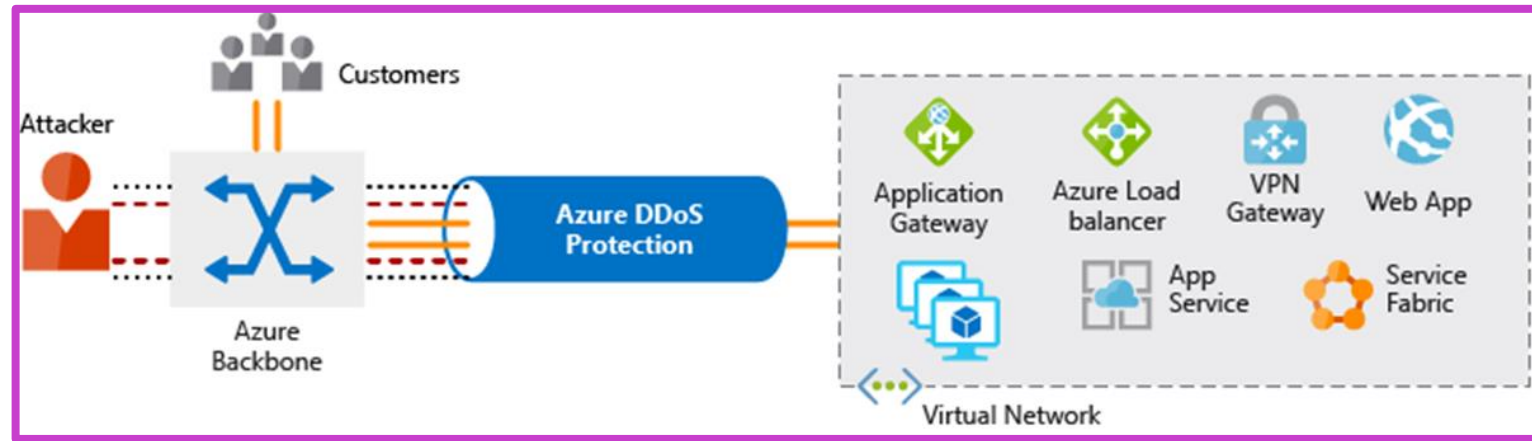
Azure DDoS Protection

Distributed Denial of Service (DDoS)

- Attacks that makes resources unresponsive.

Azure DDoS protection

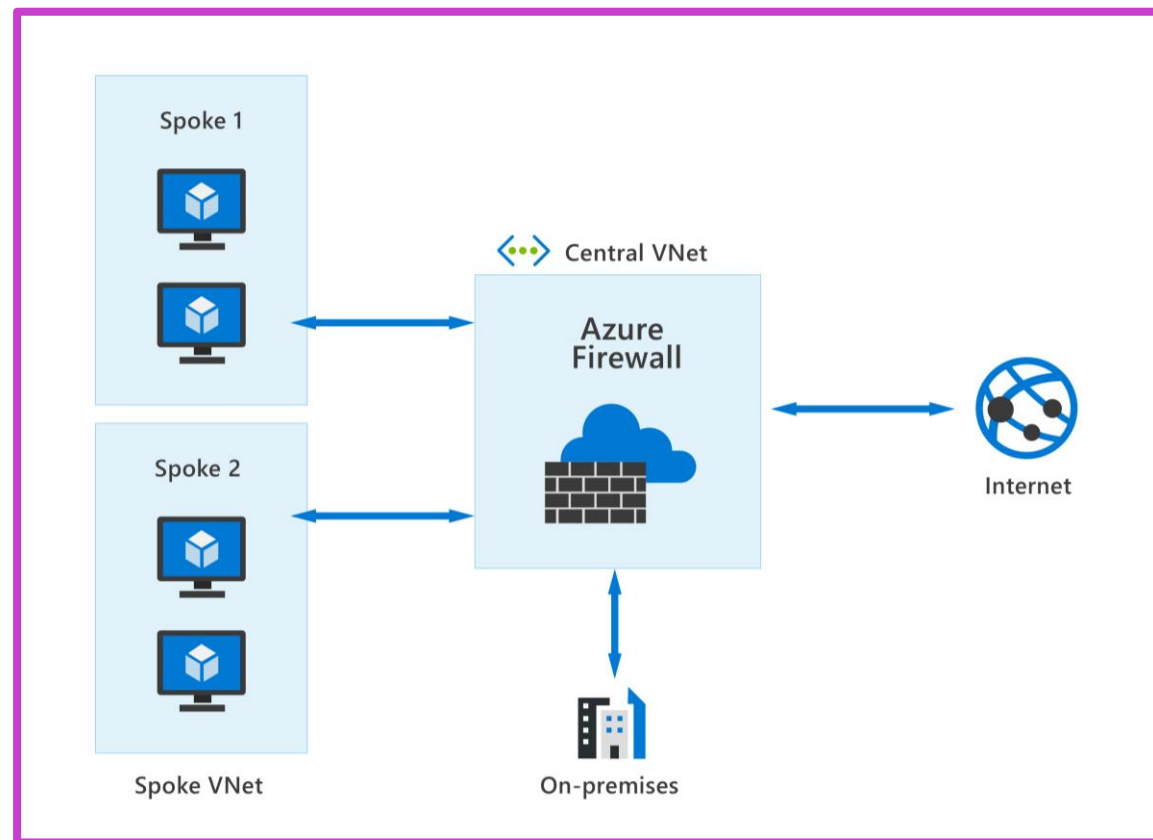
- Analyzes network traffic and discards anything that looks like a DDoS attack.
- Always-on traffic monitoring.
- Adaptive real-time tuning.
- DDoS Protection telemetry, monitoring, and alerting.



Azure Firewall

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

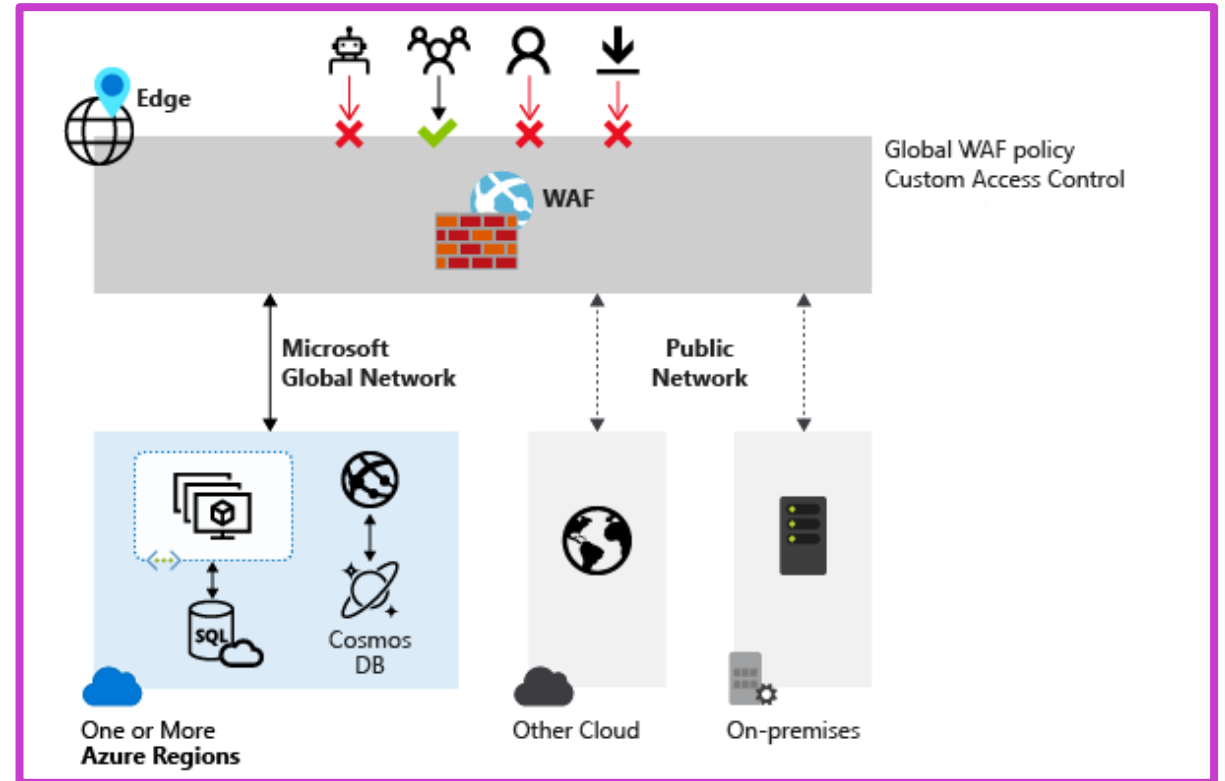
- Create *allow* or *deny* network filtering rules.
- Use Microsoft Threat Intelligence feed to alert or filter traffic from/to known malicious IP addresses and domains.
- All outbound virtual network traffic IP addresses are translated to the Azure Firewall public IP to make it harder for attackers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



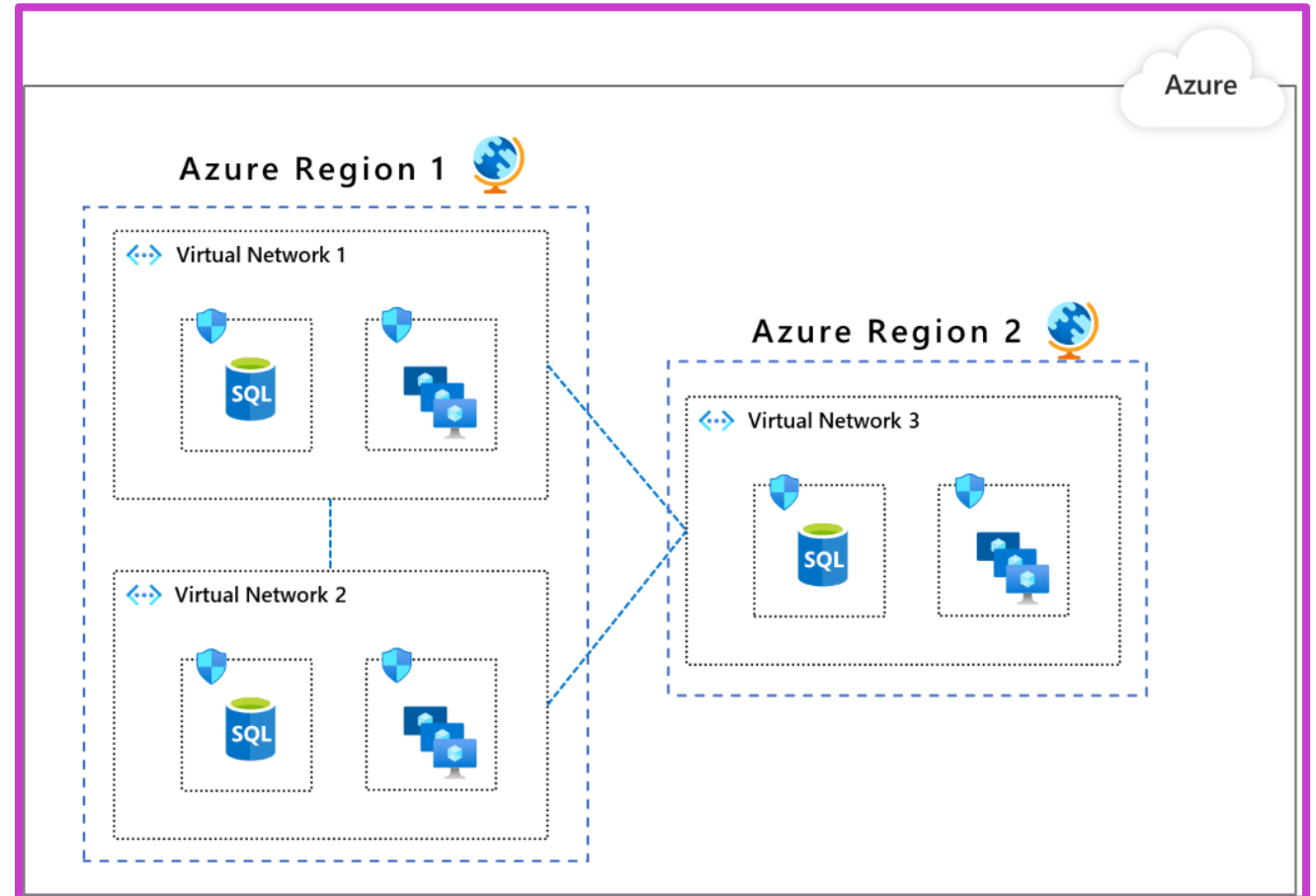
Network segmentation and Azure VNet

Reasons for network segmentation

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

Azure Virtual Network (VNet)

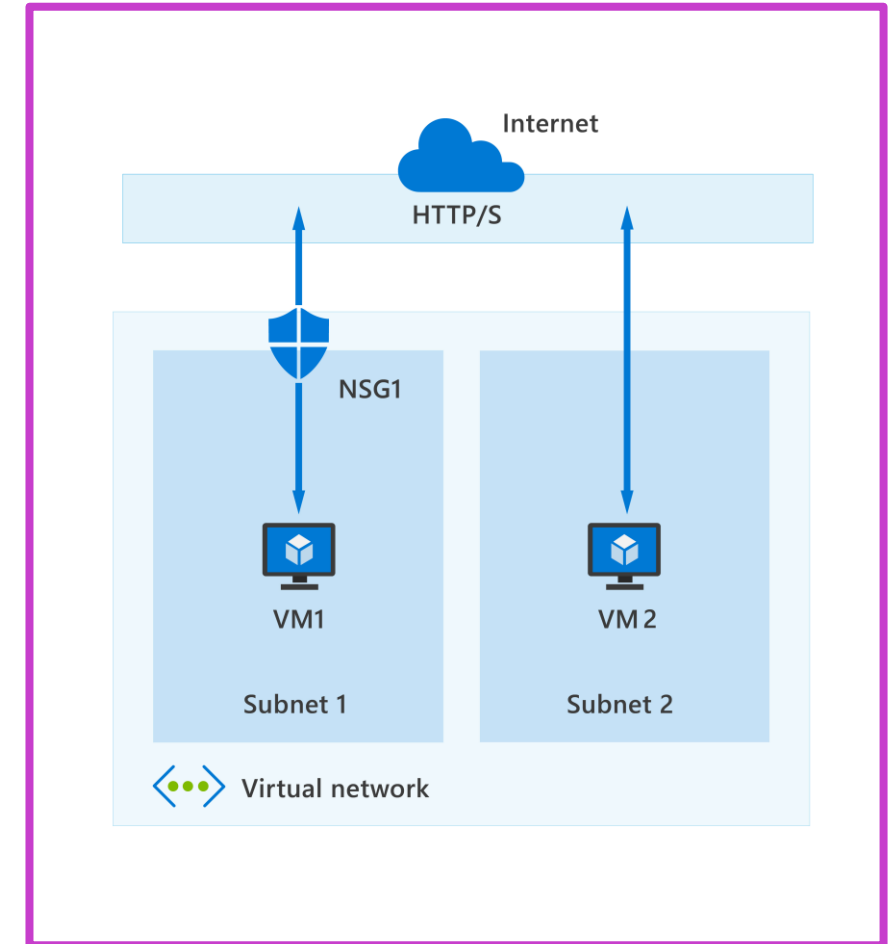
- Network level containment of resources with no traffic allowed across VNets or inbound to VNet.
- Communication needs to be explicitly provisioned.
- Control how resources in a VNet communicate with other resources, the internet, and on-premises networks.



Azure network security groups (NSGs)

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

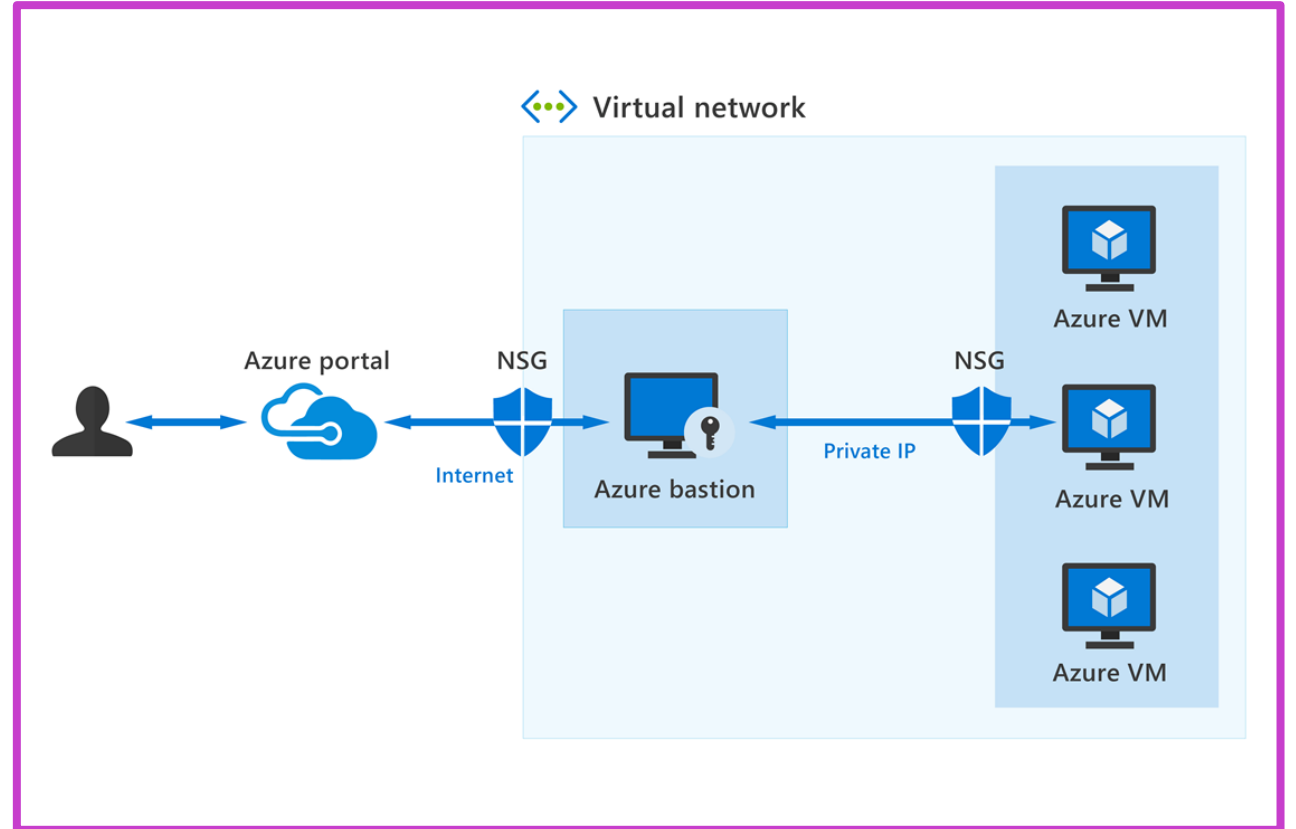
- An NSG is made up of inbound and outbound security rules that allow or deny traffic.
- An NSG can contain many rules, the rules are processed based on their assigned priority.
- When an NSG is created, it includes default inbound and outbound rules.
- You can't remove the default rules, but you can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

- Secure connectivity using Remote Desktop Protocol (RDP) or Secure Shell (SSH).
- 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.

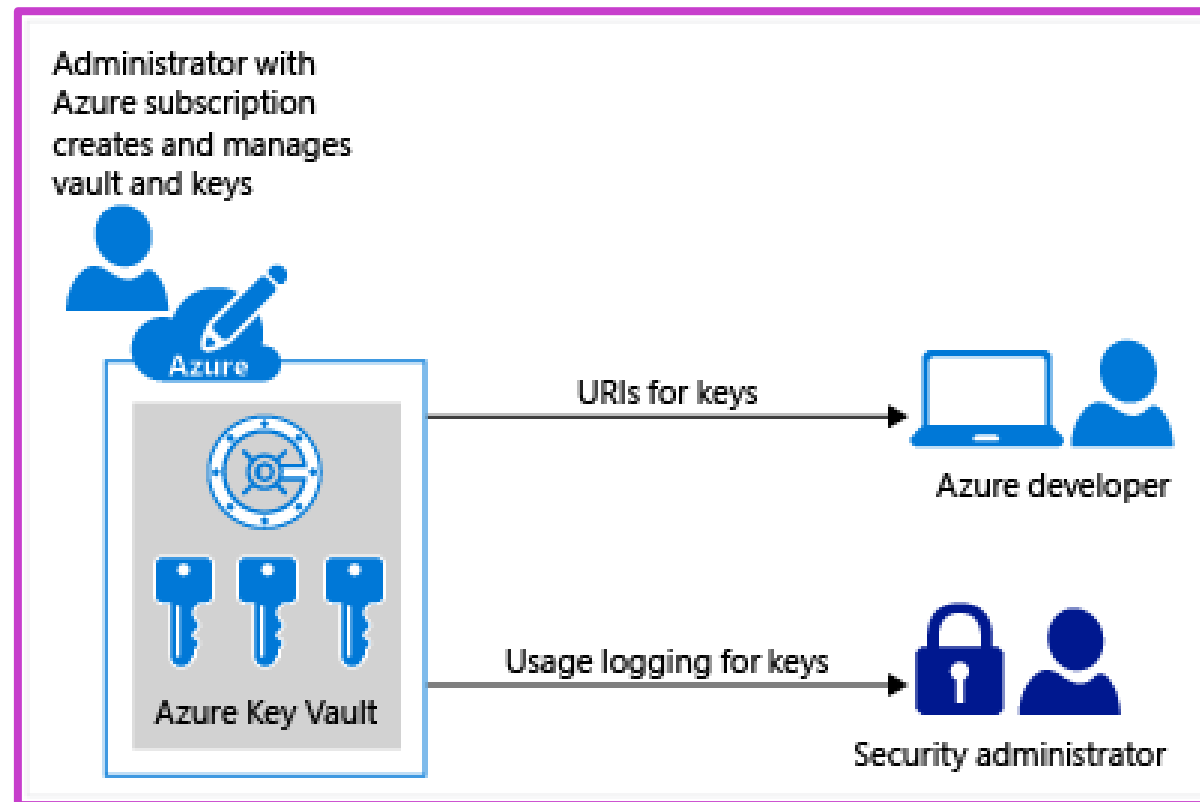


Azure Key Vault

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 2: Describe security management capabilities of Azure



Module 2 introduction

After completing this module, you should be able to:

- 1** Describe Azure security capabilities for protecting your network.
- 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)

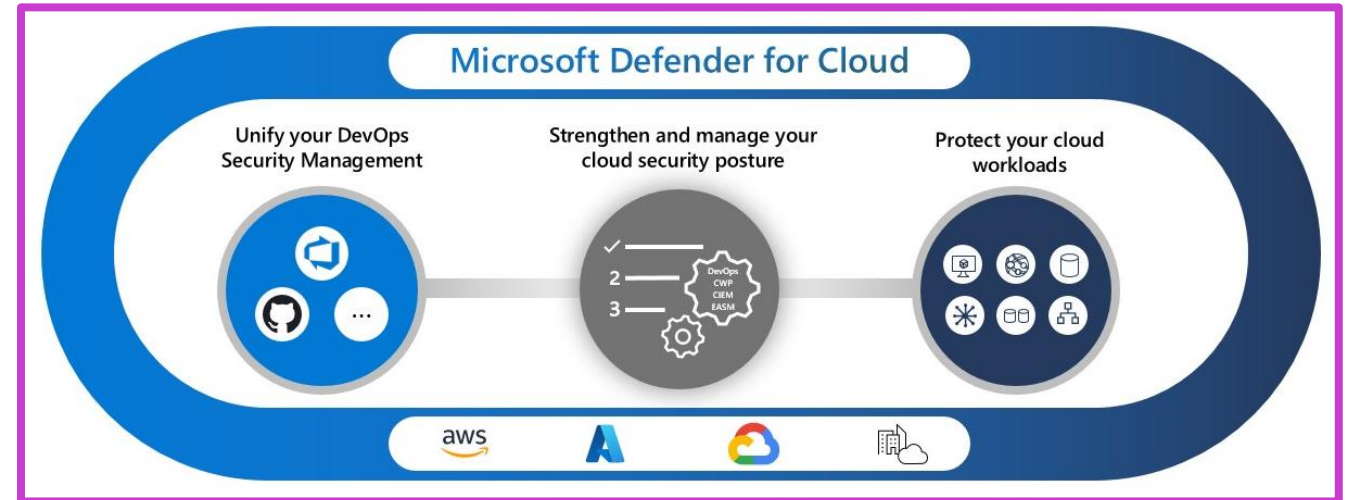
Surfaces actions that you can take to prevent breaches.

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.

Home > Microsoft Defender for Cloud

Microsoft Defender for Cloud | Regulatory compliance

Showing subscription 'Azure Pass - Sponsorship'

Search << Download report Manage compliance policies Open query Compliance over time workbook Audit reports Compliance offerings

General

- Overview
- Getting started
- Recommendations
- Security alerts
- Inventory
- Cloud Security Explorer (Preview)
- Workbooks
- Community
- Diagnose and solve problems

Cloud Security

- Security posture
- Regulatory compliance**
- Workload protections
- Firewall Manager
- DevOps Security (Preview)

Management

- Environment settings
- Security solutions
- Workflow automation

Microsoft cloud security benchmark (preview)

48 of 59 passed controls

Lowest compliance regulatory standards [Show all 4](#)

SOC TSP	13/13
PCI DSS 3.2.1	43/43
ISO 27001	20/20

Audit reports

Stay up to date on the latest privacy, security, and compliance-related information for Microsoft's cloud services.

[Open](#)

Is the regulatory compliance experience clear to you? ☐ Yes ☐ No

Microsoft cloud security benchmark ISO 27001 PCI DSS 3.2.1 SOC TSP

Recommendations from Microsoft Defender for Cloud - Regulatory Compliance should not be interpreted as a guarantee of compliance. It is up to you to evaluate and validate the effectiveness of customer controls per your regulatory environment. These services are subject to the terms and conditions in the [licensing terms](#).

Microsoft cloud security benchmark is applied to the subscription Azure Pass - Sponsorship

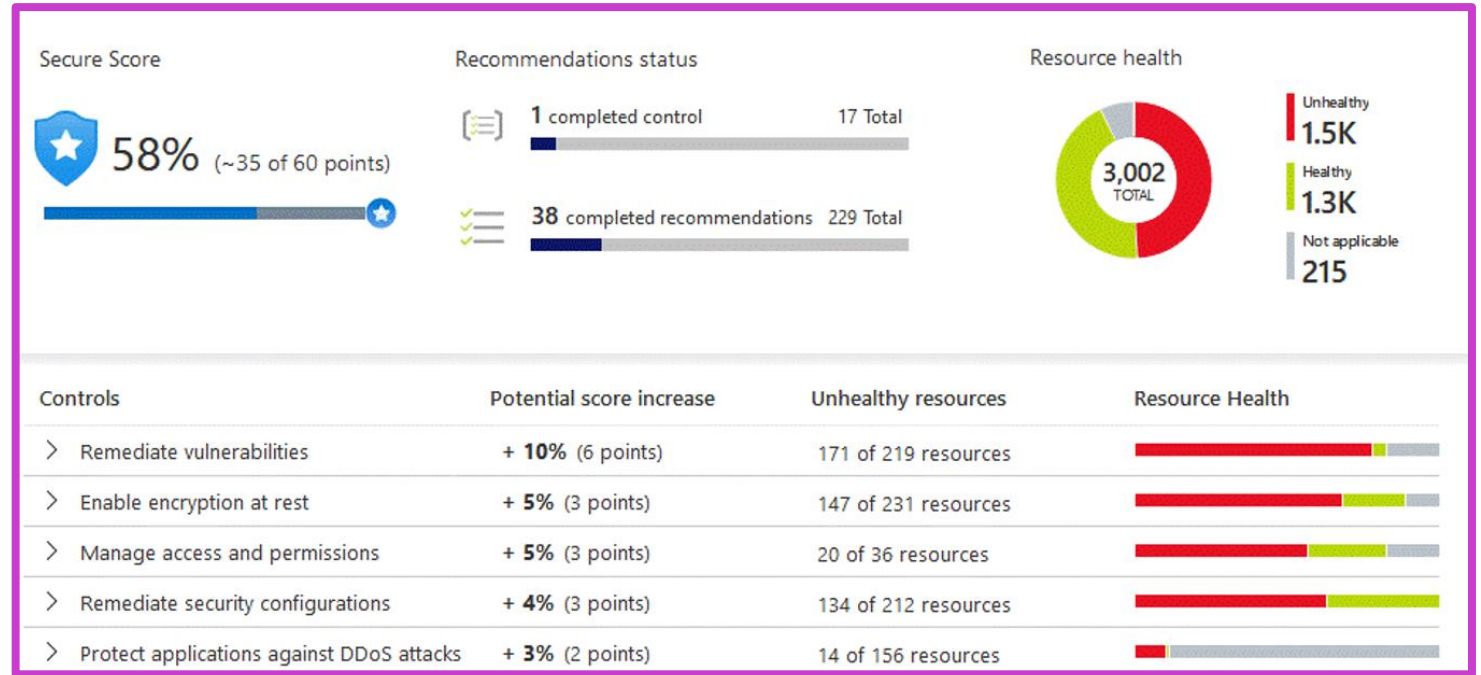
☐ Expand all compliance controls

- NS. Network Security
- IM. Identity Management
- PA. Privileged Access

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.



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

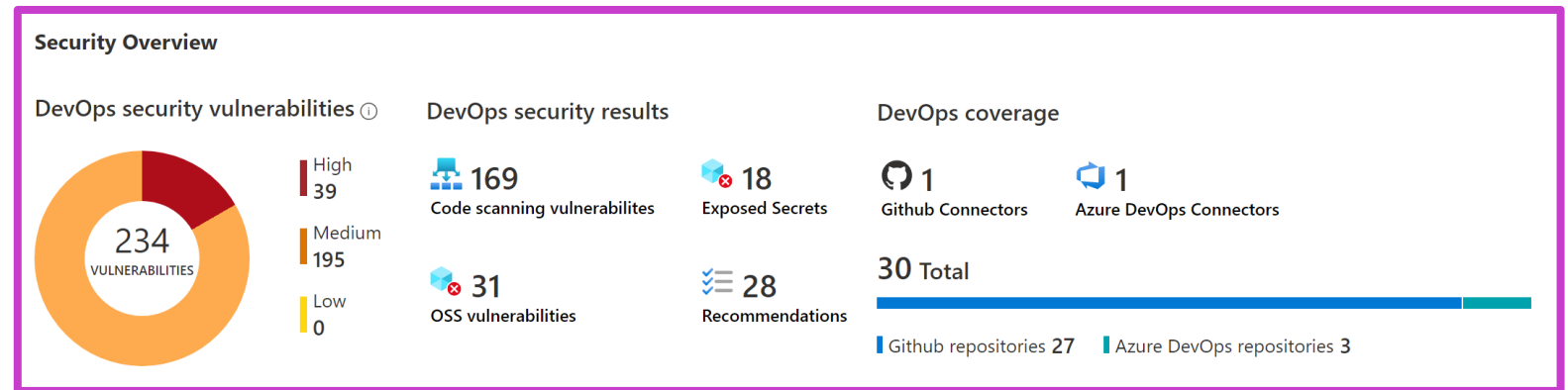
 **Enable the enhanced security features of Microsoft Defender for Cloud. [Learn more >](#)**

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 3: Describe the security capabilities of Microsoft Sentinel



Module 3 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.

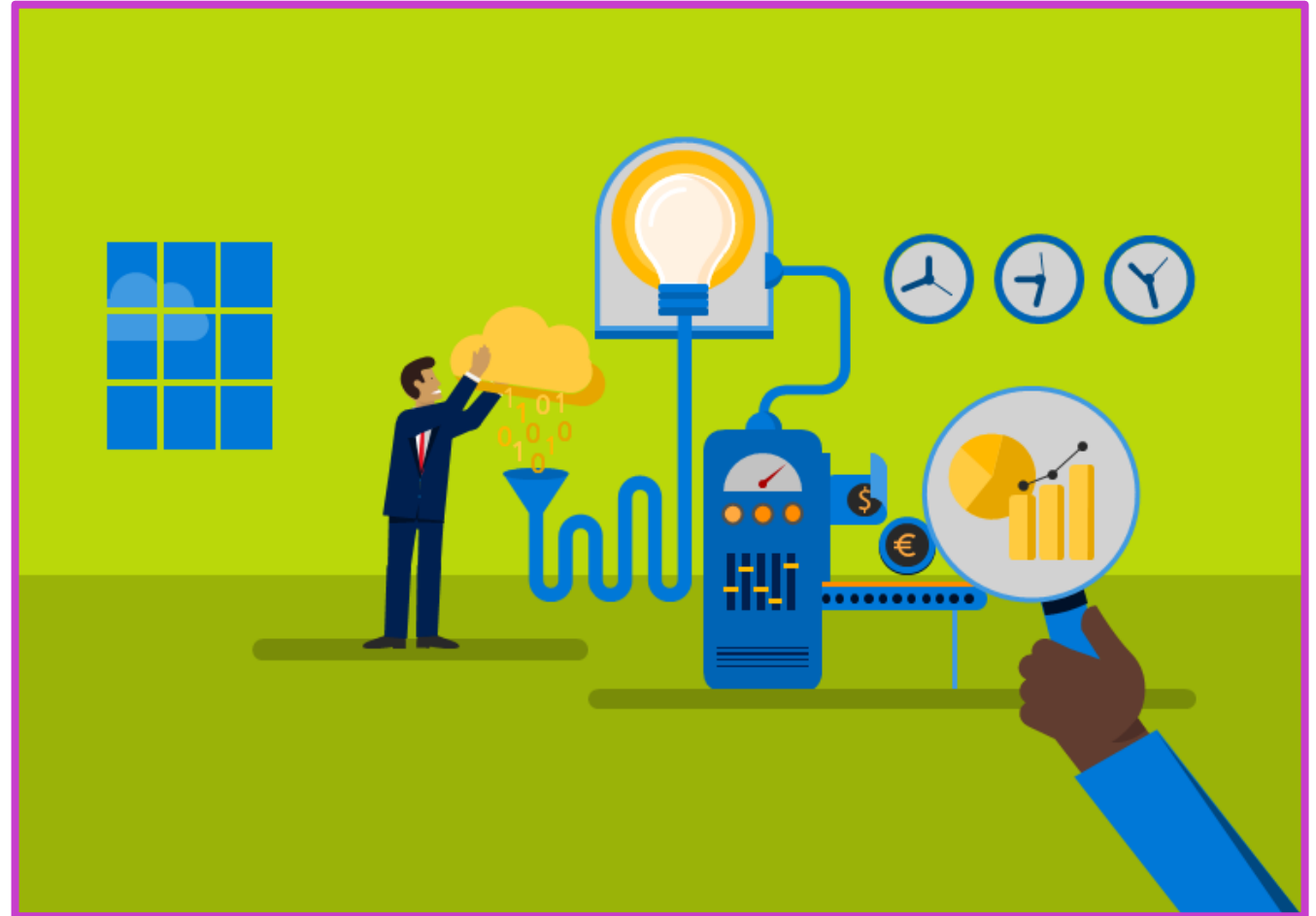
SIEM and SOAR

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

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

Detect

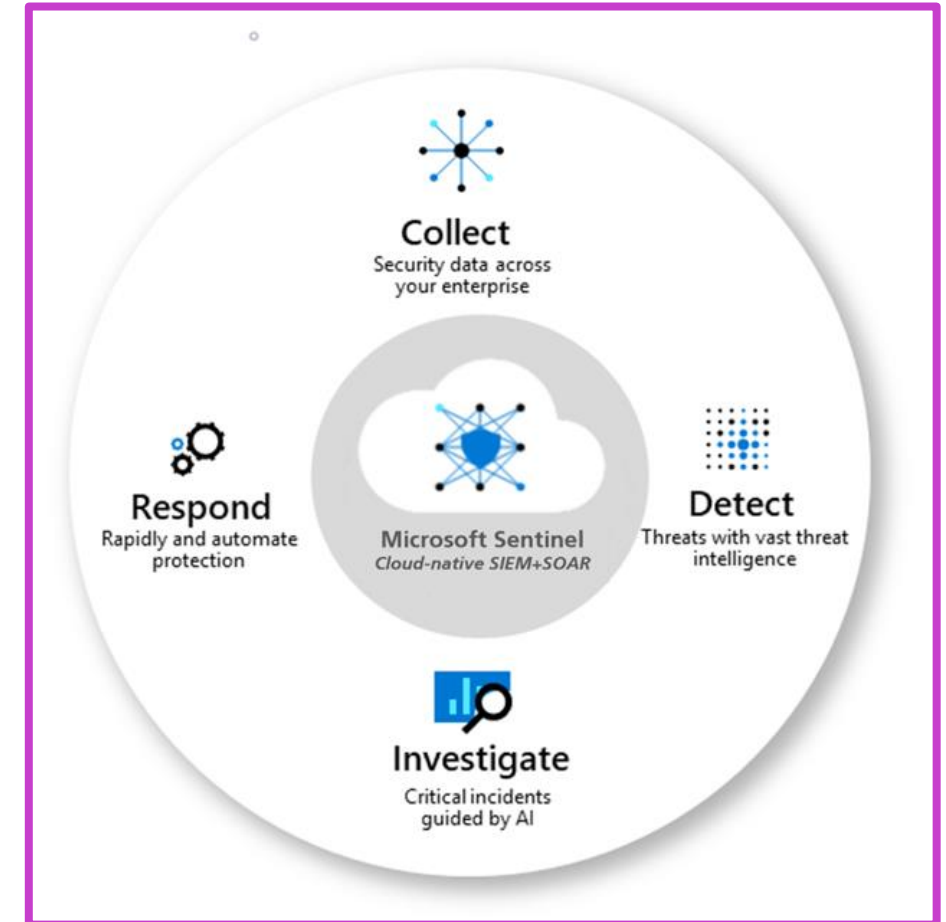
Detect previously uncovered threats and minimize false positives using analytics and unparalleled threat intelligence.

Investigate

Investigate threats with AI and hunt suspicious activities at scale, tapping into decades of cybersecurity work at Microsoft.

Respond

Respond to incidents rapidly with built-in orchestration and automation of common security.



Microsoft Security Copilot

The first and only generative AI security product to help defend organizations at machine speed and scale.

Security posture management

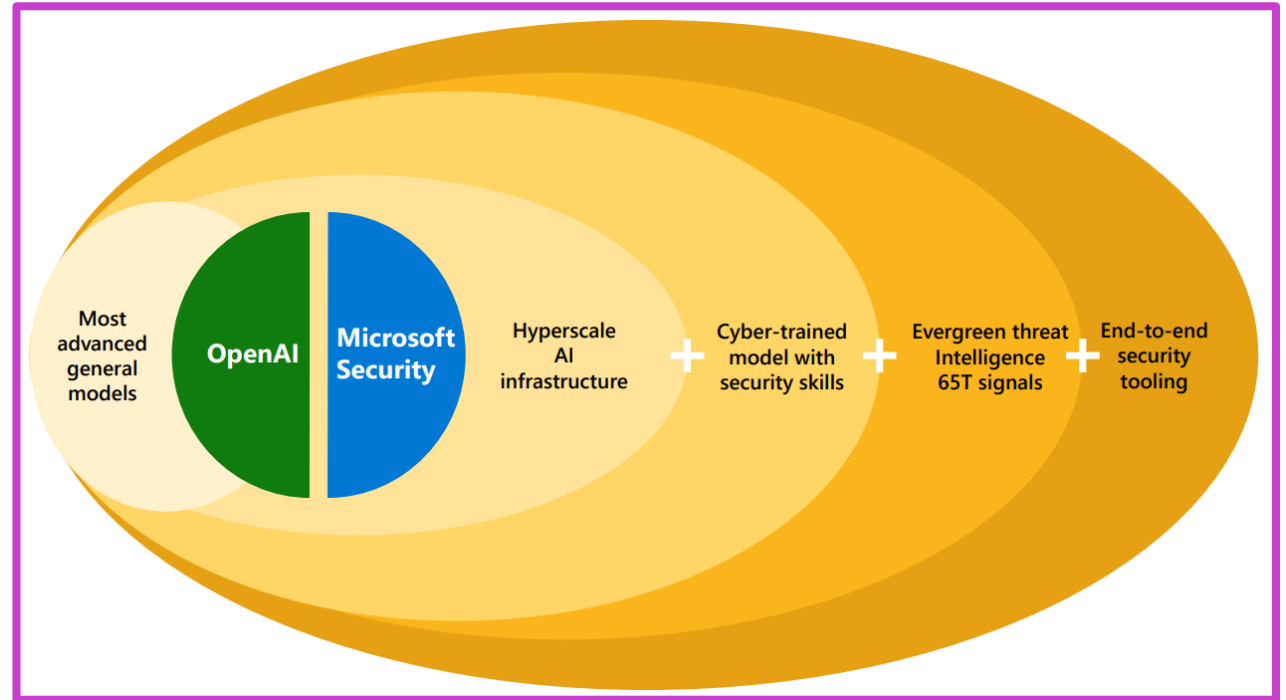
- Delivers information on anything that might expose an organization to a known threat.
- Provides prescriptive guidance on how to protect against those potential vulnerabilities.

Incident response

- Quickly surface an incident and enrich it with context from other data sources.
- Assess scale and get instructions to begin remediation.

Security reporting

- Customizable reports that are ready to share and easy to consume.



Module 4: Describe threat protection with Microsoft Defender XDR



Module 4 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.

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.

1 Microsoft Defender for Office 365

2 Microsoft Defender for Endpoint

3 Microsoft Defender for Cloud Apps

4 Microsoft Defender for Identity

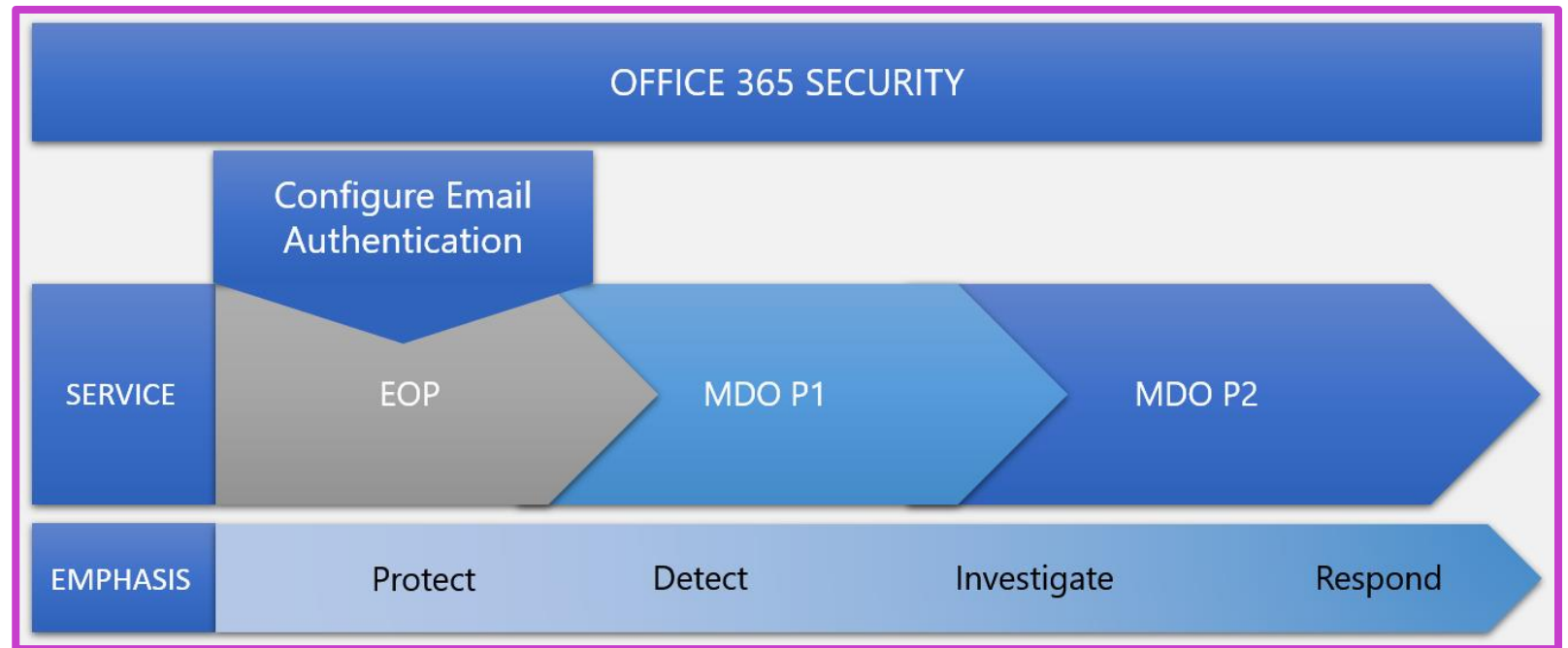
5 Microsoft Defender Vulnerability Management

6 Microsoft Defender Threat Intelligence

Microsoft Defender for Office 365

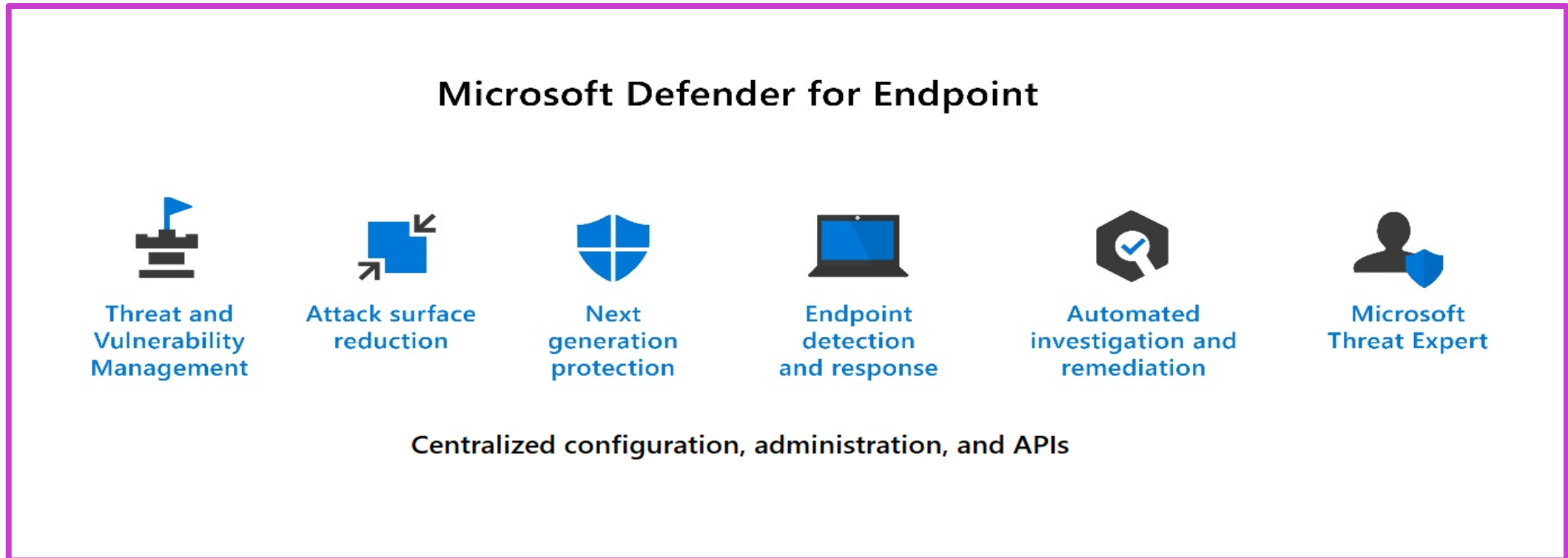
Seamless integration into your Office 365 subscription that provides protection against threats that arrive in email, links, attachments, or collaboration tools.

- Preset security policies
- Threat protection policies
- Reports
- Threat investigation and response
- Automated investigation and response



Microsoft Defender for Endpoint

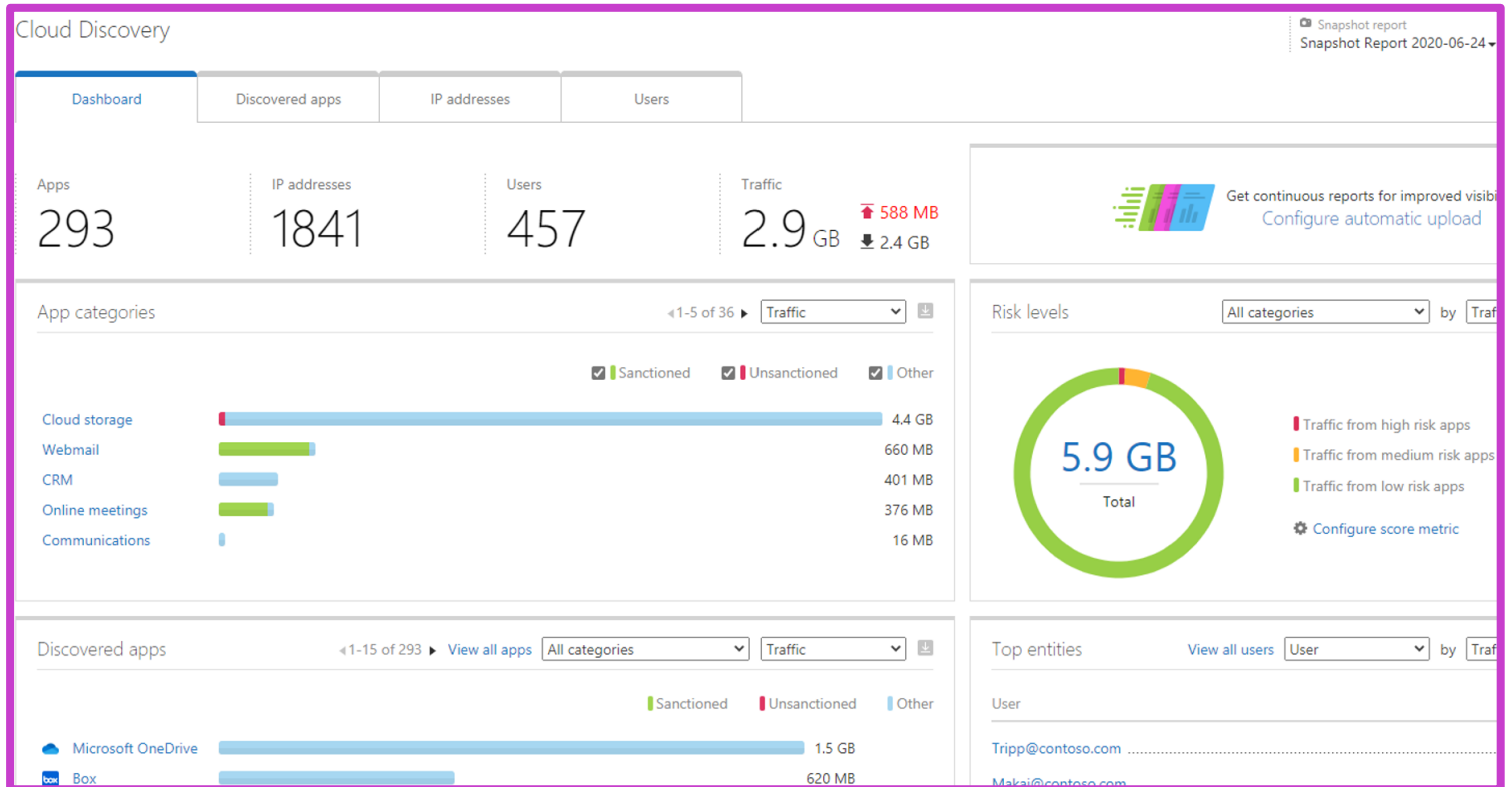
Microsoft Defender for Endpoint is a platform designed to help enterprise networks protect endpoints.



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.

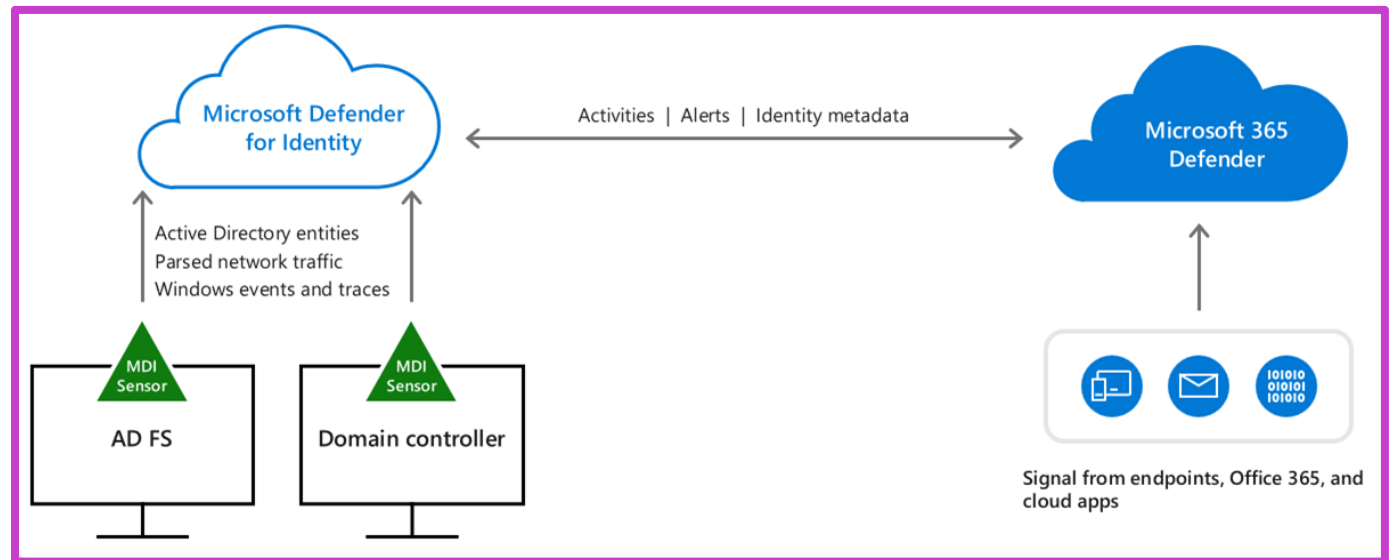
- Discover SaaS applications
- Information protection
- SaaS Security Posture Management (SSPM)
- Advanced threat protection
- App-to-app protection with app governance



Microsoft Defender for Identity

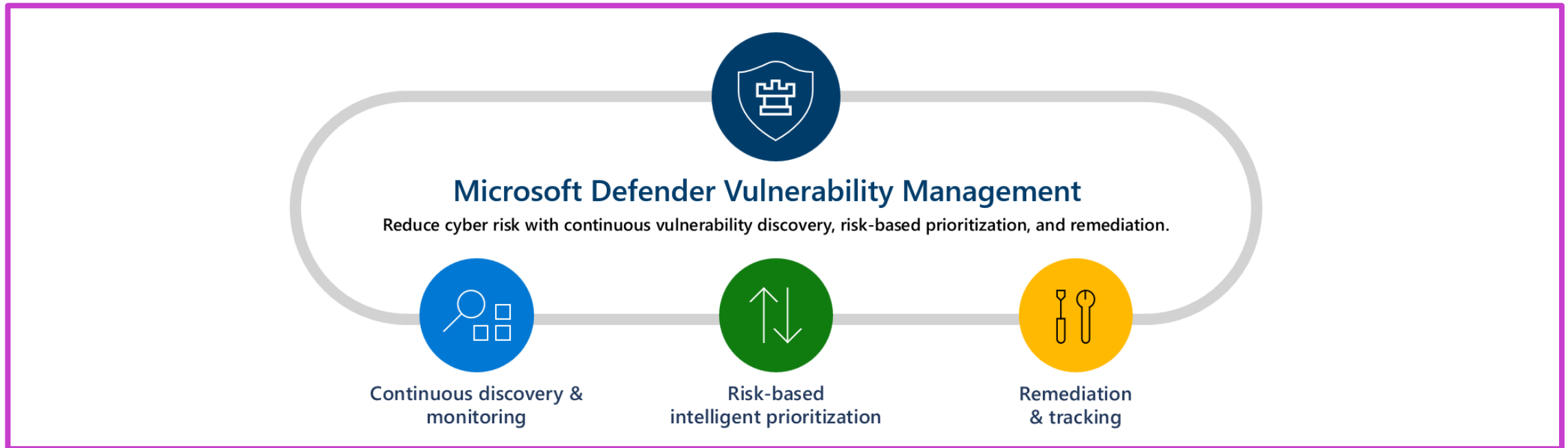
A cloud-based security solution that uses your on-premises Active Directory data to identify, detect, and investigate advanced threats, compromised identities, and malicious insider actions.

- Monitor and analyze user behavior and activities.
- Protect user identities and credentials stored in Active Directory.
- Identify suspicious activities and advanced attacks.
- Investigate alerts and user activities.



Microsoft Defender Vulnerability Management

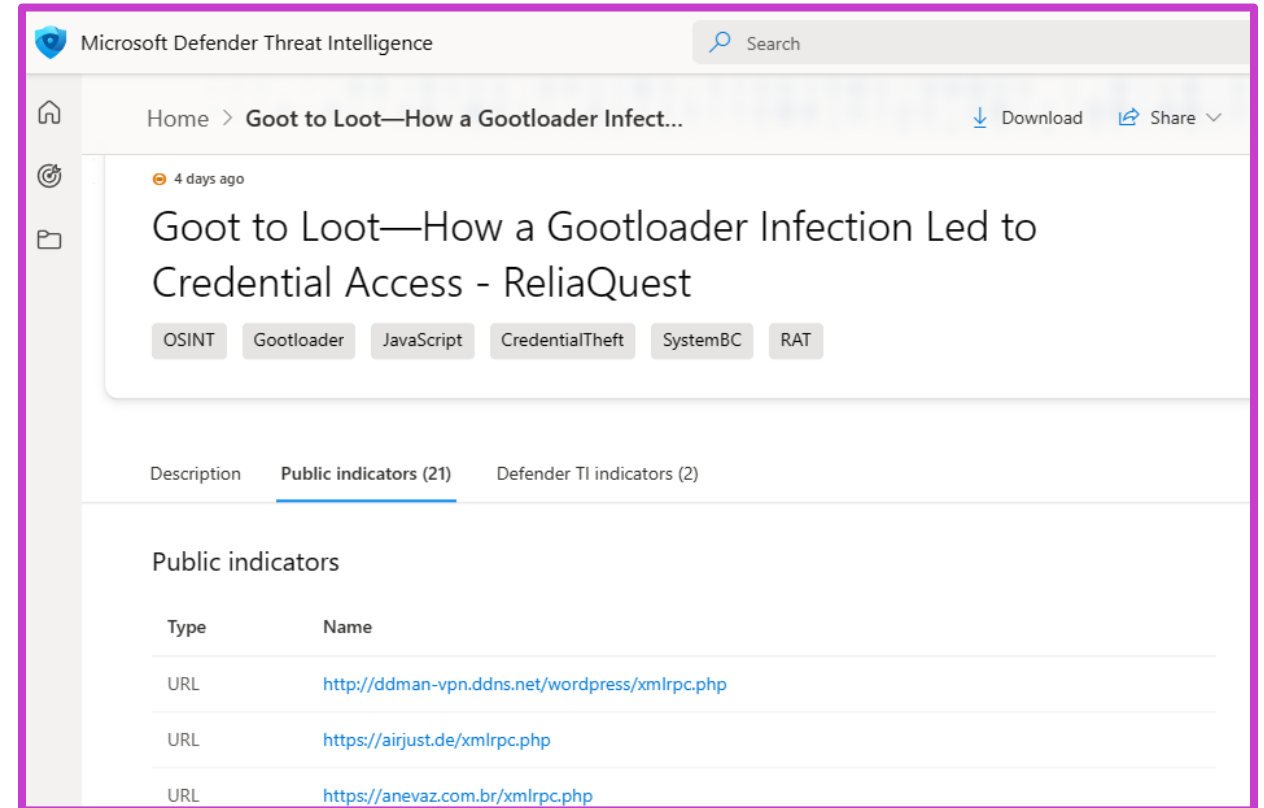
Delivers asset visibility, intelligent assessments, and built-in remediation tools for Windows, macOS, Linux, Android, iOS, and network devices.



Microsoft Defender Threat Intelligence

Helps streamline security analyst triage, incident response, threat hunting, and vulnerability management workflows.

- Quickly scan new featured articles.
- Defender TI articles provide insight into threat actors, tooling, attacks, and vulnerabilities.
- Vulnerability Articles provide key context behind CVEs of interest.
- Collects, analyzes, and indexes internet data to assist in detecting and responding to threats.

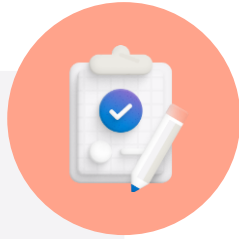


Microsoft Defender portal

Combines protection, detection, investigation, and response to devices, identities, endpoints, email and collaboration, and cloud apps, in a central place.



Learning Path Summary



Describe the capabilities of Microsoft security solutions.

In this learning path, you have:

- 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



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.

