Microsoft

Microsoft Security Virtual Training Days: Security, Compliance, and Identity Fundamentals

Microsoft

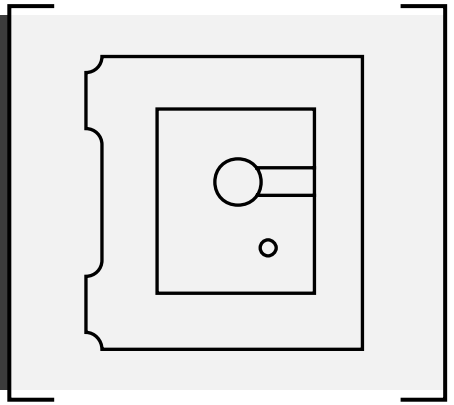
Describe the concepts of security, compliance, and identity

Module Agenda

Describe security and compliance concepts and methodologies

Describe identity concepts

Lesson 1: Describe security and compliance concepts and methodologies



Lesson 1 Introduction

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

- Describe the Zero Trust and shared responsibility models.
- Describe common security threats and ways to protect through the defense in-depth security model.
- Describe the concepts of encryption and hashing.
- Describe the cloud adoption framework.

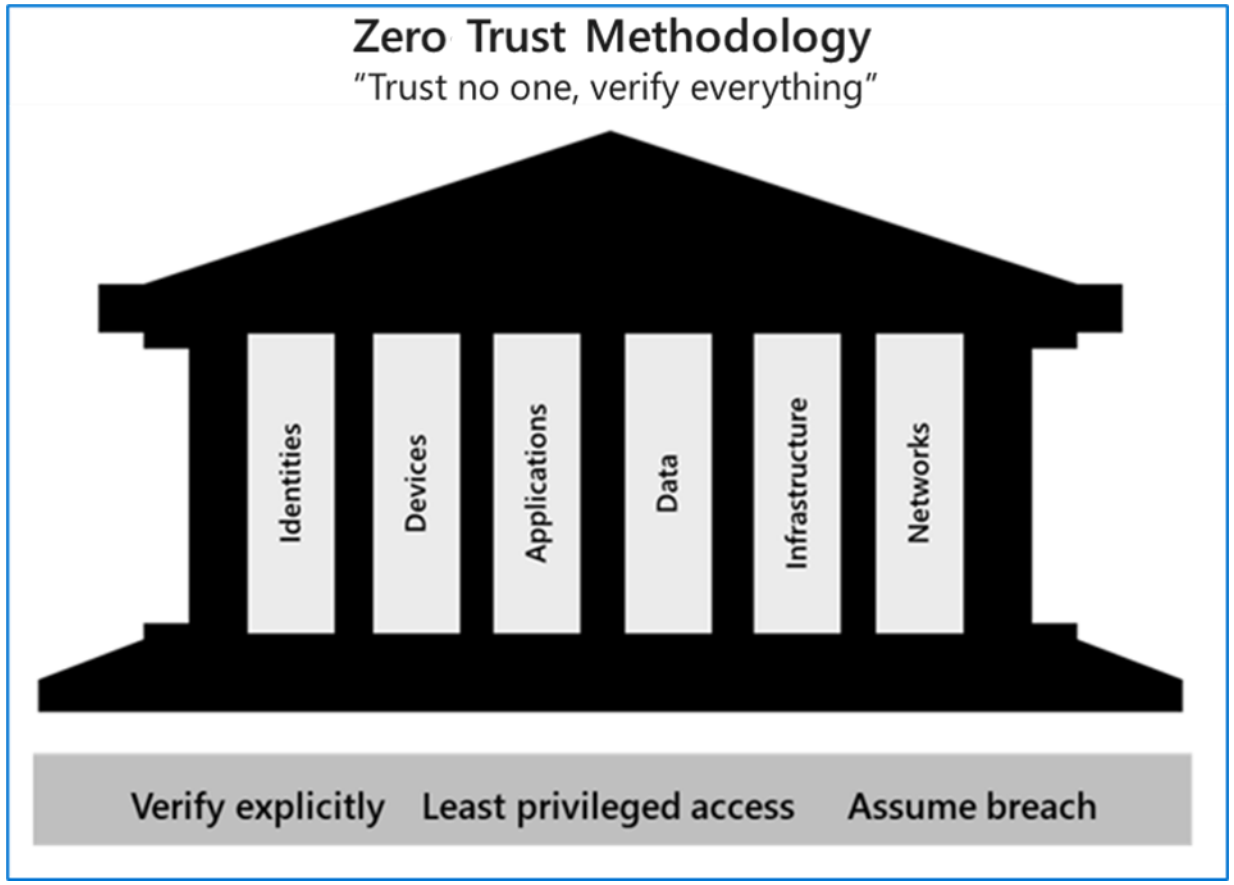
Zero-trust methodology

Zero Trust guiding principles

- Verify explicitly
- Least privileged access
- Assume breach

Six foundational pillars

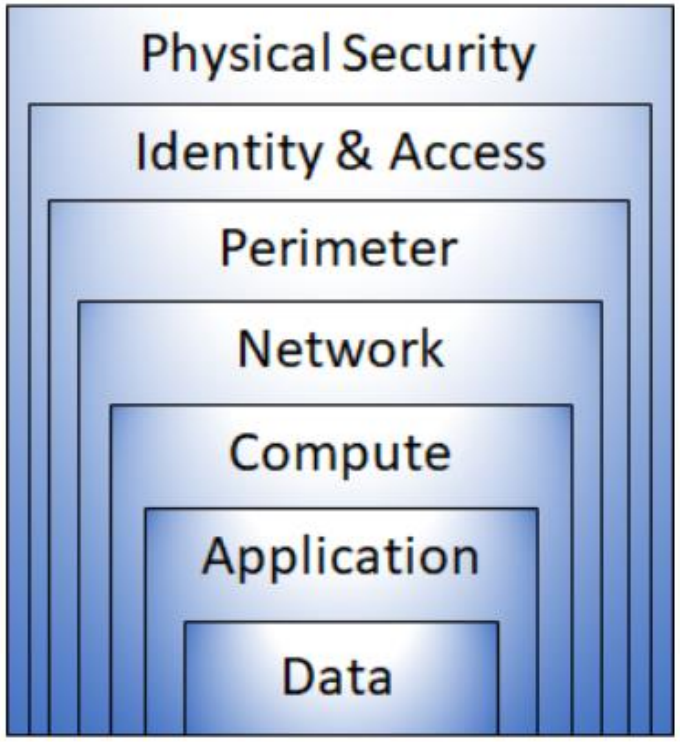
- **Identities** may be users, services, or devices.
- **Devices** create a large attack surface as data flows.
- **Applications** are the way that data is consumed.
- **Data** should be classified, labeled, and encrypted based on its attributes.
- **Infrastructure** whether on-premises or cloud based, represents a threat vector.
- **Networks** should be segmented.



Defense in depth

Defense in depth uses a layered approach to security:

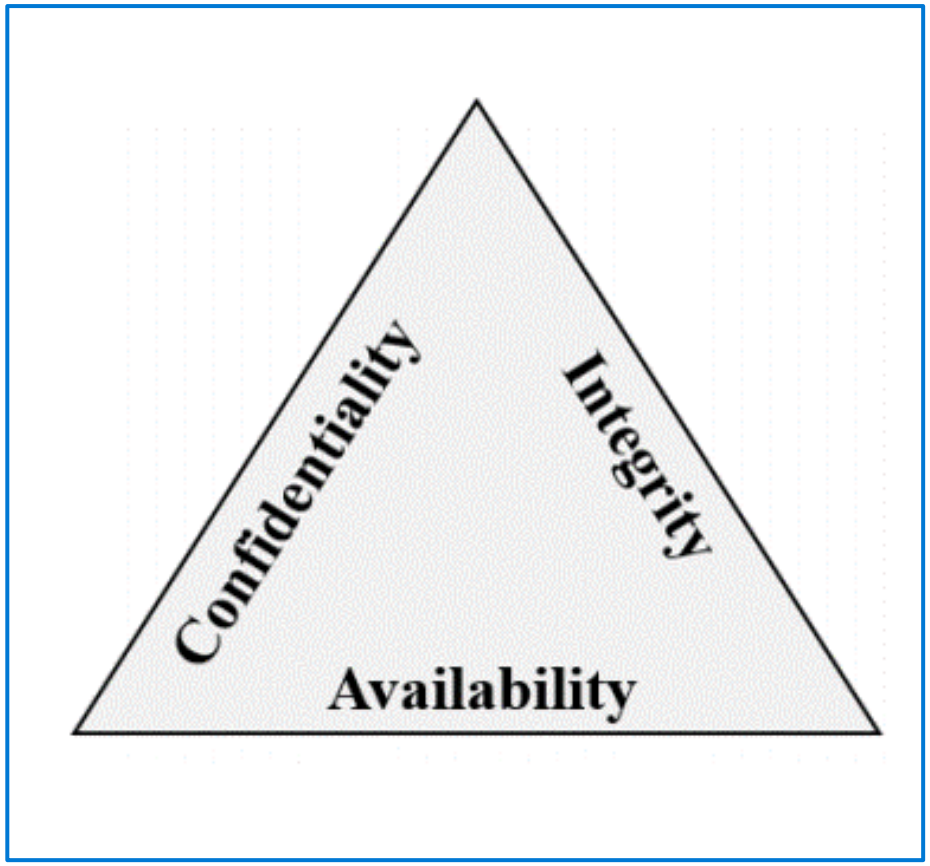
- **Physical** security such as limiting access to a datacenter to only authorized personnel.
- **Identity and access** security controlling access to infrastructure and change control.
- **Perimeter** security including distributed denial of service (DDoS) protection to filter large-scale attacks before they can cause a denial of service for users.
- **Network** security can limit communication between resources using segmentation and access controls.
- The **compute** layer can secure access to virtual machines either on-premises or in the cloud by closing certain ports.
- **Application** layer security ensures that applications are secure and free of security vulnerabilities.
- **Data** layer security controls access to business and customer data, and encryption to protect data.



Confidentiality, Integrity, Availability (CIA)

CIA - A way to think about security trade-offs.

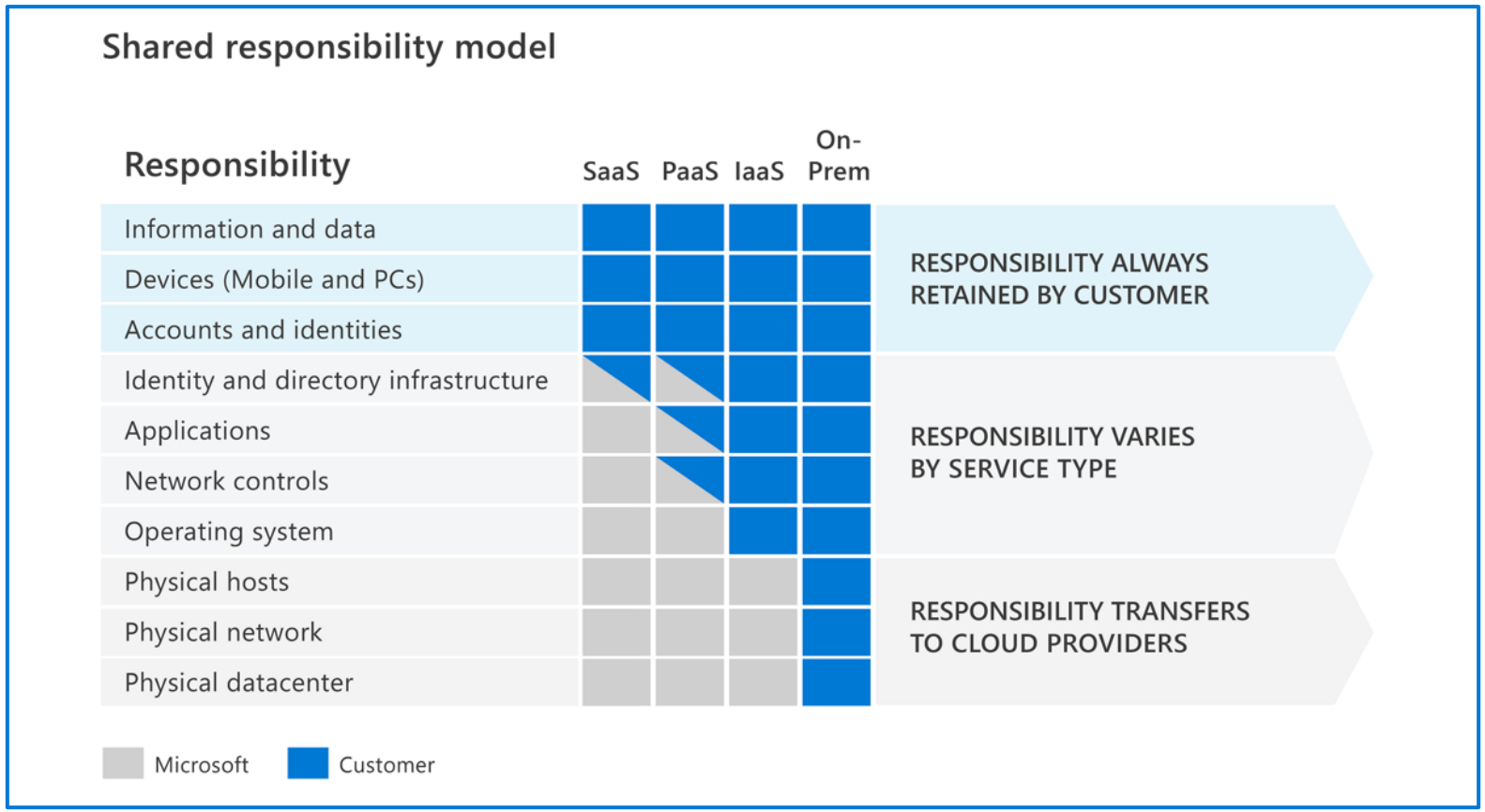
- **Confidentiality** refers to the need to keep confidential sensitive data such as customer information, passwords, or financial data.
- **Integrity** refers to keeping data or messages correct.
- **Availability** refers to making data available to those who need it.



The shared responsibility model

The responsibilities vary based on where the workload is hosted:

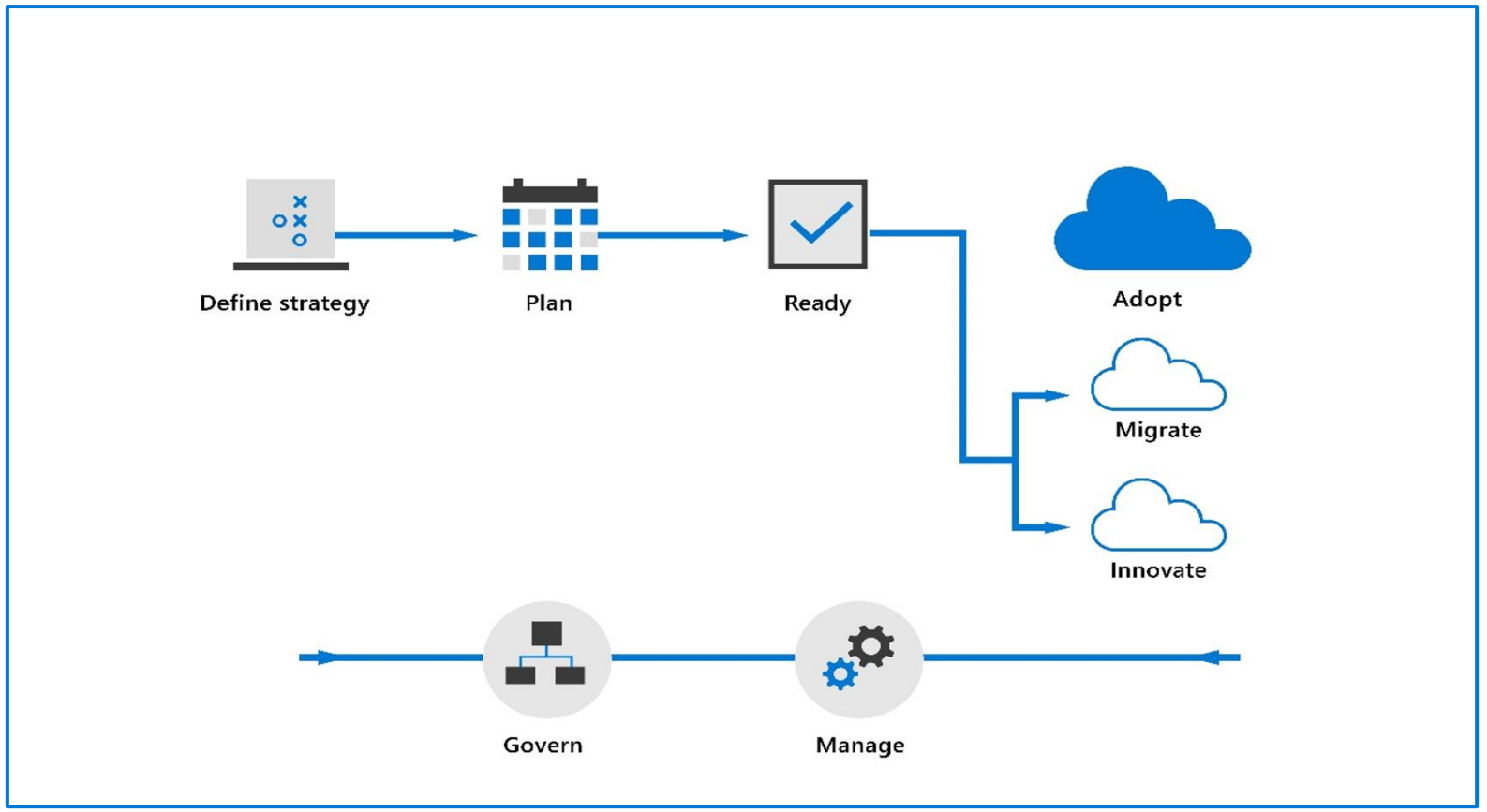
- Software as a Service (SaaS)
- Platform as a Service (PaaS)
- Infrastructure as a Service (IaaS)
- On-premises datacenter (On-prem)



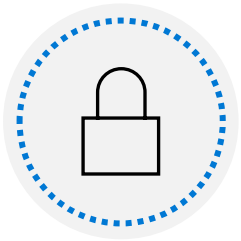
Microsoft Cloud Adoption Framework

Microsoft Cloud Adoption Framework

- Consists of documentation, implementation guidance, & best practices that support increased security and compliance
- Help businesses implement strategies necessary to succeed in the cloud.
- Lifecycle
  - Define strategy
  - Plan
  - Ready
  - Adopt (Migrate / Innovate)
  - Govern
  - Manage



Common threats



Data breach

Include:

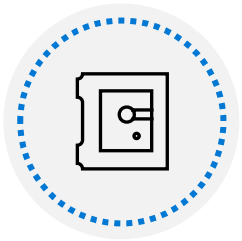
- Phishing
- Spear phishing
- Tech support scams
- SQL injection
- Malware designed to steal passwords or bank details.

Dictionary attack

It is a type of identity attack.

A hacker attempts to steal an identity by trying a large number of known passwords.

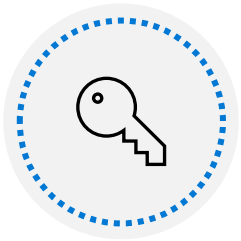
Dictionary attacks are also known as brute force attacks.



Ransomware

It is a type of malware that encrypts files and folders.

It attempts to extort money from victims.



Disruptive attacks

A Distributed Denial of Service (DDoS) attack attempts to exhaust an application's resources.

DDoS attacks can be targeted at any endpoint.

Other common threats include coin miners, rootkits, trojans, worms, and exploits and exploit kits.

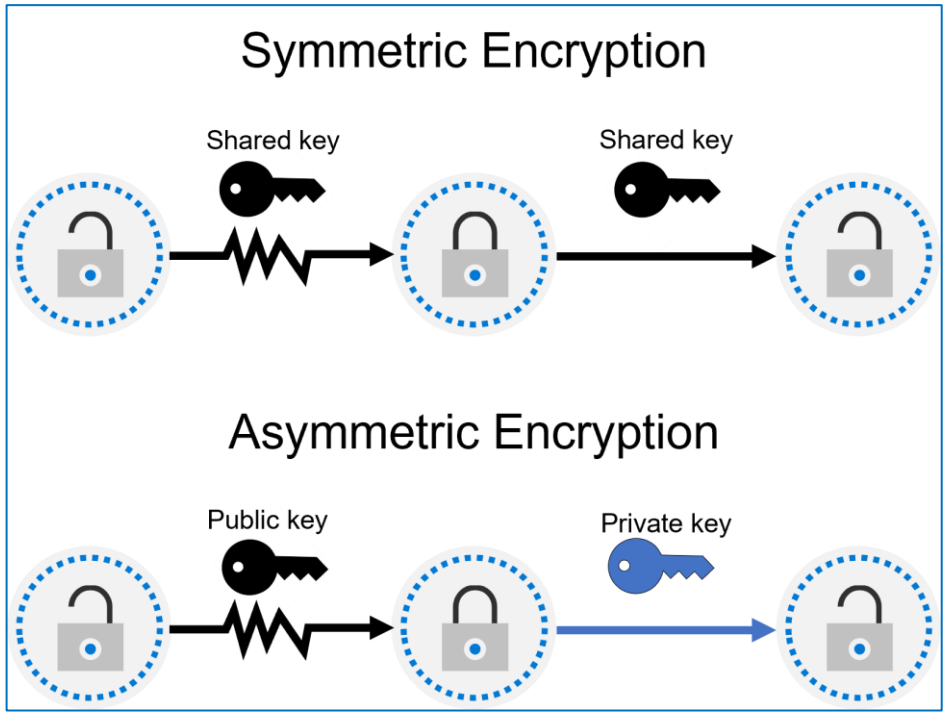
Encryption

Encryption is the process of making data unreadable and unusable to unauthorized viewers.

- Encryption of data at rest
- Encryption of data in transit

Two top-level types of encryption:

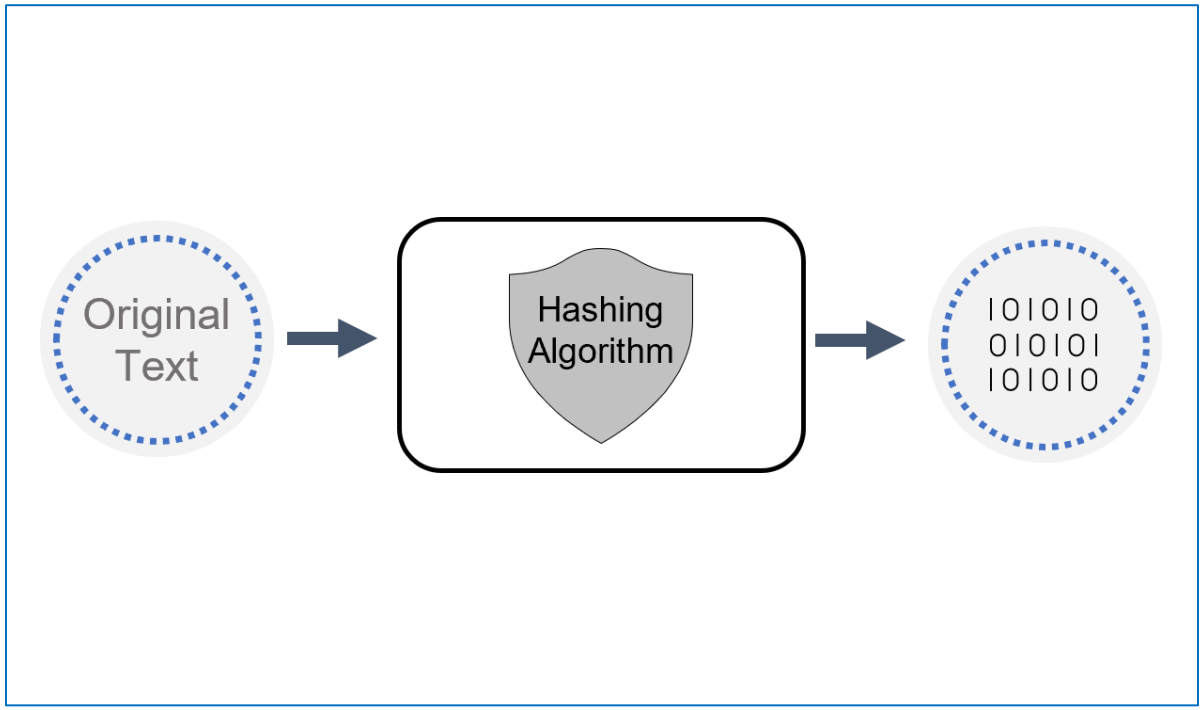
- Symmetric – uses same key to encrypt and decrypt data
- Asymmetric - uses a public key and private key pair



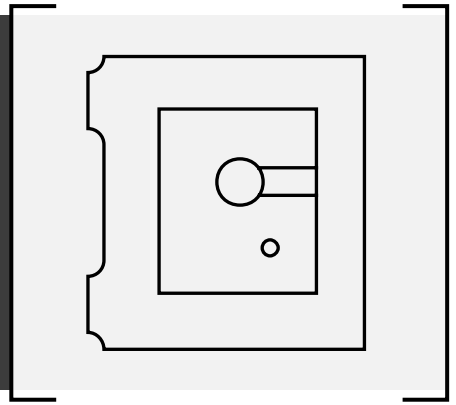
Hashing

Hashing uses an algorithm to convert the original text to a *unique* fixed-length hash value. Hash functions are:

- Deterministic, the same input produces the same output.
- A unique identifier of its associated data.
- Different to encryption in that the hashed value isn't subsequently decrypted back to the original.
- Used to store passwords. The password is "salted" to mitigate risk of brute-force dictionary attack.



Lesson 2: Describe identity concepts



Lesson 2 Introduction

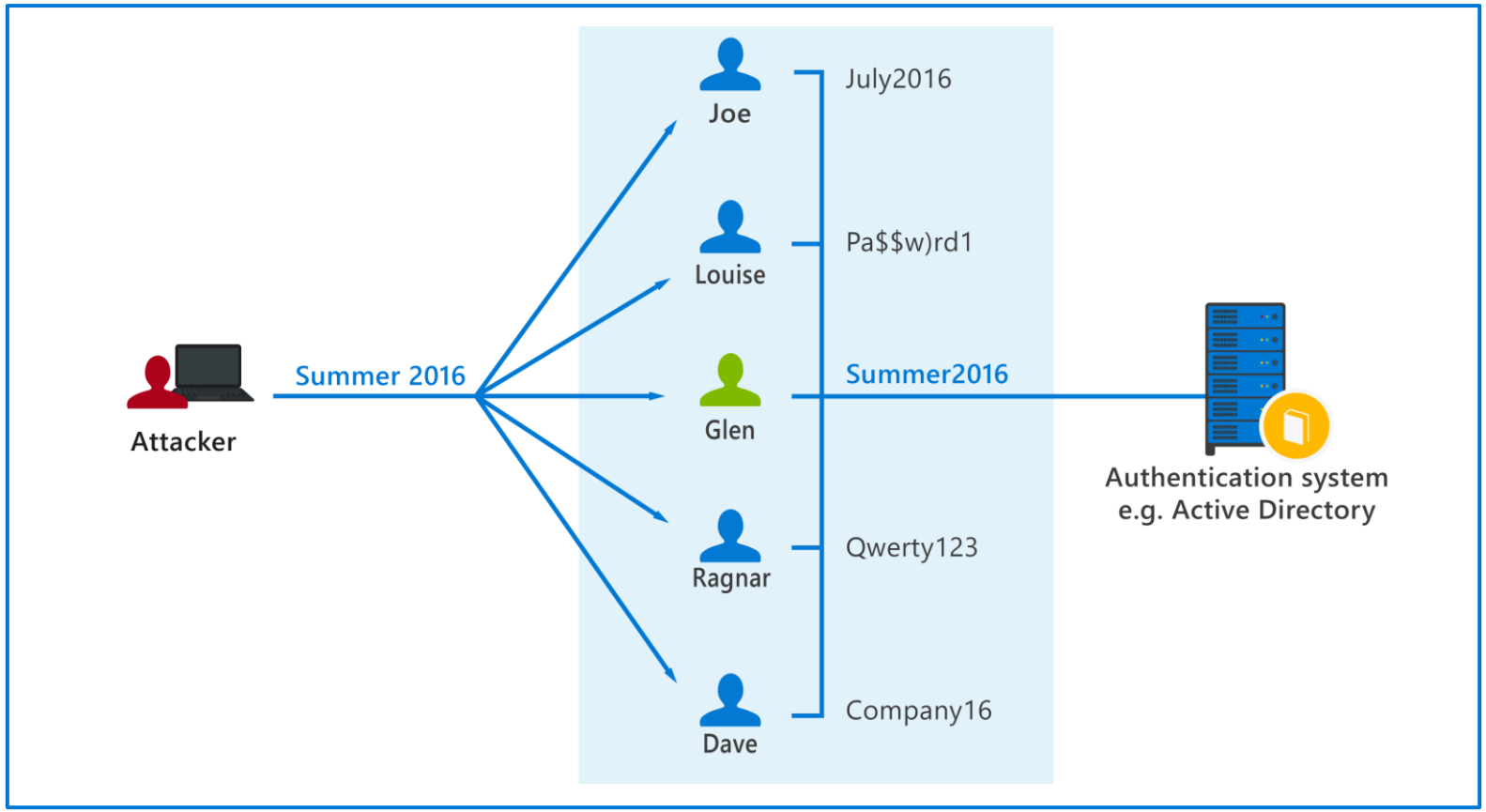
After completing this module, you'll be able to:

- Describe the concept of identity as a security perimeter
- Understand the difference between authentication and authorization
- Describe identity-related services

Common identity attacks

Types of security threats:

- Password-based attacks
- Phishing
- Spear phishing



Identity as the primary security perimeter

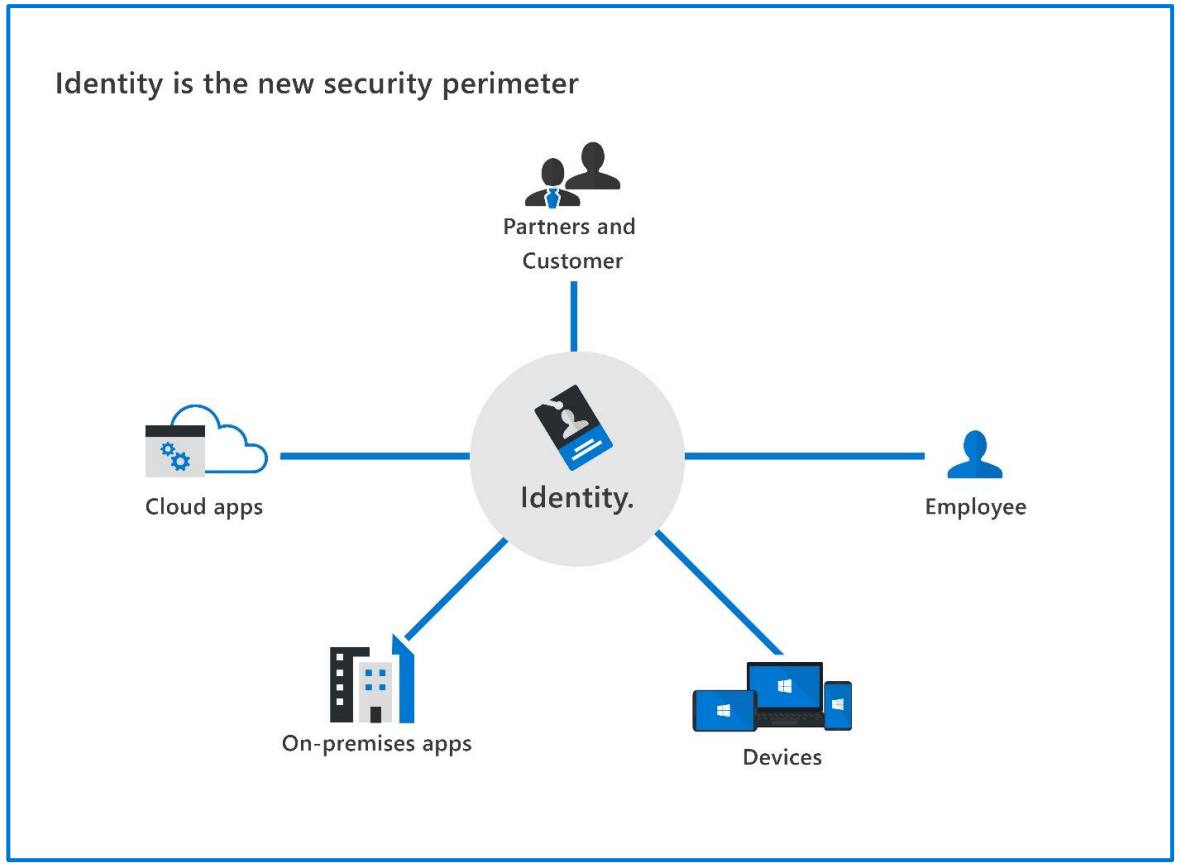
Identity has become the new security perimeter that enables organizations to secure their assets.

An identity is how someone or something can be verified and authenticated and may be associated with:

- User
- Application
- Device
- Other

Four pillars of identity:

- Administration
- Authentication
- Authorization
- Auditing



Modern authentication and the role of the identity provider

Modern authentication is an umbrella term for authentication and authorization methods between a client and a server.

At the center of modern authentication is the role of the ***identity provider (IdP)***.

IdP offers authentication, authorization, and auditing services.

IdP enables organizations to establish authentication and authorization policies, monitor user behavior, and more.

A fundamental capability of an IdP and “modern authentication” is the support for single sign-on (SSO).

Microsoft Azure Active Directory is an example of a cloud-based identity provider.

The concept of Federated Services

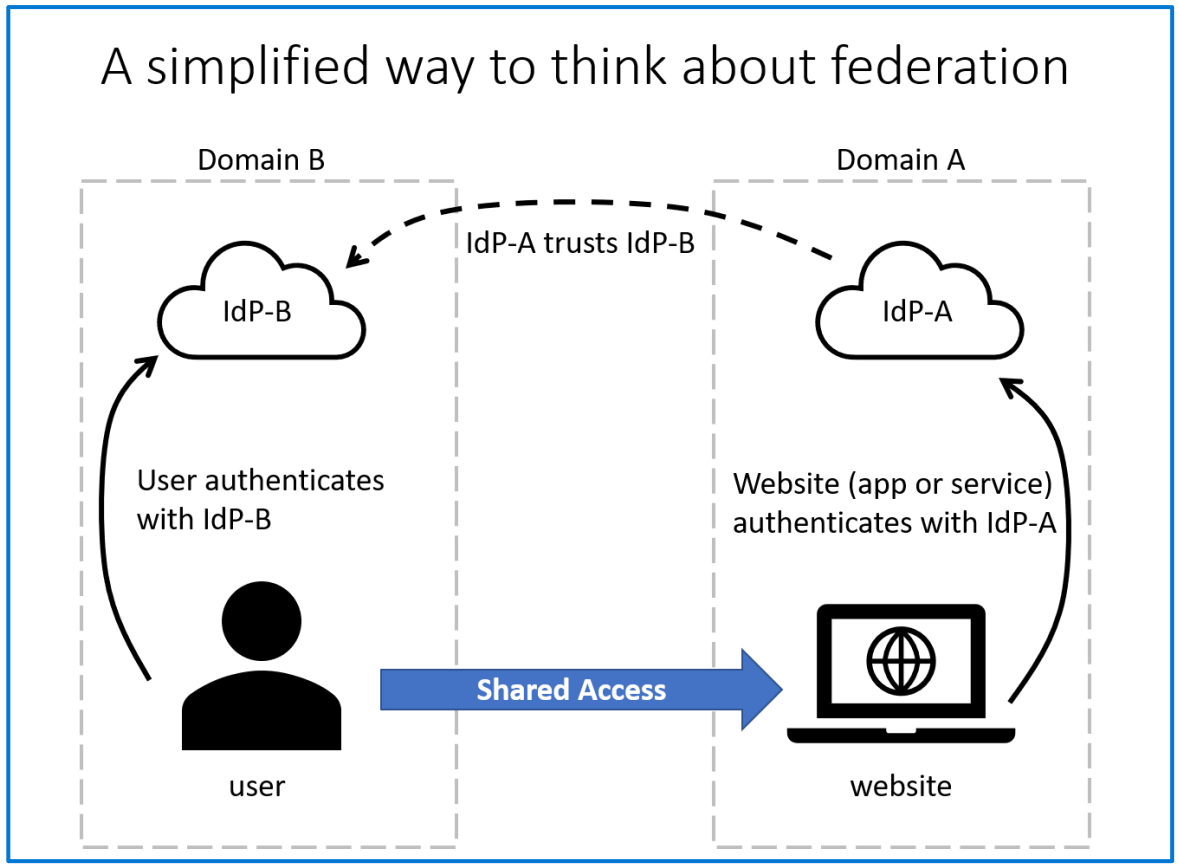
Simplification method of federation scenario:

The website uses the authentication services of IdP-A

The user authenticates with IdP-B

IdP-A has a trust relationship configured with IdP-B

When the user's credentials are passed to the website, the website trusts the user and allows access



The concept of directory services and Active Directory

A directory is a hierarchical structure that stores information about objects on the network.

A directory service stores directory data and makes it available to network users, administrators, services, and applications.

The best-known service of this kind is Active Directory Domain Services (AD DS), a central component in organizations with on-premises IT infrastructure.

Azure Active Directory is the evolution of identity and access management solutions, providing organizations an Identity as a Service (IDaaS) solution for all their apps across cloud and on-premises.

Module Summary

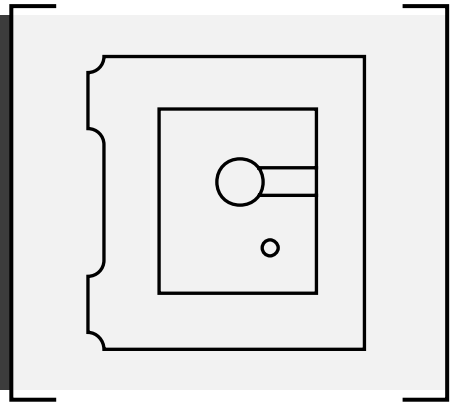
In this module, you have:

- Learned about some important security concepts and methodologies.
  - Learned about the Zero Trust methodology, the guiding principles and the six foundational elements used in the Zero Trust model.
  - Looked at the shared responsibility model.
  - Learned about defense in depth and the tradeoffs associated with CIA triad.
  - Learned about common cybersecurity threats including threats to business and personal data.
  - Learned about the cloud adoption framework.
- Learned about some important identity concepts.
  - Learned about the concept of identity as a security perimeter & the four pillars of identity
  - Learned about identity-related services, including the role of identity provider, federation, and directory services

Microsoft

Describe the capabilities of Microsoft identity and access management solutions

Lesson 1: Explore the services and identity types in Azure Active Directory



Lesson 1 Introduction

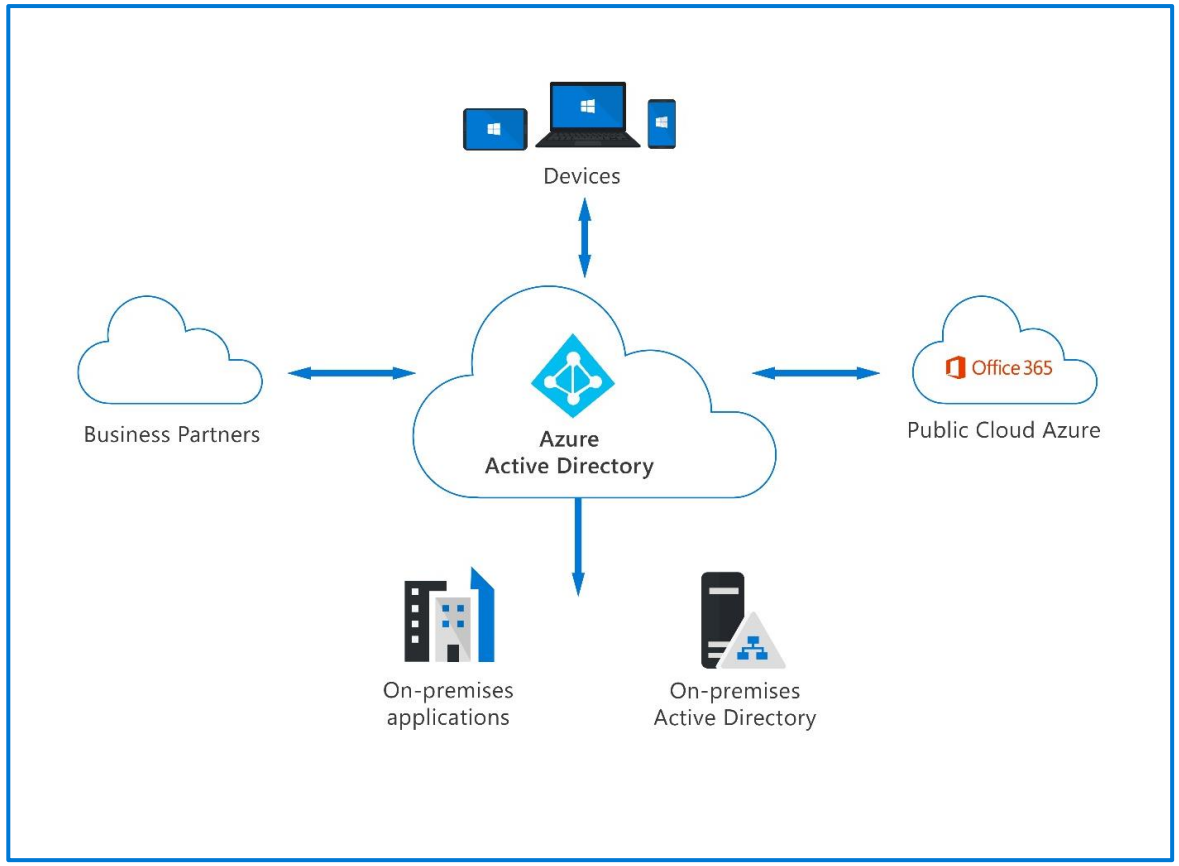
After completing this module, you'll be able to:

- Describe what is Azure Active Directory
- Describe the identity types that Azure Active Directory supports

Azure Active Directory

Azure AD is Microsoft's cloud-based identity and access management service. Capabilities of Azure AD include:

- Organizations can enable their employees, guests, and others to sign in and access the resources they need.
- Provide a single identity system for their cloud and on-premises applications.
- Protect user identities and credentials and to meet an organization's access governance requirements.
- Each Microsoft 365, Office 365, Azure, and Dynamics 365 Online subscription automatically use an Azure AD tenant.



Azure AD identity types

Azure AD manages different types of identities: users, service principals, managed identities, and devices.

User - a representation of something that's managed by Azure AD. Employees and guests are represented as users in Azure AD.

Service principal - a security identity used by applications or services to access specific Azure resources. You can think of it as an identity for an application.

Managed identity - typically used to manage the credentials for authenticating a cloud application with an Azure service. Two types: system assigned and user assigned.

Device - a piece of hardware, such as mobile devices, laptops, servers, or printer. Device identities can be set up in different ways in Azure AD, to determine properties such as who owns the device.

Microsoft Security

Demo

Azure Active Directory user settings

External identities in Azure AD

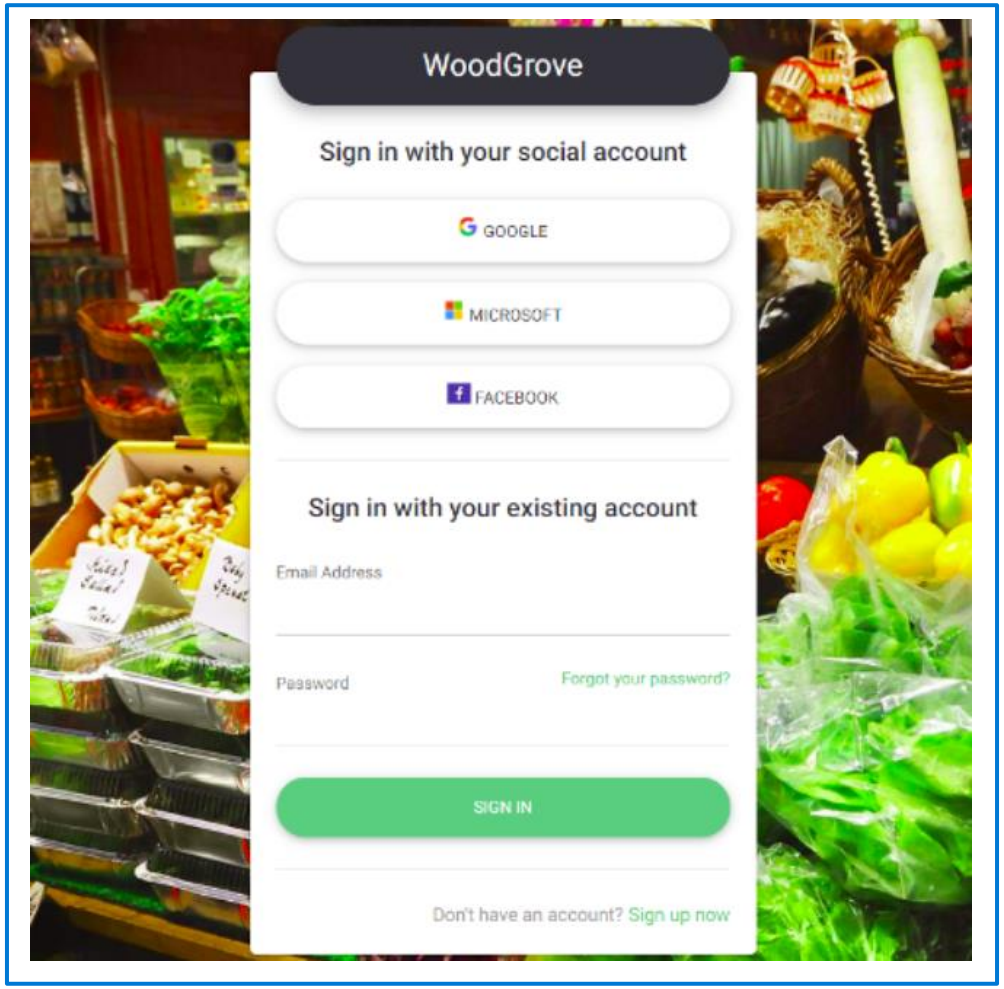
Two different Azure AD External Identities:

B2B collaboration

B2B collaboration allows you to share your apps and resources with external users

B2C access management

B2C is an identity management solution for consumer and customer facing apps



The concept of hybrid identities

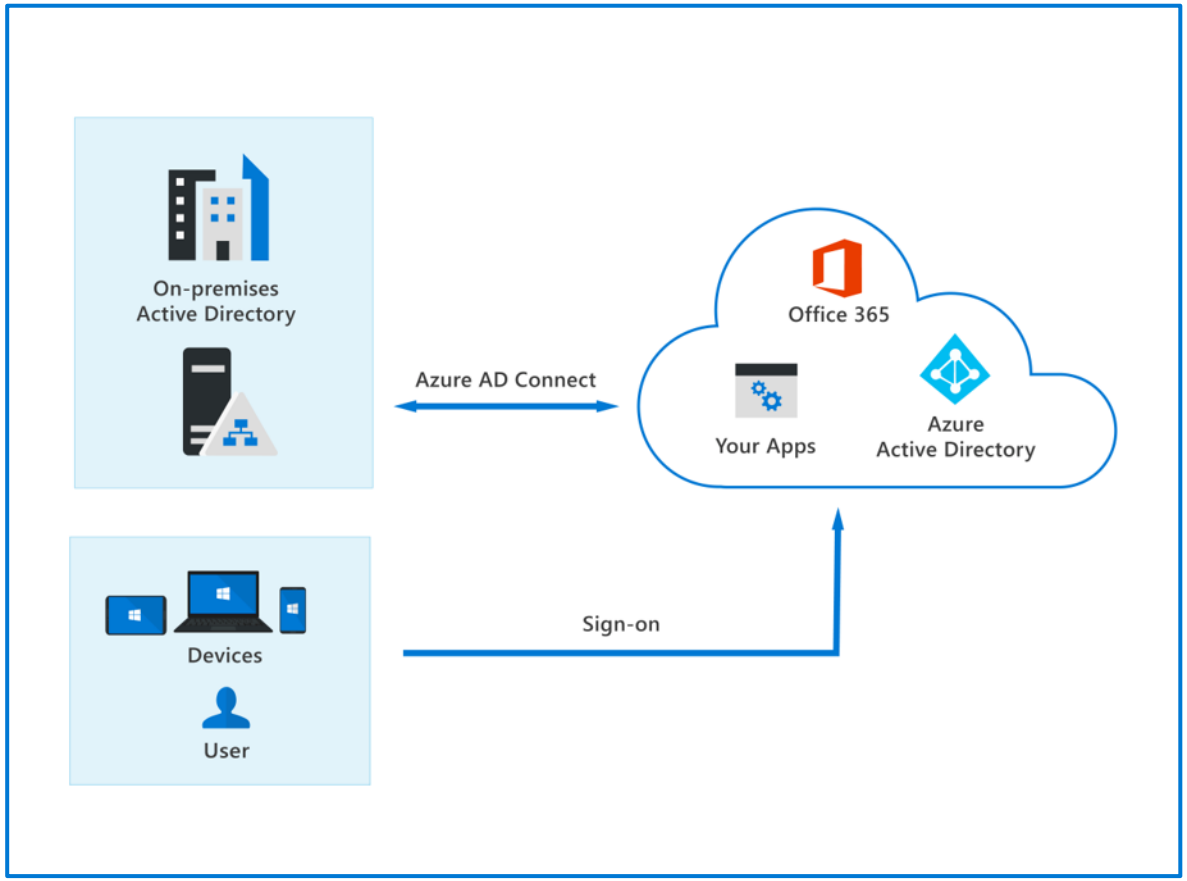
Hybrid identities and authentication

Hybrid identity model

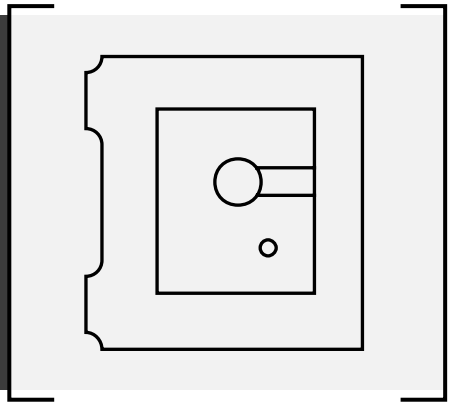
- With the hybrid model, users accessing both on-premises and cloud apps are hybrid users managed in the on-premises Active Directory.
- When you make an update in your on-premises AD DS, all updates to user accounts, groups, and contacts are synchronized to your Azure AD with *Azure AD Connect*

Methods of authentication

- Password hash synchronization
- Pass-through authentication (PTA)
- Federated authentication



Lesson 2: Explore the authentication capabilities of Azure Active Directory



Lesson 2 Introduction

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

- Describe the secure authentication methods of Azure AD
- Describe the password protection and management capabilities of Azure AD

Authentication methods of Azure AD

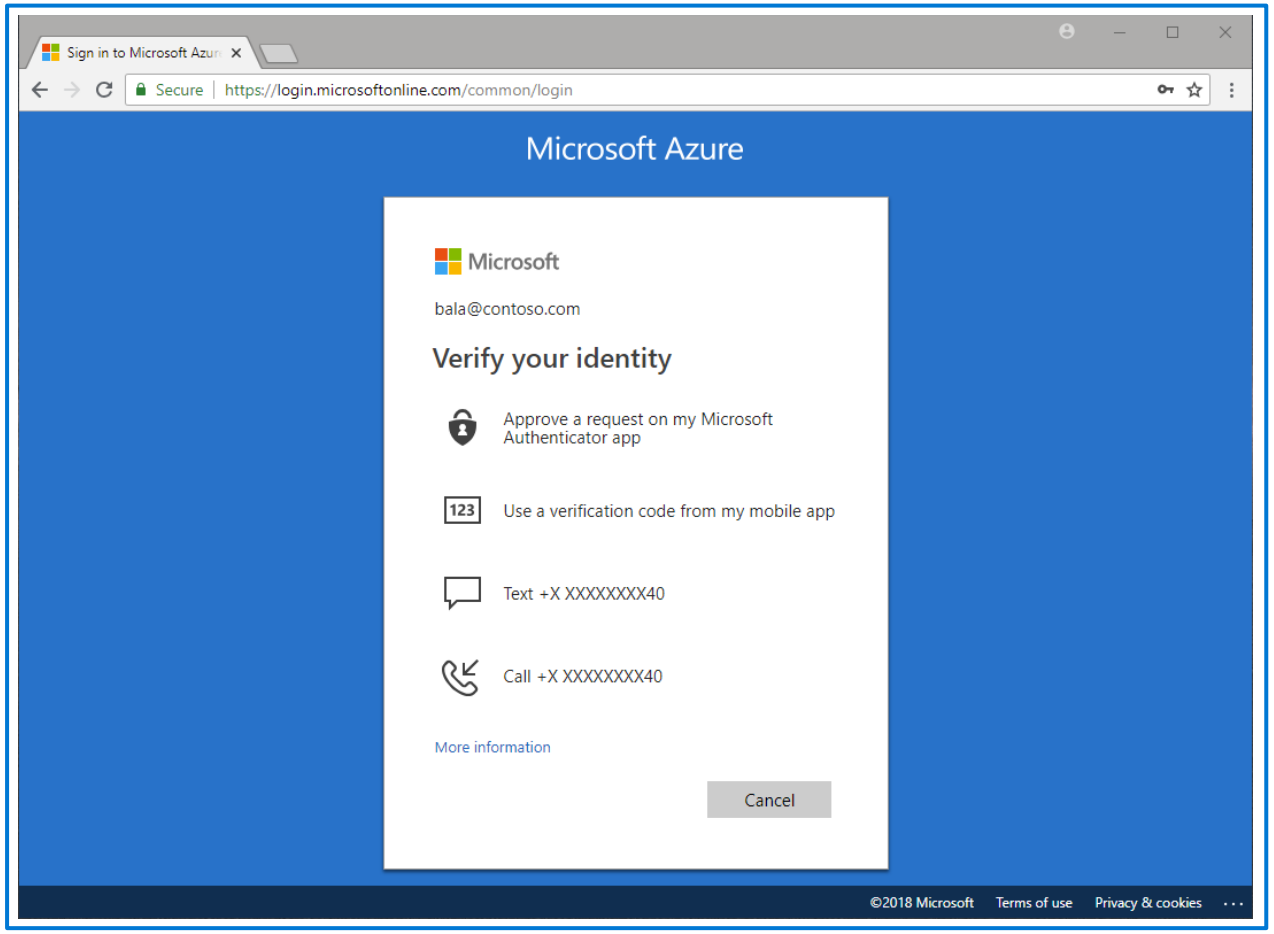
Multifactor authentication (MFA) & Security Defaults

MFA requires more than one form of verification:

- Something you know
- Something you have
- Something you are

Security defaults:

- A set of basic identity security mechanisms recommended by Microsoft.
- A great option for organizations that want to increase their security posture but don't know where to start, or for organizations using the free tier of Azure AD licensing.



Multi-factor authentication (MFA) in Azure AD

Different authentication methods that can be used with MFA

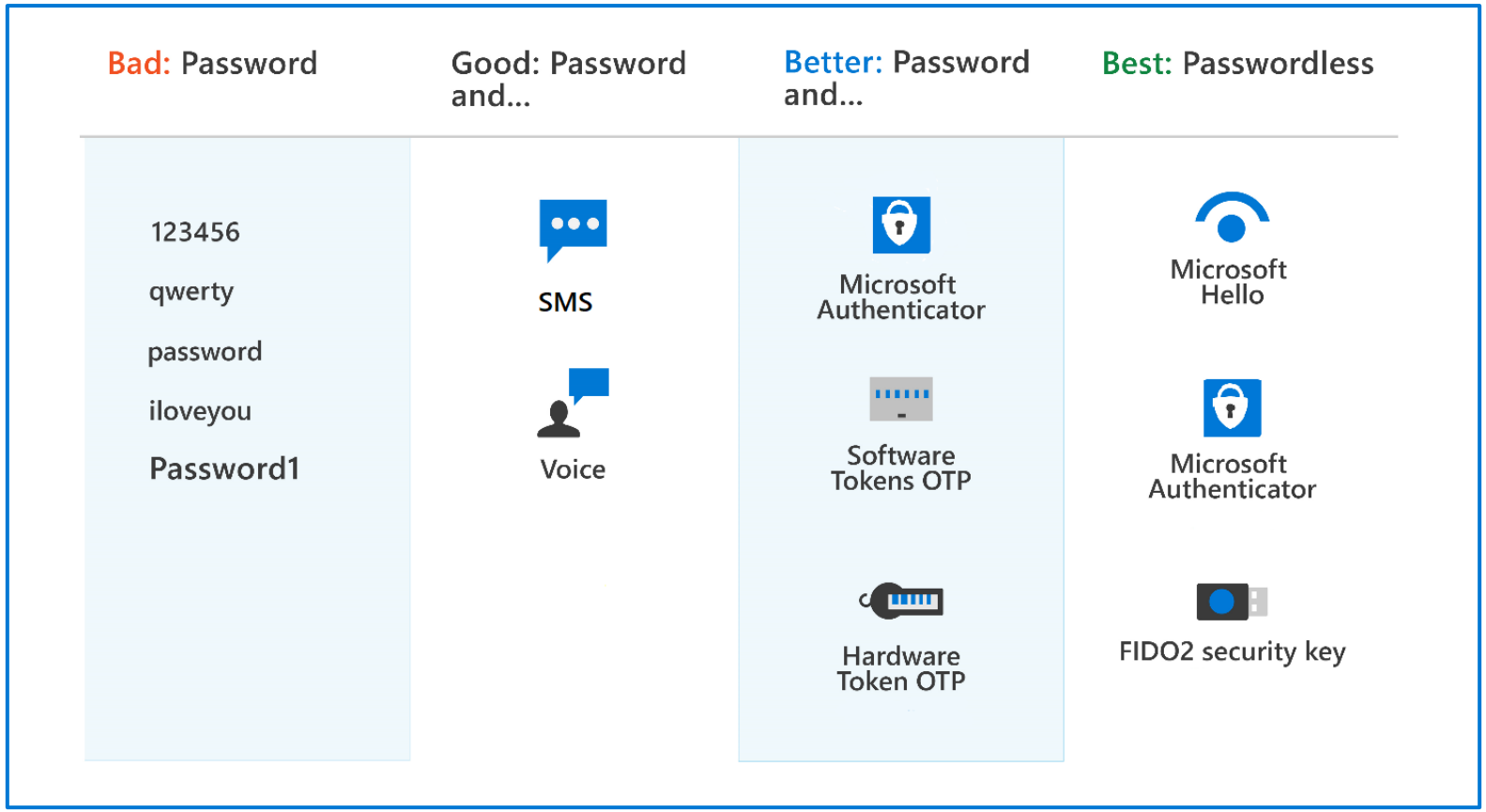
Passwords

Password & additional verification

- Phone (voice or SMS)
- Microsoft Authenticator
- Open Authentication (OATH) with software or hardware tokens

Passwordless

- Biometrics (Windows Hello)
- Microsoft Authenticator
- FIDO2



Windows Hello for Business

Windows Hello lets users authenticate to:

- A Microsoft account
- An Active Directory account
- An Azure Active Directory (Azure AD) account
- Identity Provider Services or Relying Party Services that support Fast ID Online v2.0 authentication

Why is Windows Hello safer than a password?

Because it's tied to the specific device on which it was set up. Without the hardware, the PIN is useless

Self-service password reset (SSPR) in Azure AD

Benefits of Self-service password reset:

- It increases security.
- It saves the organization money by reducing the number of calls and requests to help desk staff.
- It increases productivity, allowing the user to return to work faster.

Self-service password reset works in the following scenarios:

- Password change
- Password reset
- Account unlock

Authentication method of SSPR:

- Mobile app notification
- Mobile app code
- Email

Microsoft Security

Demo

Azure Active Directory
self-service password reset (SSPR)

Password protection & management capabilities in Azure AD

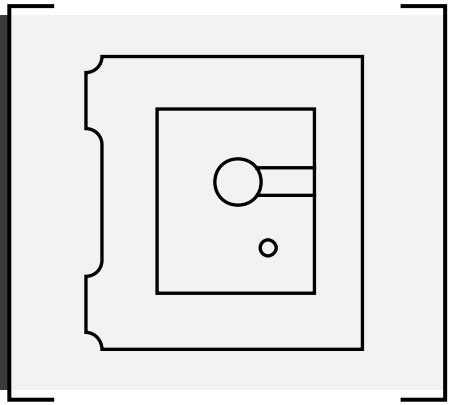
Global banned password list

Custom banned password lists

Protecting against password spray

Hybrid security

Lesson 3: Explore the access management capabilities of Azure Active Directory



Lesson 3 Introduction

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

- Describe Conditional Access and its benefits
- Describe Azure AD roles

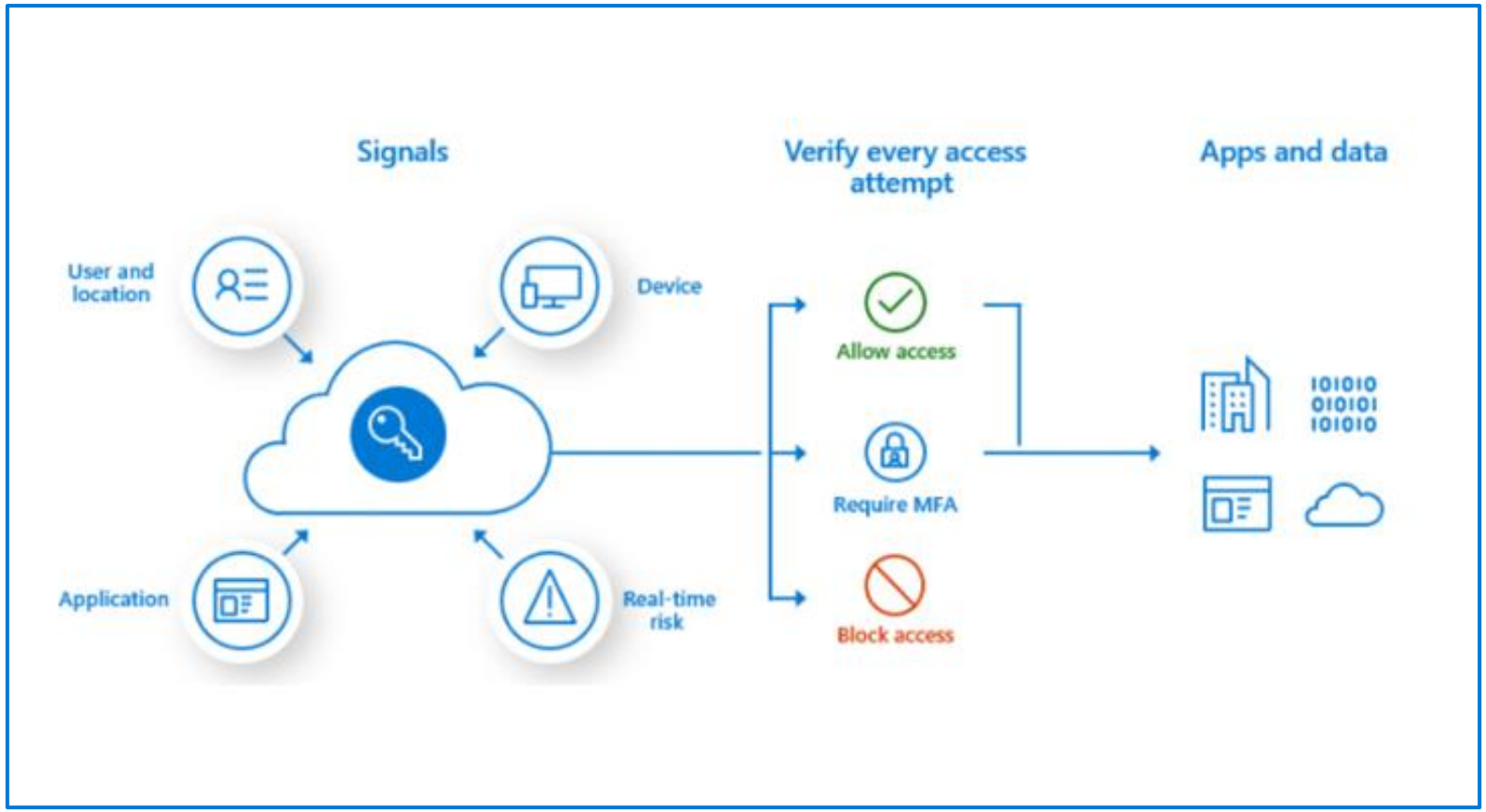
Conditional access

Conditional Access signals:

- User or group membership
- Named location information
- Device
- Application
- Real-time sign-in risk detection
- Cloud apps or actions
- User risk

Access controls:

- Block access
- Grant access
- Require one or more conditions to be met before granting access
- Control user access based on session controls to enable limited experiences within specific cloud applications



Microsoft Security

Demo

Azure Active Directory Conditional Access

Azure AD role-based access control (RBAC)

Azure AD roles control permissions to manage Azure AD resources.

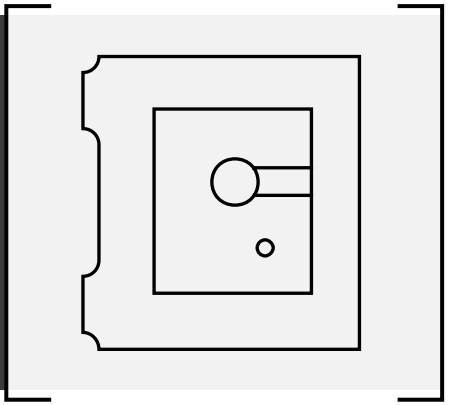
Built-in roles

Custom roles

Azure AD role-based access control

Only grant the access users need

Lesson 4: Describe the identity protection and governance capabilities of Azure Active Directory



Lesson 4 Introduction

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

- Describe the identity governance capabilities of Azure AD.
- Describe the benefits of Privileged Identity Management (PIM).
- Describe the capabilities of Azure AD Identity Protection.

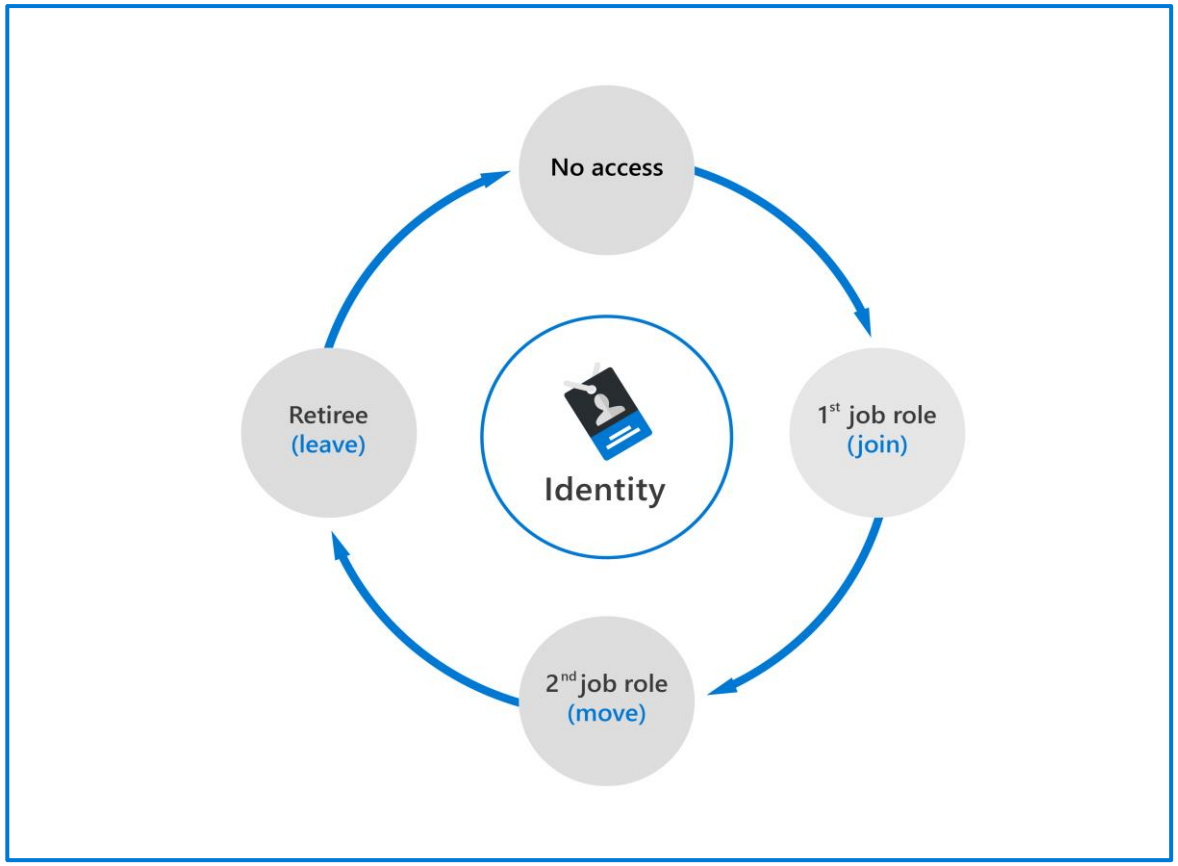
Identity governance in Azure AD

The tasks of Azure AD identity governance

- Govern the identity lifecycle.
- Govern access lifecycle.
- Secure privileged access for administration.

Identity lifecycle

- Join: A new digital identity is created.
- Move: Update access authorizations.
- Leave: Access may need to be removed.



Entitlement management and access reviews

Entitlement management

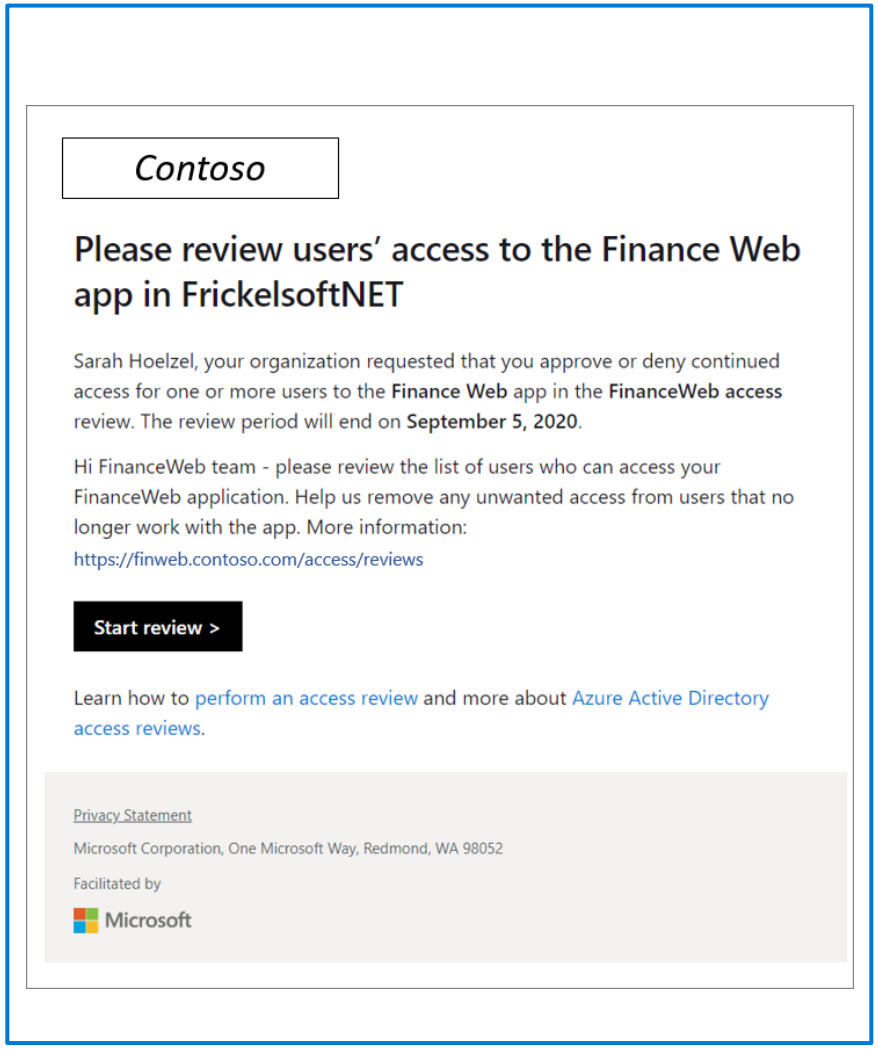
- It is an identity governance feature that enables organizations to manage identity and access lifecycle at scale.
- It automates access request workflows, access assignments, reviews, and expiration.

Access reviews

- Enable organizations to efficiently manage group memberships, access to enterprise applications, and role assignment.
- Ensure that only the right people have access to resources
- Used to review and manage access for both users and guests

Terms of use

- Allow information to be presented to users, before they access data or an application.
- Ensure users read relevant disclaimers for legal or compliance requirements.



Privileged Identity Management (PIM)

PIM enables you to manage, control, and monitor access to important resources in your organization.

Just in time, providing privileged access only when needed, and not before.

Time-bound, by assigning start and end dates that indicate when a user can access resources.

Approval-based, requiring specific approval to activate privileges.

Visible, sending notifications when privileged roles are activated.

Auditable, allowing a full access history to be downloaded.

Azure Identity Protection

Enables organizations to accomplish three key tasks:

- Automate the detection and remediation of identity-based risks.
- Investigate risks using data in the portal.
- Export risk detection data to third-party utilities for further analysis.

It can categorize and calculate risk:

- Categorize risk into three tiers: low, medium, and high.
- Calculate the sign-in risk, and user identity risk.

It provides organizations with three reports:

- Risky users
- Risky sign-ins
- Risk detections

Module Summary

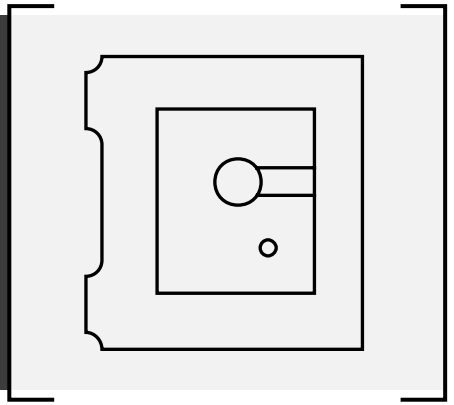
In this module, you have:

- Learned about Azure AD and services and identity types Azure AD supports
- Explore the authentication capabilities of Azure AD, including MFA
- Explore the access management capabilities of Azure AD with Conditional Access and Azure AD RBAC
- Describe identity protection and governance capabilities of Azure AD, including PIM, entitlement management, and access reviews.
- Learned about the capabilities of Azure AD Identity Protection.

Microsoft

Describe the capabilities of Microsoft security solutions (Segment 1 of 2)

Lesson 1: Describe basic security capabilities in Azure



Lesson 1 Introduction

After completing this module, you should be able to:

Describe Azure security capabilities for protecting your network

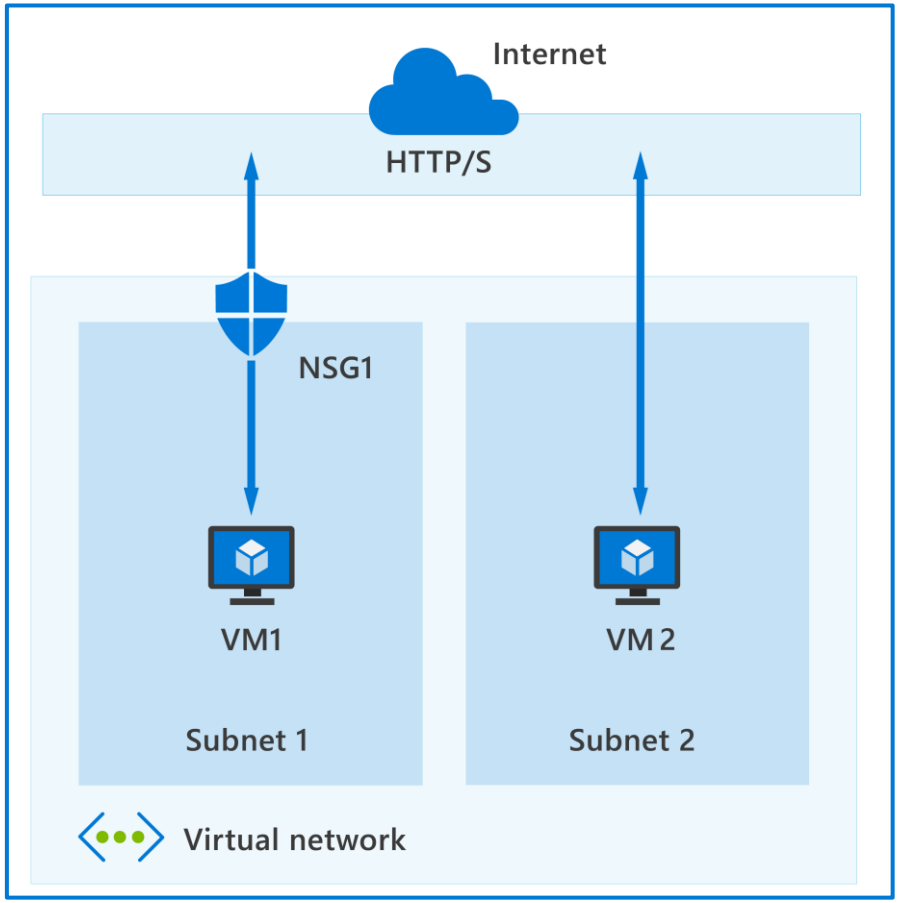
Describe how Azure can protect your VMs

Describe how encryption on Azure can protect your data

Azure 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
  - Source or destination
  - Direction
  - Action
  - Priority
  - Protocol
  - Port range



Microsoft Security

Demo

Azure Network Security Groups

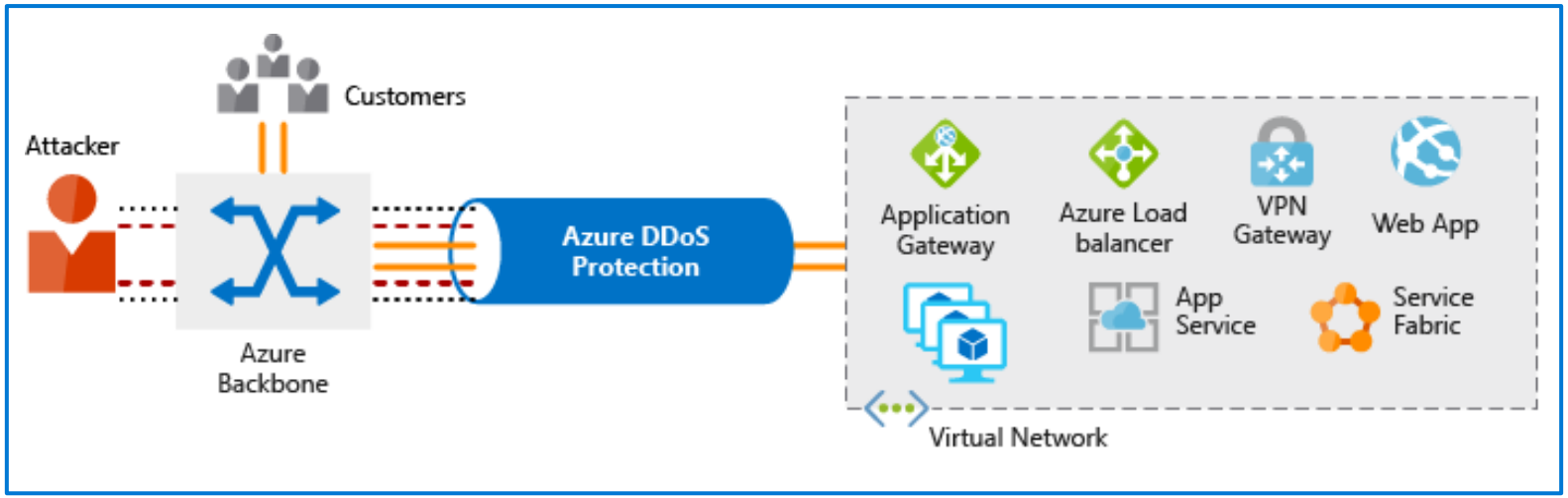
Azure DDoS protection

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:

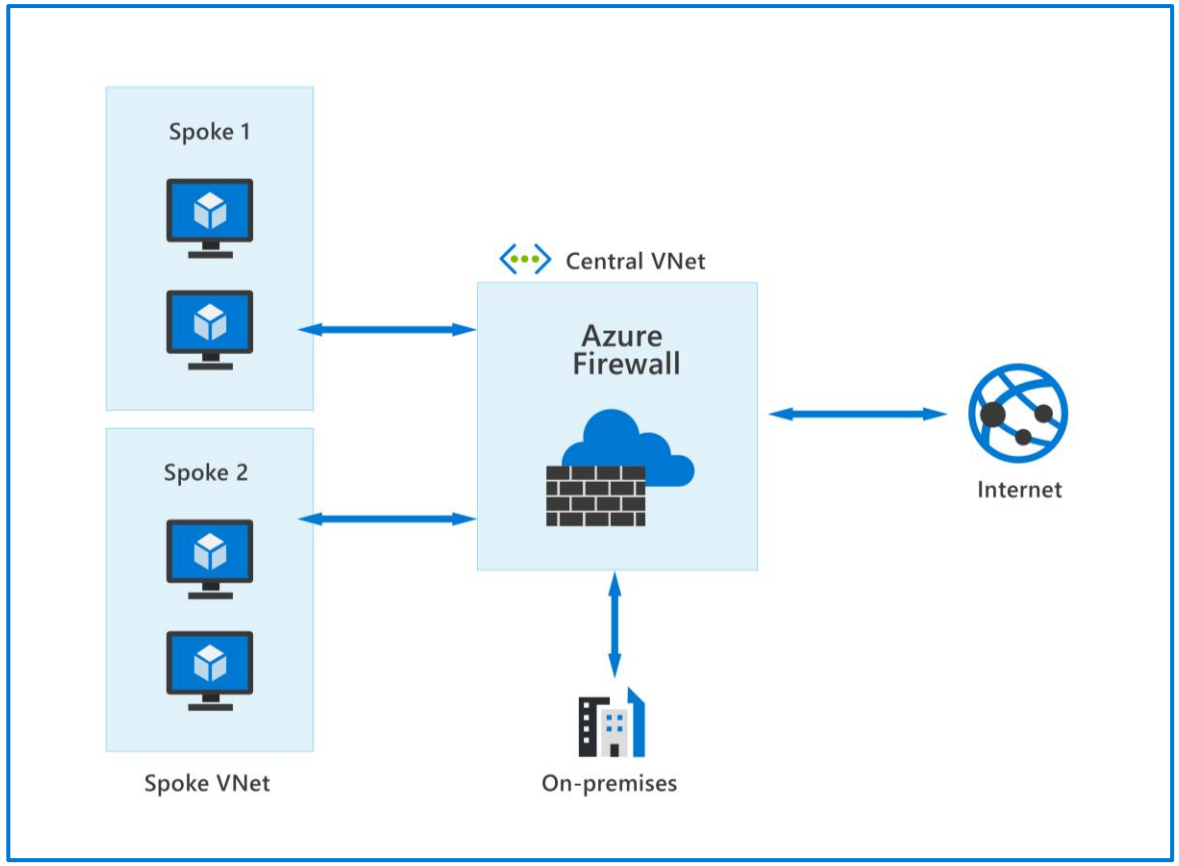
- Basic
- Standard



Azure Firewall

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

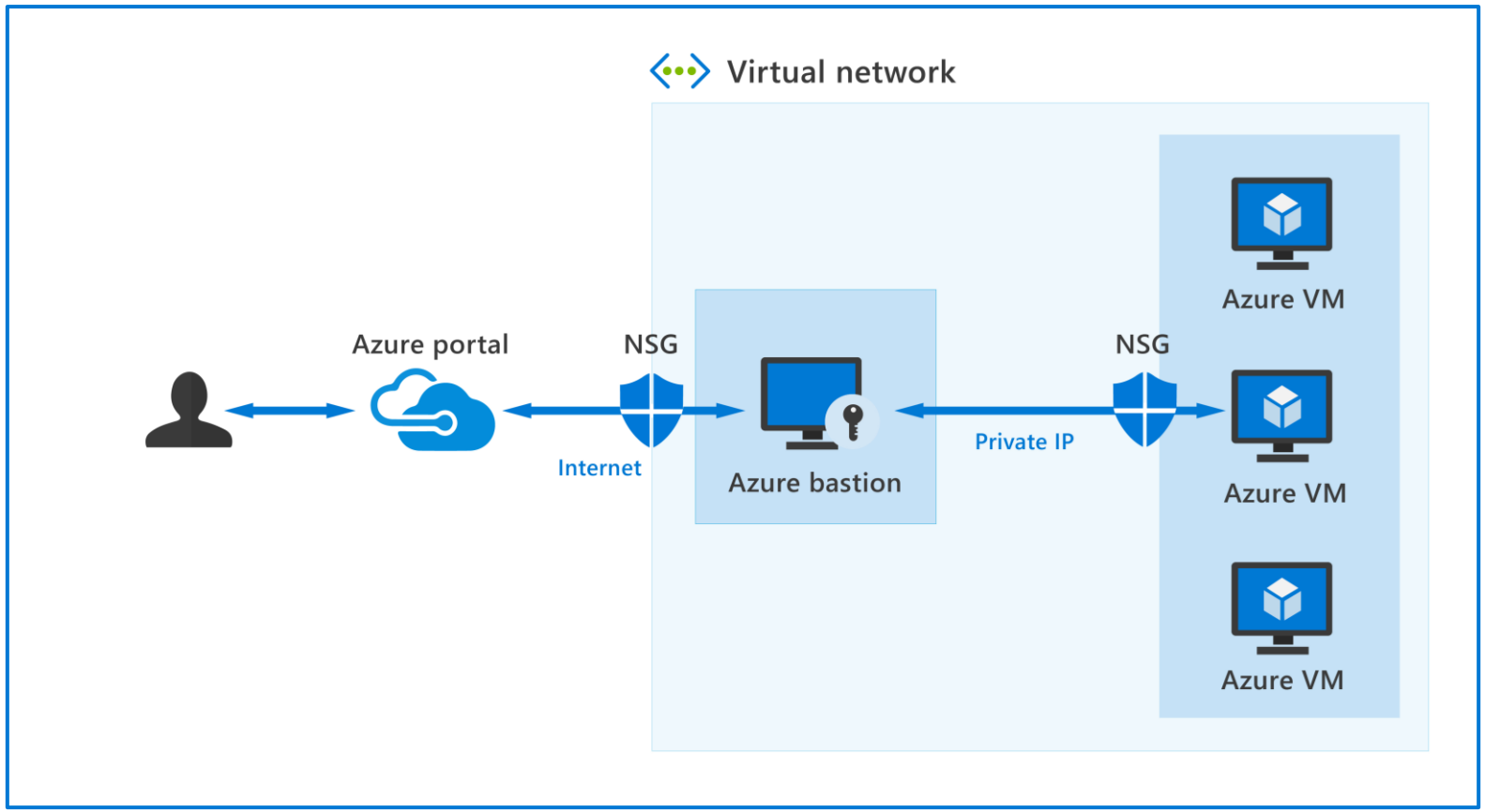
- Built-in high availability & Availability Zones
- Outbound SNAT & inbound DNAT
- Threat intelligence
- Network & application-level filtering
- Multiple public IP addresses
- Integration with Azure Monitor



Azure Bastion

Azure Bastion provides secure connectivity to your VMs directly from the Azure portal using Transport Layer Security (TLS). Features include:

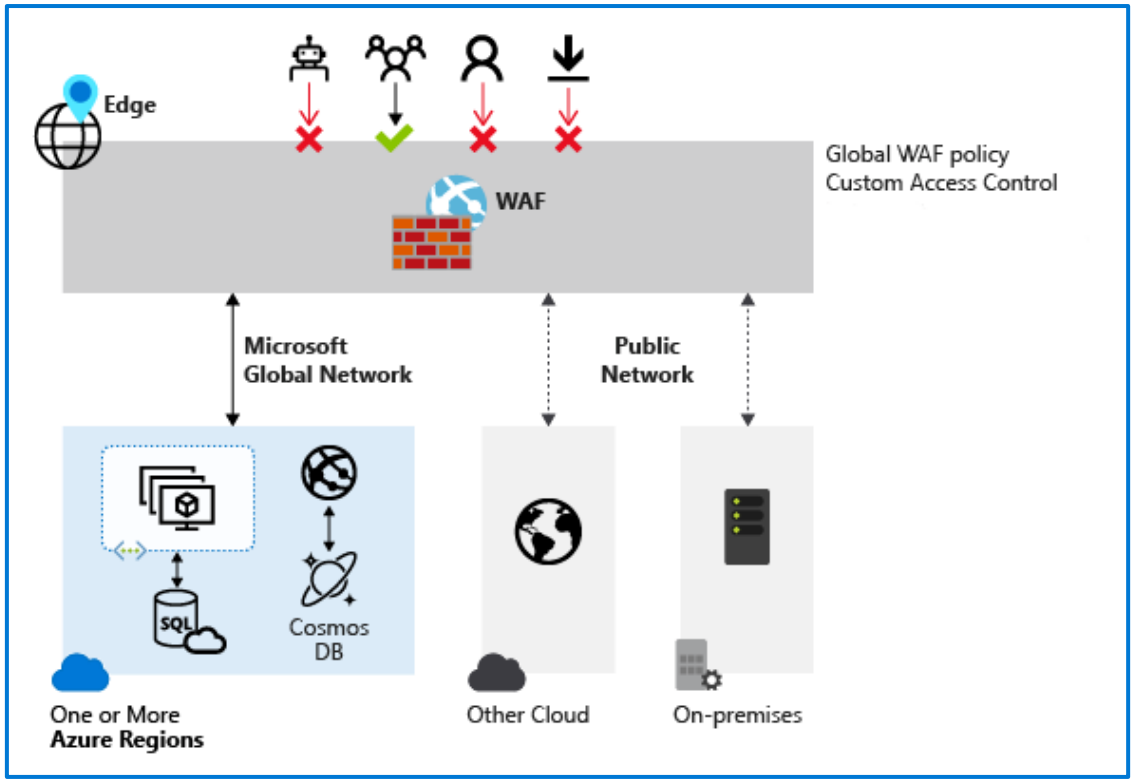
- RDP and SSH directly in Azure portal.
- Remote session over TLS and firewall traversal for RDP/SSH.
- No Public IP required on the Azure VM.
- No hassle of managing NSGs.
- Protection against port scanning.
- Protect against zero-day exploits.



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.



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?

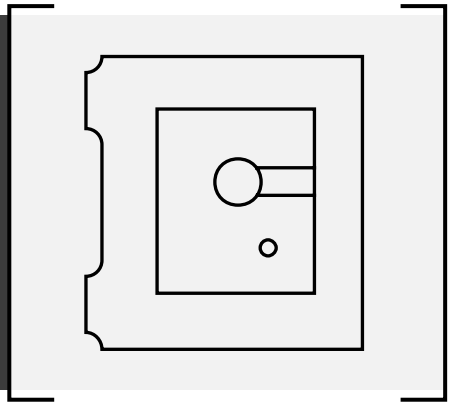
Secrets management

Key management

Certificate management

Store secrets backed by HW or SW

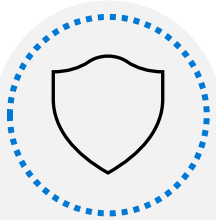
Lesson 2: Describe security management capabilities of Azure



Lesson 2 Introduction

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

Describe the security management capabilities of Azure.



Describe the benefits and use cases of Azure Defender.

Understand Cloud Security Posture Management and the security baseline.

Cloud security posture management

Cloud security posture management (CSPM), tools designed to improve your cloud security management.

CSPM uses a combination of tools & services:

- Zero Trust-based access control
- Real-time risk scoring
- Threat and vulnerability management (TVM)
- Discover sharing risks
- Technical policy
- Threat modeling systems & architectures

CSPM can be useful to many teams:

- Threat intelligence team
- Information technology
- Compliance & risk management teams
- Business leaders and SMEs
- Security architecture and operations
- Audit team

Azure Security Center

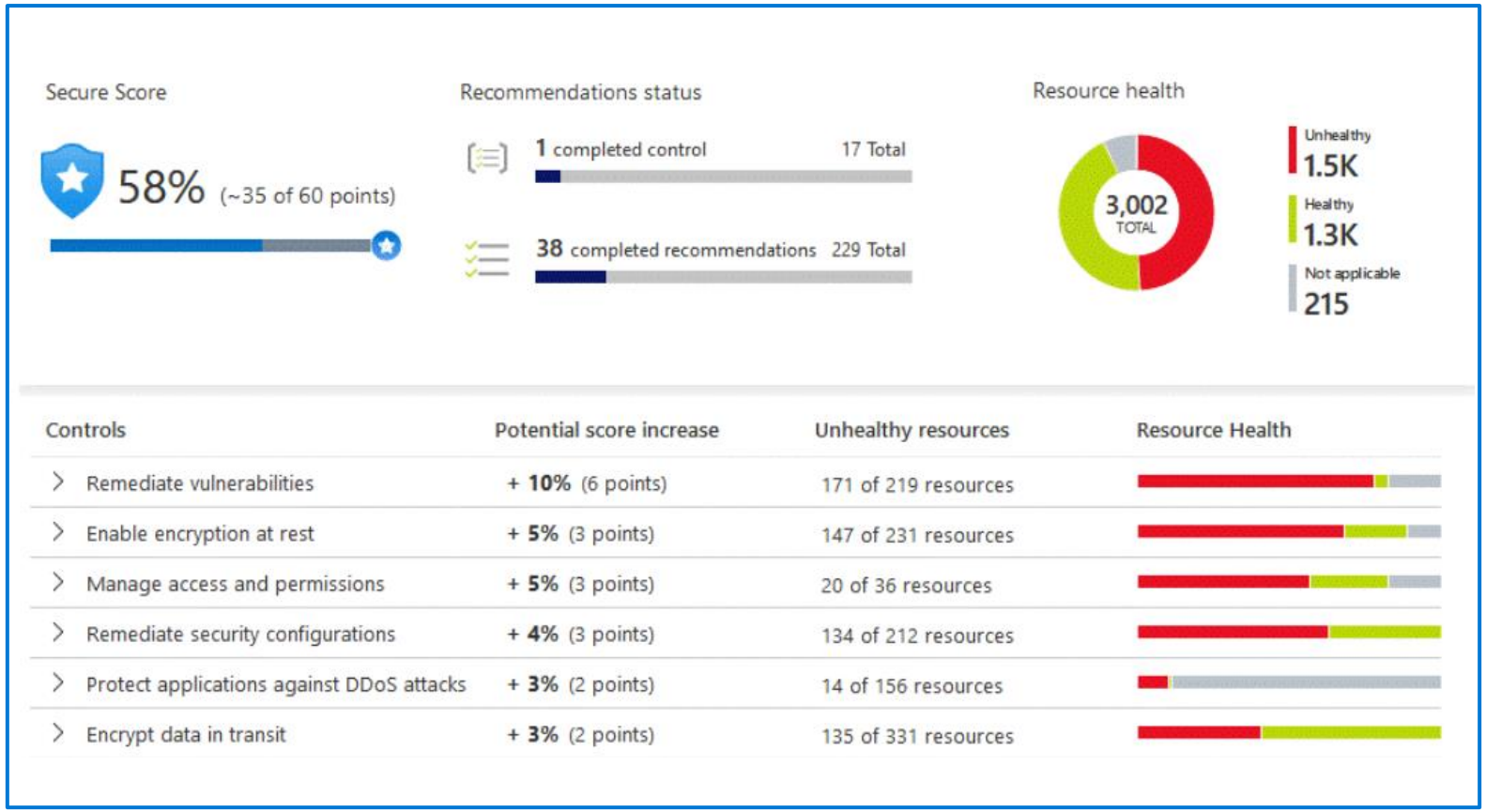
Strengthen security posture across your machines, data services, and applications.

Continuous assessment – ordered list of recommendations of what needs to be fixed for maximum protection.

Protect against threats - Detect and prevent threats on IaaS, non-Azure servers, and PaaS.

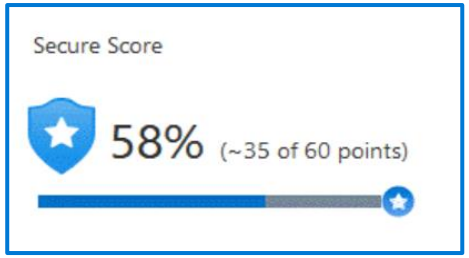
Network map - topology view of your workloads, so you can see if each node is properly configured.

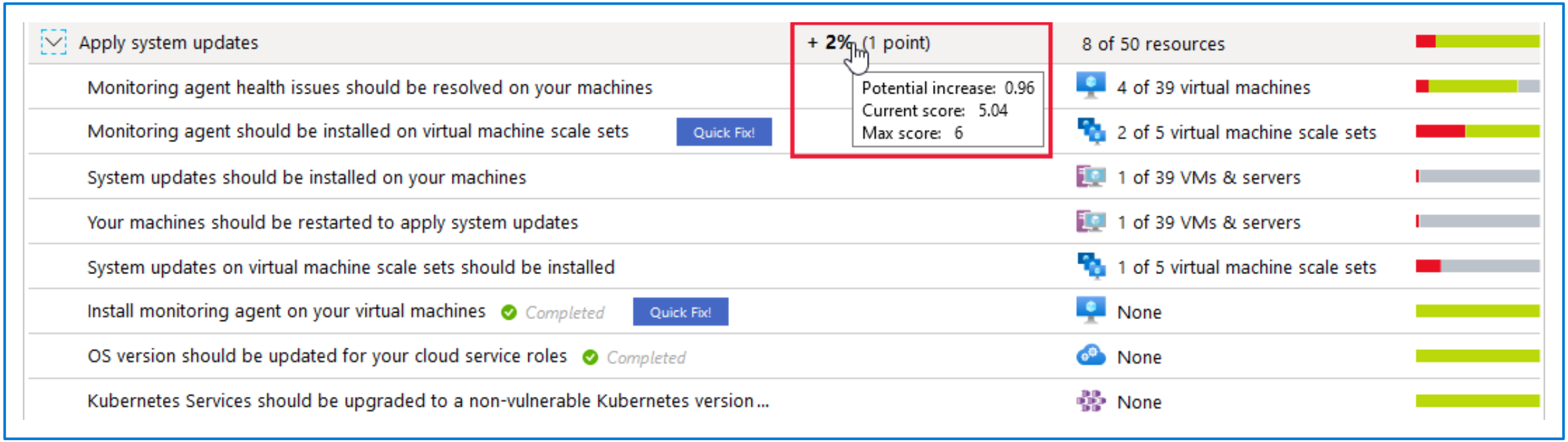
Get secure faster - Integration with other Microsoft security solutions for complete security across all your Azure resources.



Azure Secure Score

The secure score is shown in the Azure portal pages as a percentage value. To improve your secure score, remediate security recommendations from your recommendations list.





Azure Defender

Scope of Azure Defender

Servers

App Service

Storage

SQL

Kubernetes

Container registries

Key Vault

Hybrid cloud protection

Protect your non-Azure servers.

Protect your virtual machines in other clouds (such as AWS and GCP).

Azure Defender alerts

Advanced protection

Vulnerability assessment

Security baselines & the Azure Security Benchmark

Security baselines for Azure offer a consistent experience when securing your environment. They apply prescriptive best practices and recommendations from the Azure Security Benchmark (ASB) to improve the security of workloads, data, and services on Azure. Each recommendation includes the following information:

Azure ID: The Azure Security Benchmark ID that corresponds to the recommendation.

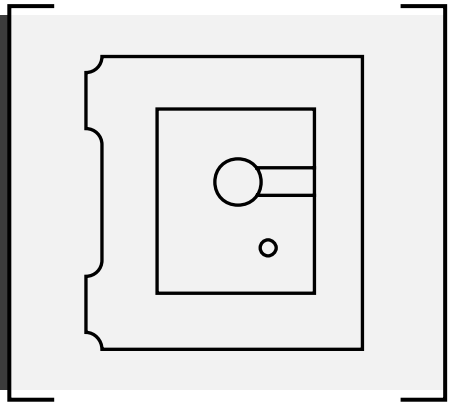
Recommendation: The recommendation provides a high-level description of the control.

Guidance: The rationale for the recommendation and links to guidance on how to implement it.

Responsibility: Who is responsible for implementing the control?

Azure Security Center monitoring: Does Azure Security Center monitor the control?

Lesson 3: Describe security capabilities of Azure Sentinel

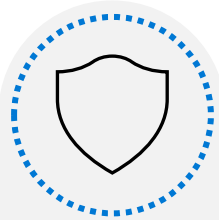


Lesson 3 Introduction

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

Describe the security concepts for SIEM, SOAR, and XDR.

Describe how Azure Sentinel provides integrated threat protection.



Describe the capabilities of Azure Sentinel.

SIEM, SOAR, and XDR

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.

What is extended detection and response?

An XDR system is designed to deliver intelligent, automated, and integrated security across an organization's domain. It helps prevent, detect, and respond to threats across identities, endpoints, applications, email, IoT, infrastructure, and cloud platforms.

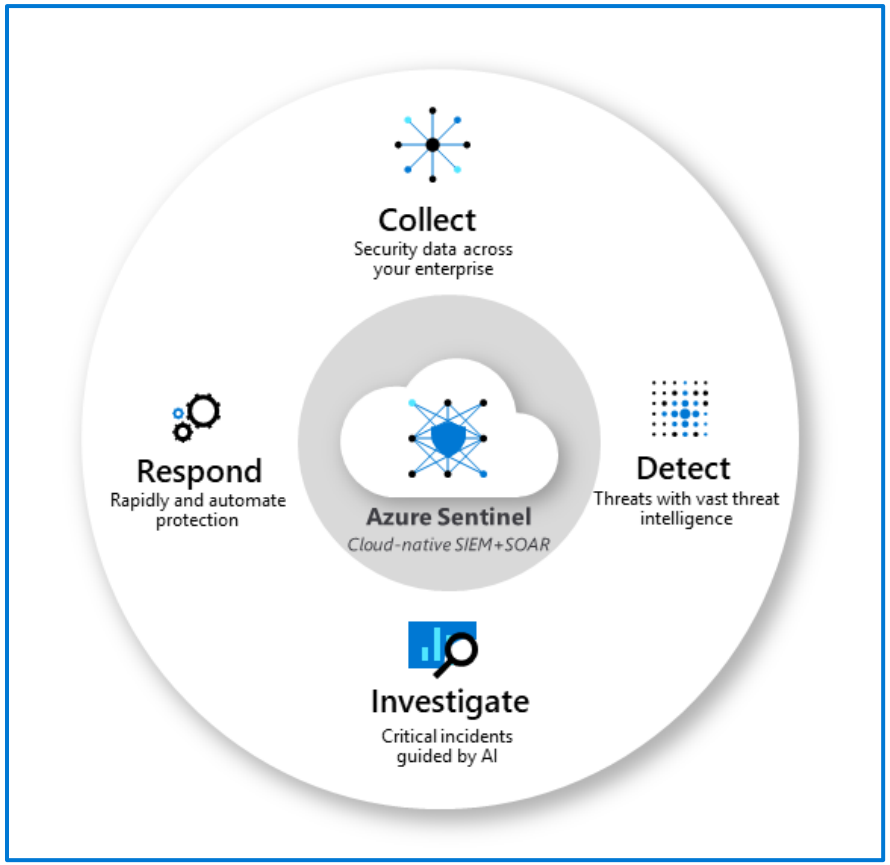
Sentinel provides integrated threat protection (Slide 1)

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.



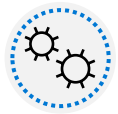
Sentinel provides integrated threat protection (Slide 2)

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

Workbooks: monitor the data using the Azure 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 Azure Logic Apps, to create workflows

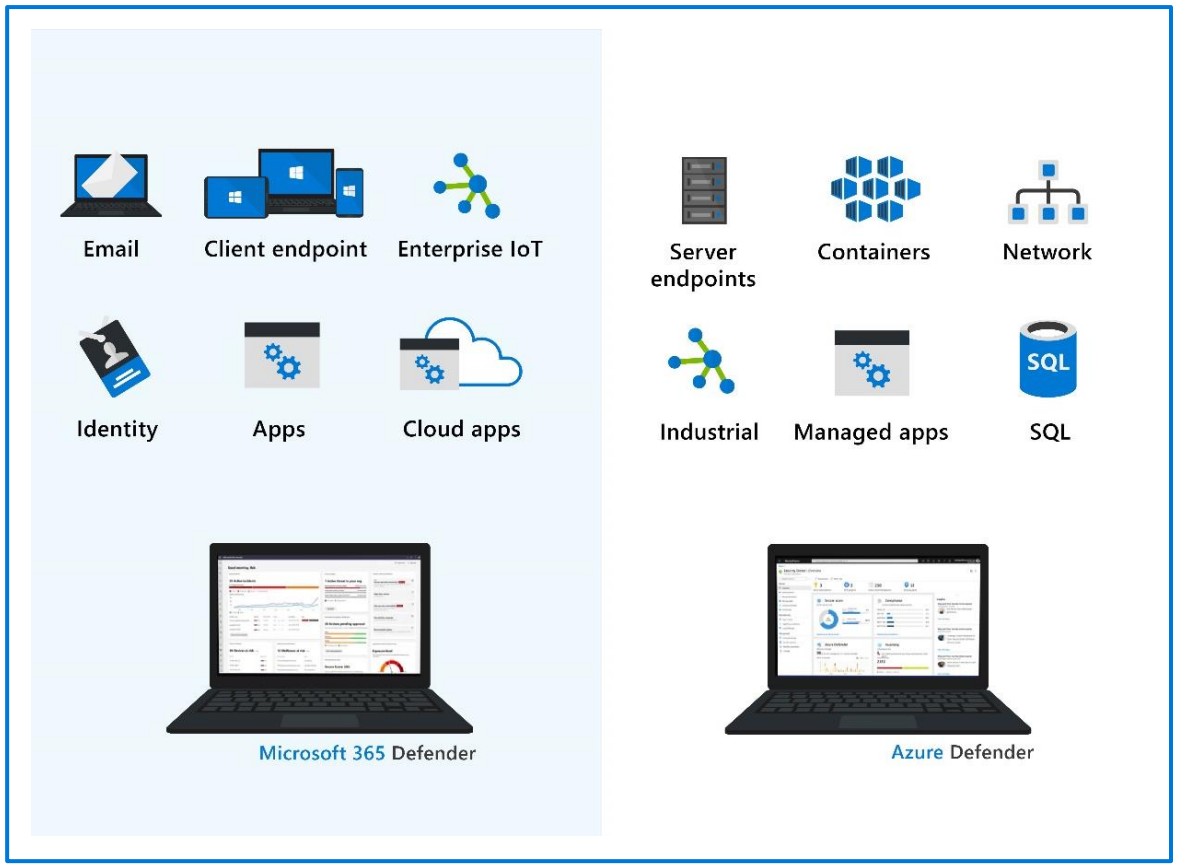
Playbooks: A collection of procedures that can help automate and orchestrate your response.

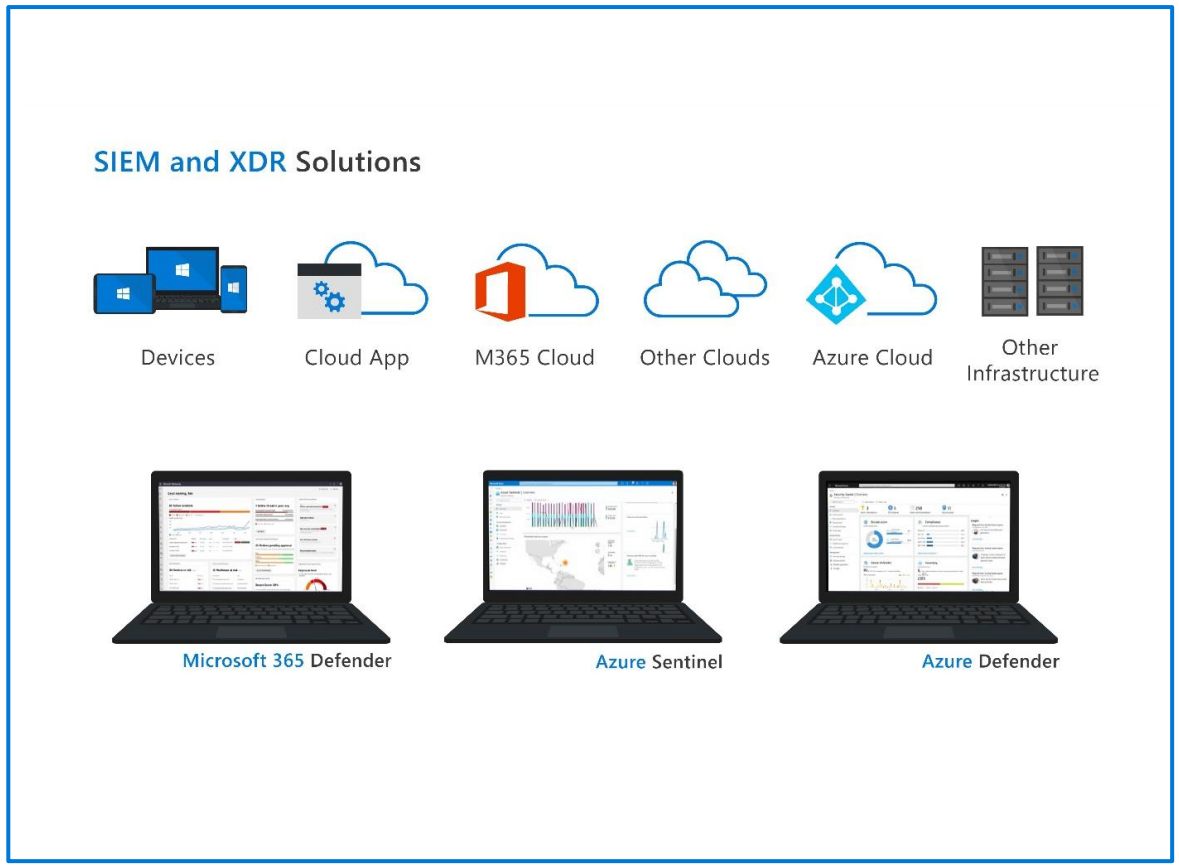
Investigation: Understand the scope of a potential security threat and find the root cause.

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

Integrated threat protection: XDR with Microsoft 365 Defender and Azure Defender integration.

Sentinel provides integrated threat protection (Slide 3)





Module Summary

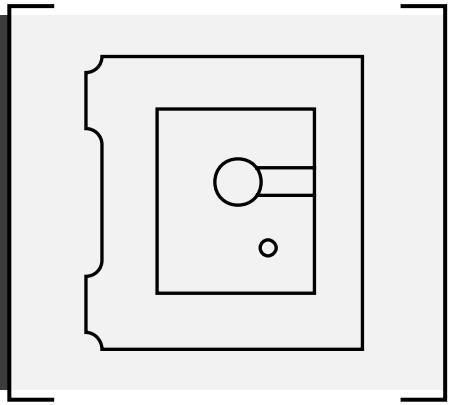
In this module, you have:

- Learned about basic security capabilities in Azure, including NSGs, DDoS, Bastion, and more.
- Learned about security management capabilities of Azure, including Azure Security Center and Secure Score
- Learned about SIEM, SOAR and the security capabilities of Azure Sentinel

Microsoft

Describe the capabilities of Microsoft security solutions (Segment 1 of 2)

Lesson 1: Describe basic security capabilities in Azure



Lesson 1 Introduction

After completing this module, you should be able to:

Describe Azure security capabilities for protecting your network

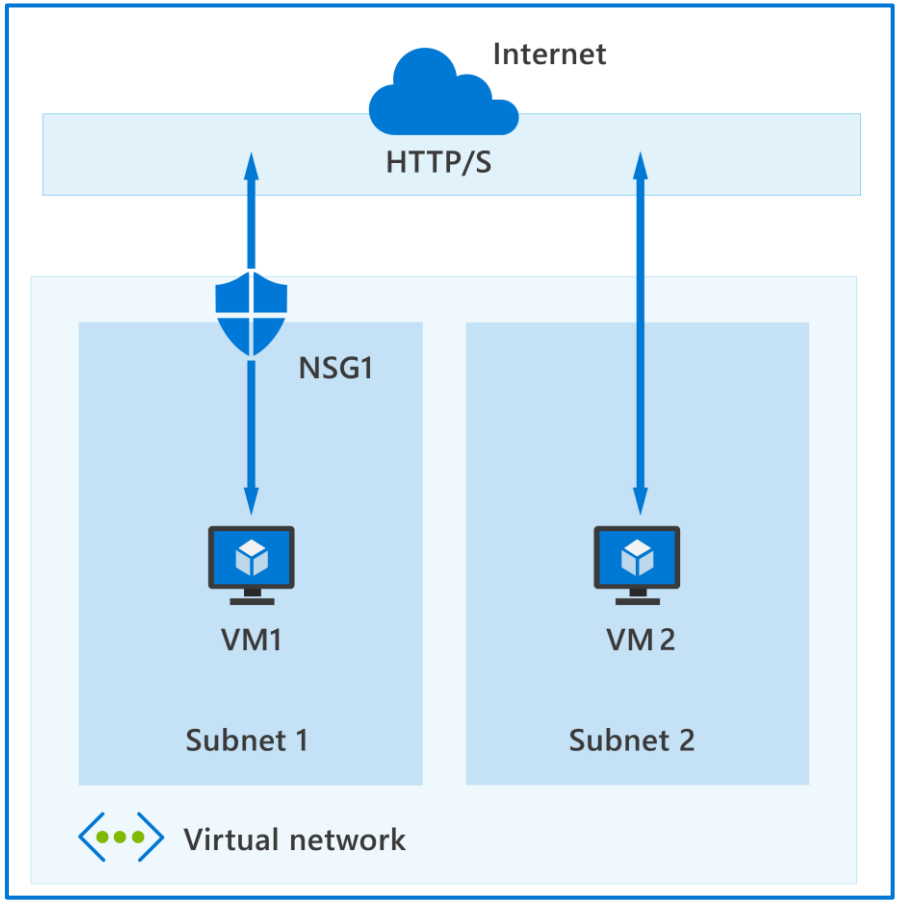
Describe how Azure can protect your VMs

Describe how encryption on Azure can protect your data

Azure 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
  - Source or destination
  - Direction
  - Action
  - Priority
  - Protocol
  - Port range



Microsoft Security

Demo

Azure Network Security Groups

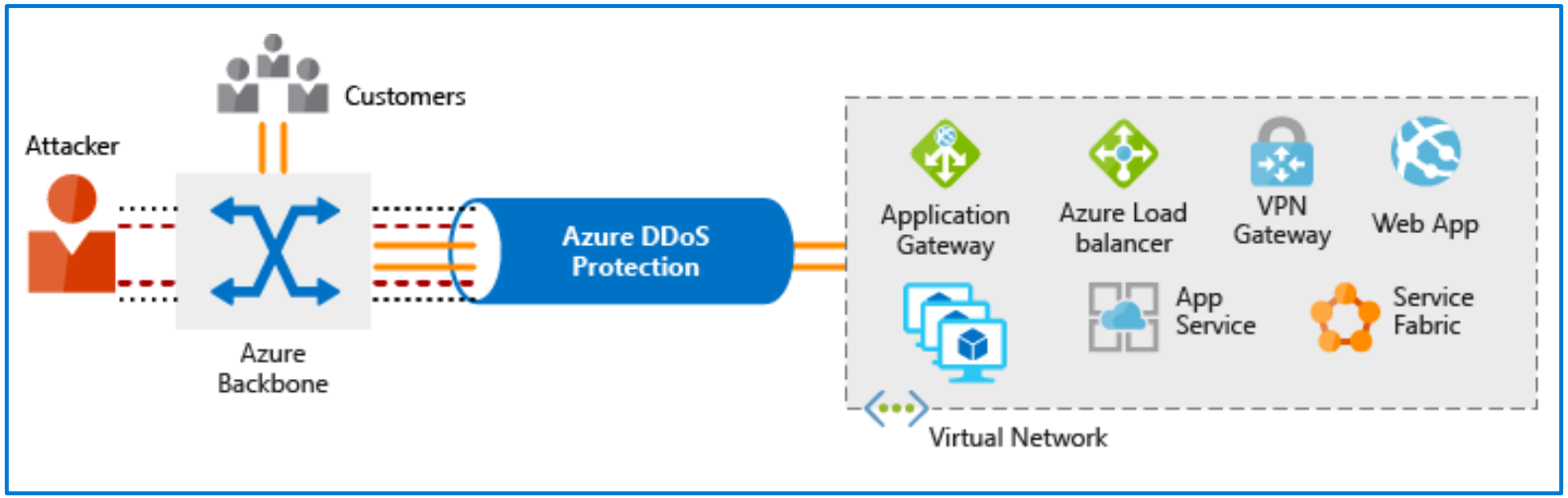
Azure DDoS protection

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:

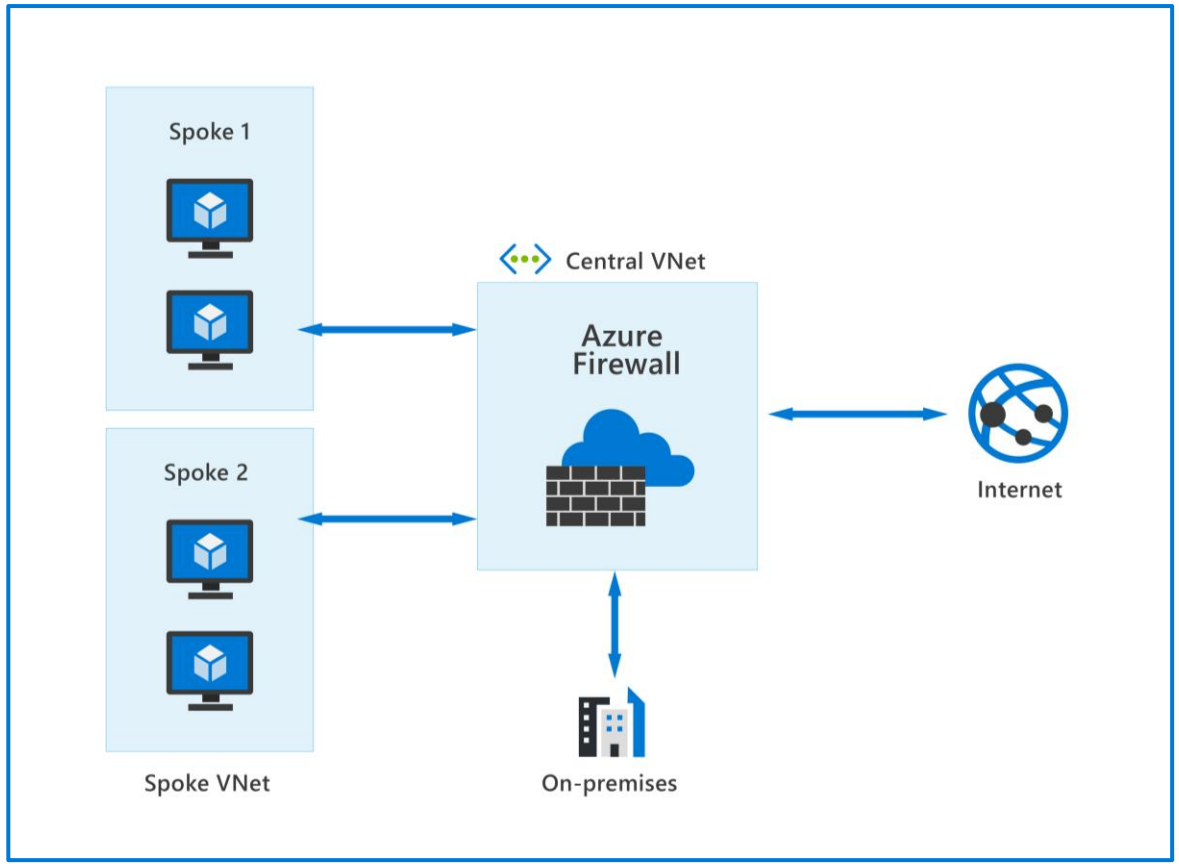
- Basic
- Standard



Azure Firewall

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

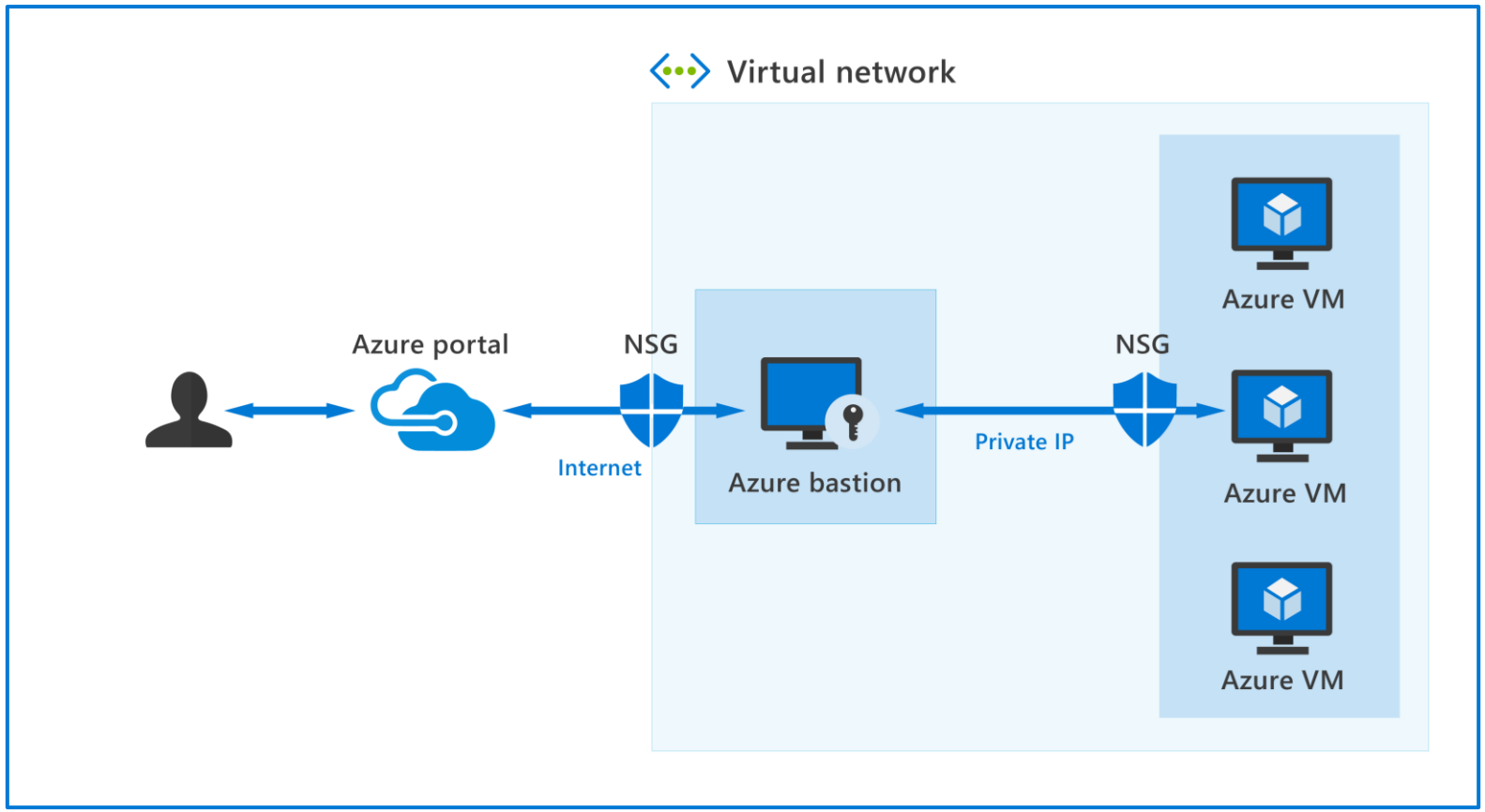
- Built-in high availability & Availability Zones
- Outbound SNAT & inbound DNAT
- Threat intelligence
- Network & application-level filtering
- Multiple public IP addresses
- Integration with Azure Monitor



Azure Bastion

Azure Bastion provides secure connectivity to your VMs directly from the Azure portal using Transport Layer Security (TLS). Features include:

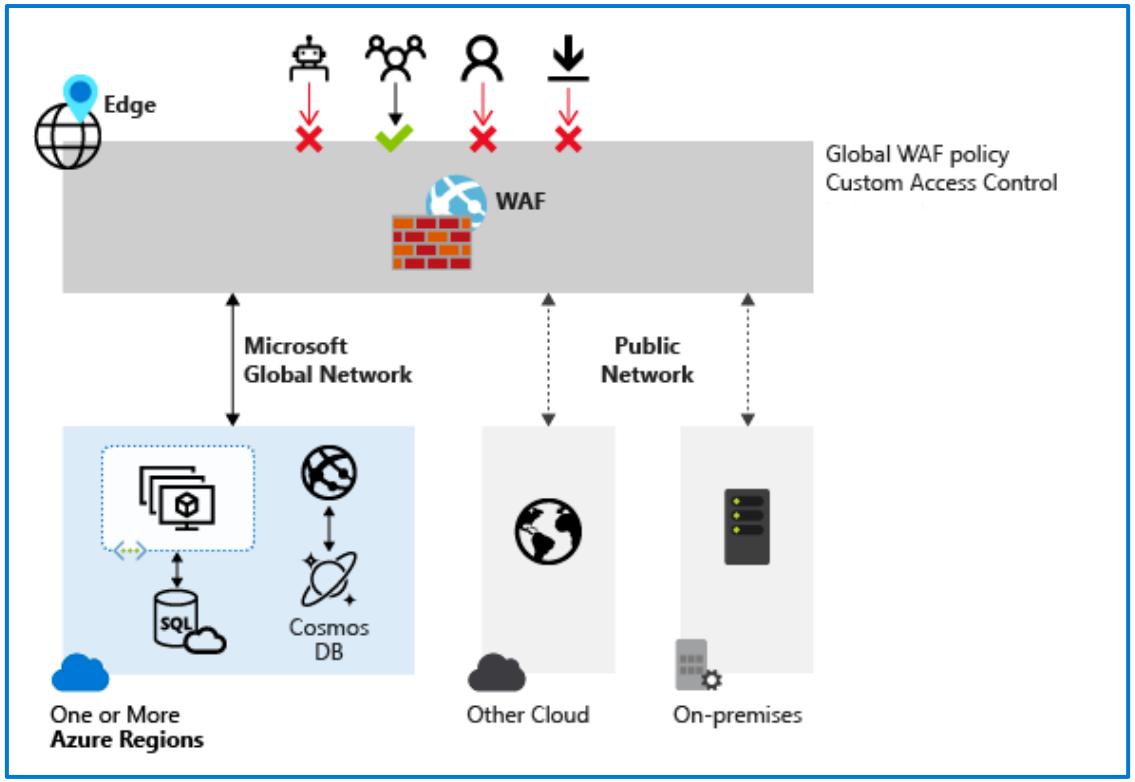
- RDP and SSH directly in Azure portal.
- Remote session over TLS and firewall traversal for RDP/SSH.
- No Public IP required on the Azure VM.
- No hassle of managing NSGs.
- Protection against port scanning.
- Protect against zero-day exploits.



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.



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?

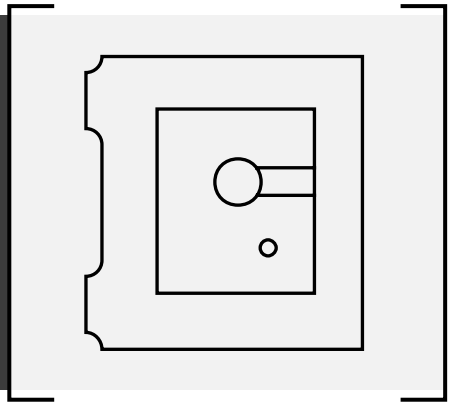
Secrets management

Key management

Certificate management

Store secrets backed by HW or SW

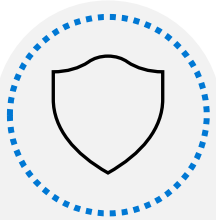
Lesson 2: Describe security management capabilities of Azure



Lesson 2 Introduction

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

Describe the security management capabilities of Azure.



Describe the benefits and use cases of Azure Defender.

Understand Cloud Security Posture Management and the security baseline.

Cloud security posture management

Cloud security posture management (CSPM), tools designed to improve your cloud security management.

CSPM uses a combination of tools & services:

- Zero Trust-based access control
- Real-time risk scoring
- Threat and vulnerability management (TVM)
- Discover sharing risks
- Technical policy
- Threat modeling systems & architectures

CSPM can be useful to many teams:

- Threat intelligence team
- Information technology
- Compliance & risk management teams
- Business leaders and SMEs
- Security architecture and operations
- Audit team

Azure Security Center

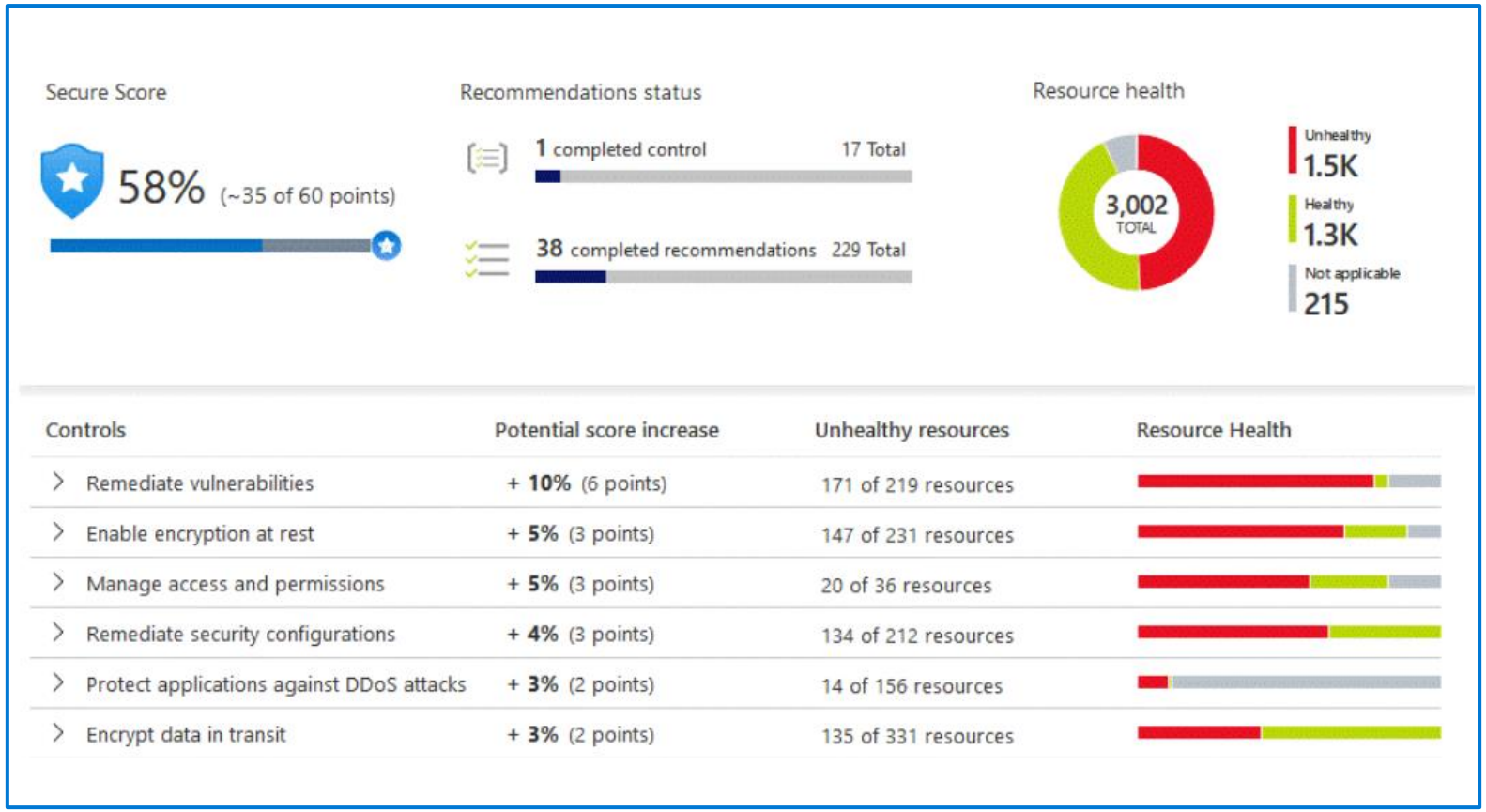
Strengthen security posture across your machines, data services, and applications.

Continuous assessment – ordered list of recommendations of what needs to be fixed for maximum protection.

Protect against threats - Detect and prevent threats on IaaS, non-Azure servers, and PaaS.

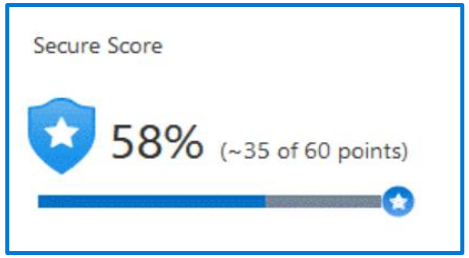
Network map - topology view of your workloads, so you can see if each node is properly configured.

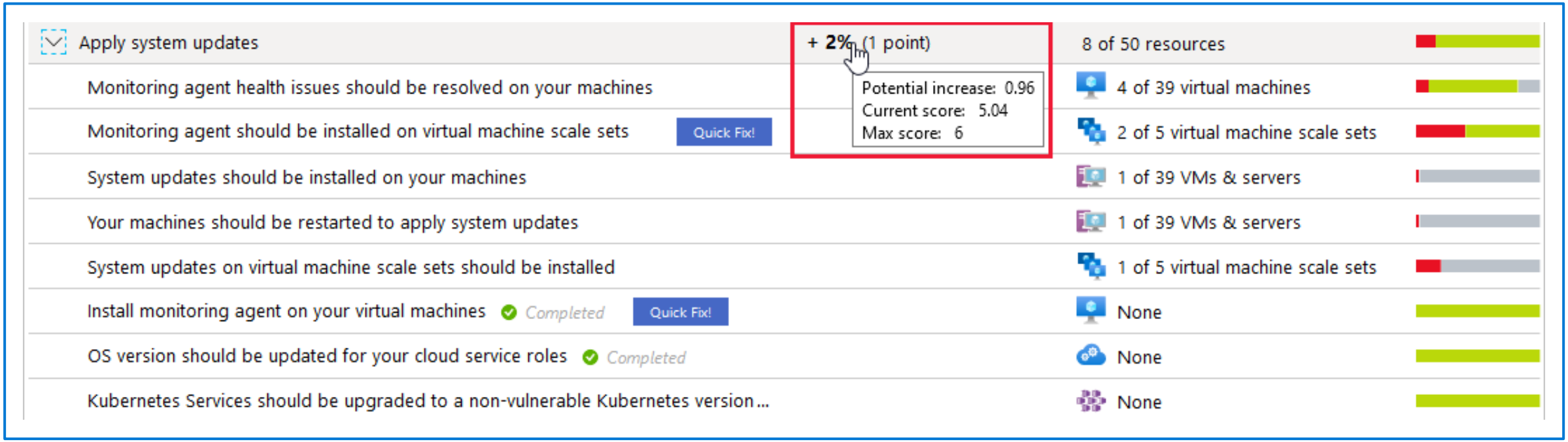
Get secure faster - Integration with other Microsoft security solutions for complete security across all your Azure resources.



Azure Secure Score

The secure score is shown in the Azure portal pages as a percentage value. To improve your secure score, remediate security recommendations from your recommendations list.





Azure Defender

Scope of Azure Defender

Servers

App Service

Storage

SQL

Kubernetes

Container registries

Key Vault

Hybrid cloud protection

Protect your non-Azure servers.

Protect your virtual machines in other clouds (such as AWS and GCP).

Azure Defender alerts

Advanced protection

Vulnerability assessment

Security baselines & the Azure Security Benchmark

Security baselines for Azure offer a consistent experience when securing your environment. They apply prescriptive best practices and recommendations from the Azure Security Benchmark (ASB) to improve the security of workloads, data, and services on Azure. Each recommendation includes the following information:

Azure ID: The Azure Security Benchmark ID that corresponds to the recommendation.

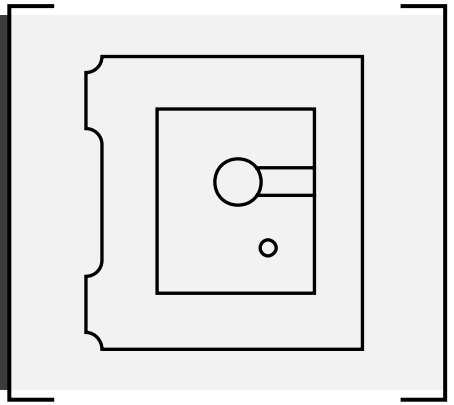
Recommendation: The recommendation provides a high-level description of the control.

Guidance: The rationale for the recommendation and links to guidance on how to implement it.

Responsibility: Who is responsible for implementing the control?

Azure Security Center monitoring: Does Azure Security Center monitor the control?

Lesson 3: Describe security capabilities of Azure Sentinel

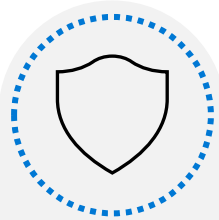


Lesson 3 Introduction

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

Describe the security concepts for SIEM, SOAR, and XDR.

Describe how Azure Sentinel provides integrated threat protection.



Describe the capabilities of Azure Sentinel.

SIEM, SOAR, and XDR

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.

What is extended detection and response?

An XDR system is designed to deliver intelligent, automated, and integrated security across an organization's domain. It helps prevent, detect, and respond to threats across identities, endpoints, applications, email, IoT, infrastructure, and cloud platforms.

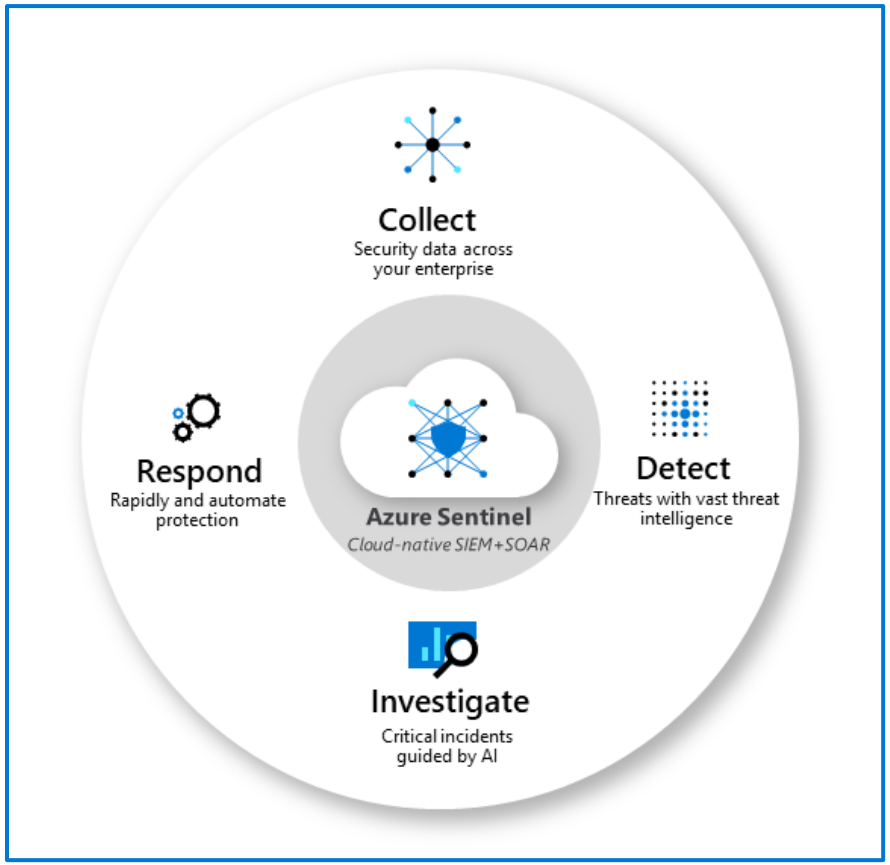
Sentinel provides integrated threat protection (Slide 1)

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.



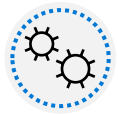
Sentinel provides integrated threat protection (Slide 2)

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

Workbooks: monitor the data using the Azure 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 Azure Logic Apps, to create workflows

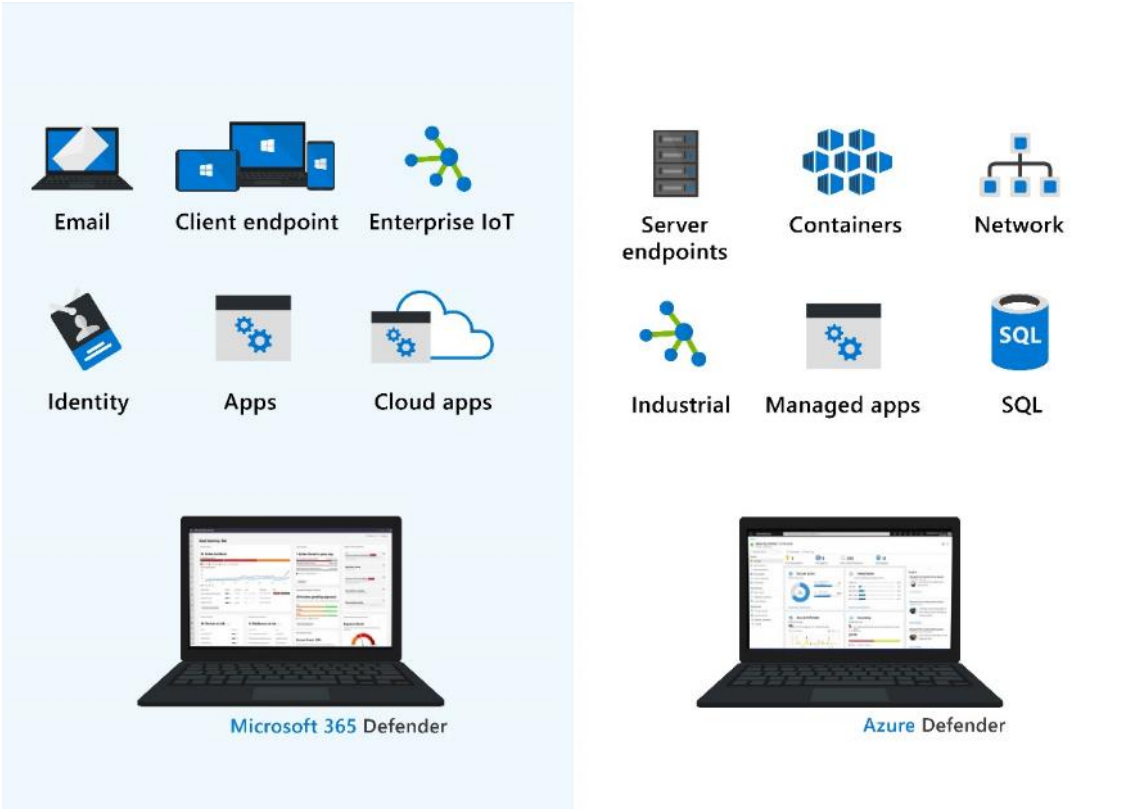
Playbooks: A collection of procedures that can help automate and orchestrate your response.

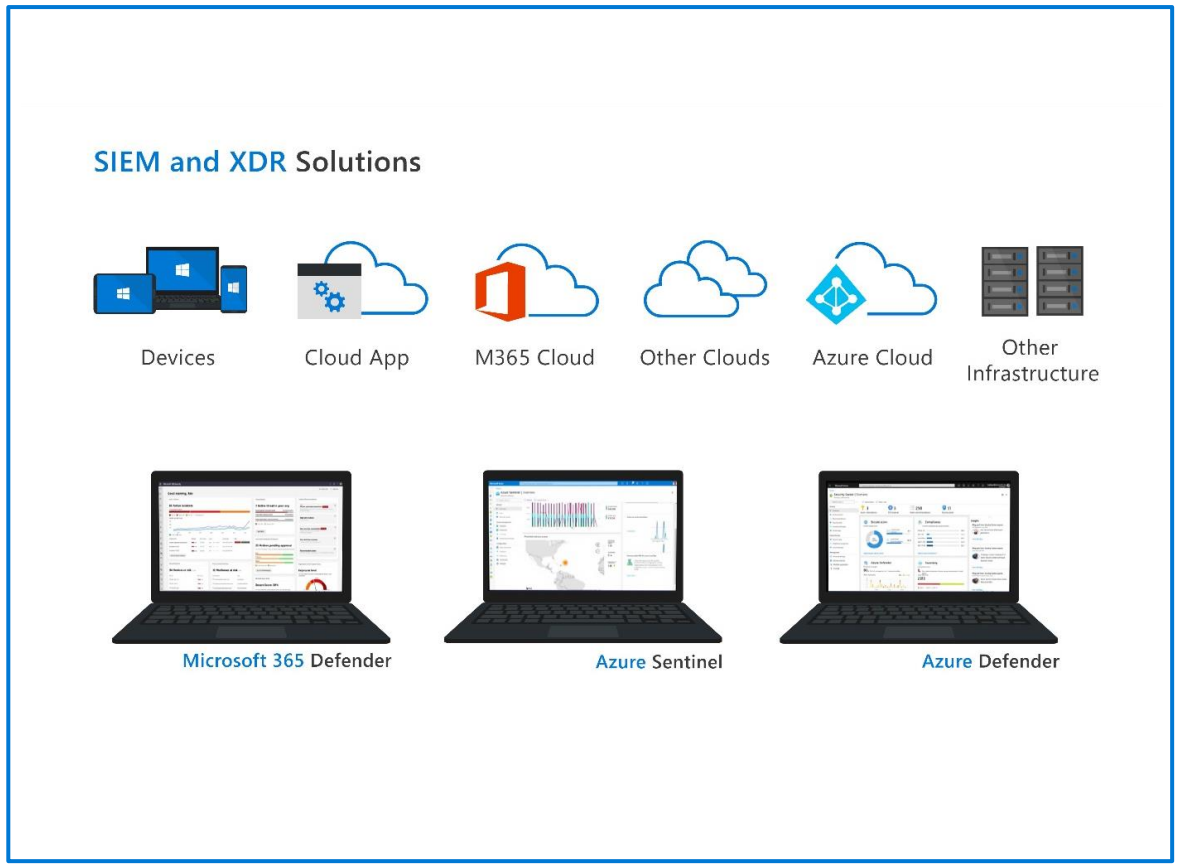
Investigation: Understand the scope of a potential security threat and find the root cause.

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

Integrated threat protection: XDR with Microsoft 365 Defender and Azure Defender integration.

Sentinel provides integrated threat protection (Slide 3)





Module Summary

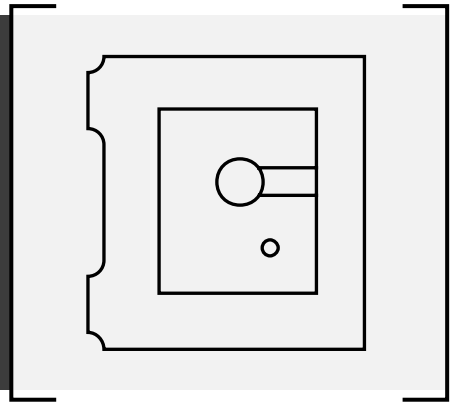
In this module, you have:

- Learned about basic security capabilities in Azure, including NSGs, DDoS, Bastion, and more.
- Learned about security management capabilities of Azure, including Azure Security Center and Secure Score
- Learned about SIEM, SOAR and the security capabilities of Azure Sentinel

Microsoft

Describe the capabilities of Microsoft compliance solutions

Lesson 1: Describe the compliance management capabilities in Microsoft



Lesson 1 Introduction

After completing this module, you should be able to:

- Describe the benefit of the Service Trust Portal.
- Describe Microsoft's privacy principles.
- Explore the Microsoft 365 compliance center.
- Describe the benefits of Compliance Manager.

Common compliance needs

Several measures to protect data:

Granting individuals the right to access their data at any time.

Granting individuals the right to correct or delete data about them if needed.

Introducing minimum or maximum retention periods for data.

Enabling governments and regulatory agencies the right to access and examine data when necessary.

Defining rules for what data can be processed and how that should be done.

Service Trust Portal

The Service Trust Portal provides:

- Information
- Tools
- Other resources about Microsoft security, privacy, and compliance practices.

You can access below offerings:

- Service Trust Portal
- Compliance Manager
- Trust Documents
- Industries & Regions
- Trust Center
- Resources
- My Library

Microsoft's privacy principles

Control: Putting you, the customer, in control of your privacy with easy-to-use tools and clear choices.

Transparency: Being transparent about data collection and use so that everyone can make informed decisions.

Security: Protecting the data that's entrusted to Microsoft by using strong security and encryption.

Strong legal protections: Respecting local privacy laws and fighting for legal protection of privacy as a fundamental human right.

No content-based targeting: Not using email, chat, files, or other personal content to target advertising.

Benefits to you: When Microsoft does collect data, it's used to benefit you, the customer, and to make your experiences better.

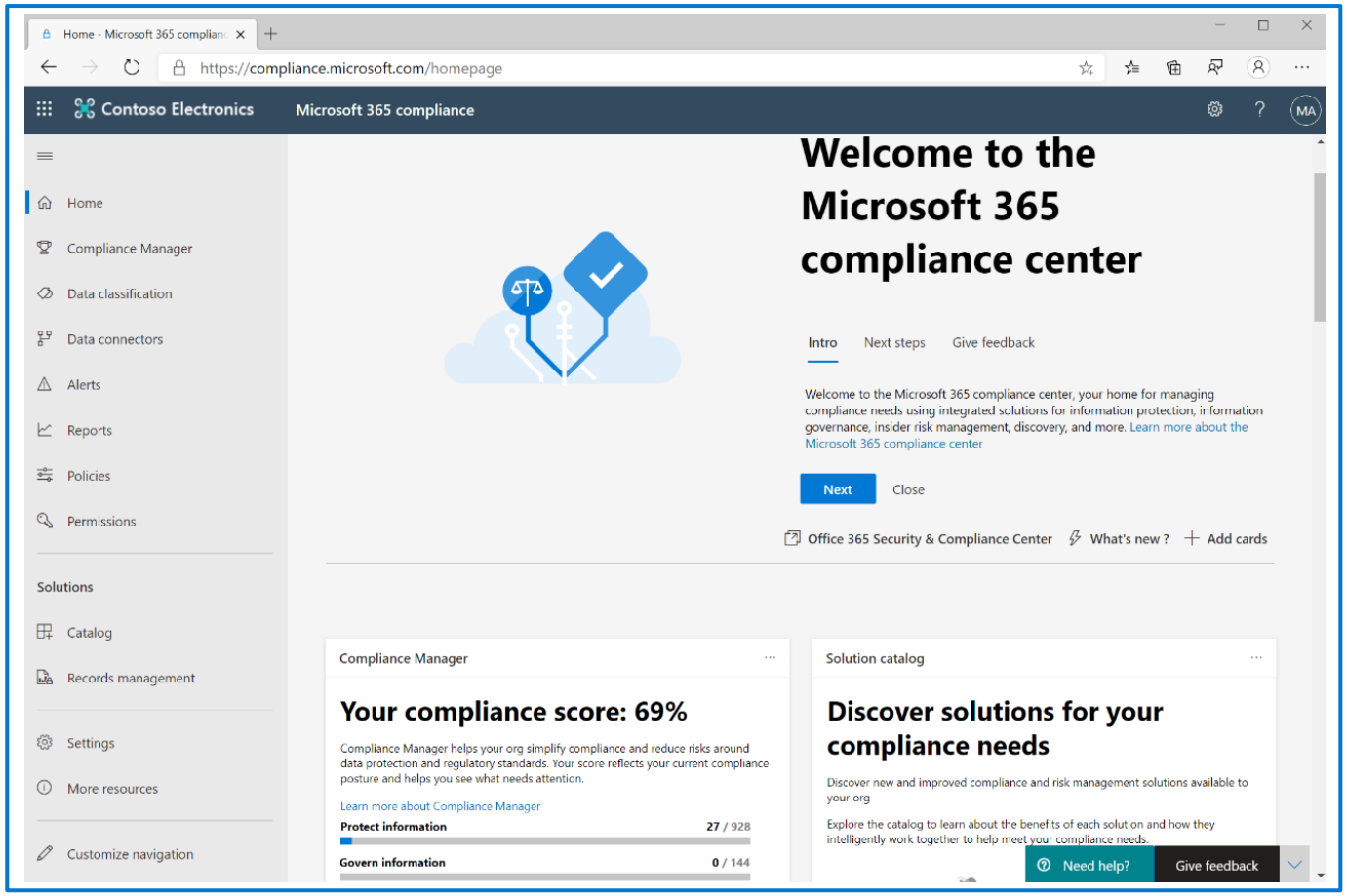
Microsoft 365 Compliance Center

Microsoft 365 Compliance center portal

- A view of how the organization is meeting its compliance requirements
- Solutions that can be used to help with compliance
- Information about active alerts
- And more…

Navigation

- Access to alerts, reports, policies, compliance solutions, and more.
- Add or remove options for a customized navigation pane.
- Customize navigation control.



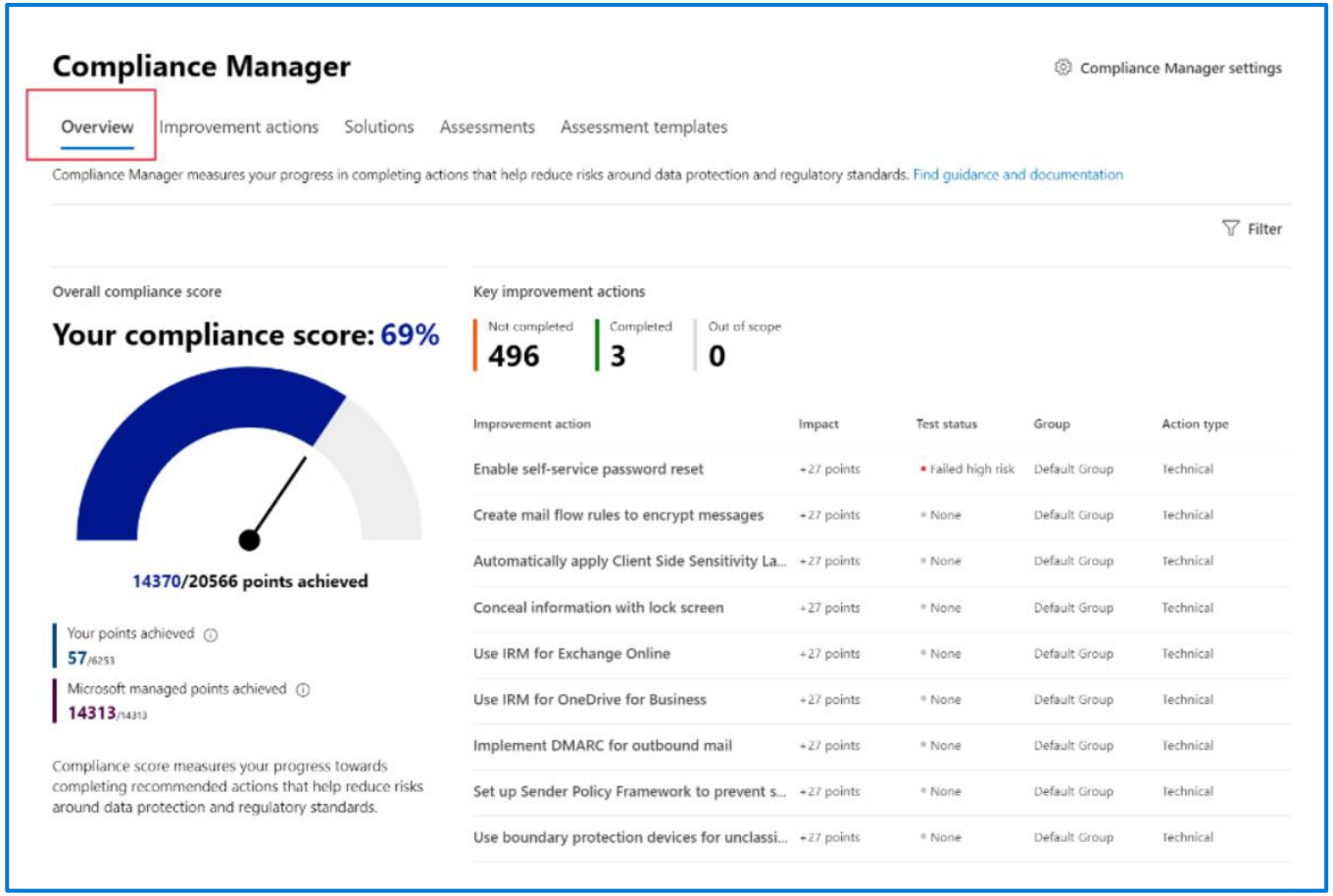
Compliance Manager

Compliance Manager simplifies compliance and reduces risk by providing:

- Prebuilt assessments based on common standards
- Workflow capabilities to complete risk assessments
- Step-by-step improvement actions
- Compliance score, shows overall compliance posture

Key elements of Compliance Manager

- Controls
- Assessments
- Templates
- Improvement actions



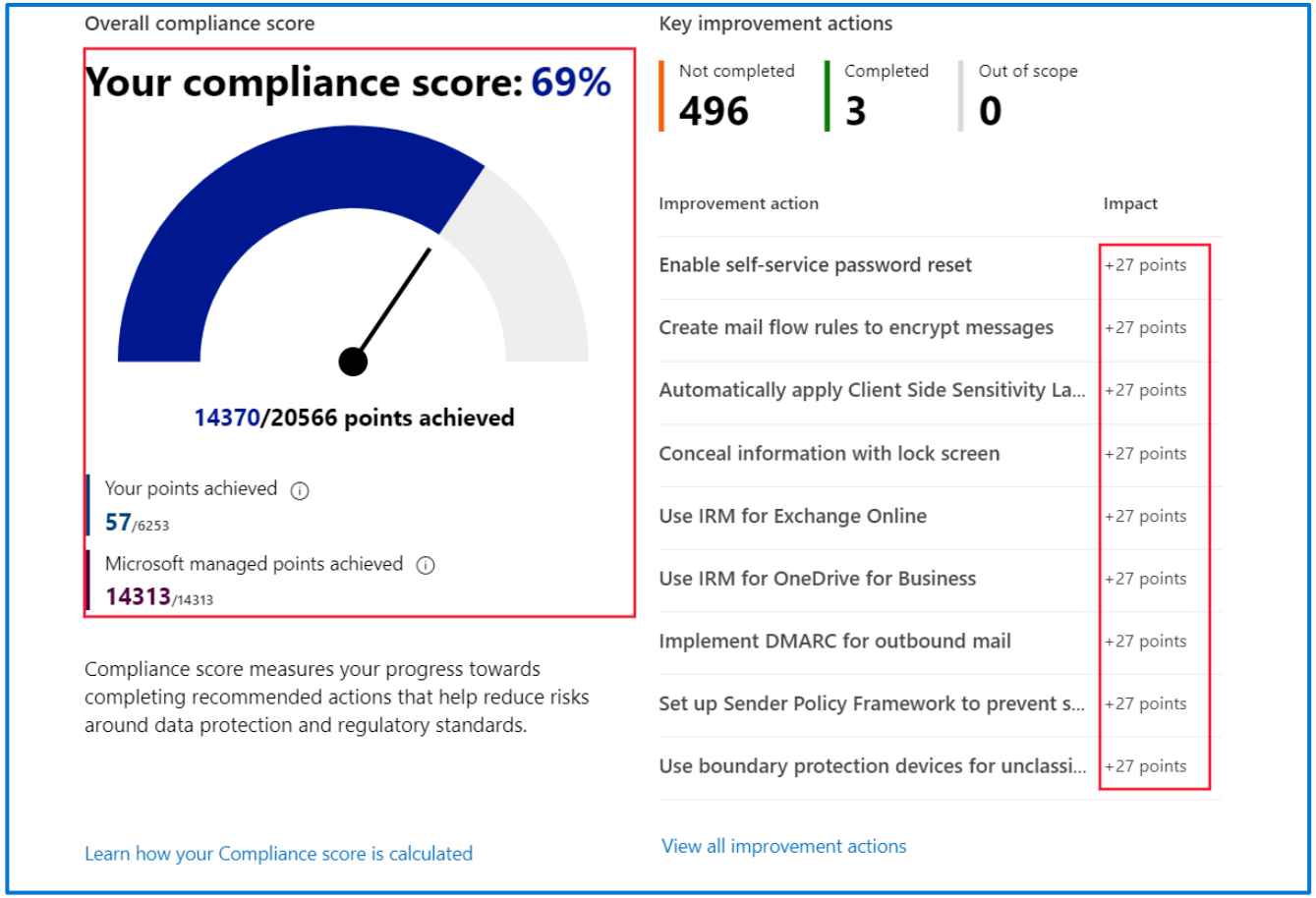
Compliance score

Benefits of compliance score:

- Help an organization understand its current compliance posture.
- Help prioritize actions based on their potential to reduce risk.

Understand your compliance score

- Actions
  - Your improved actions
  - Microsoft actions
- Action types (& action subcategory)
  - Mandatory (preventive, detective, or corrective)
  - Discretionary (preventive, detective, or corrective)

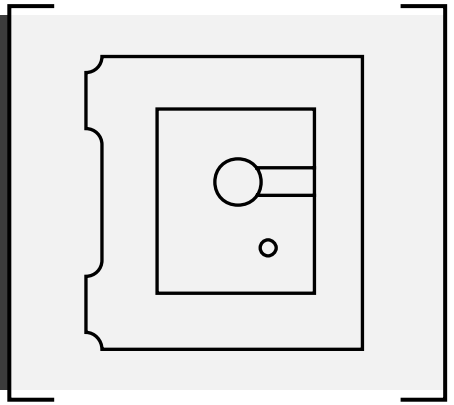


Microsoft Security

Demo

Microsoft 365 Compliance Center

Lesson 2: Describe information protection and governance capabilities of Microsoft 365



Lesson 2 Introduction

After completing this module, you should be able to:

- Describe data classification capabilities.
- Describe records management.
- Describe data loss prevention.

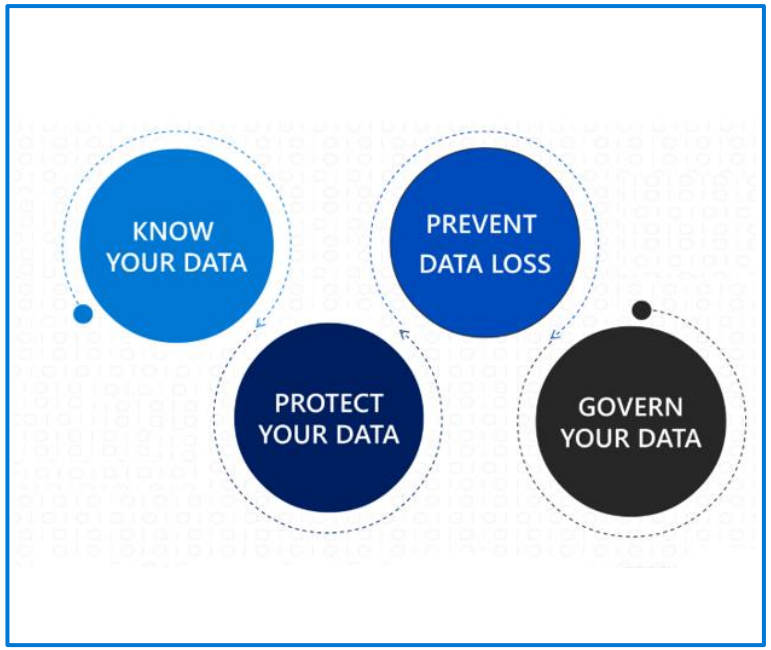
Know your data, protect your data, and govern your data

Know your data: Understand your data landscape and identify important data across on-premises, cloud, and hybrid environments.

Protect your data: Apply flexible protection actions including encryption, access restrictions, and visual markings.

Prevent data loss: Detect risky behavior and prevent accidental oversharing of sensitive information.

Govern your data: Automatically keep, delete, and store data and records in a compliant manner.



Data classification capabilities in the Microsoft 365 Compliance Center

Sensitive information types.

Trainable classifiers: Pre-trained classifiers and Custom trainable classifiers.

Understand and explore the data.

The content explorer: It enables administrators to gain visibility into the content that has been summarized in the overview pane.

The activity explorer: It can monitor what's being done with labeled content across the organization.

Sensitivity labels and policies

Sensitivity labels

Labels are:

- Customizable
- Clear text
- Persistent

Usage:

- Encrypt email and documents.
- Mark the content.
- Apply the label automatically.
- Protect content in containers: sites and groups.
- Extend sensitivity labels to third-party apps and services.
- Classify content without using any protection settings.

Label policies

Policies enable admins to:

- Choose the users and groups that can see labels
- Apply a default label to all new emails and documents
- Require justifications for label changes
- Require users to apply a label (mandatory labeling)
- Link users to custom help pages

Once a sensitivity label is applied to an email or document, any configured protection settings for that label are enforced on the content.

Microsoft Security

Demo

Sensitivity labels

Describe data loss prevention (DLP)

DLP protects sensitive information and prevents its inadvertent disclosure.

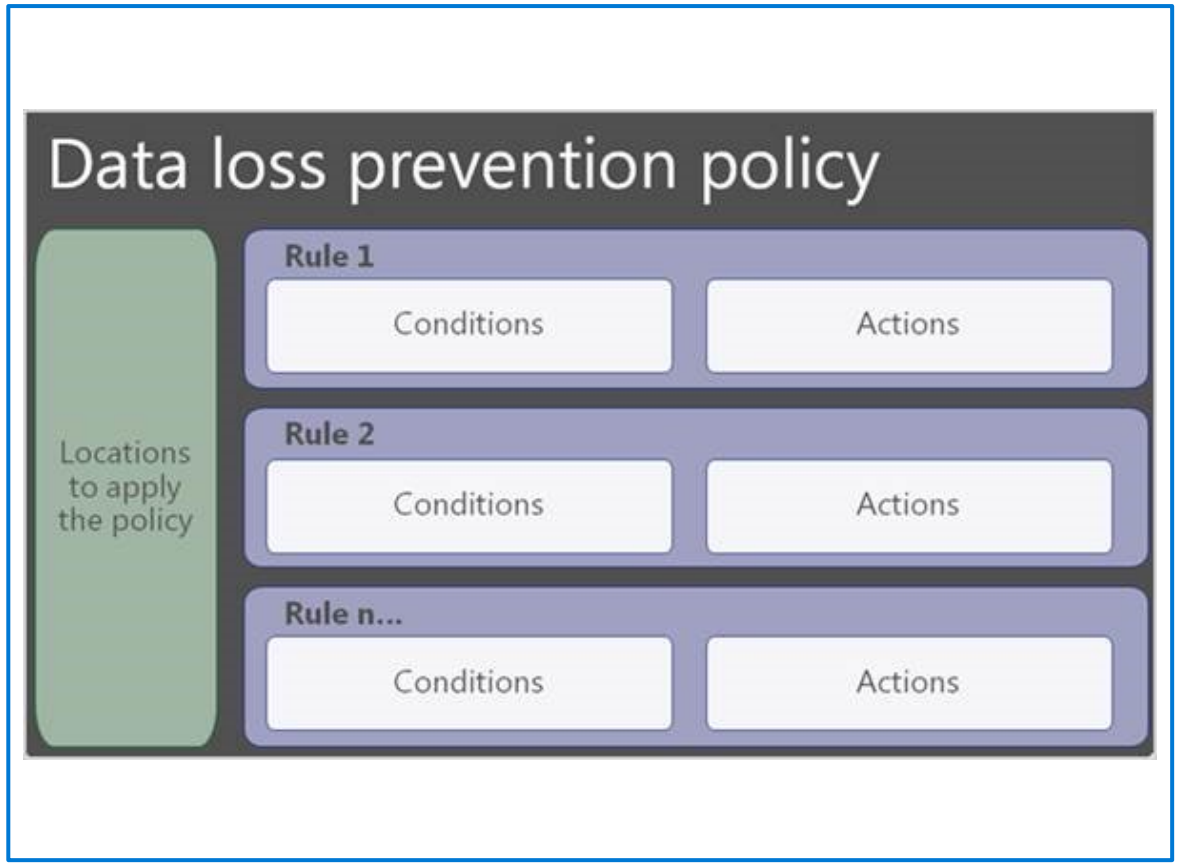
- DPL policies protect information by identifying and automatically protecting sensitive data.
- Protect sensitive information across Microsoft 365 – OneDrive for Business, SharePoint Online, Exchange Online and Microsoft Teams

Endpoint Data Loss Prevention

- DLP extended to Windows 10 devices.
- Audit and manage activities including creating, coping, printing, & renaming items

Data Loss Prevention in Microsoft Teams

- DPL capabilities extended to Microsoft Teams chat and channel message.



Retention polices and labels

Retention settings work with SharePoint, OneDrive, Teams, Yammer and Exchange and help organizations manage and govern information by ensuring content is kept only for a required time, and then permanently deleted.

Retention policies:

- Are applied at site or mailbox level,
- Can be applied to multiple locations or specific locations or users.
- Items inherit the retention settings from their container.
- If an item is moved, the retention setting does not travel to the new location.

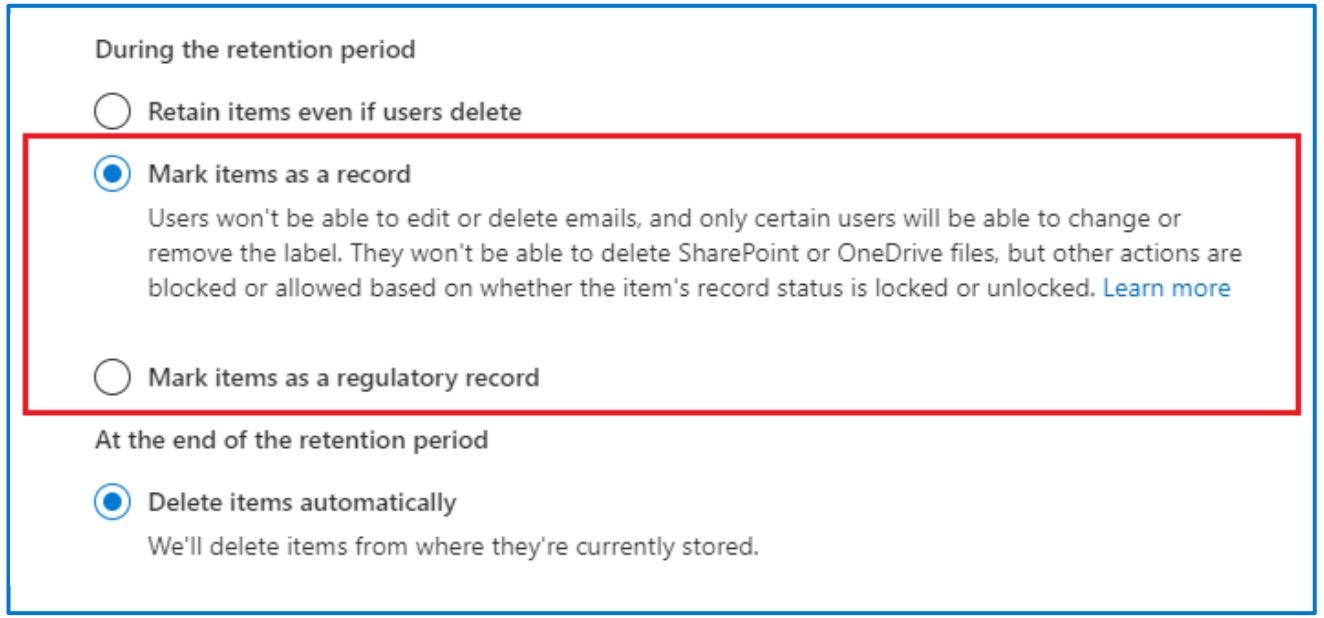
Retention labels:

- Are applied at an item level.
- Emails and documents can have only a single retention label assigned to it at a time.
- Retention settings from retention labels travel with the content in your Microsoft 365 tenant.
- Can be applied manually or automatically.
- Retention labels support disposition review of the content before it's permanently deleted.

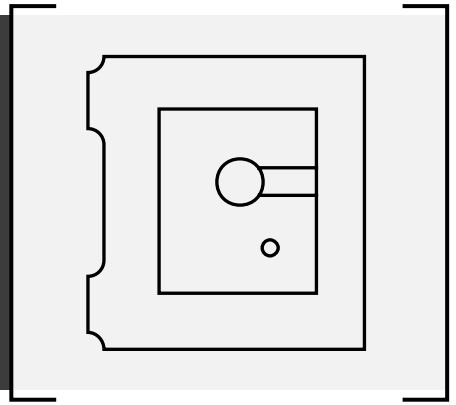
Records management

Records management in Microsoft 365 helps an organization look after their legal obligations and helps to demonstrate compliance with regulations.

- When content is labeled as a record, the following happens:
  - Restrictions are put in place to block certain activities.
  - Activities are logged.
  - Proof of disposition is kept at the end of the retention period.
- To enable items to be marked as records, an administrator sets up retention labels.



Lesson 3: Describe insider risk capabilities in Microsoft 365



Lesson 3 Introduction

After completing this module, you should be able to:

- Describe how Microsoft 365 can help organizations identify insider risks and take appropriate action.

Insider risk solutions in Microsoft 365 (Slide 1)

Insider risk management helps minimize internal risks by enabling you to detect, investigate, and act on malicious and inadvertent activities in your organization.

Communication compliance helps minimize communication risks by helping you detect, capture, and act on inappropriate messages in your organization. Supported services: Microsoft Teams, Exchange Online, Yammer, & 3rd party communications in an org.

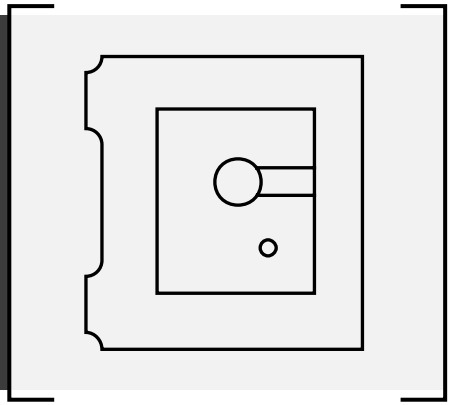
Information barriers allow you to restrict communication and collaboration between two internal groups to avoid a conflict of interest from occurring in your organization. Supported in Microsoft Teams, OneDrive for Business, SharePoint Online, and more.

Insider risk solutions in Microsoft 365 (Slide 2)

Privileged access management allows granular access control over privileged Exchange Online admin tasks in Office 365.

Customer Lockbox ensures that Microsoft cannot access customer content to perform a service operation without the customer's explicit approval. Supported services: Exchange Online, SharePoint Online, OneDrive for Business.

Lesson 4: Describe eDiscovery & audit capabilities in Microsoft 365



Lesson 4 Introduction

After completing this module, you should be able to:

- Describe the purpose of eDiscovery & the capabilities of the content search tool.
- Describe the core & advanced eDiscovery workflows.
- Describe the core and advanced audit capabilities of Microsoft 365.

eDiscovery & content search

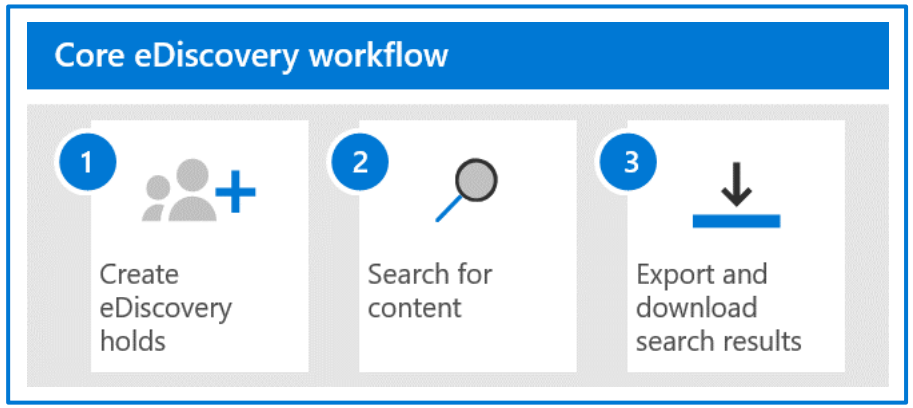
Purpose of eDiscovery

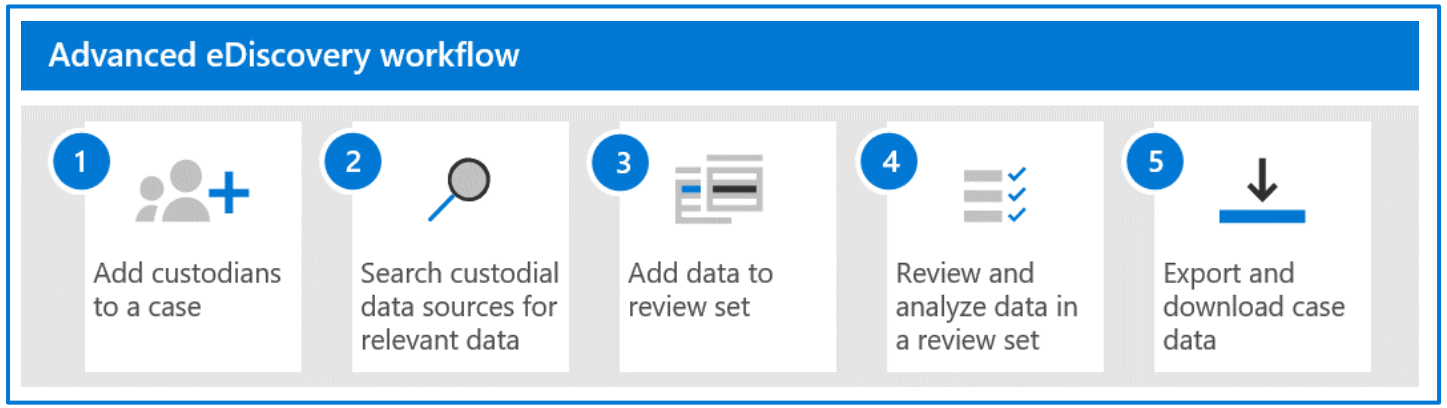
- Find electronic information to be used as evidence when a company is involved in litigation..
- Search for content in Exchange Online mailboxes, Microsoft 365 Groups, Microsoft Teams, SharePoint Online and OneDrive for Business sites, Skype for Business conversations, and Yammer teams.
- Use to identify, hold, and export content found in mailboxes and sites.

Content Search

- Search Exchange Online mailboxes, SharePoint Online sites, OneDrive for Business, Teams, Microsoft 365 groups, Yammer groups
- Build search queries and use conditions
- Create, report on, and delete multiple searches
- View keyword statistics
- Search for third-party data
- PowerShell scripts for more complex search related tasks

Core and advanced eDiscovery workflows





Core eDiscovery

1. Create a hold to preserve content that might be relevant to the case (mailboxes, sites, and public folders).
2. Create and run searches for content that relates to the case.
3. Export and download search results.

Advanced eDiscovery builds on core eDiscovery

1. Add persons of interest (custodians) and data sources that aren't associated with a specific user.
2. Use the built-in collections tool to search data sources for content relevant to the case.
3. Data added to a review set are copied from their original location to a secure Azure Storage location. The data is reindexed again to optimize for fast searches
4. Use a wide-variety of tools and capabilities to view and analyze the case data with goal of reducing the data set to what is most relevant to the case
5. Export and download case data

Audit capabilities of Microsoft 365

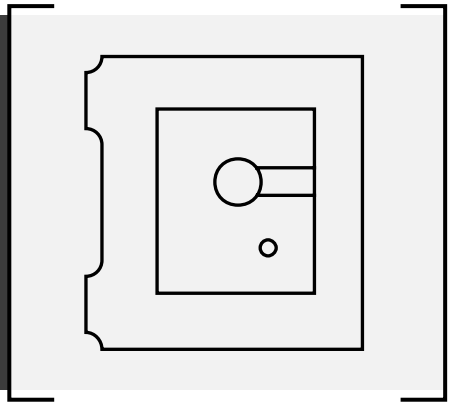
Core Audit

- Allows organizations to view user and administrator activity.
- An audited activity generates an audit record that is stored in the audit log.
- Searching the audit log requires the search capability to be turned on and assigned the appropriate role.
- The results can be filtered and exported to a CSV file.

Advanced Audit - Core Audit, plus:

- Long-term retention of audit logs
- High-bandwidth access to Office 365 Management Activity API
- Access to crucial events for investigations
  - MailItemsAccessed
  - Send
  - SearchQueryInitiatedExchange
  - SearchQueryInitiatedSharePoint

Lesson 5: Describe resource governance capabilities in Azure



Lesson 5 Introduction

After completing this module, you should be able to:

- Describe some of the resource governance capabilities in Azure.

Azure Resource Manager locks

Azure Resource Manager locks

- Prevent resources from being accidentally deleted or changed.
- Apply a lock at a parent scope, all resources within that scope inherit that lock.
- Apply only to operations that happen in the management plane.
- Changes to the actual resource are restricted, but resource operations aren't restricted.

A lock level

- CanNotDelete
- ReadOnly

Azure Blueprints

- Azure Blueprints provide a way to define a repeatable set of Azure resources.
- Rapidly provision environments, that are in line with the organization's compliance requirements.
- Provision Azure resources across several subscriptions simultaneously for quicker delivery.
- Declarative way to orchestrate the deployment of various resource templates and artifacts, including:
  - Role Assignments
  - Policy Assignments
  - Azure Resource Manager templates (ARM templates)
  - Resource Groups
- Blueprint objects are replicated to multiple Azure regions.
- The relationship between the blueprint definition and the blueprint assignment is preserved.

Azure Policy

Function:

- Azure Policy is designed to help enforce standards and assess compliance across your organization.
- Through its compliance dashboard, you can access an aggregated view to help evaluate the overall state of the environment.
- Common use cases for Azure Policy include implementing governance for resource consistency, regulatory compliance, security, cost, and management.
- Azure Policy evaluates all resources in Azure and Arc enabled resources (specific resource types hosted outside of Azure).

The following can trigger a policy evaluation:

- A resource has been created, deleted, or updated in scope with a policy assignment.
- A policy or an initiative is newly assigned to a scope.
- A policy or an initiative that's been assigned to a scope is updated.
- The standard compliance evaluation cycle (happens once every 24 hours).

Example responses to non-compliant resources:

- Deny a change to a resource.
- Log changes to a resource.
- Alter a resource before or after a change.
- Deploy related compliant resources.

Microsoft Security

Demo

Azure policy

Module Summary

In this lesson, you have:

- Learned about the compliance management capabilities in Microsoft, including the Service Trust Portal, Microsoft 365 compliance center, Microsoft privacy principles, and more.
- Learned about the information protection and governance capabilities of Microsoft 365, including sensitivity & retention labels, DLP, and more.
- Learned about insider risk capabilities in Microsoft 365
- Learned about eDiscovery & audit capabilities of Microsoft 365
- Describe resource governance capabilities in Azure, including Azure policy, resource locks, Blueprints, and more.

Microsoft Security