

# SC-900

## Learning Path: 3

### Describe the Capabilities of Microsoft Security Solutions



# Learning Path Agenda



Describe basic security capabilities in Azure.



Describe security management capabilities of Azure.



Describe security capabilities of Microsoft Sentinel.



Describe threat protection with Microsoft 365 Defender.

# Module 1: Describe basic security capabilities in Azure



# Module 1 Introduction

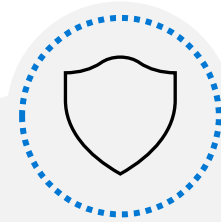
After completing this module, you should be able to:



**Describe  
Azure security  
capabilities  
for protecting  
your network.**



**Describe  
how Azure can  
protect your VMs.**



**Describe  
how encryption  
on Azure can  
protect your data.**

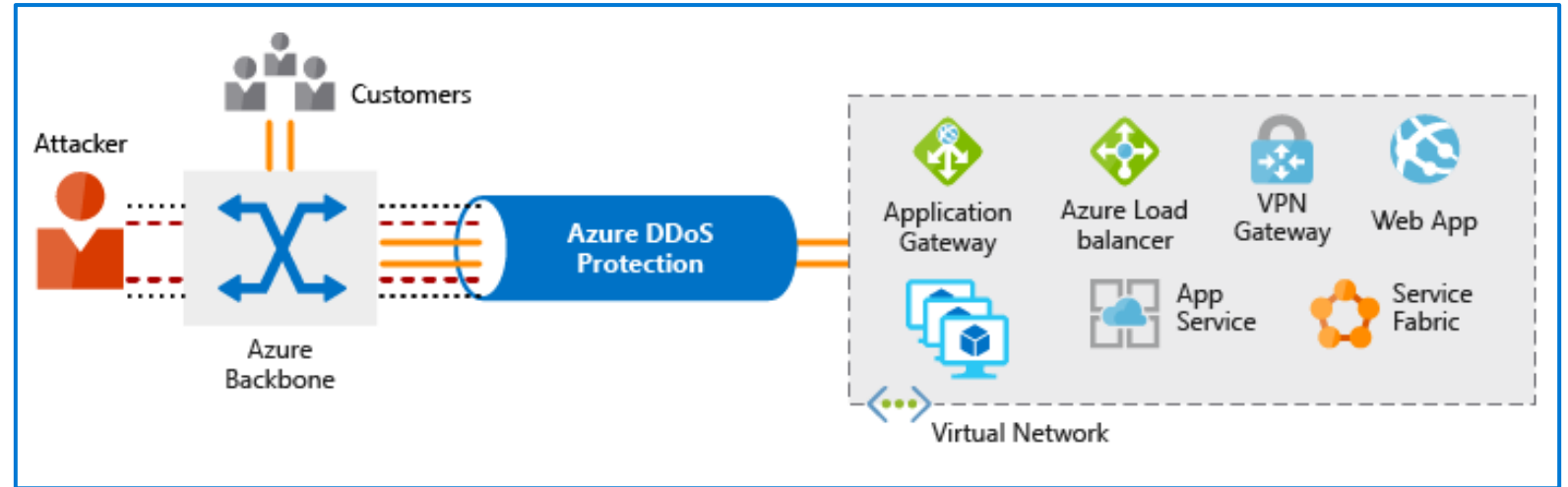
# Azure DDoS protection

A Distributed Denial of Service (DDoS) attack makes resources unresponsive.

Azure DDoS Protection analyzes network traffic and discards anything that looks like a DDoS attack.

Azure DDoS Protection tiers:

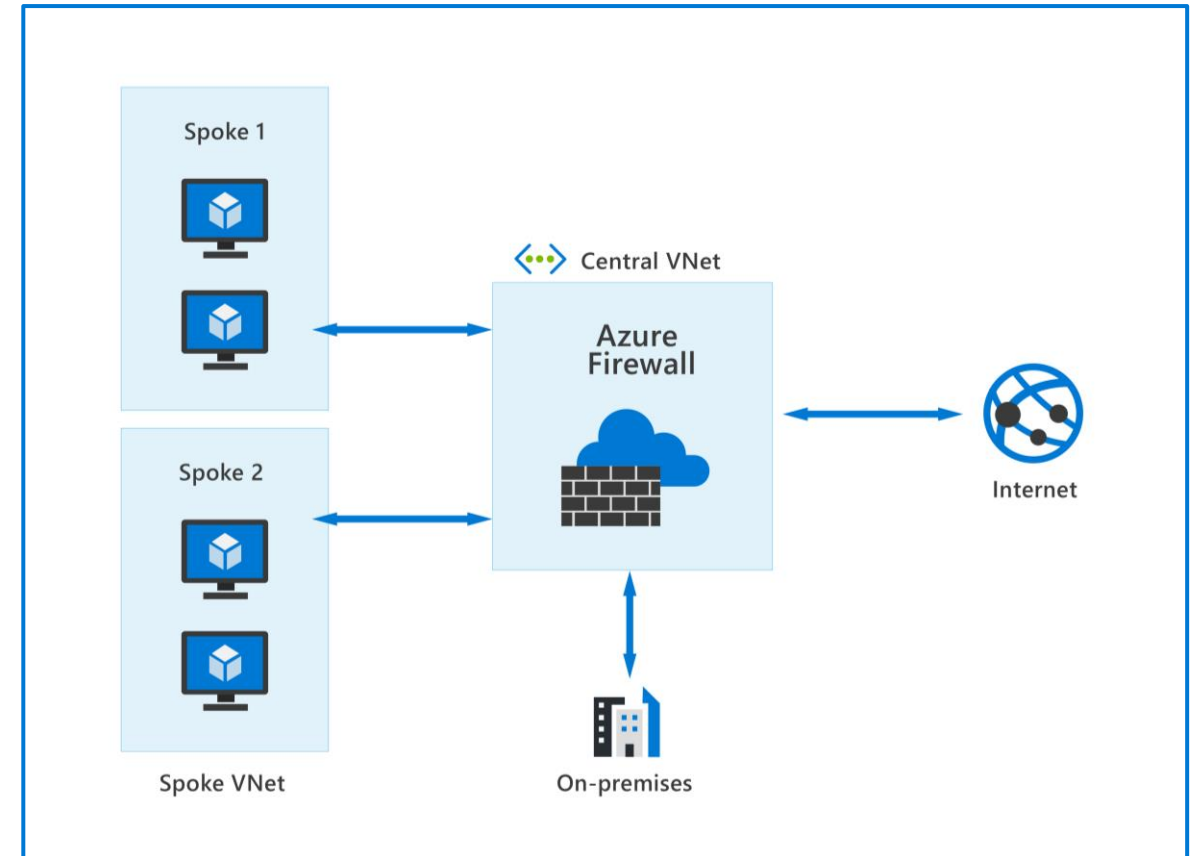
- Default DDoS infrastructure protection (free)
- DDoS Protection Standard (available SKU)



# Azure Firewall

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

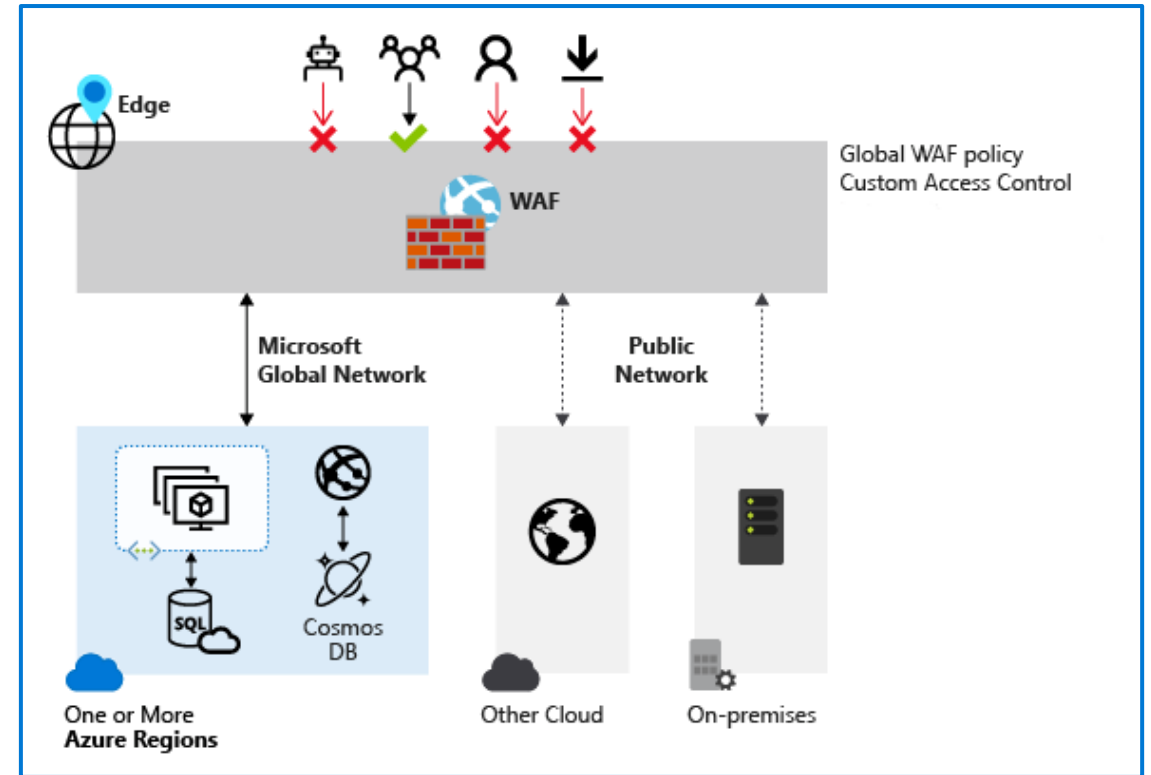
- Built-in high availability & Availability Zones
- Outbound SNAT & inbound DNAT
- Threat intelligence
- Network & application-level filtering
- Multiple public IP addresses
- Integration with Azure Monitor



# Web Application Firewall

Web Application Firewall (WAF) provides centralized protection of your web applications from common exploits and vulnerabilities.

- Simpler security management
- Improves the response time to a security threat
- Patching a known vulnerability in one place
- Protection against threats and intrusions.



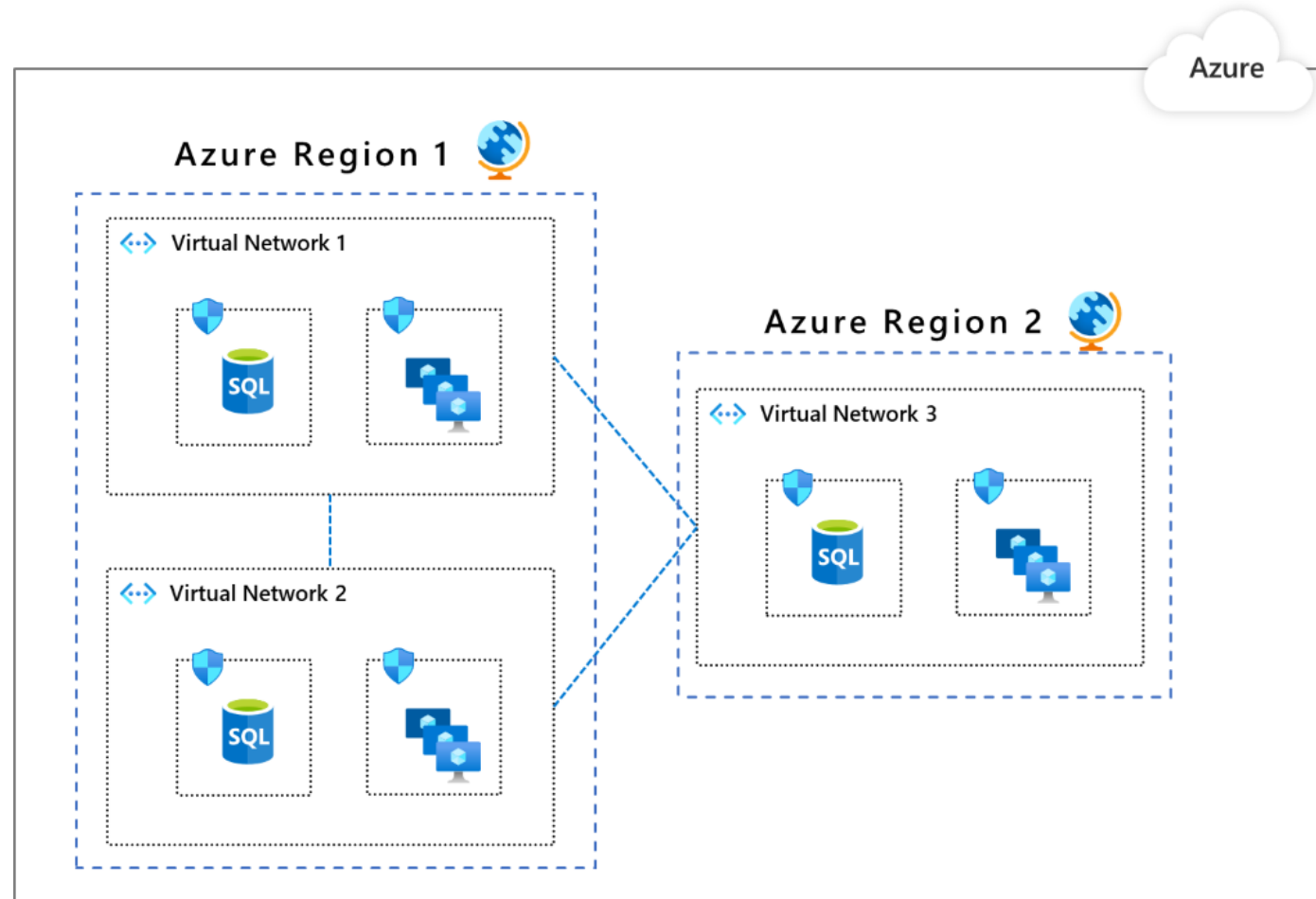
# Network segmentation and Azure VNet

## 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.



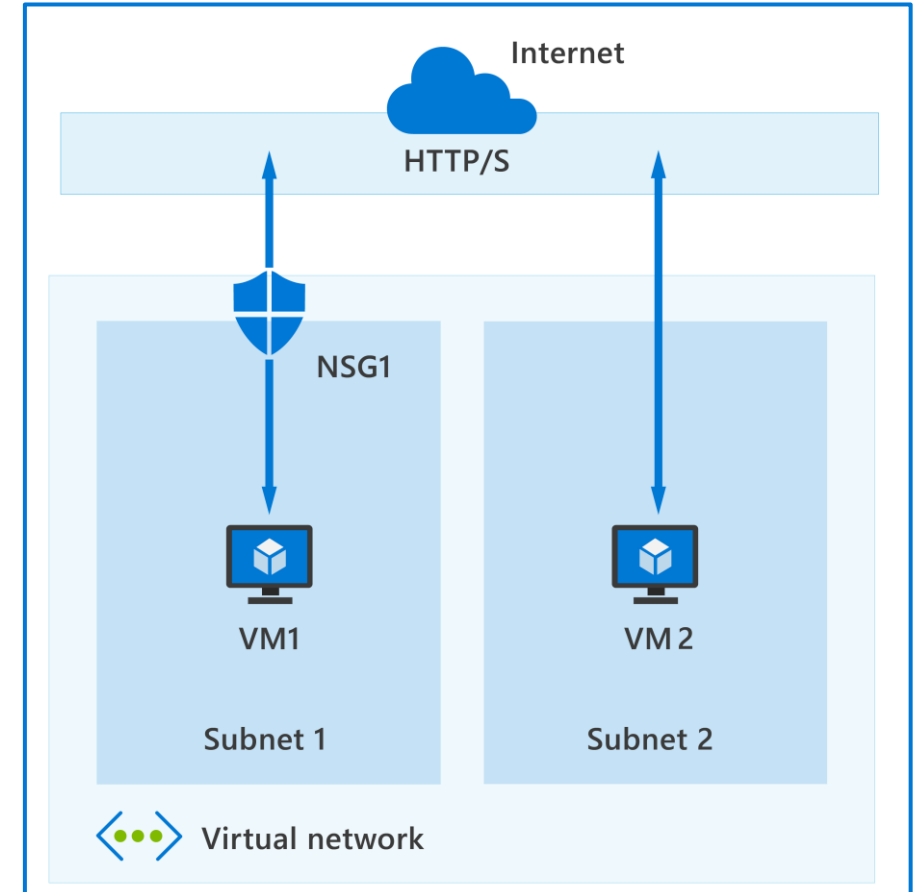


# Azure Network Security groups

Network security groups (NSG) let you allow or deny network traffic to and from Azure resources that exist in your Azure Virtual Network.

- An NSG can be associated with multiple subnets or network interfaces in a VNet.
- An NSG is made up of inbound and outbound security rules.
- Each rule specifies one or more of the following properties:
  - Name
  - Priority
  - Source or destination
  - Protocol
  - Direction
  - Port range
  - Action
- Example default inbound rule labeled "DenyAllInbound"

Priority	Source	Source ports	Destination	Destination ports	Protocol	Access
6500	0.0.0.0/0	0-65535	0.0.0.0/0	0-65535	Any	Any



# Demo

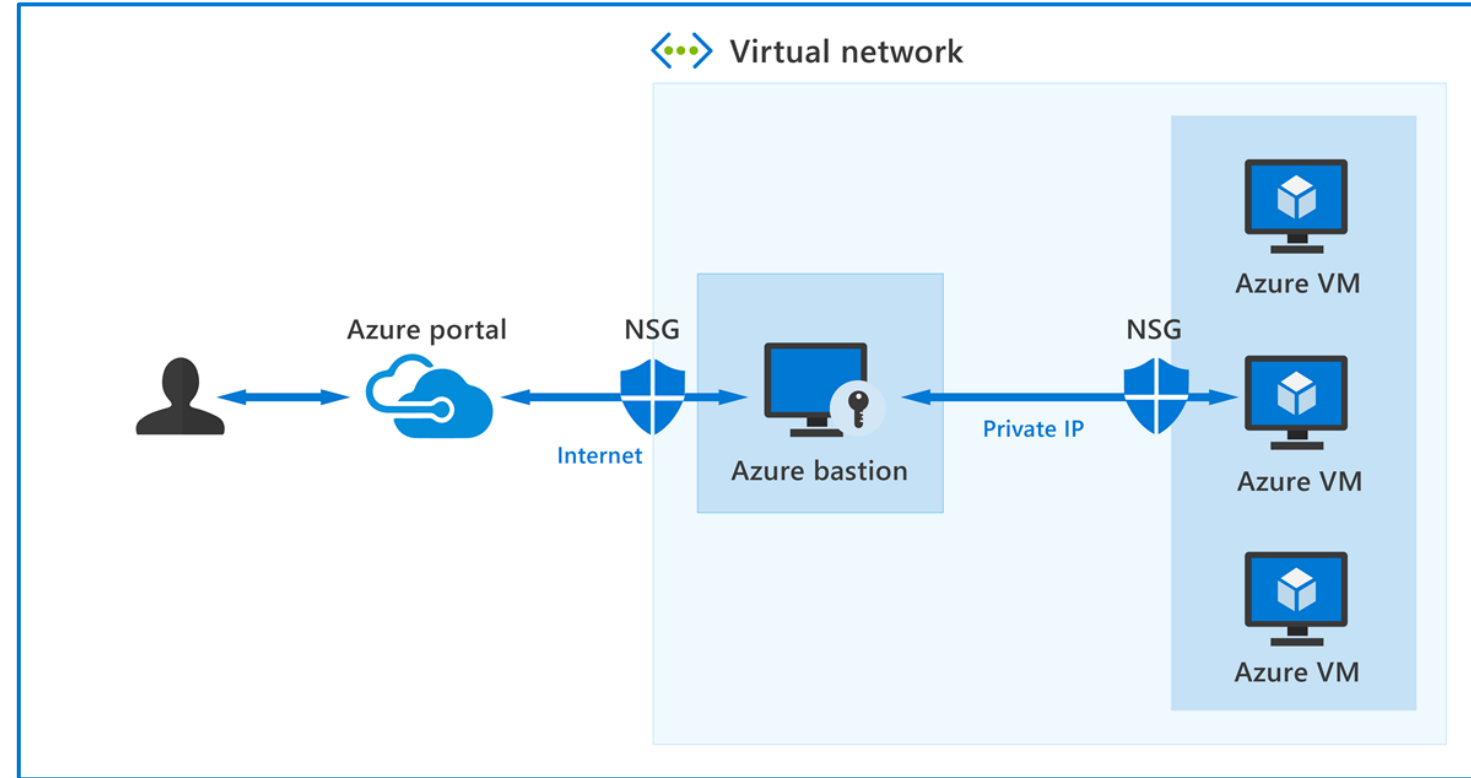
## Azure Network Security Groups



# Secure remote access to VMs: Azure Bastion & Just-in-time access

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

Just-in-time access – secure access when needed.



# Ways Azure encrypts data & use of Key Vault

## Encryption on Azure



Azure Storage Service Encryption

---



Azure Disk Encryption

---



Transparent data encryption (TDE)

## What is Azure Key Vault?



Secrets management

---



Key management

---



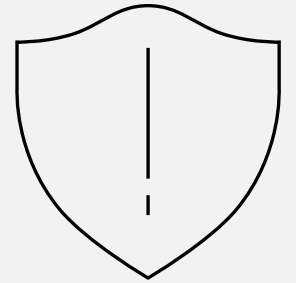
Certificate management

---



Store secrets backed by HW or SW

# Module 2: Describe security management capabilities of Azure

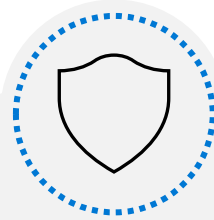


# Module 2 Introduction

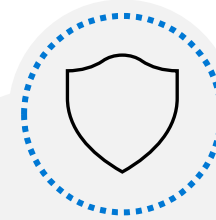
After completing this module, you'll be able to:



Describe cloud security posture management.

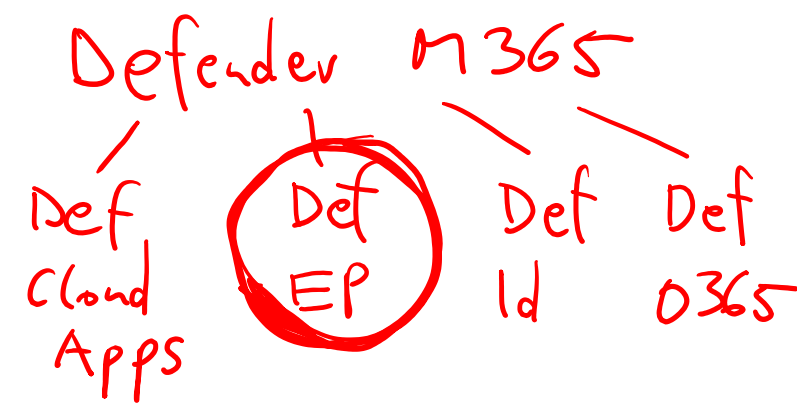


Describe Microsoft Defender for Cloud.



Understand the Microsoft Cloud Security Benchmark and security baselines in Azure.

Defender Cloud  
Azure



# Microsoft Defender for Cloud

**Microsoft Defender for Cloud** is a tool for security posture management and threat protection. It strengthens the security posture of your cloud resources, and with its integrated Microsoft Defender plans, protects workloads running in Azure, hybrid, and other cloud platforms. Microsoft Defender for Cloud features cover two broad pillars of cloud security:



## Cloud security posture management(CSPM):

Free

- Tools & services designed to improve cloud security management.
- Monitor and prioritize security enhancements and features in your cloud environment.
- Secure score in Microsoft Defender for Cloud provides visibility to your current security situation & hardening guidance to help improve security.

Azure Policies → 42%  
Azure Monitor



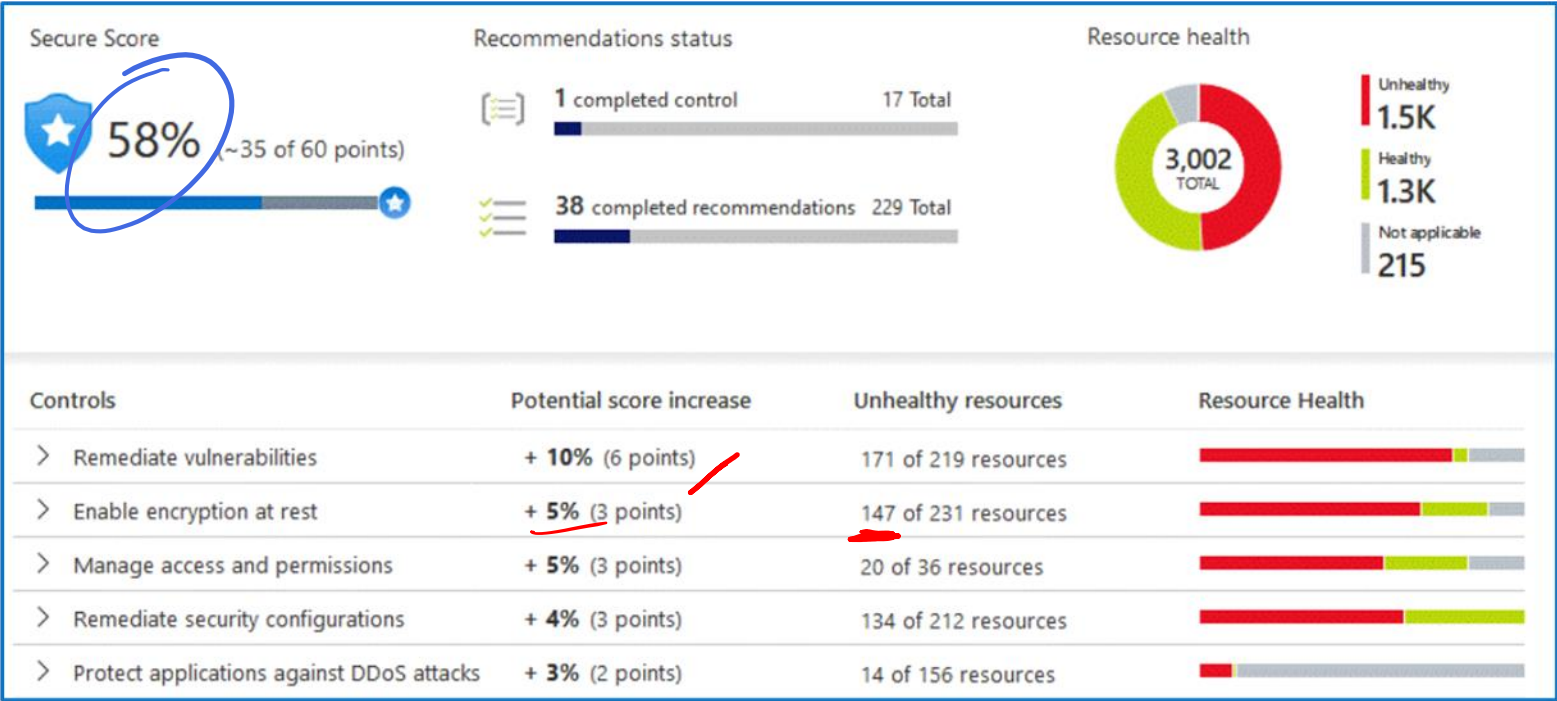
## Cloud workload protection (CWP):

- Detect and resolve threats to resources, workloads, and services.
- CWP provided through **Microsoft Defender plans** specific to the types of resources in your subscriptions.
- Defender plans include Microsoft Defender for servers, App Service, SQL, Key Vault, and more...

# Secure score in Microsoft Defender for Cloud

## Your security posture at-a-glance

- Continually assesses your resources, subscriptions, and organization for security issue.
- Aggregates all the findings into a single score.
- Hardening recommendations on any identified security misconfigurations & weaknesses.






# Enhanced security of Microsoft Defender for Cloud

Microsoft Defender for Cloud plans offer Enhanced security features for your workloads:

- Endpoint detection and response
- Vulnerability scanning
- Multi-cloud security **ARC**
- 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
✓ <u>Secure score</u>	✓ 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

# Demo

## Microsoft Defender for Cloud



# Microsoft Cloud Security Benchmark & Azure Security baselines

SOC

## Microsoft Cloud Security Benchmark (MCSB)

- Provides prescriptive best practices & recommendations to improve the security of workloads, data, and services on Azure.

## Security baselines for Azure

- Apply guidance from the MCSB to the specific service for which it is defined.
- The image is an excerpt from the Azure Key Vault security baseline.

The screenshot displays the MCSB interface for Azure Key Vault. It includes a table for feature support and a list of available policies in Microsoft Defender for Cloud (MDC).

Control ID	Control Description
DP-6: Use a secure key management process	

Feature Name	Feature Description	Feature Configuration Guidance
Key Management in Azure Key Vault	Description: The service supports Azure Key Vault integration for any customer keys, secrets, or certificates. <a href="#">Learn more.</a>	Configuration Guidance: Follow the Azure Key Vault best practices to securely manage your key lifecycle in key vault. This includes the key generation, distribution, storage, rotation, and revocation. Reference: <a href="#">Azure Key Vault key management</a>

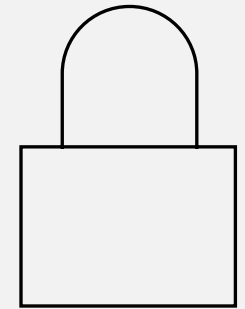
  

Supported	Enabled By Default	Configuration Responsibility
True	False	Customer

Name (Azure portal)	Description	Effect(s)	Version (GitHub)
<a href="#">Key Vault keys should have an expiration date</a>	Cryptographic keys should have a defined expiration date and not be permanent. Keys that are valid forever provide a potential attacker with more time to compromise the key. It is a recommended security practice to set expiration dates on cryptographic keys.	Audit, Deny, Disabled	1.0.2 <a href="#">u</a>
<a href="#">Key Vault secrets should have an expiration date</a>	Secrets should have a defined expiration date and not be permanent. Secrets that are valid forever provide a potential attacker with more time to compromise them. It is a recommended security practice to set expiration dates on secrets.	Audit, Deny, Disabled	1.0.2 <a href="#">u</a>

# Module 3: Describe security capabilities of Microsoft Sentinel



# Module 3 Introduction

After completing this module, you'll be able to:



**Describe  
the security  
concepts for  
SIEM and SOAR.**



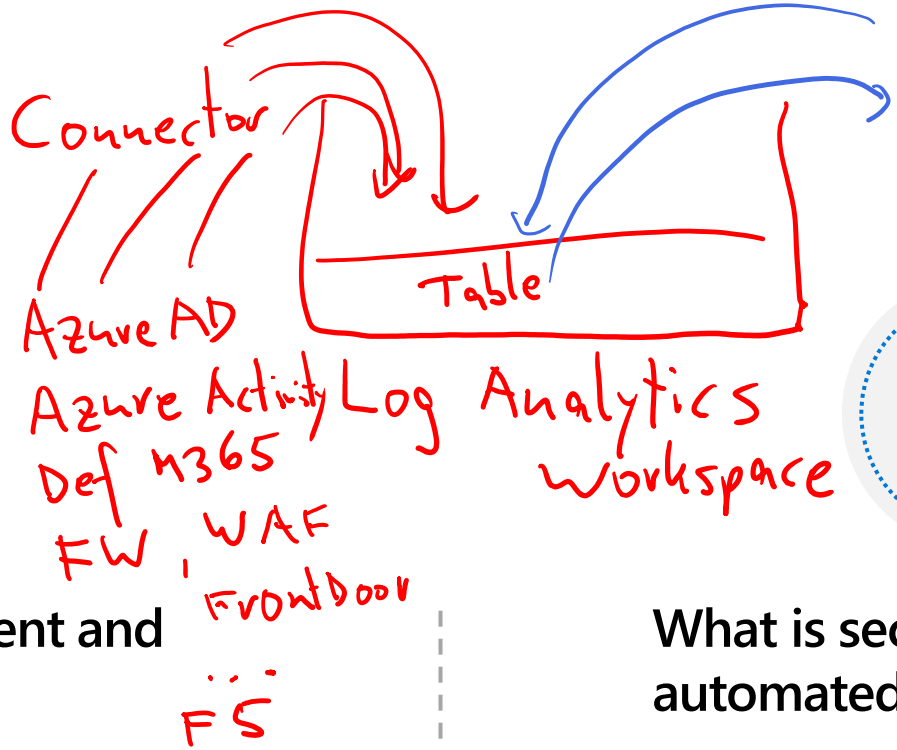
**Describe  
how Microsoft  
Sentinel provides  
integrated threat  
management.**

# SIEM and SOAR



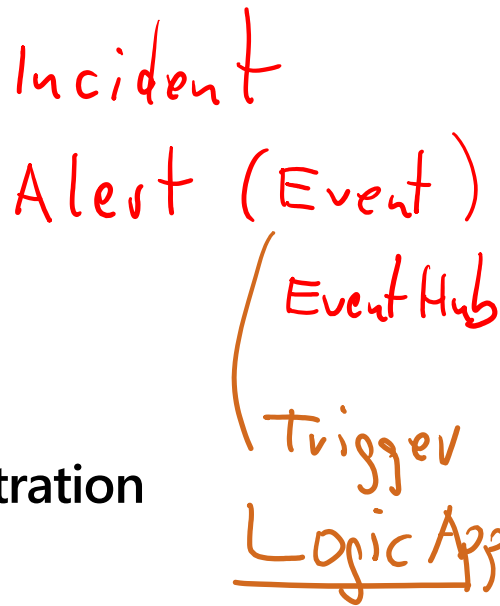
## What is security incident and event management?

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?

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.



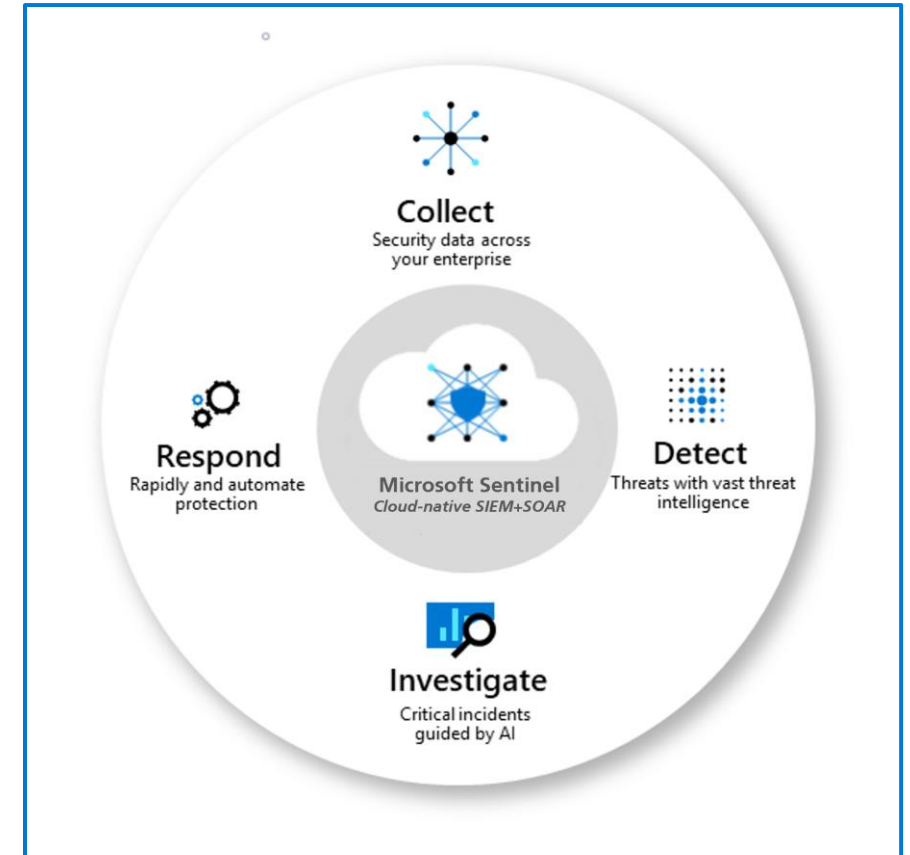
# Microsoft Sentinel provides integrated threat management (Slide 1)

**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 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 provides integrated threat management (Slide 2)



**Connect Microsoft Sentinel to your data:** Use connectors for Microsoft solutions providing real-time integration.



**Workbooks:** Monitor the data using the Microsoft Sentinel integration with Azure Monitor Workbooks.



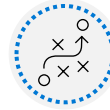
**Analytics:** Using built-in analytics alerts, you'll get notified when anything suspicious occurs.



**Manage incidents:** An incident is created when an alert that you've enabled is triggered.



**Security automation and orchestration:** Integrate with Logic Apps, to create workflows & playbooks.



**Notebooks:** Use Jupyter notebooks to extend the scope of what you can do with Microsoft Sentinel data.



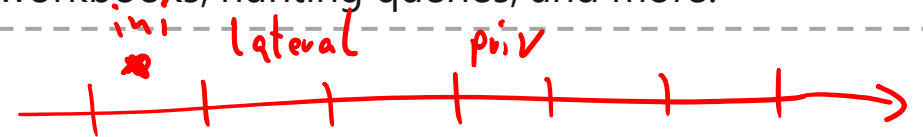
**Investigation:** Understand the scope of a potential security threat and find the root cause.



**Hunting:** Use search-and-query tools, to hunt proactively for threats, before an alert is triggered.



**Community:** Download content from the private community GitHub repository to create custom workbooks, hunting queries, and more.



MITRE cyber kill chain

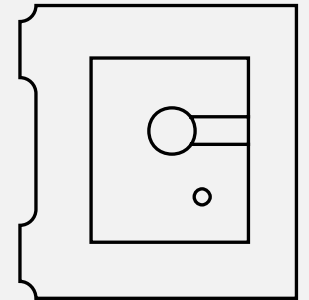


# Demo

## Microsoft Sentinel



# Module 4: Describe threat protection with Microsoft 365 Defender

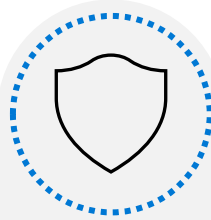


# Module 4 Introduction

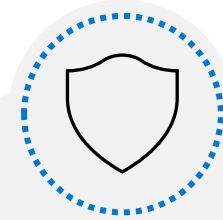
After completing this module, you'll be able to:



**Describe  
the Microsoft  
365 Defender  
service.**



**Describe  
how Microsoft 365  
Defender provides  
integrated  
protection against  
sophisticated  
attacks.**



**Describe and  
explore the  
Microsoft 365  
Defender portal.**

# Microsoft 365 Defender services

## Microsoft 365 Defender



Natively coordinate the detection, prevention, investigation, and response to threats.



Protects identities, endpoints, apps, and email & collaboration.

## Integrated Microsoft 365 Defender experience



### Identity

Microsoft Defender  
for Identity

+



### Endpoints

Microsoft Defender  
for Endpoints

+



### Apps

Microsoft Defender  
for Cloud Apps

+



### Email/Collaboration

Microsoft Defender  
for Office 365

# Microsoft Defender for Office 365

## Microsoft Defender for Office 365 covers:

1

Threat protection  
policies

2

Reports

3

Threat investigation and  
response capabilities

4

Automated investigation  
and response capabilities

### Microsoft Defender for Office 365 Plan 1

- Safe Attachments
- Safe Links
- Safe Attachments for SharePoint, OneDrive, & Microsoft Teams
- Anti-phishing protection
- Real-time detections

### Microsoft Defender for Office 365 Plan 2

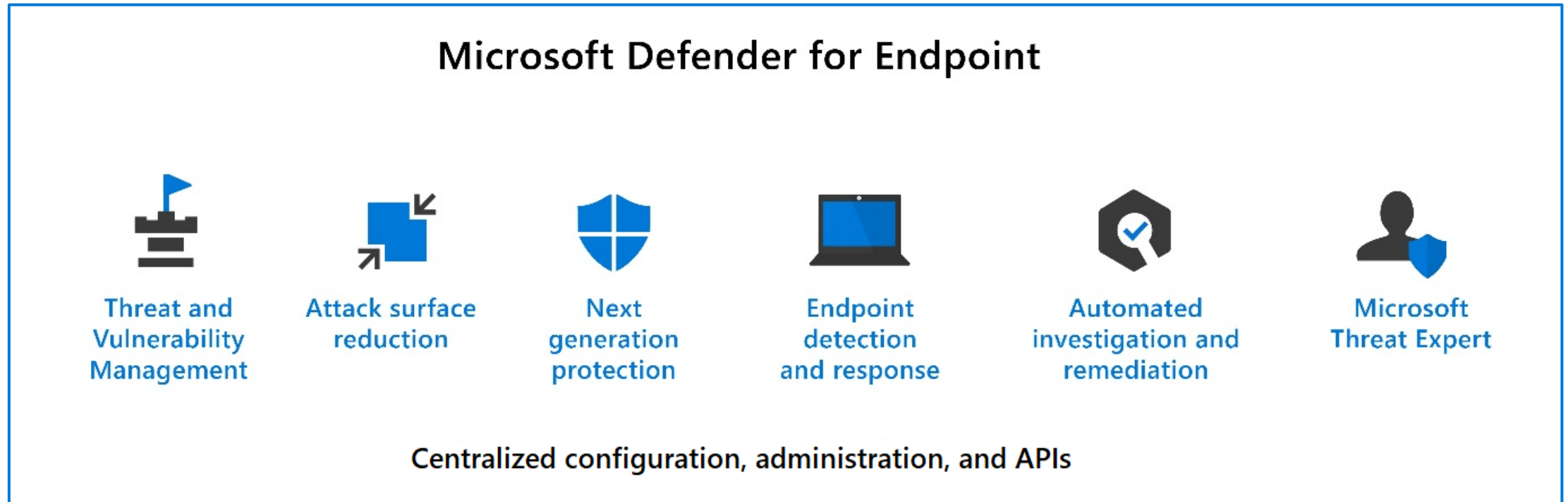
- Threat Trackers & Threat Explorer
- Automated investigation & response (AIR)
- Attack Simulator
- Proactively hunt for threats
- Investigate incidents and alerts

### Microsoft Defender for Office 365 availability

- Microsoft 365 E5
- Office 365 E5
- Office 365 A5
- Microsoft 365 Business Premium

# Microsoft Defender for Endpoint

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



# Microsoft Defender for Cloud Apps

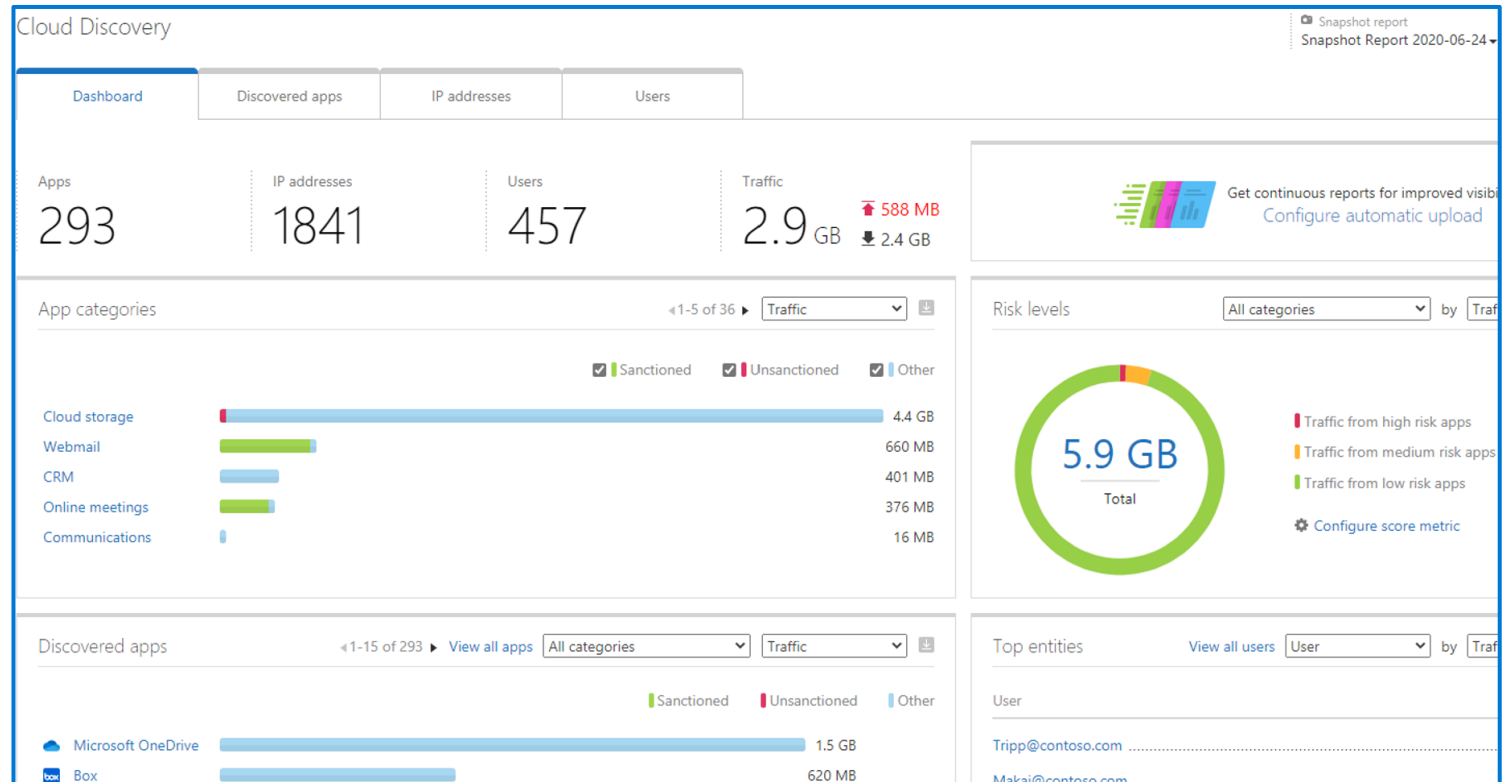
Microsoft Defender for Cloud Apps provides rich visibility to your cloud services, control over data travel, and sophisticated analytics to identify and combat cyberthreats across all your Microsoft and third-party cloud services.

## The Defender for Cloud Apps framework

- Discover and control the use of Shadow IT.
- Protect your sensitive information anywhere in the cloud.
- Protect against cyberthreats and anomalies.
- Assess your cloud apps' compliance.

## Office 365 Cloud App Security

## Enhanced Cloud App Discovery in Azure Active Directory





# Demo

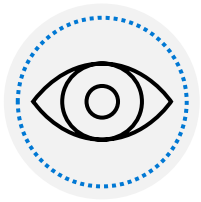
## Microsoft Defender for Cloud Apps





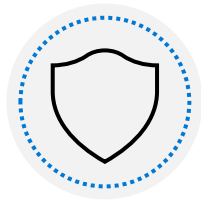
# Microsoft Defender for Identity

## Microsoft Defender for Identity covers following key areas



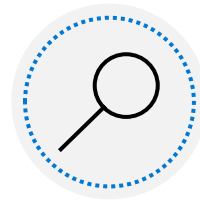
### **Monitor and profile user behavior and activities**

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.



### **Protect user identities and reduce the attack surface**

Defender for Identity gives invaluable insights on identity configurations and suggested security best practices. Through security reports and user profile analytics.



### **Identify suspicious activities and advanced attacks across the cyberattack kill-chain**

- Reconnaissance
- Compromised credentials
- Lateral movements
- Domain dominance



### **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.

# Microsoft 365 Defender portal

The Microsoft 365 Defender portal combines protection, detection, investigation, and response to email, collaboration, identity, and device threats, in a central portal.



View the security health of your organization.

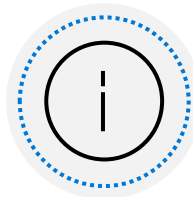


Act to configure devices, users, and apps.

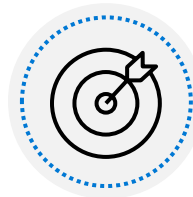


Get alerts for suspicious activity.

The Microsoft 365 Defender navigation pane include these options and more:



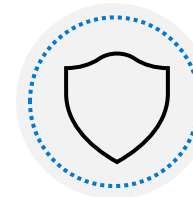
**Incidents  
& alerts**



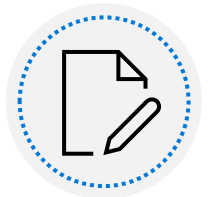
**Hunting**



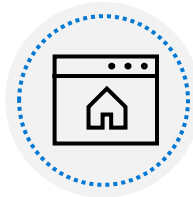
**Action  
center**



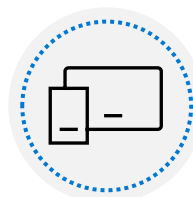
**Threat  
analytics**



**Secure  
Score**



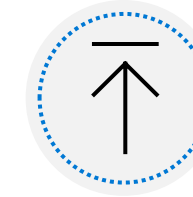
**Learning  
hub**



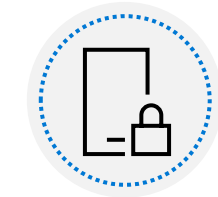
**Endpoints**



**Email &  
collaboration**



**Reports**



**Permissions  
& roles**

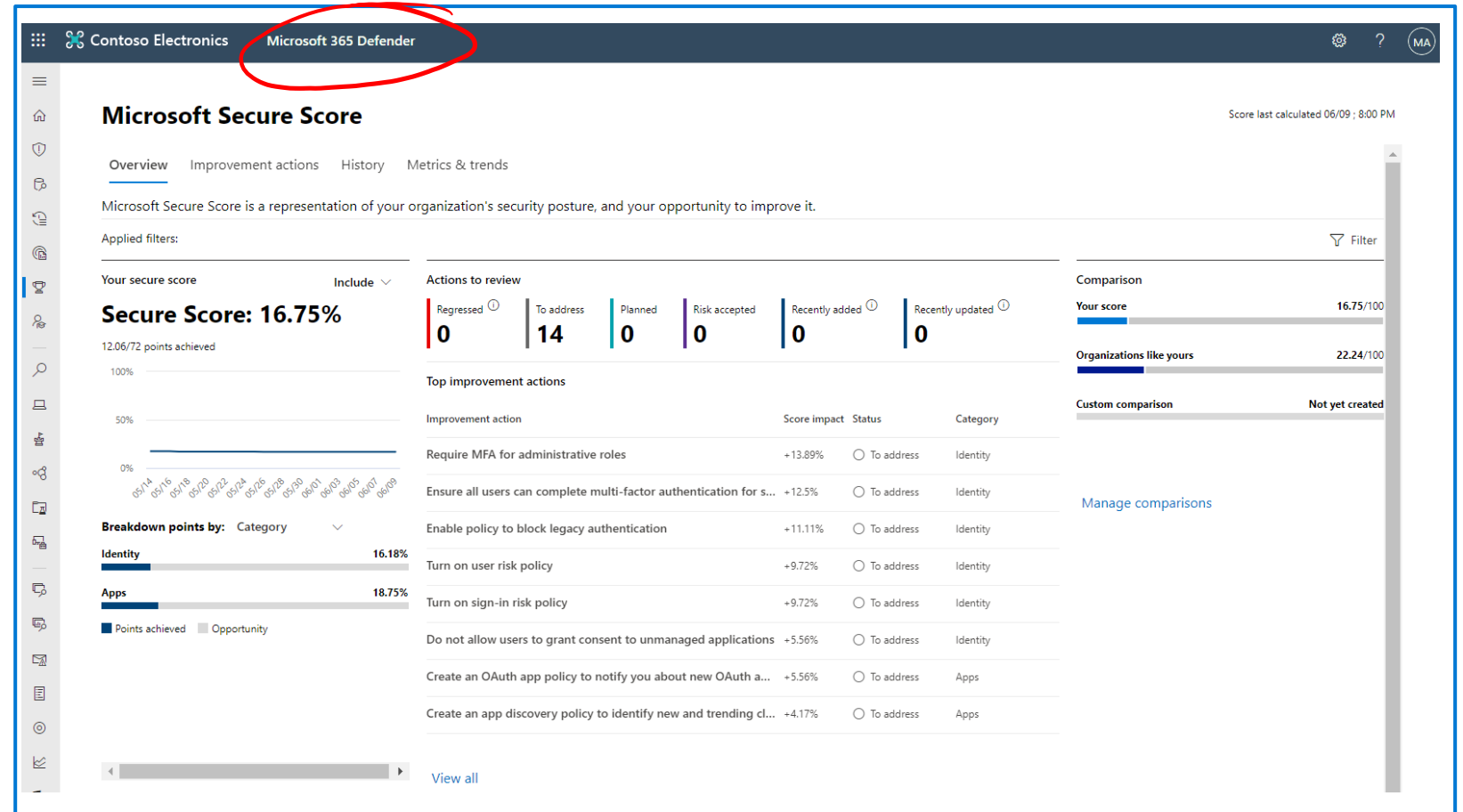
# Microsoft Secure Score

Microsoft Secure Score is a representation of a company's security posture.

Will show all possible improvements for the product, whatever the license edition, subscription, or plan.

Supports recommendations for:

- Microsoft 365
- Azure Active Directory
- Microsoft Defender for Endpoint
- Microsoft Defender for Identity
- Microsoft Defender for Cloud Apps



# Demo

## The Microsoft 365 Defender portal



# Learning Path Summary

In this learning path, you have:

- Learned about basic security capabilities 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 365 Defender.

Network

Def

SIEM

Def EP  
Def O365  
-----  
Def  
Def

