

# Microsoft Security Virtual Training



Technology partner to organizations worldwide



# Table of Contents

- Security, Compliance & Identity
- Microsoft Identity and Access Management Solutions
- Microsoft Security Solutions

# Security

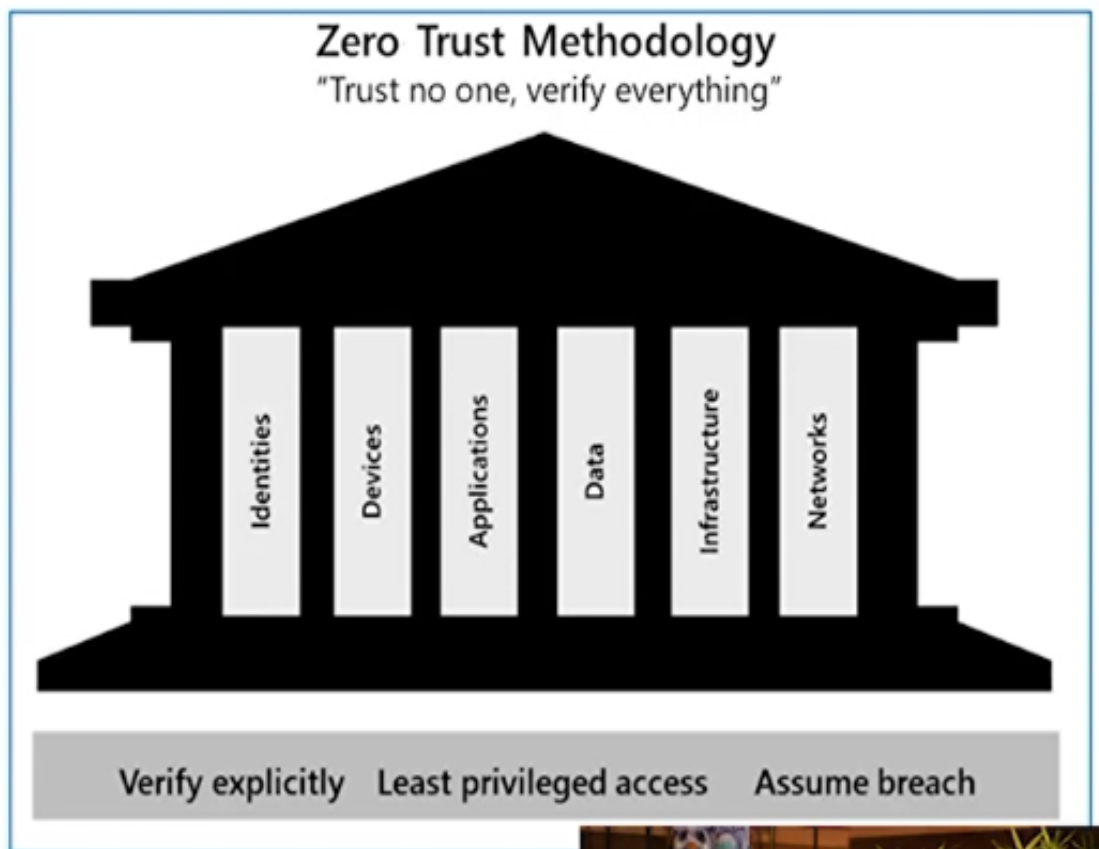
## Zero-trust methodology

### 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.
- **Networks** should be segmented.
- **Infrastructure** whether on-premises or cloud based, represents a threat vector.
- **Data** should be classified, labeled, and encrypted based on its attributes.

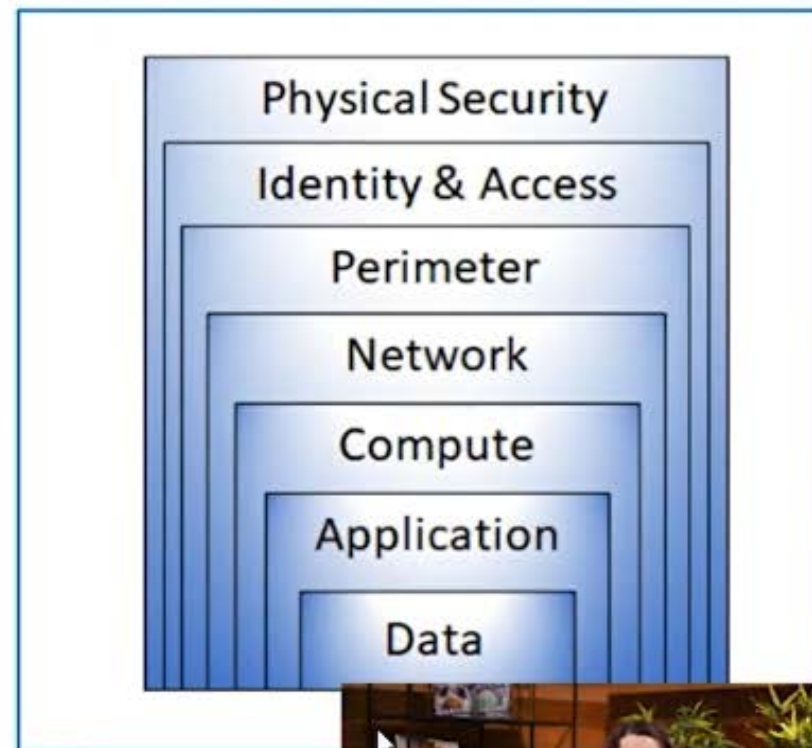


# Security

## 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.





# Security

## 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)

Shared responsibility model

Responsibility	SaaS	PaaS	IaaS	On-Prem	
Information and data	Customer	Customer	Customer	Customer	RESPONSIBILITY ALWAYS RETAINED BY CUSTOMER
Devices (Mobile and PCs)	Customer	Customer	Customer	Customer	
Accounts and identities	Customer	Customer	Customer	Customer	
Identity and directory infrastructure	Microsoft	Customer	Customer	Customer	RESPONSIBILITY VARIES BY SERVICE TYPE
Applications	Microsoft	Customer	Customer	Customer	
Network controls	Microsoft	Customer	Customer	Customer	
Operating system	Microsoft	Microsoft	Customer	Customer	RESPONSIBILITY TRANSFERS TO CLOUD PROVIDERS
Physical hosts	Microsoft	Microsoft	Microsoft	Customer	
Physical network	Microsoft	Microsoft	Microsoft	Customer	
Physical datacenter	Microsoft	Microsoft	Microsoft	Customer	

■ Microsoft ■ Customer



# Security

## 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.



# Security

## 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.

# Security

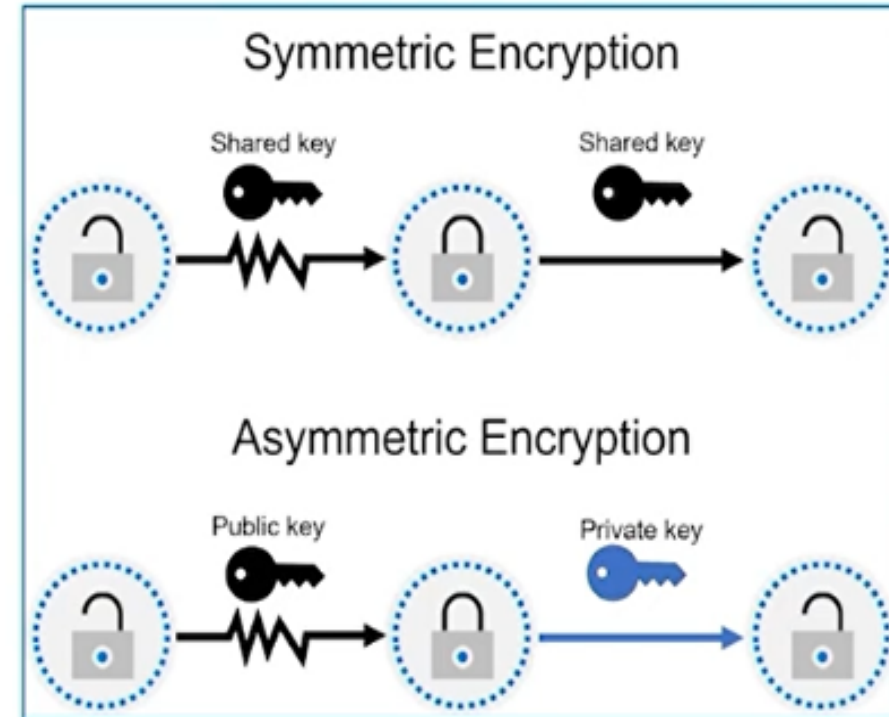
## Encryption

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



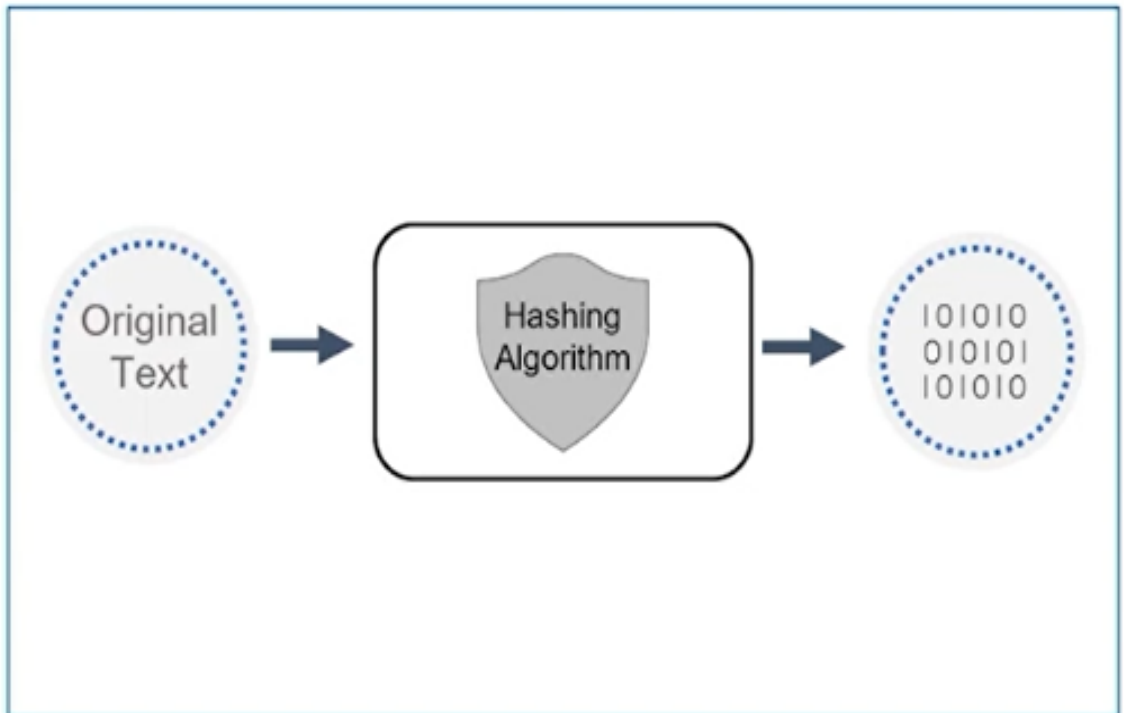


# Security

## 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.

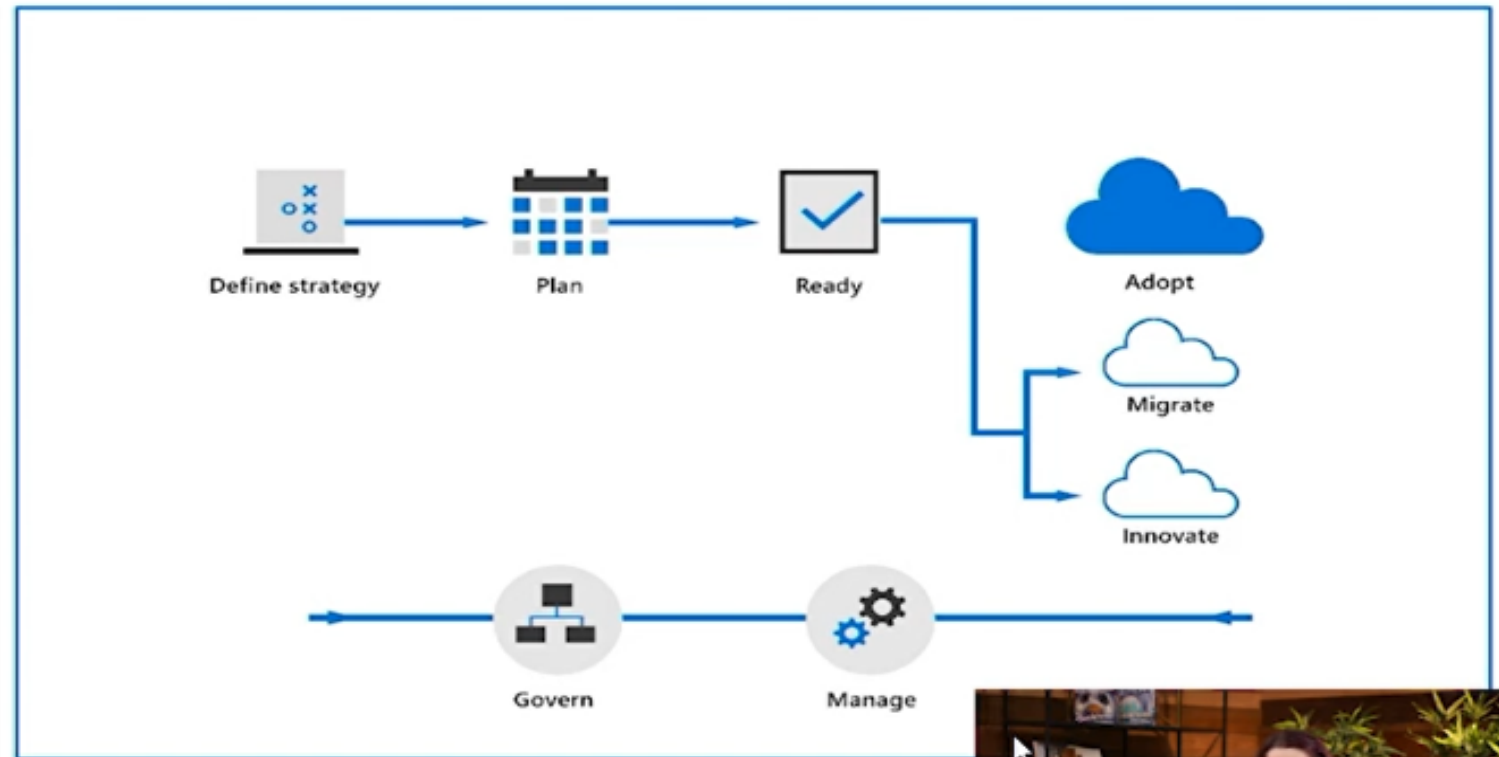


# Security

## 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

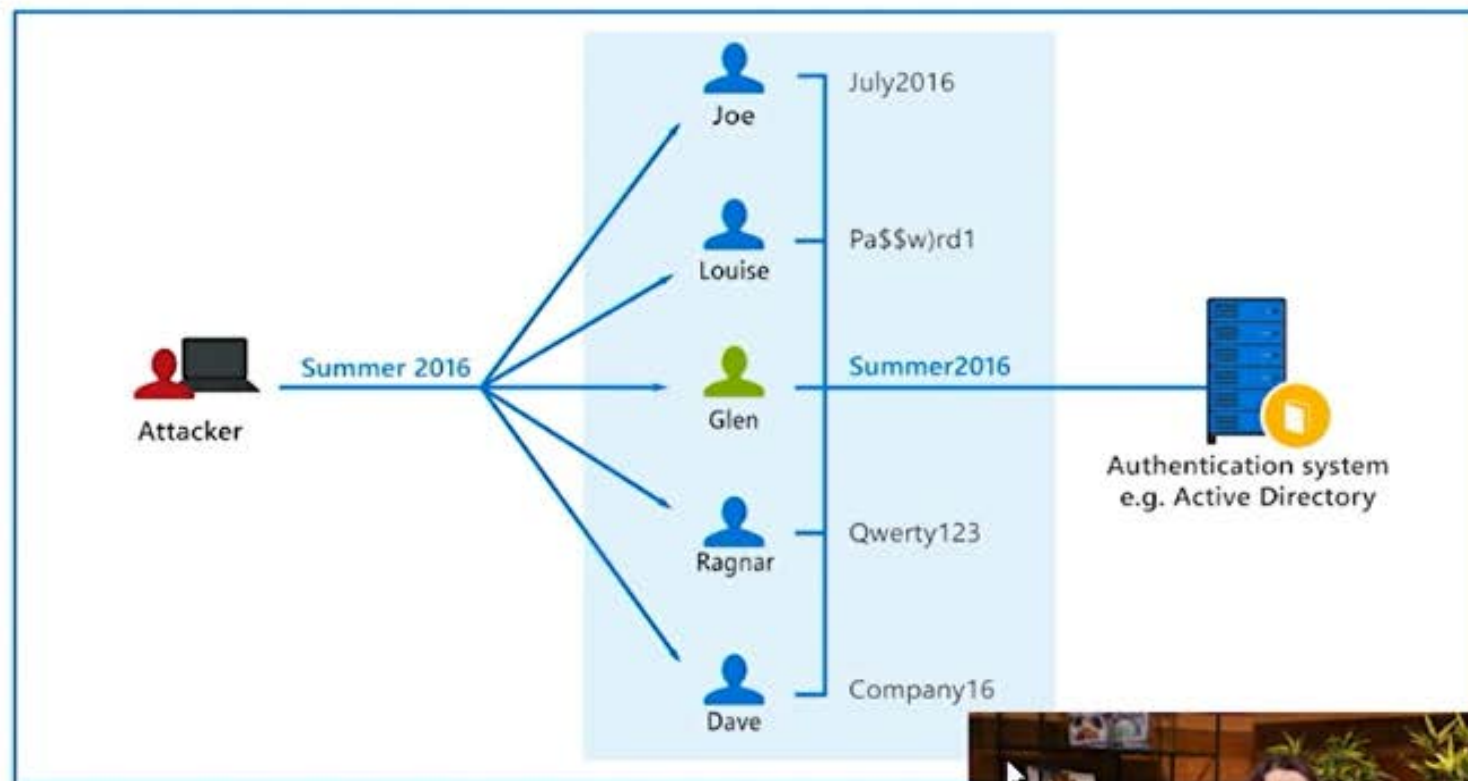


# Identity

## Common identity attacks

### Types of security threats:

- Password-based attacks
- Phishing
- Spear phishing



# Identity

## Identity as the primary security perimeter

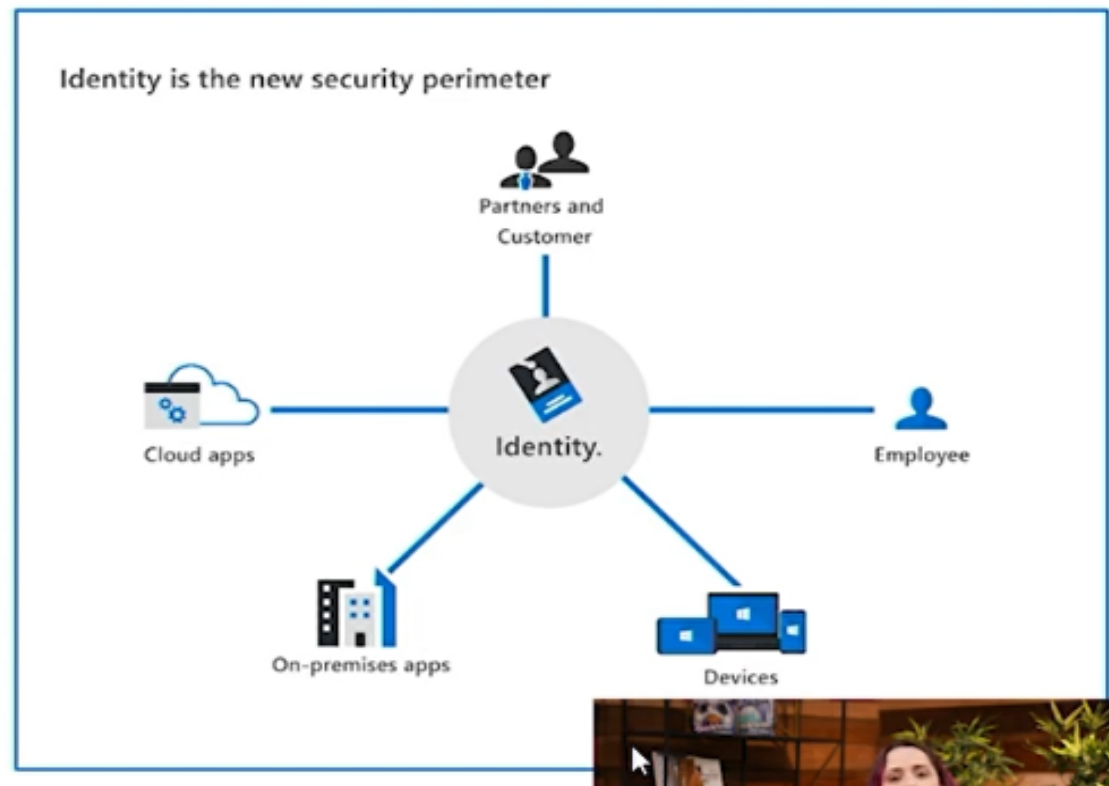
Identity has become the new security perimeter that enables organizations to secure their assets.

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



# Identity

## 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.

---

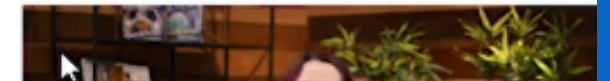


A fundamental capability of an IdP and "modern authentication" is the support for single sign-on (SSO).

---



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





# Identity

## The concept of Federated Services

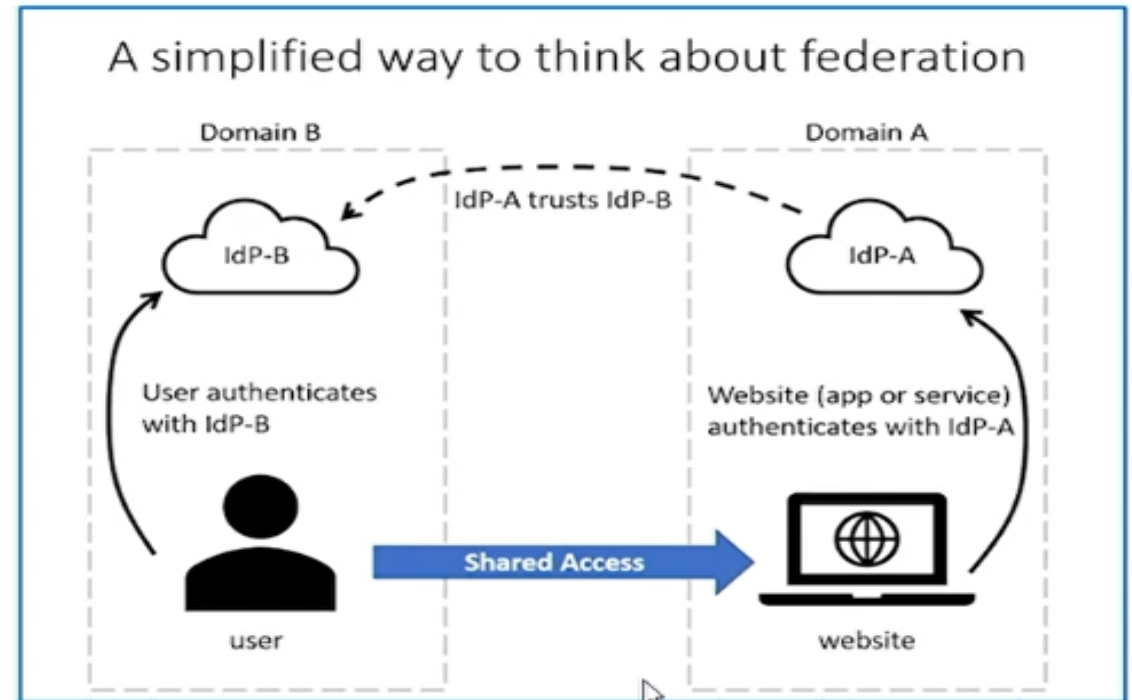
Simplification method of federation scenario:

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



# Identity

## 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.

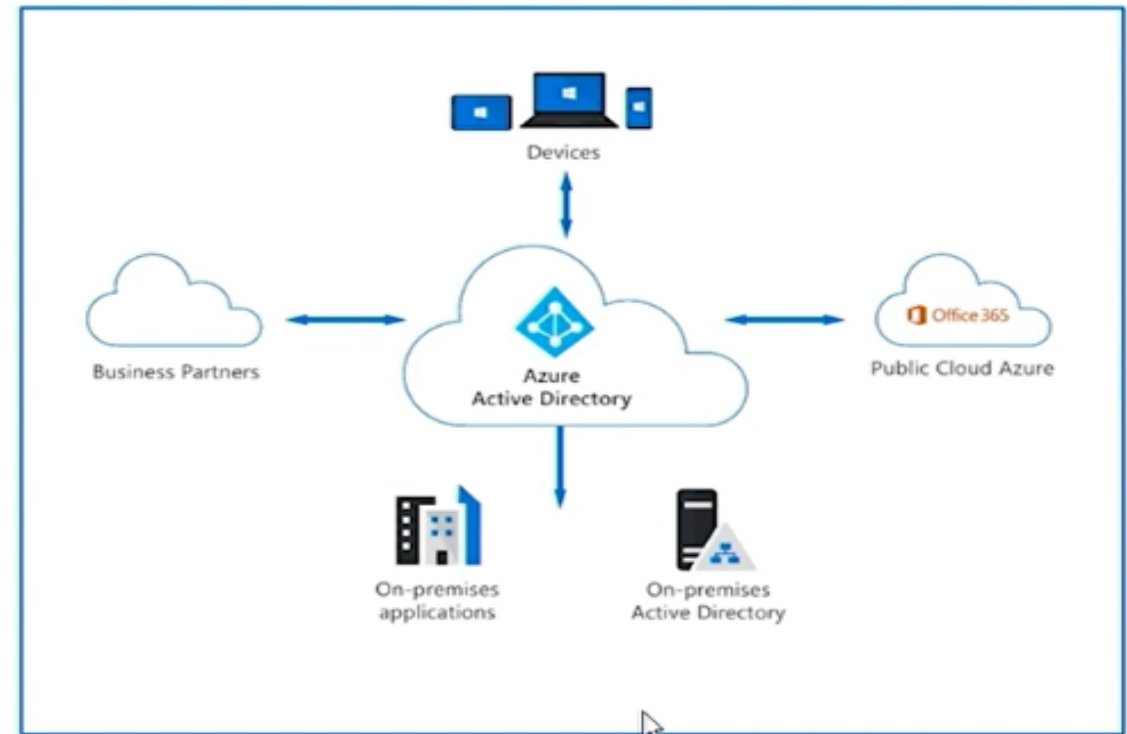


# Microsoft Access & Identity Solutions

## 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.



# Microsoft Access & Identity Solutions

## 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 Access & Identity Solutions


**Microsoft Azure**



admin@M365x678143....  
CONTOSO (M365X678143.ONMI...)

## Welcome to Azure!


Don't have a subscription? Check out the following options.



### Start with an Azure free trial

Get \$200 free credit toward Azure products and services, plus 12 months of popular free services.


[Start](#) [Learn more](#)



### Manage Azure Active Directory

Manage access, set smart policies, and enhance security with Azure Active Directory.

[View](#) [Learn more](#)





### Access student benefits


Get free software, Azure credit, or access Azure Dev Tools for Teaching after you verify your academic status.


[Explore](#) [Learn more](#)


## Azure services


[Create a resource](#)


[Quickstart Center](#)


[Virtual machines](#)


[App Services](#)

[Storage accounts](#)

[SQL databases](#)

[Azure Cosmos DB](#)

[Kubernetes services](#)

[Function App](#)



# Microsoft Access & Identity Solutions

The screenshot displays the Microsoft Azure portal interface. At the top, the header includes the Microsoft Azure logo, a search bar, and navigation icons. The user is logged in as admin@M365x678143... (CONTOSO (M365X678143.ONMI...)).

The main content area is titled "Contoso | Overview" under "Azure Active Directory". The left sidebar contains a navigation menu with the following items:

- Overview
- Preview features
- Diagnose and solve problems
- Manage
  - Users
  - Groups
  - External Identities
  - Roles and administrators
  - Administrative units
  - Enterprise applications
  - Devices
  - App registrations
  - Identity Governance
  - Application proxy
  - Licenses

The main content area has tabs for "Overview", "Monitoring", and "Tutorials". Below the tabs is a search bar labeled "Search your tenant".

The "Basic information" section displays the following details:

Property	Value	Count
Name	Contoso	Users: 34
Tenant ID	92ef26a4-46f9-460c-92f1-0e1436a460b6	Groups: 44
Primary domain	M365x678143.onmicrosoft.com	Applications: 4
License	Azure AD Premium P2	Devices: 0

The "My feed" section shows two items:

- MOD Administrator** (MA) with ID 37b444fe-8d5d-4808-a05c-4e8a06964d5b, Global administrator, and a link to [More info](#).
- TLS 1.0, 1.1 and 3DES deprecation** warning: Upcoming TLS 1.0, 1.1 and 3DES deprecation for Azure AD. Please enable support for TLS 1.2 on clients(applications/platform) to avoid any service impact.

# Microsoft Access & Identity Solutions

Microsoft Azure Search resources, services, and docs (G+)

admin@M365x678143....  
CONTOSO (M365X678143.ONMI...)

Home > Contoso >

## New user

Contoso

Got feedback?

☒ **Create user**  
Create a new user in your organization. This user will have a user name like `alice@m365x678143.onmicrosoft.com`.  
[I want to create users in bulk](#)

☐ **Invite user**  
Invite a new guest user to collaborate with your organization. The user will be emailed an invitation they can accept in order to begin collaborating.  
[I want to invite guest users in bulk](#)

[Help me decide](#)

### Identity

User name \* ⓘ

Example: chris @ m365x678143.onmicroso...

The domain name I need isn't shown here

# Microsoft Access & Identity Solutions

Microsoft Azure Search resources, services, and docs (G+)

admin@M365x678143....  
CONTOSO (M365X678143.ONMI...)

Home > Contoso >

## New user


Contoso

Got feedback?

Help me decide

### Identity

User name \* ⓘ

Example: chris @ m365x678143.onmicroso... 

The domain name I need isn't shown here

Name \* ⓘ

Example: 'Chris Green'

First name

Last name

### Groups and roles

# Microsoft Access & Identity Solutions

The screenshot displays the Microsoft Azure portal interface. The top navigation bar includes the 'Microsoft Azure' logo, a search bar, and user information for 'admin@M365x678143....' in the 'CONTOSO' environment. The left sidebar shows navigation options: 'Home > Contoso >', 'New user', 'Groups and roles', and 'Settings'. The 'New user' section is active, showing options for password generation (Auto-generated or Let me create) and a 'Create' button. The 'Groups and roles' section shows '1 groups selected' and 'User' roles. The main content area is titled 'Directory roles' and lists various roles with checkboxes and descriptions. The 'Global administrator' role is highlighted.

Role	Description
<input type="checkbox"/> Directory writers	Can read and write basic directory information. For granting access to applications, not intended for users.
<input type="checkbox"/> Domain name administrator	Can manage domain names in cloud and on-premises.
<input type="checkbox"/> Dynamics 365 administrator	Can manage all aspects of the Dynamics 365 product.
<input type="checkbox"/> Exchange administrator	Can manage all aspects of the Exchange product.
<input type="checkbox"/> Exchange recipient administrator	Can create or update Exchange Online recipients within the Exchange Online organization.
<input type="checkbox"/> External ID user flow administrator	Can create and manage all aspects of user flows.
<input type="checkbox"/> External ID user flow attribute administrator	Can create and manage the attribute schema available to all user flows.
<input type="checkbox"/> External Identity Provider administrator	Can configure identity providers for use in direct federation.
<input checked="" type="checkbox"/> Global administrator	Can manage all aspects of Azure AD and Microsoft services that use Azure AD identities.
<input type="checkbox"/> Global reader	Can read everything that a global administrator can, but not update anything.
<input type="checkbox"/> Groups administrator	Can manage all aspects of groups and group settings like naming and expiration policies.
<input type="checkbox"/> Guest inviter	Can invite guest users independent of the 'members can invite guests'...

# Microsoft Access & Identity Solutions

Microsoft Azure

Search resources, services, and docs (G+)

admin@M365x678143...  
CONTOSO (M365X678143.ONML...)

Home > Contoso >

## Users | All users (Preview)

Contoso - Azure Active Directory

+ New user + New guest user Bulk operations Refresh Reset password Per-user MFA Delete user

This page includes previews available for your evaluation. View previews →

Search: Jane Add filters

1 user found

	Name	User principal n...	User type	Directory synced	Identity issuer	Company name	Creation
<input type="checkbox"/>	Jane Doe	jd...@m365x678143...	Member	No	M365x678143.onmicro		

Activity

- Sign-ins
- Audit logs
- Bulk operation results

Troubleshooting + Support

- New support request



# Microsoft Access & Identity Solutions

## External identities in Azure AD

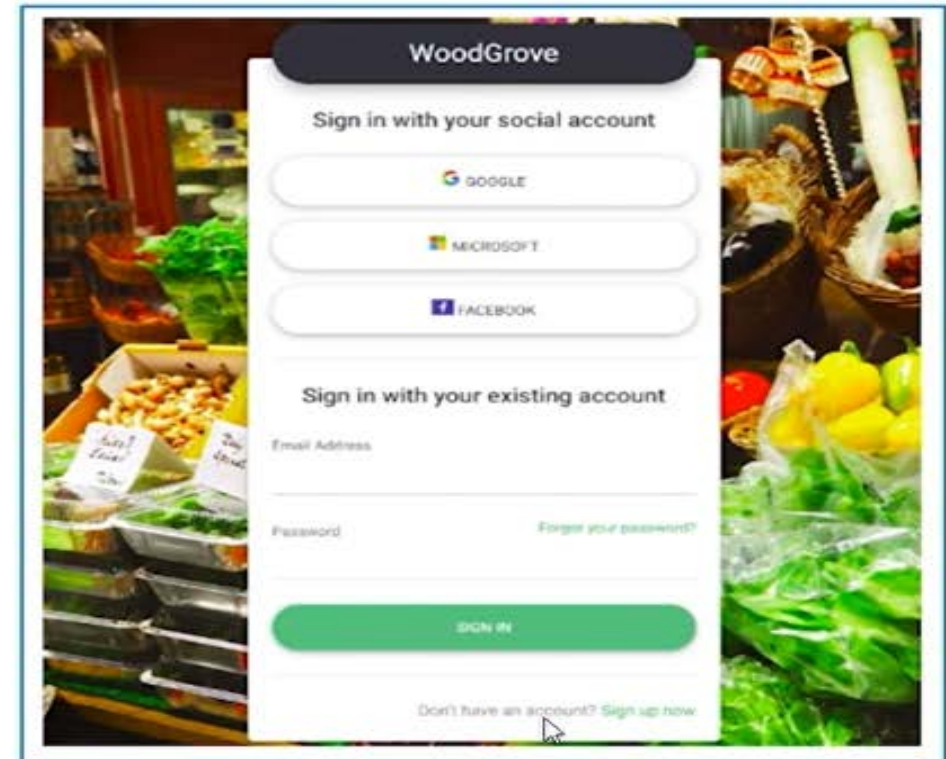
Two different Azure AD External Identities:

### 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



# Microsoft Access & Identity Solutions

## The concept of hybrid identities

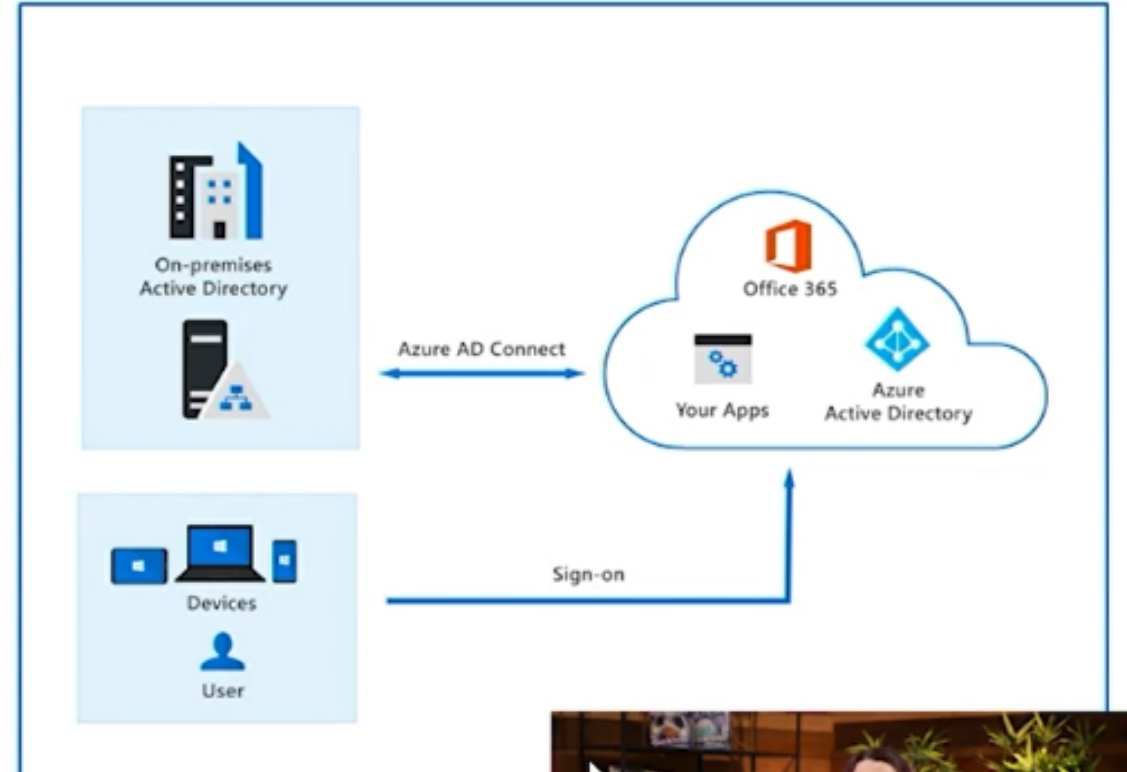
### Hybrid identities and authentication

#### 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



# Microsoft Access & Identity Solutions

## Authentication methods of Azure AD

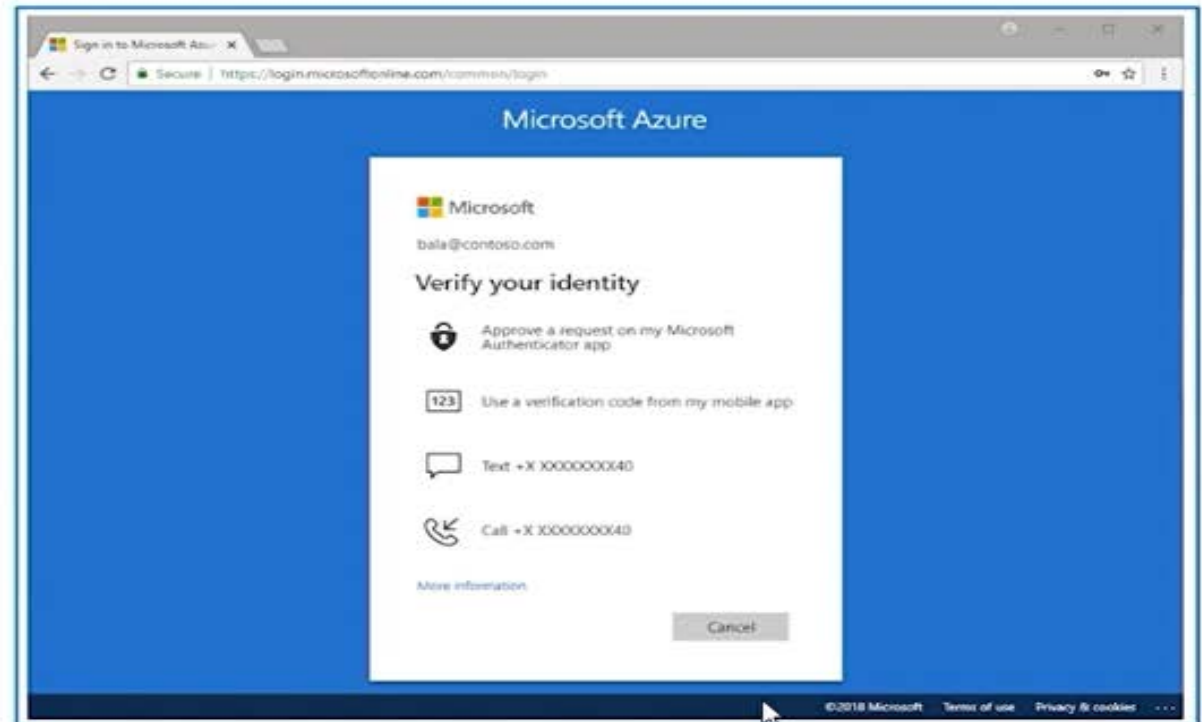
### Multifactor authentication (MFA) & Security Defaults

#### 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.



# Microsoft Access & Identity Solutions

## 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

**Bad:** Password

123456

qwerty

password

iloveyou

Password1

**Good:** Password  
and...



SMS



Voice

**Better:** Password  
and...



Microsoft  
Authenticator



Software  
Tokens OTP



Hardware  
Token OTP

**Best:** Passwordless



Microsoft  
Hello



Microsoft  
Authenticator



FIDO2 security key

# Microsoft Access & Identity Solutions

## 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



# Microsoft Access & Identity Solutions

## Self-service password reset (SSPR) in Azure AD

### Benefits of Self-service password reset:

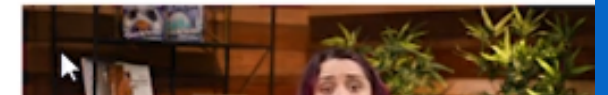
- It increases security.
- It saves the organization money by reducing the number of calls and requests to help desk staff.
- It increases productivity, allowing the user to return to work faster.

### 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 Access & Identity Solutions

## Password protection & management capabilities in Azure AD



Global banned password list

---



Custom banned password lists

---

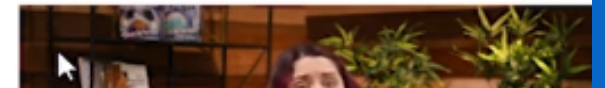


Protecting against password spray

---



Hybrid security



# Microsoft Access & Identity Solutions

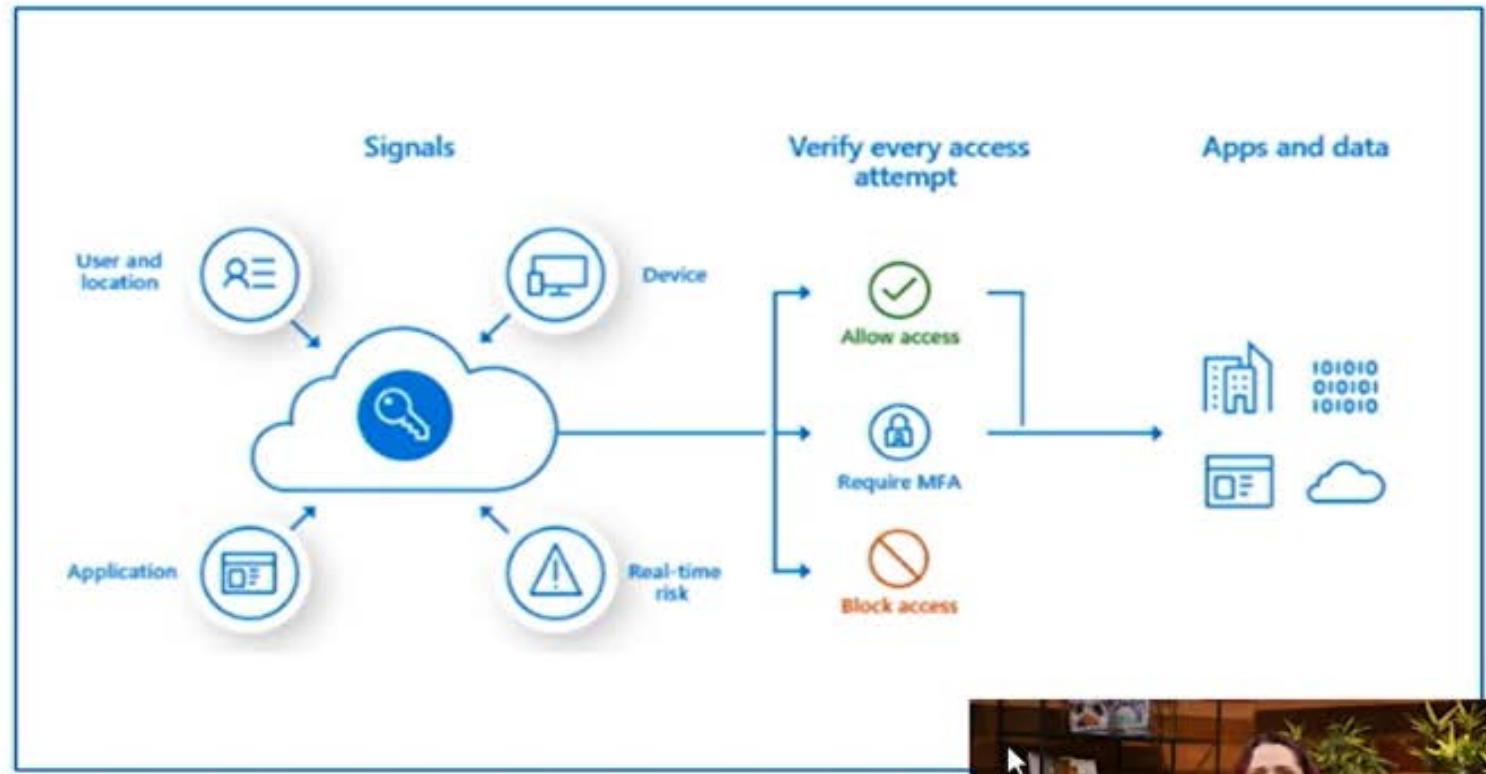
## Conditional access

### 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 Access & Identity Solutions

## 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

# Microsoft Access & Identity Solutions

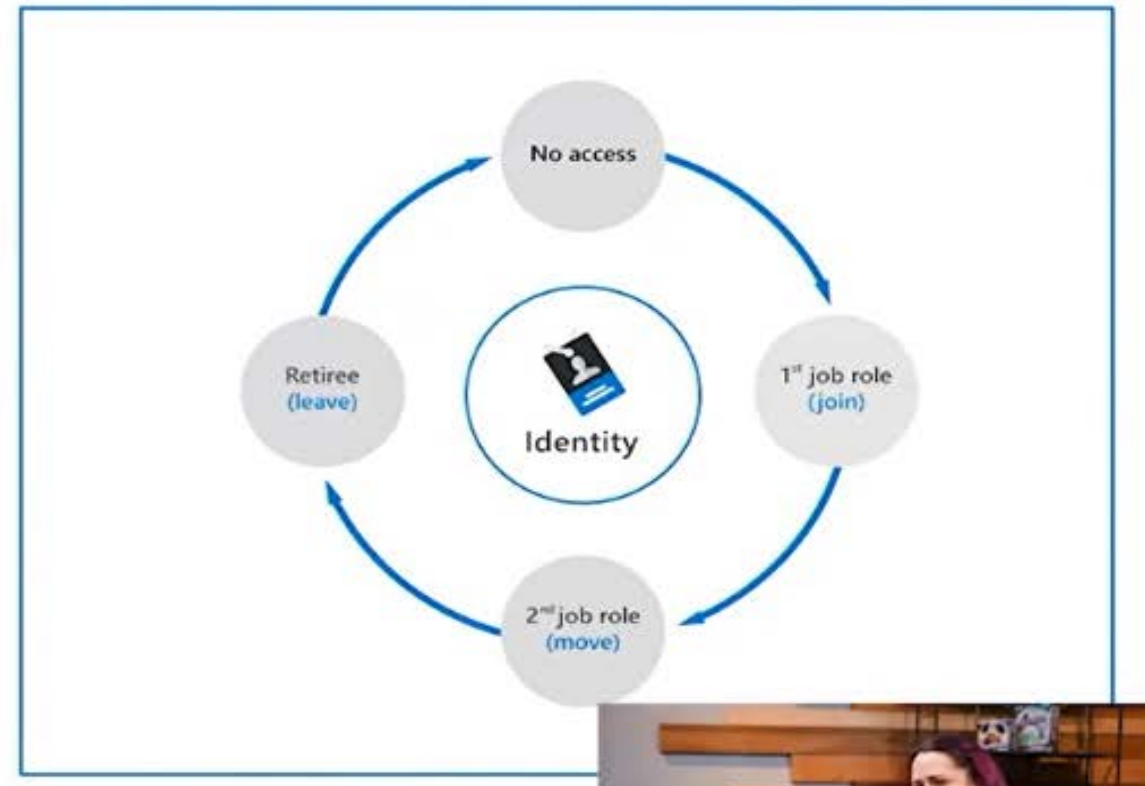
## Identity governance in Azure AD

### 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.





# Microsoft Access & Identity Solutions

## 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.

---

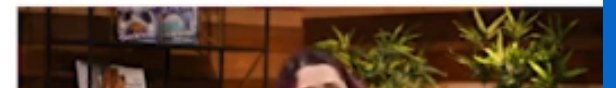


Visible, sending notifications when privileged roles are activated.

---



Auditable, allowing a full access history to be downloaded.



# Microsoft Access & Identity Solutions

## Azure Identity Protection

Enables organizations to accomplish three key tasks:

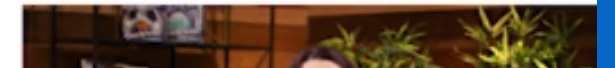
- Automate the detection and remediation of identity-based risks.
- Investigate risks using data in the portal.
- Export risk detection data to third-party utilities for further analysis.

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



# Microsoft Access & Identity Solutions

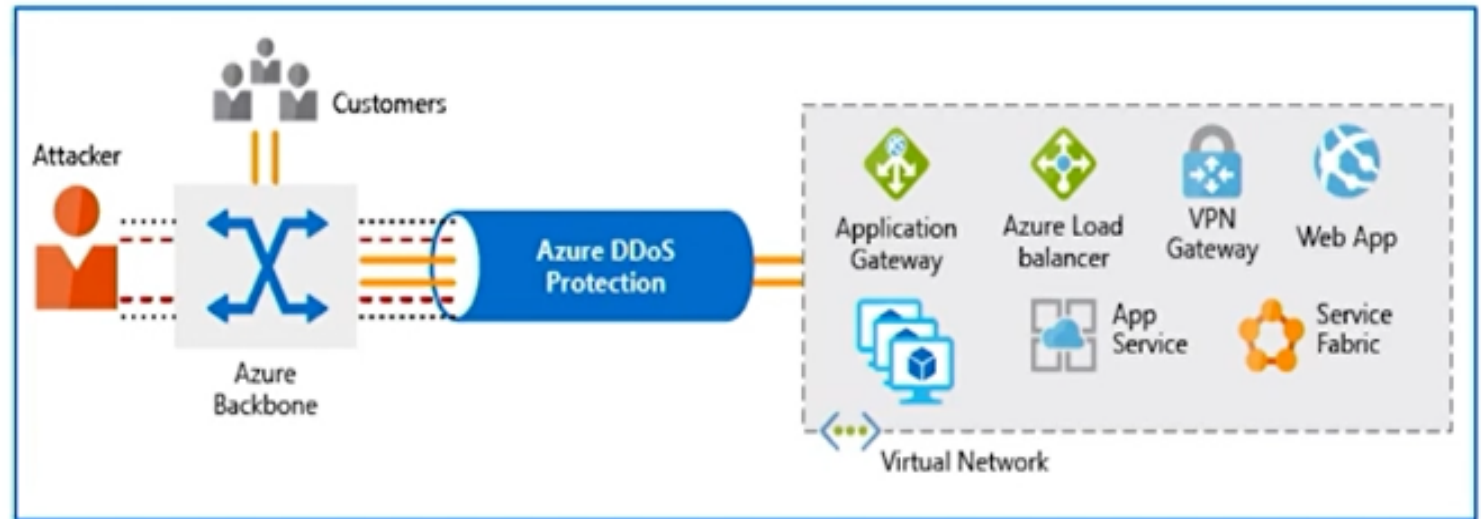
## Azure DDoS protection

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

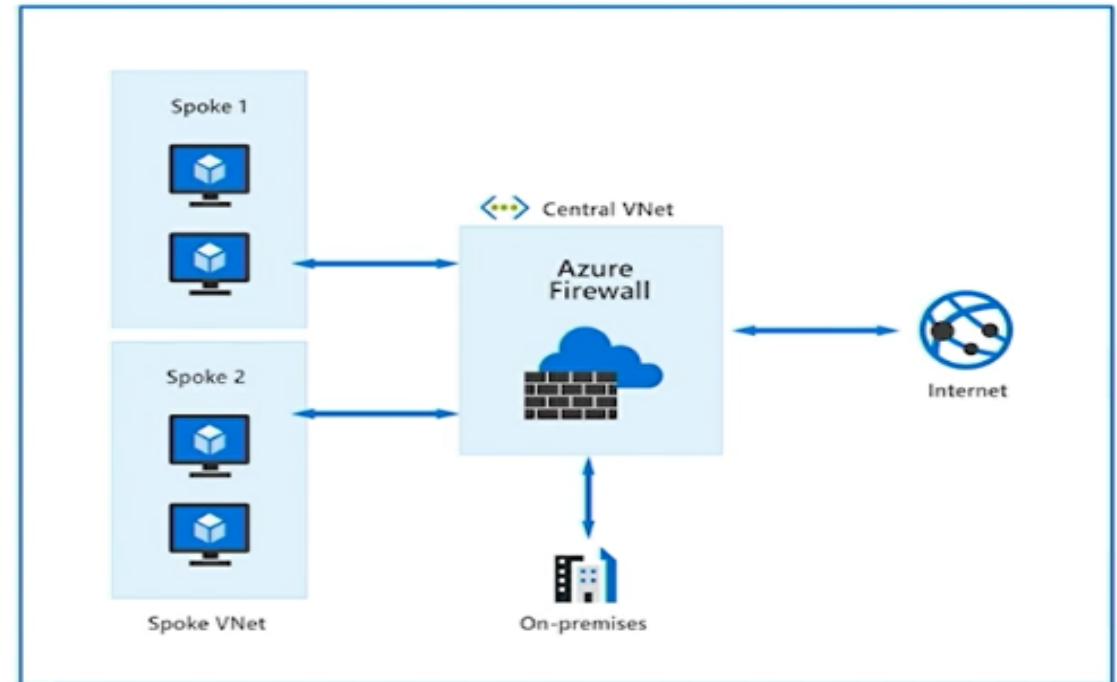


# Microsoft Access & Identity Solutions

## 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

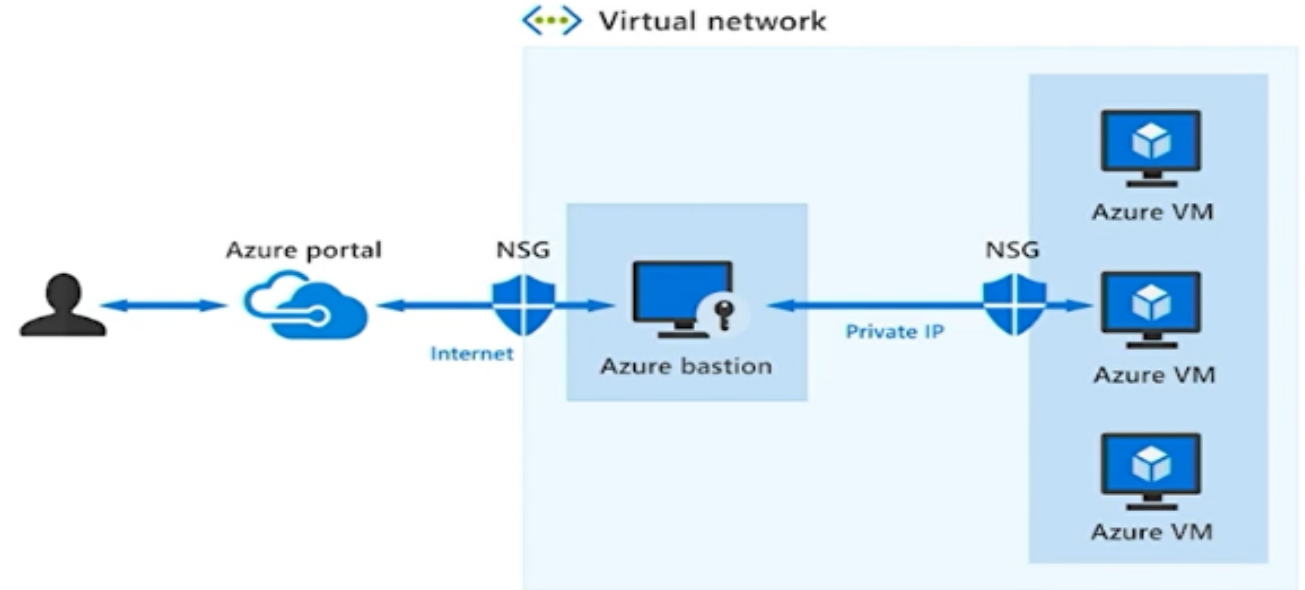


# Microsoft Access & Identity Solutions

## 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.



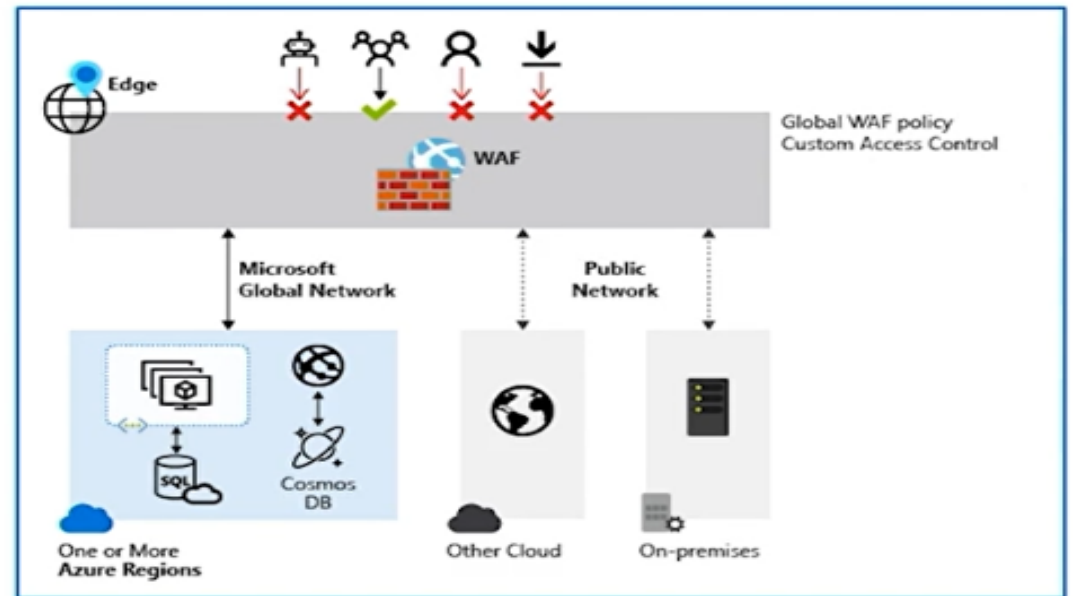


# Microsoft Access & Identity Solutions

## 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.



# Microsoft Access & Identity Solutions

## 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

# Microsoft Access & Identity Solutions

## 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

# Microsoft Access & Identity Solutions

## 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.

# Microsoft Security Solutions

## Azure Security Center

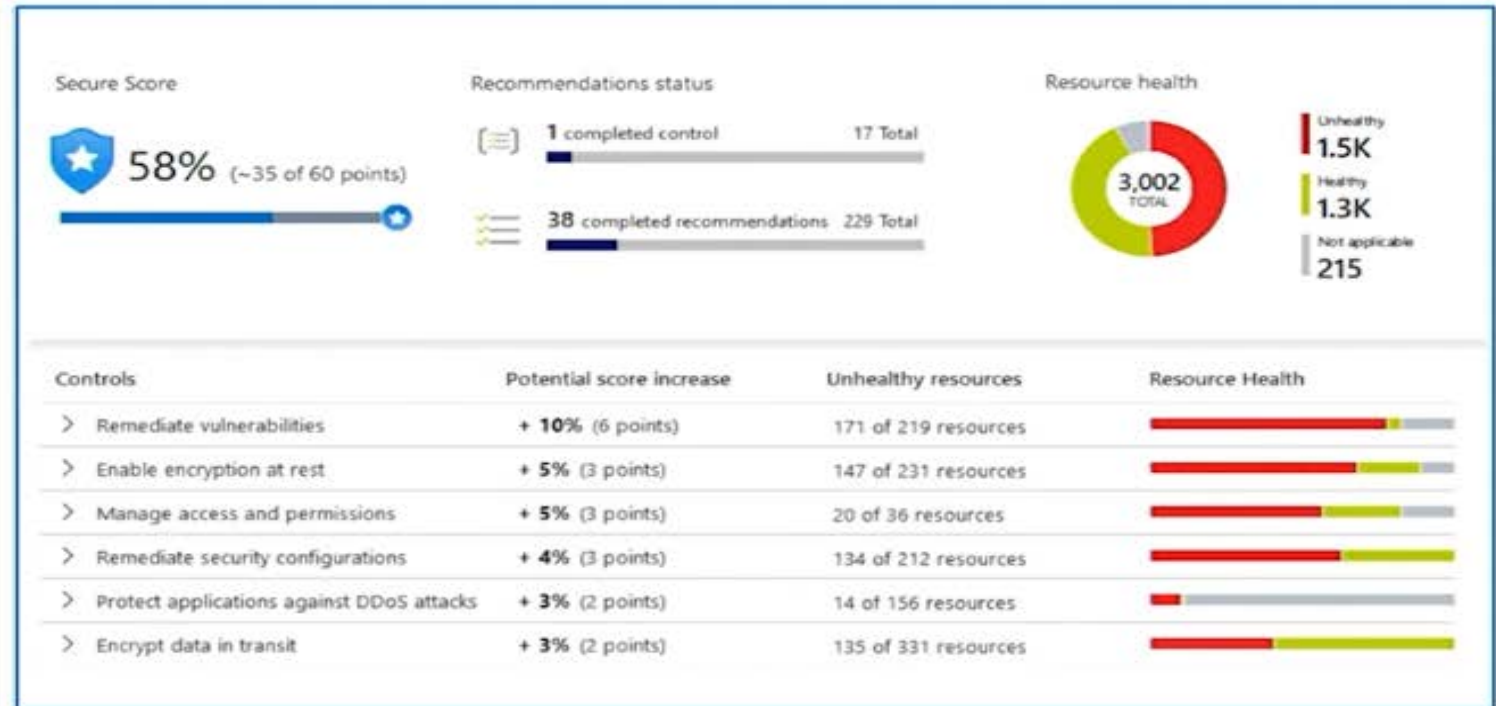
Strengthen security posture across your machines, data services, and applications.

**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.





# Microsoft Security Solutions

## 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?

# Microsoft Security Solutions

## SIEM, SOAR, and XDR



### SIEM

#### 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.



### SOAR

#### 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.



### XDR

#### 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.

# Microsoft Security Solutions

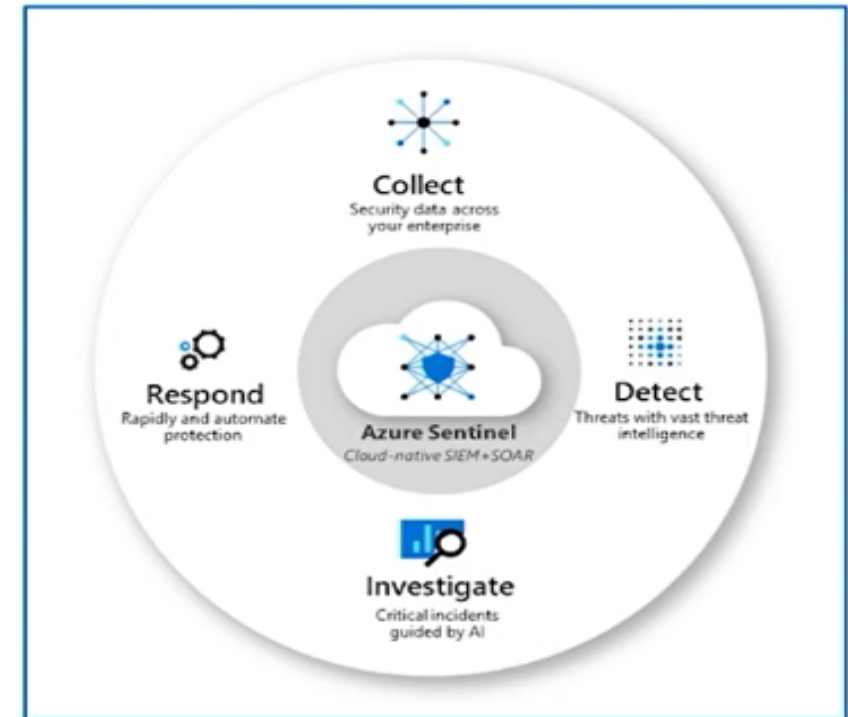
## Sentinel provides integrated threat protection (Slide 1)

**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.



# Microsoft Security Solutions

## 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.

---



# Thanks!

Vidyatech and VidyaMagic are trademarks of Vidyatech Solutions Private Limited.

The names of actual companies and products mentioned herein may be the trademarks of their respective owners. © Vidyatech Solutions Private Limited. All rights reserved.....