Microsoft Security Virtual Training

Technology partner to organizations worldwide

Table of Contents

Security

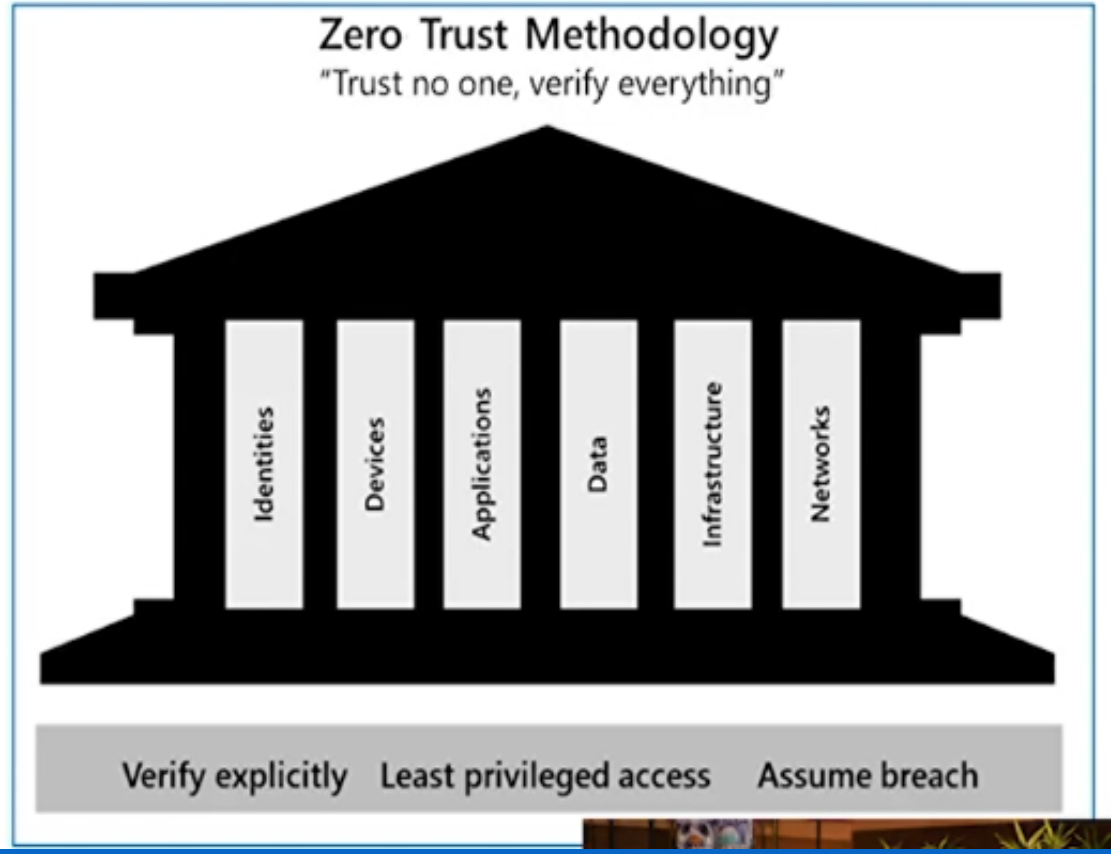
Zero-trust methodology

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.

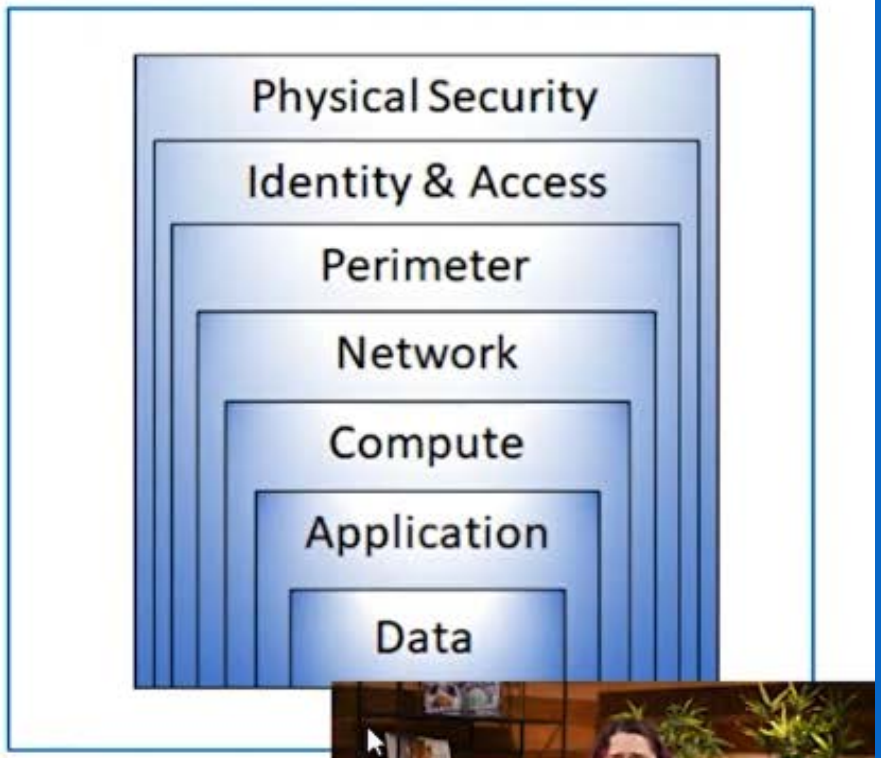


Security

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.

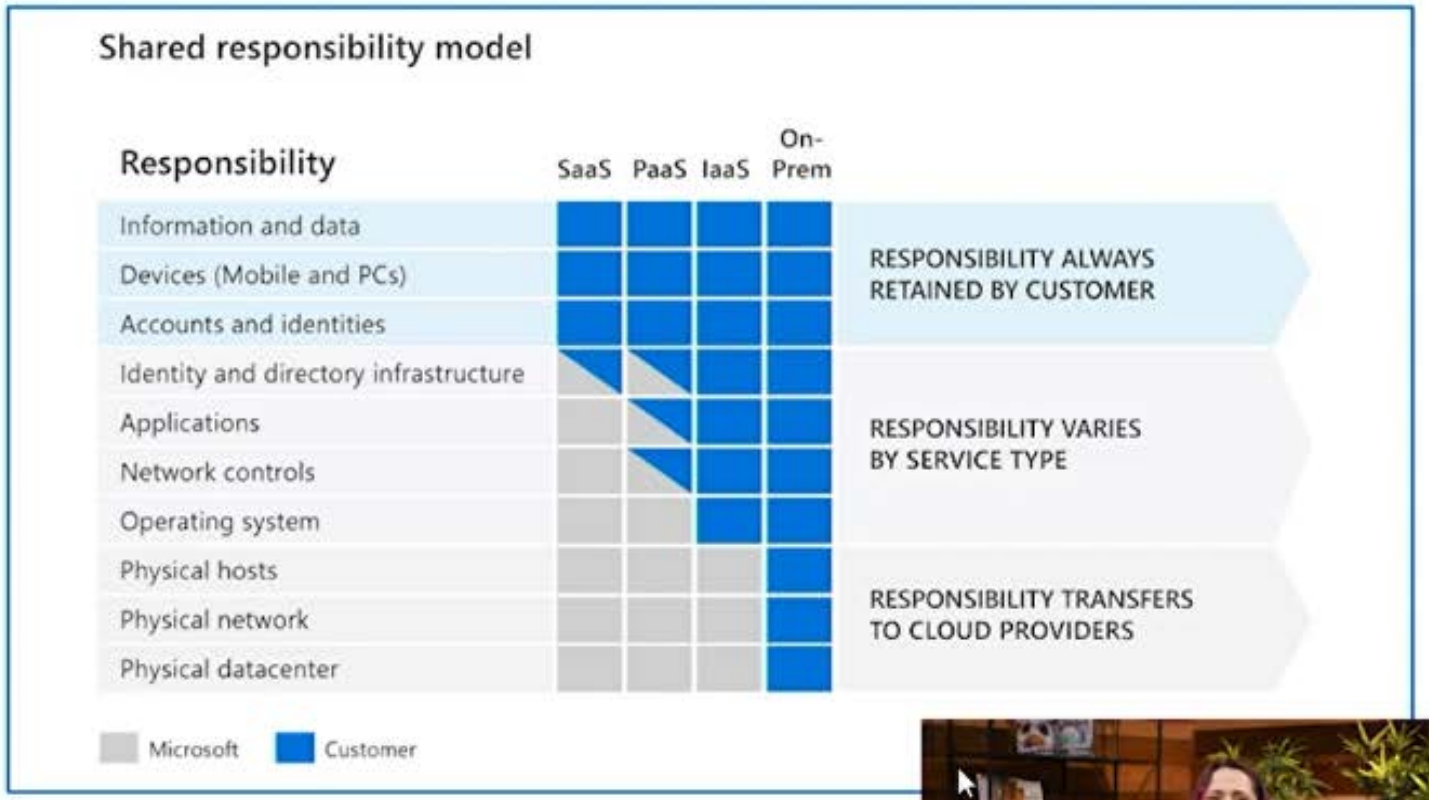


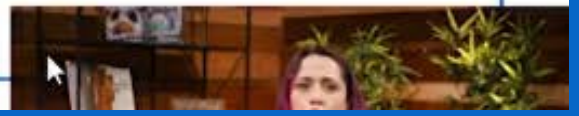
Security

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)



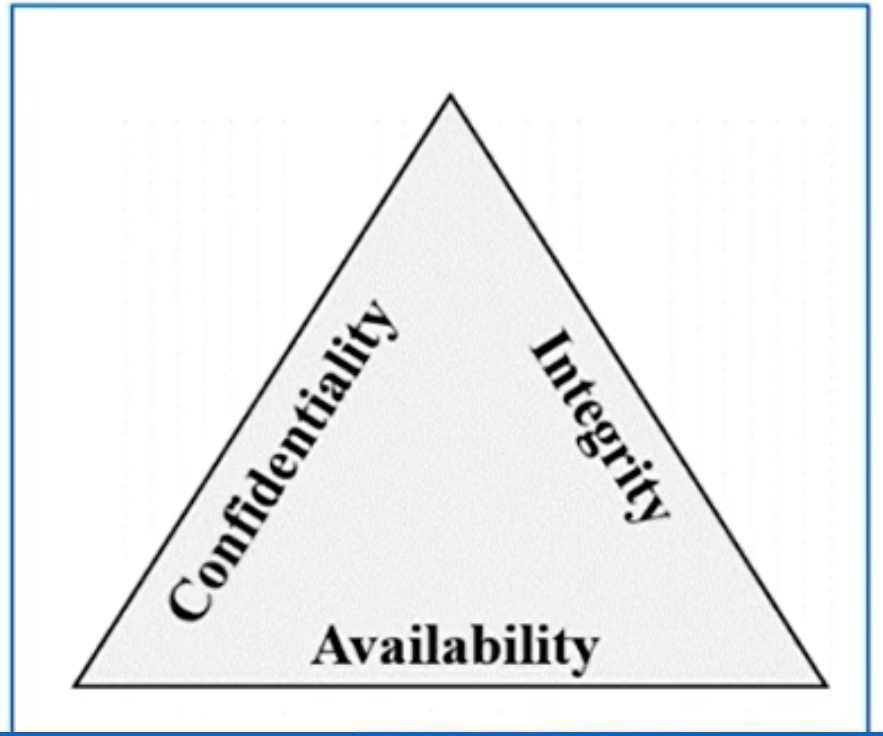


Security

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

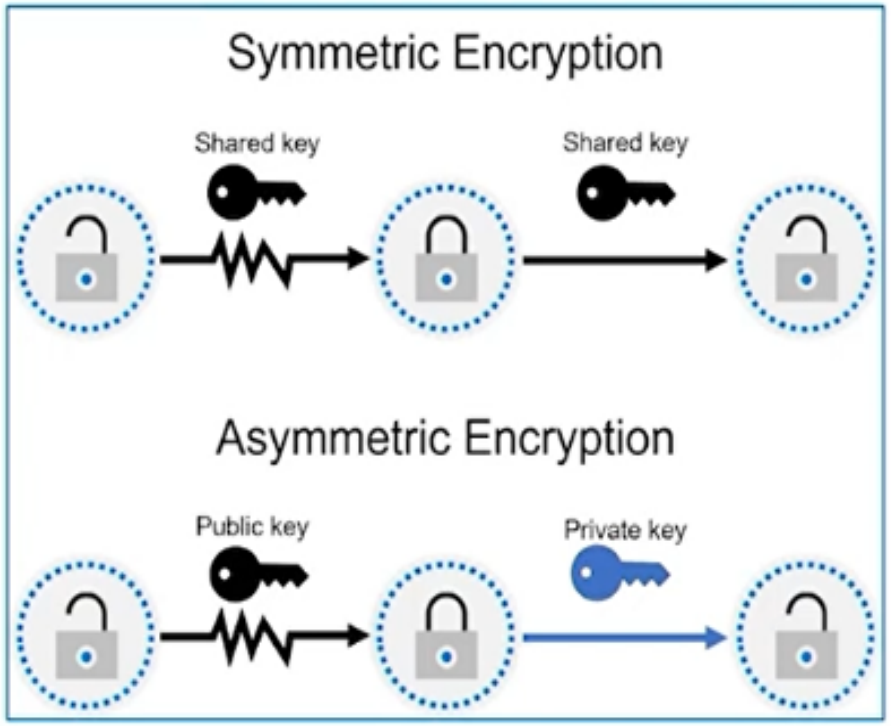
Encryption

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

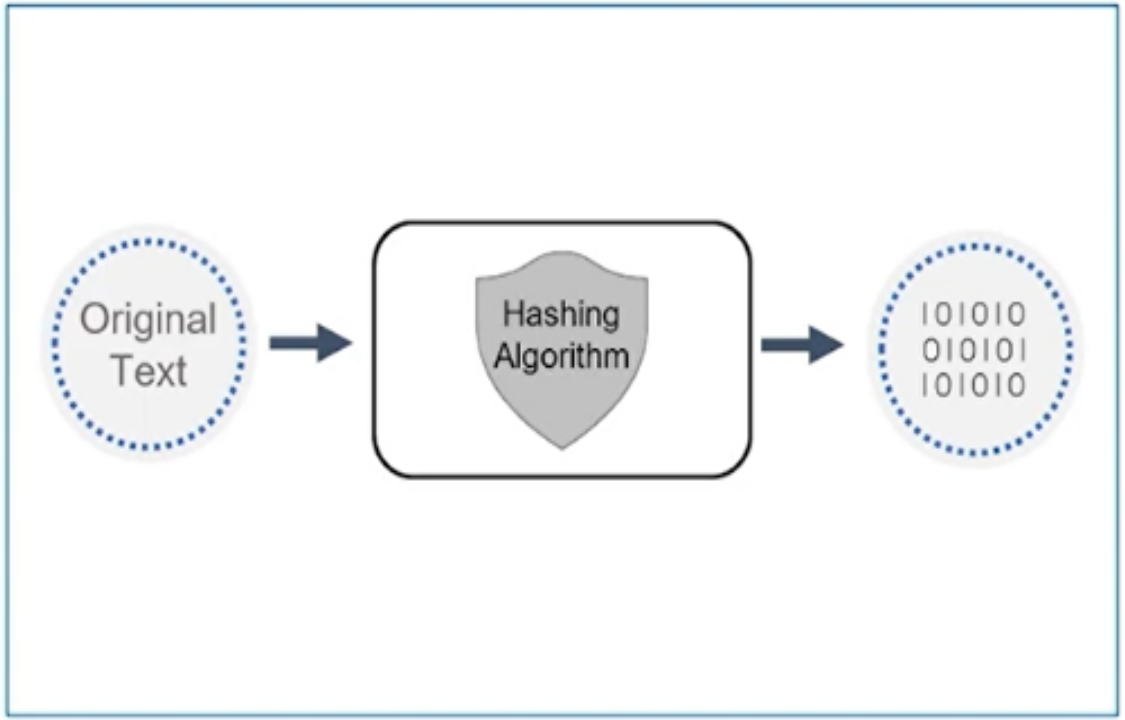


Security

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.

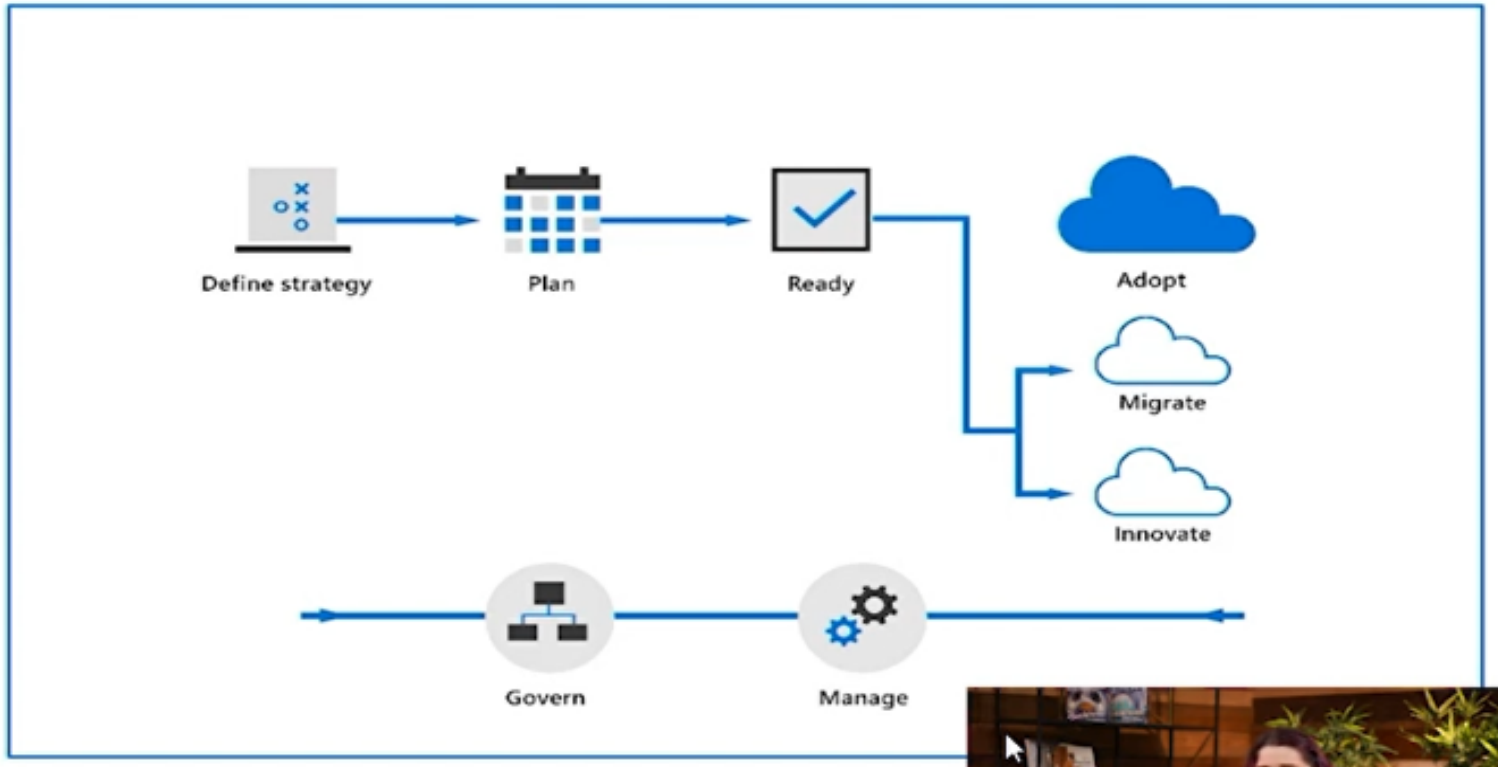


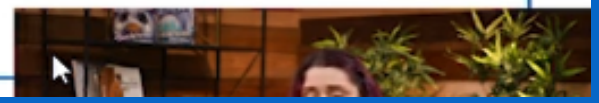
Security

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



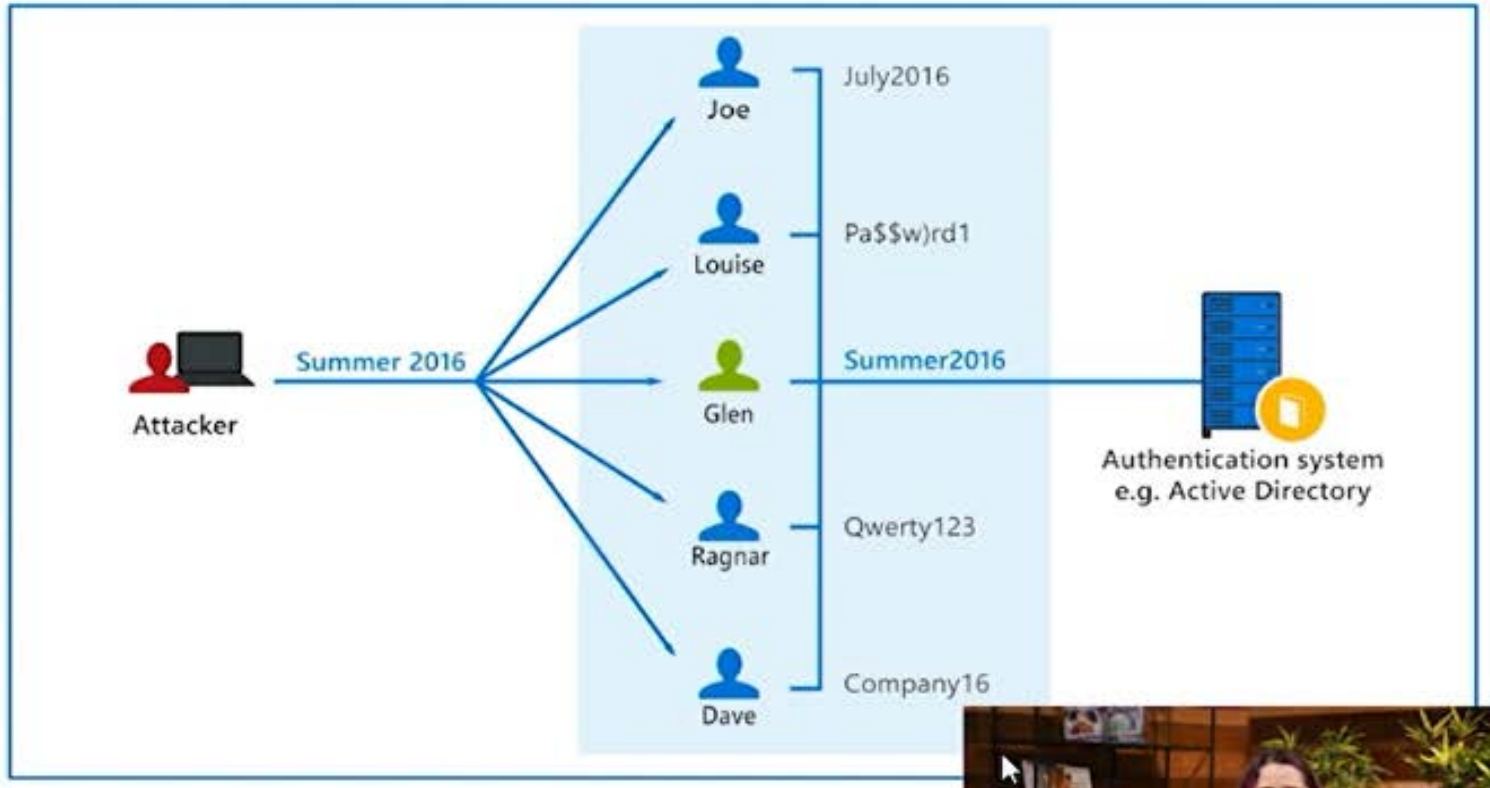


Identity

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:

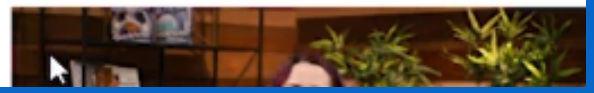
- Administration
- Authentication
- Authorization
- Auditing

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

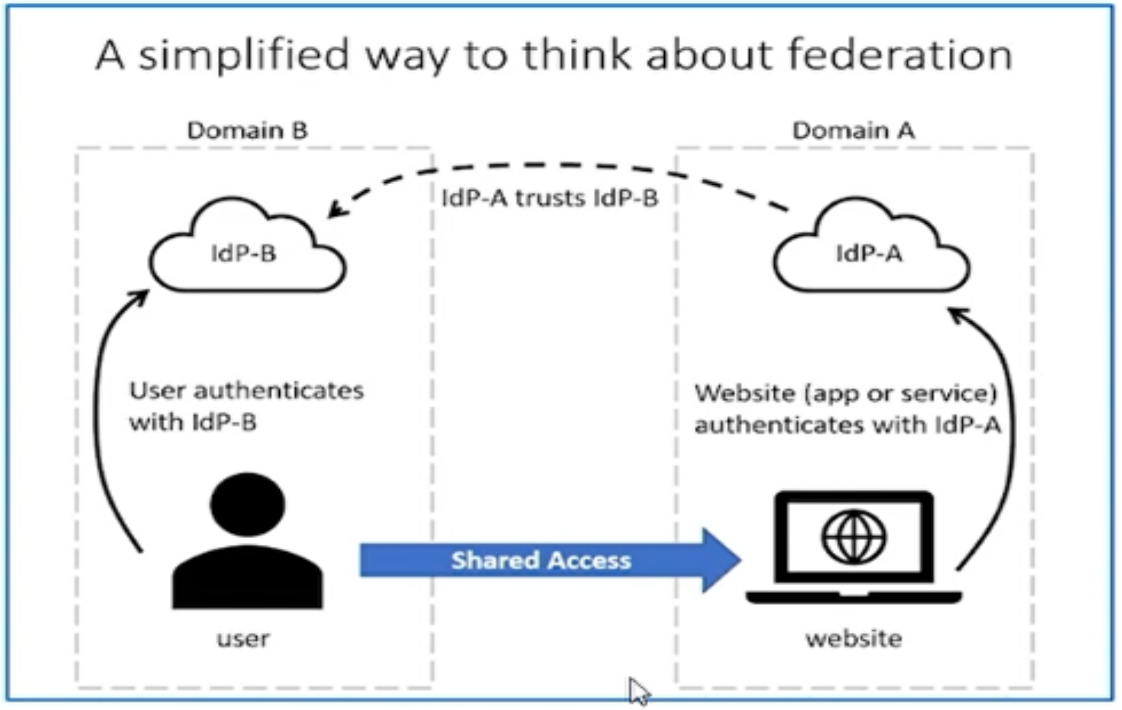
Simplification method of federation scenario:

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.

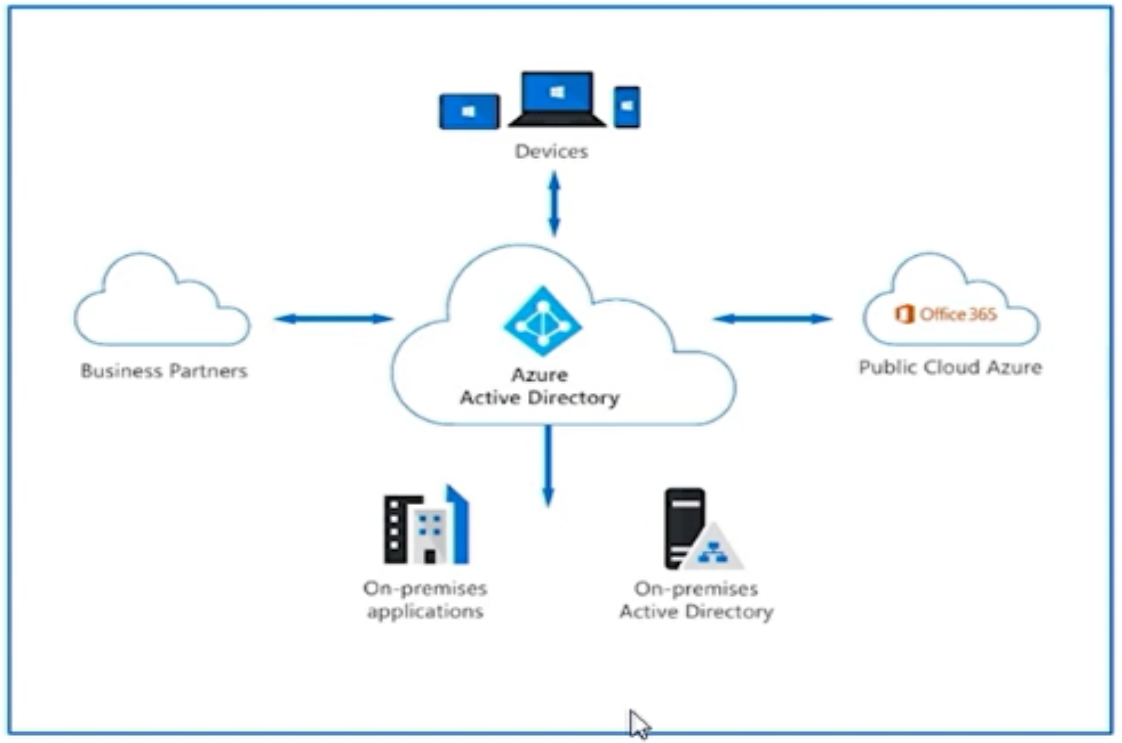
Azure Active Directory is the evolution of identity and access management solutions, providing organizations an Identity as a Service (IDaaS) solution for all their apps across cloud and on-premises.

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.

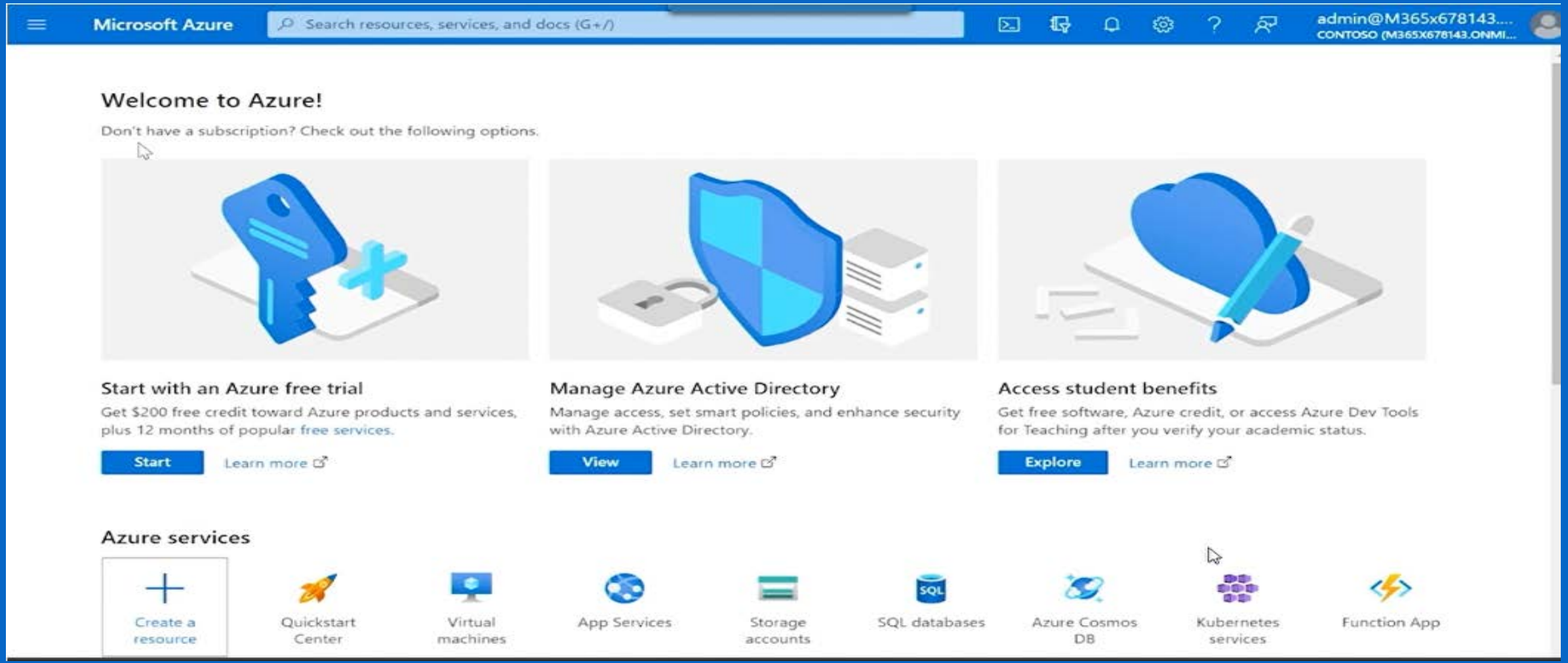
User - a representation of something that's managed by Azure AD. Employees and guests are represented as users in Azure AD.

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.

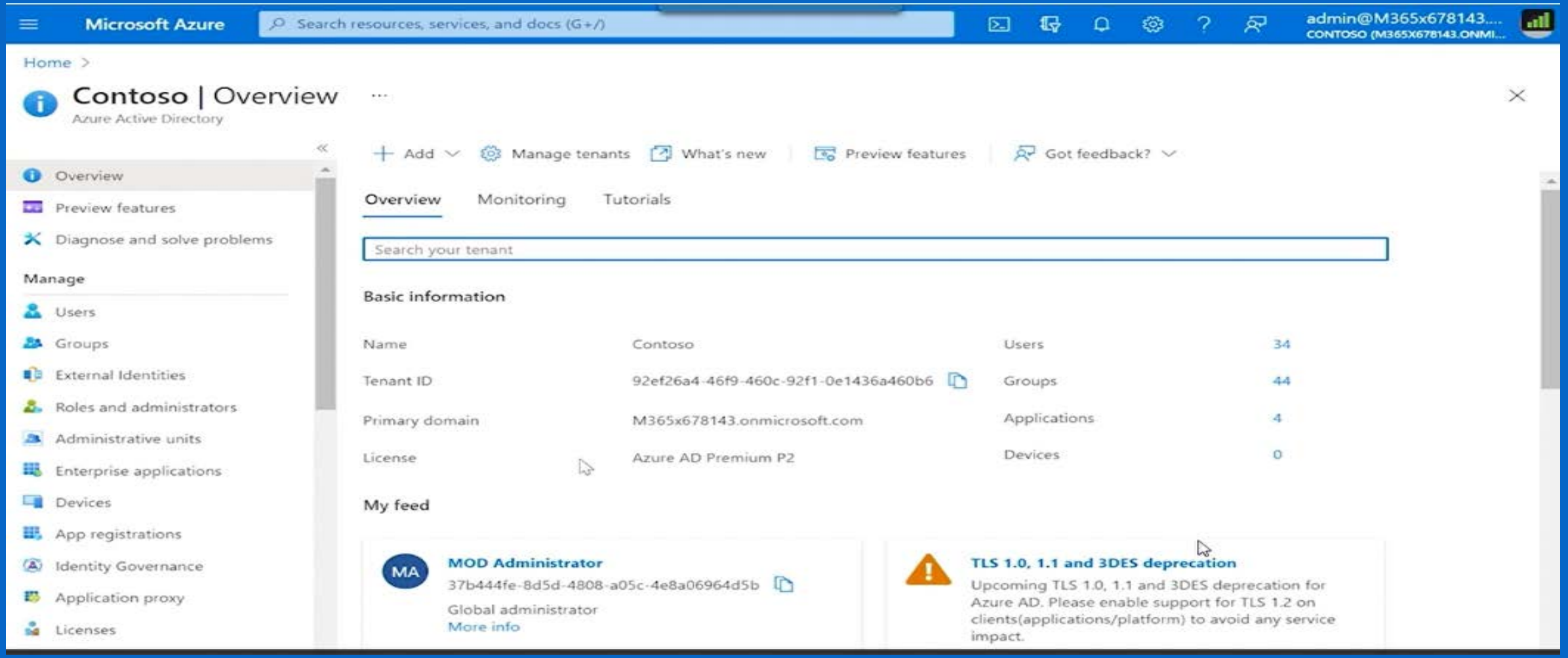
Managed identity - typically used to manage the credentials for authenticating a cloud application with an Azure service. Two types: system assigned and user assigned.

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.

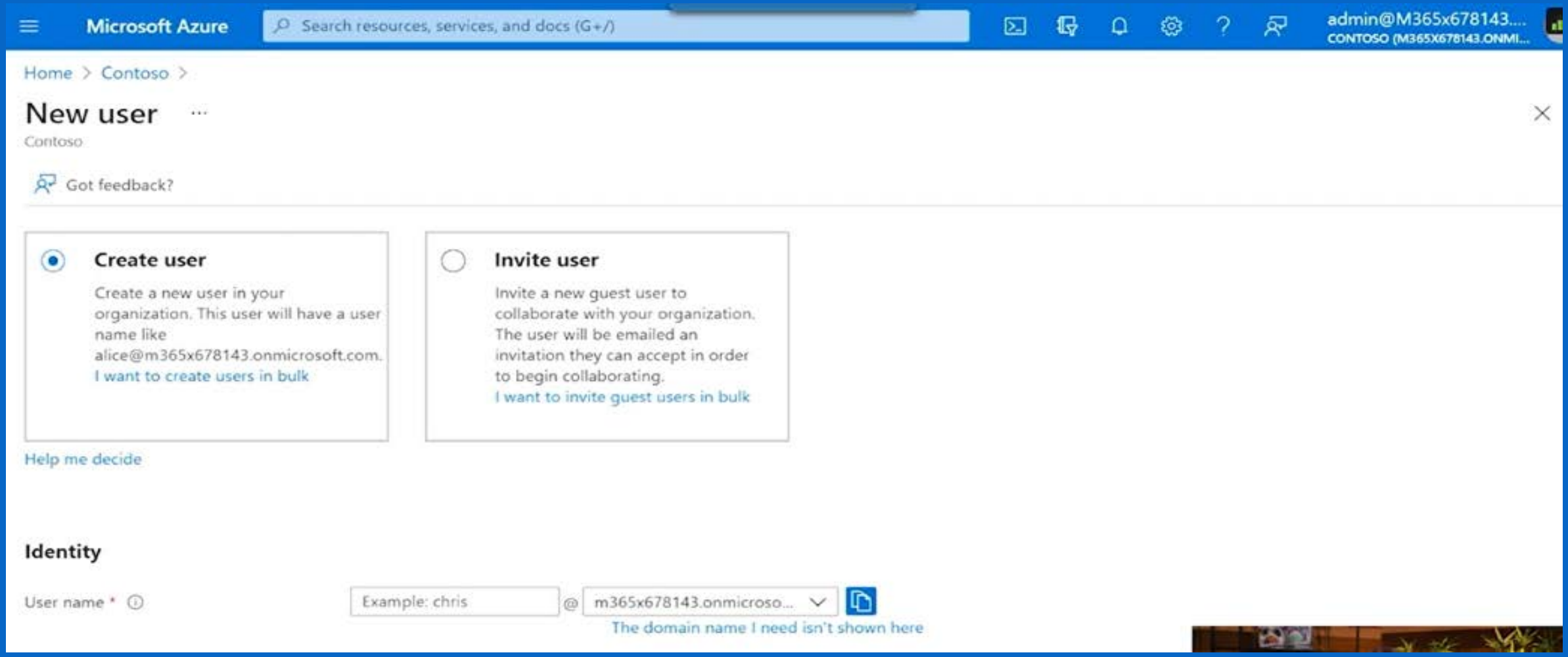
Microsoft Access & Identity Solutions



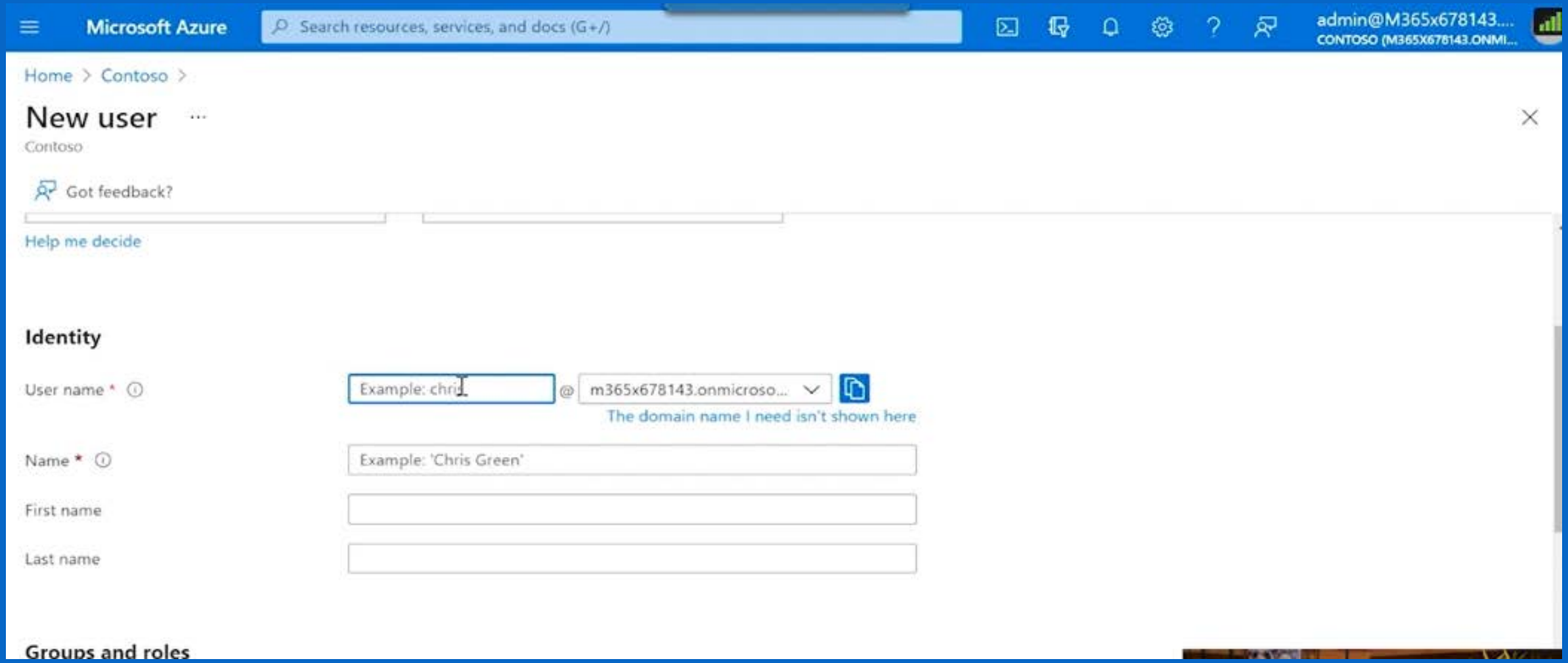
Microsoft Access & Identity Solutions



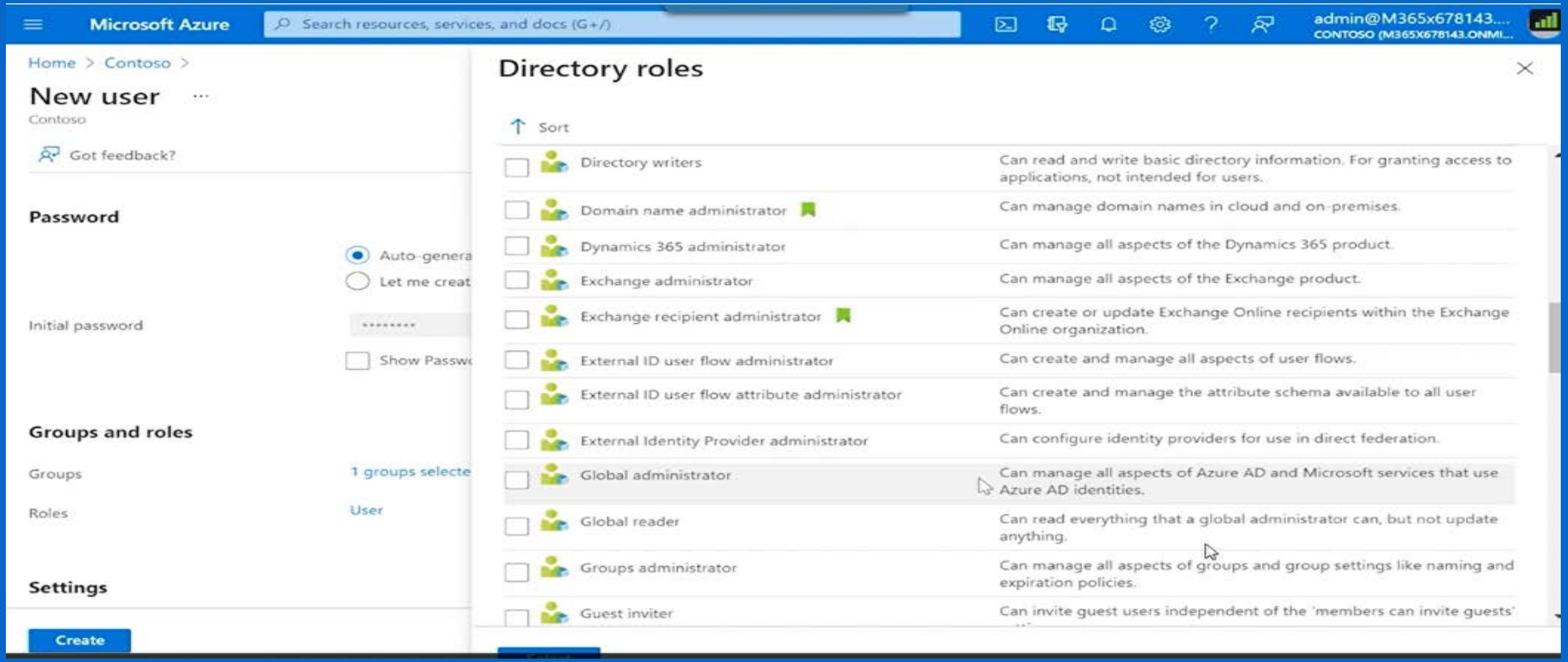
Microsoft Access & Identity Solutions



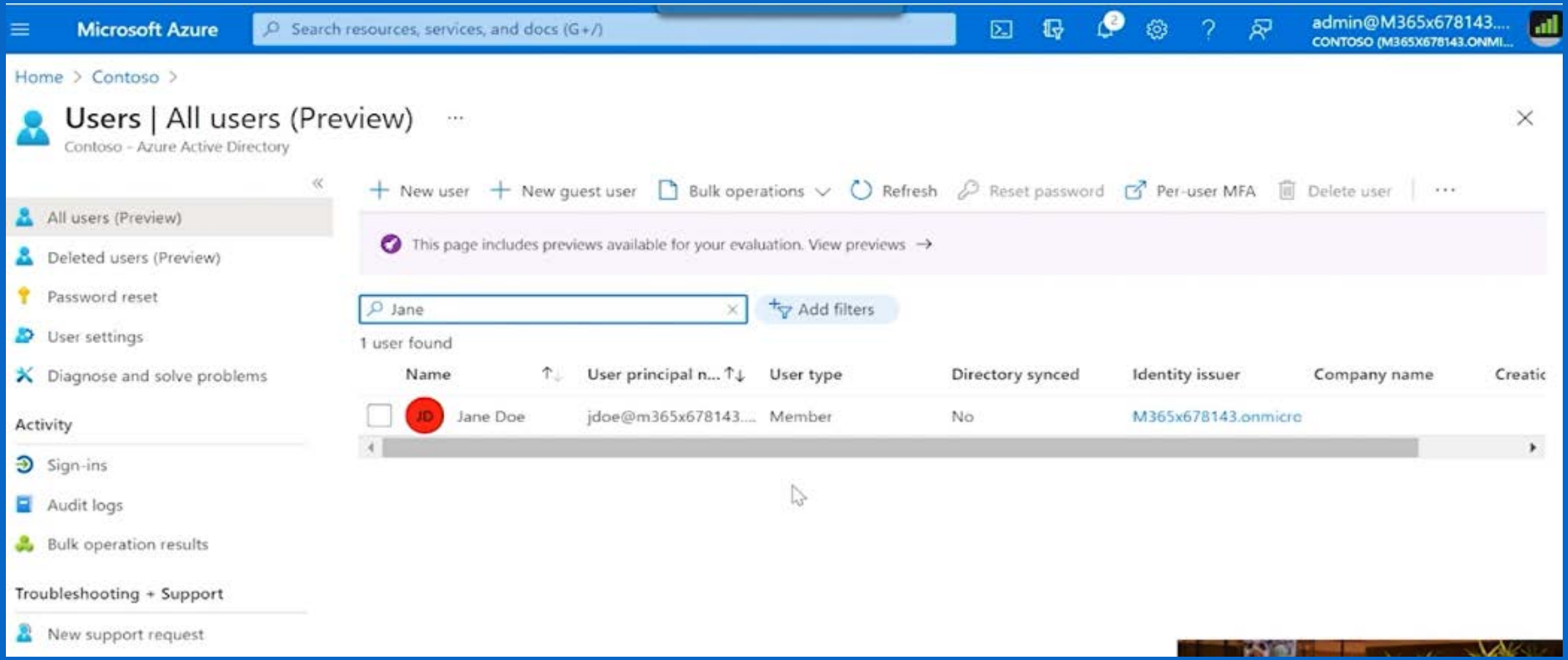
Microsoft Access & Identity Solutions



Microsoft Access & Identity Solutions



Microsoft Access & Identity Solutions



Microsoft Access & Identity Solutions

External identities in Azure AD

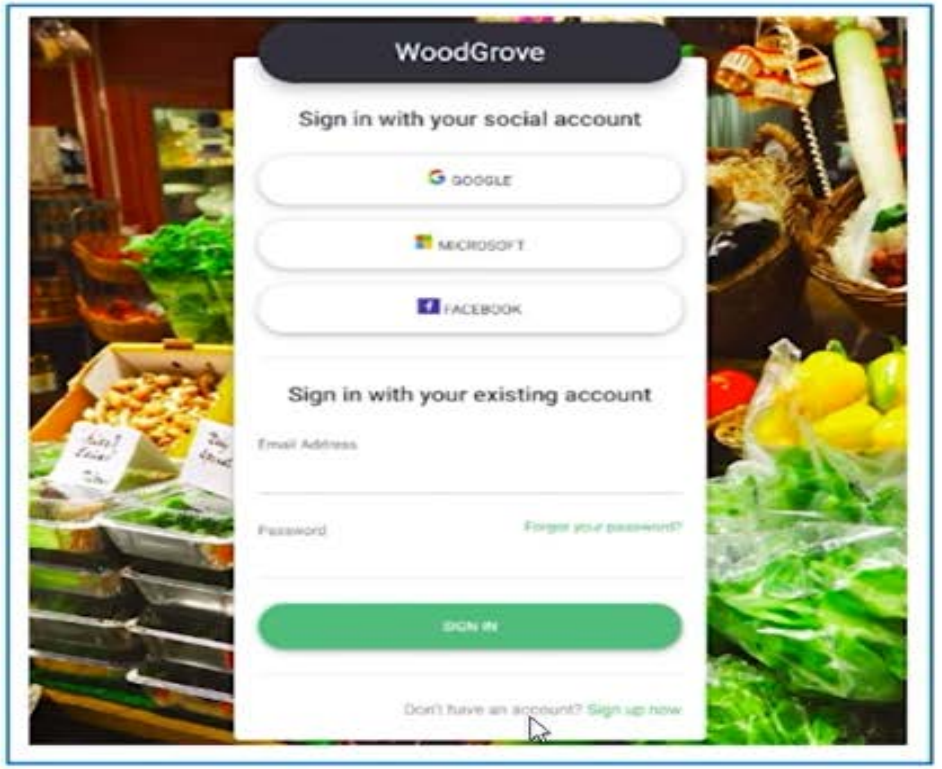
Two different Azure AD External Identities:

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

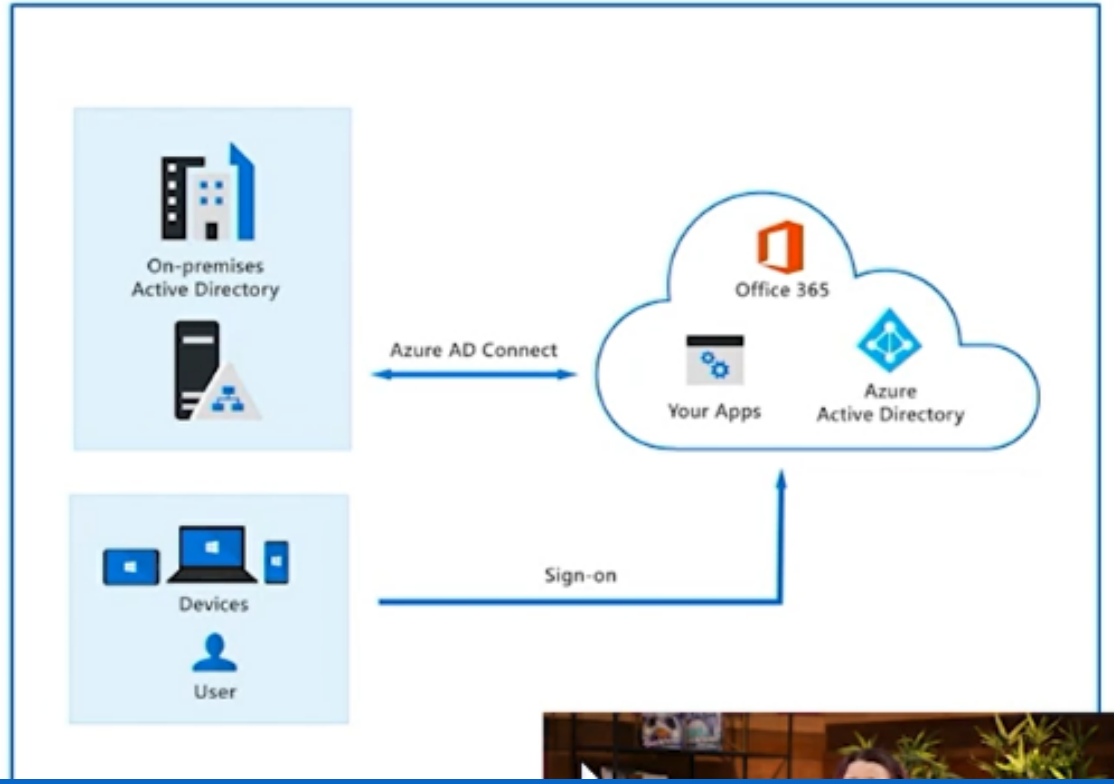
Hybrid identities and authentication

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

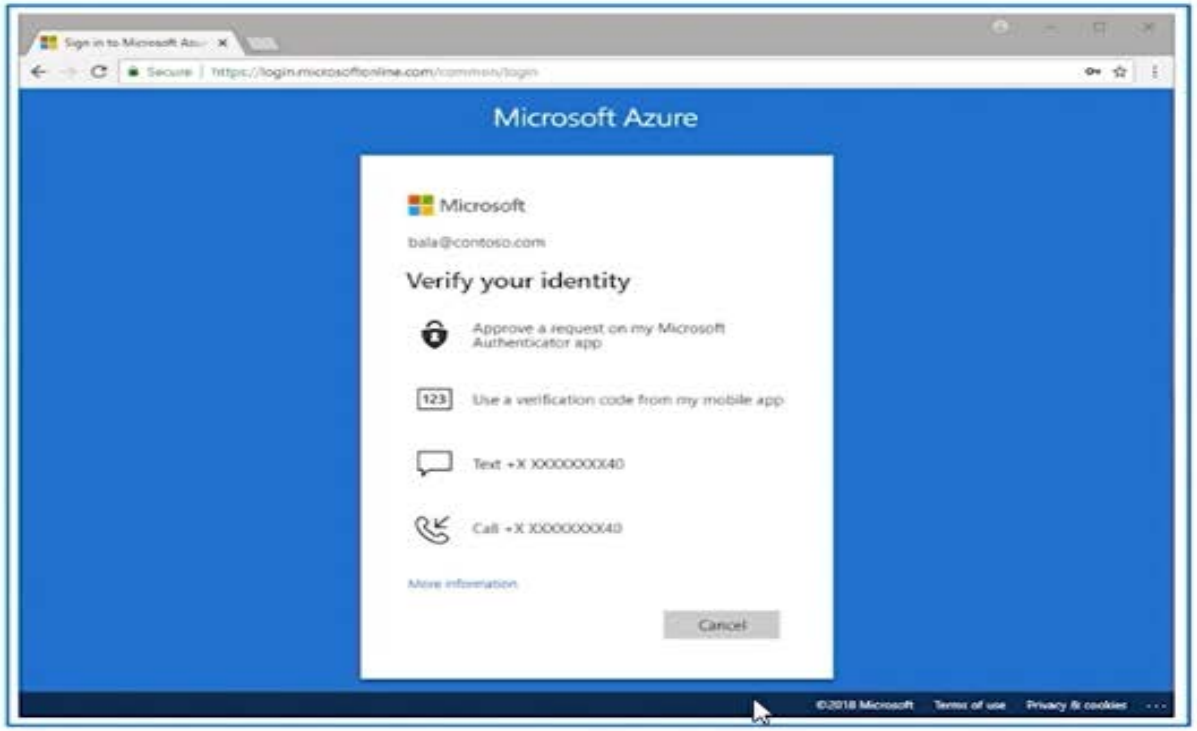
Multifactor authentication (MFA) & Security Defaults

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

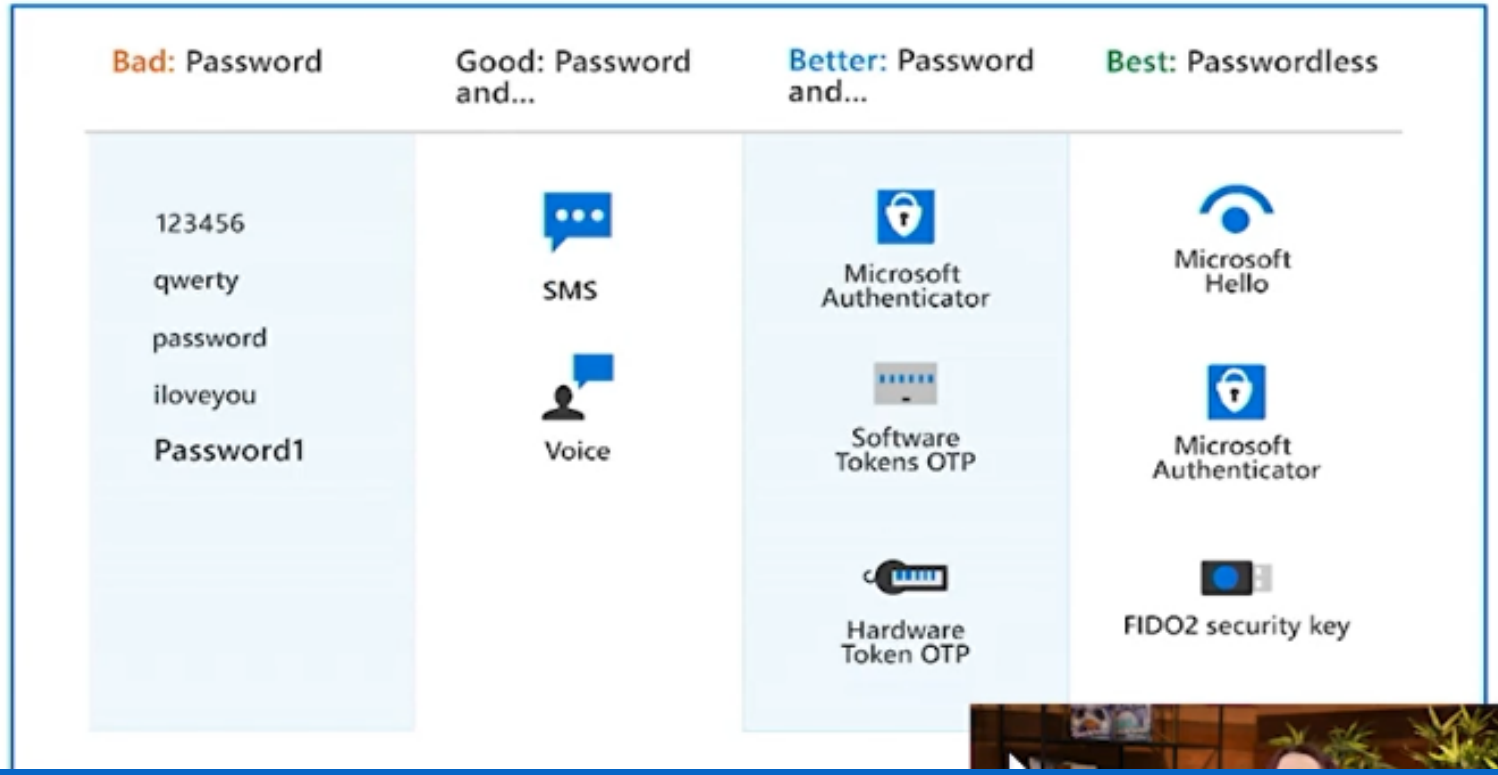
Passwords

Password & additional verification

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

Passwordless

- Biometrics (Windows Hello)
- Microsoft Authenticator
- FIDO2



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:

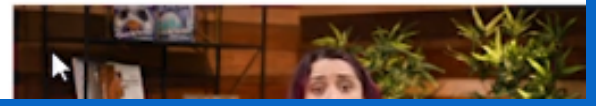
- It increases security.
- It saves the organization money by reducing the number of calls and requests to help desk staff.
- It increases productivity, allowing the user to return to work faster.

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

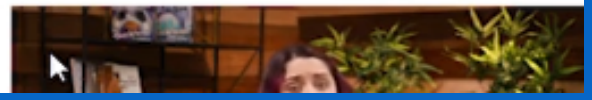


Vidyatech

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

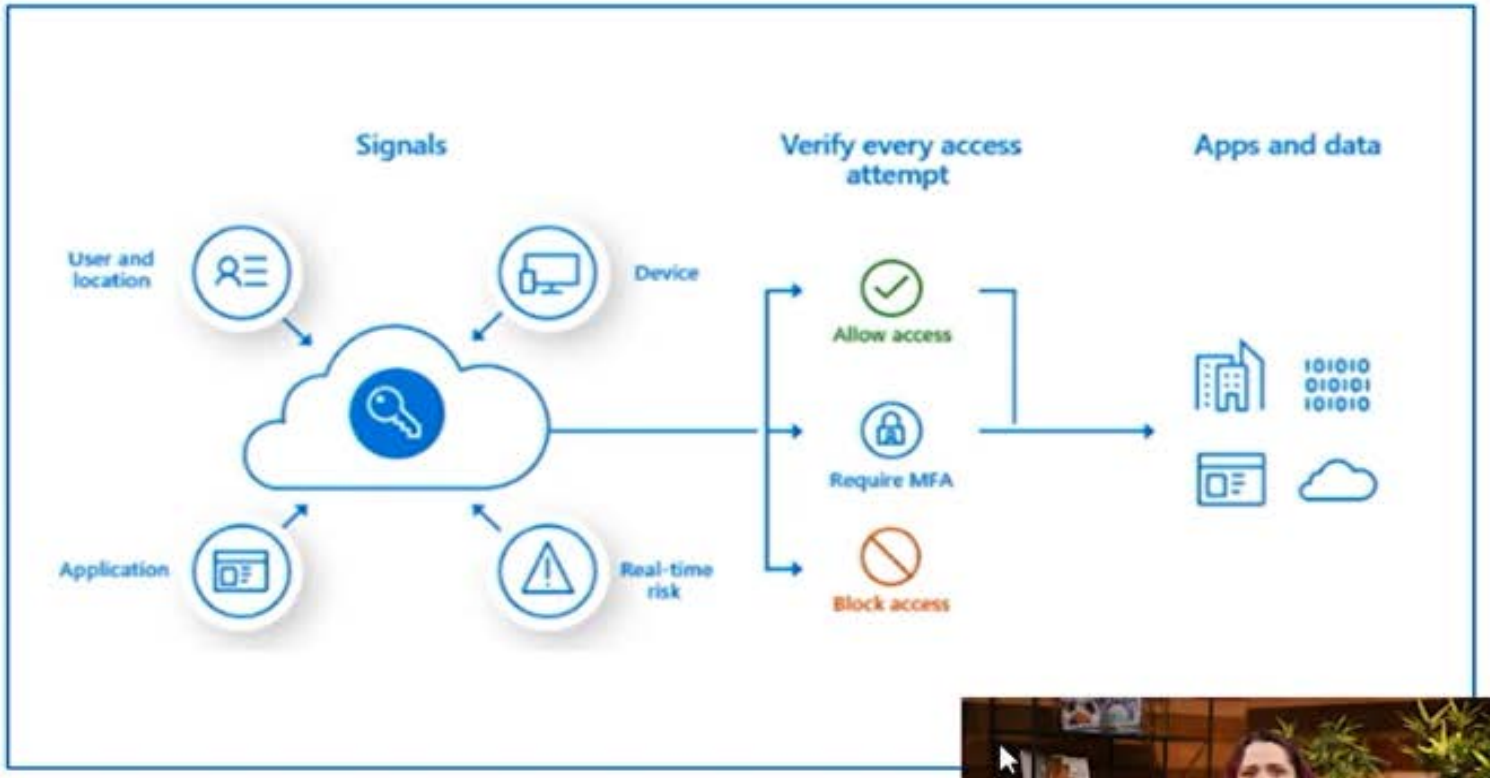
Conditional access

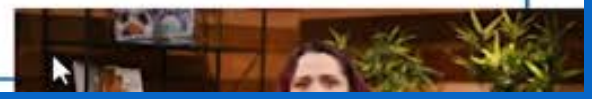
Conditional Access signals:

- 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

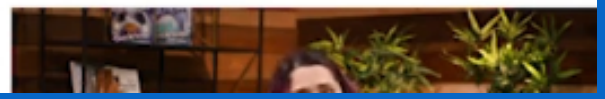
- Join: A new digital identity is created.
- Move: Update access authorizations.
- Leave: Access may need to be removed.

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:

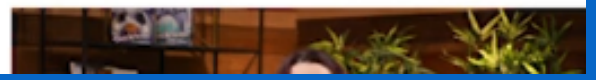
- Automate the detection and remediation of identity-based risks.
- Investigate risks using data in the portal.
- Export risk detection data to third-party utilities for further analysis.

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

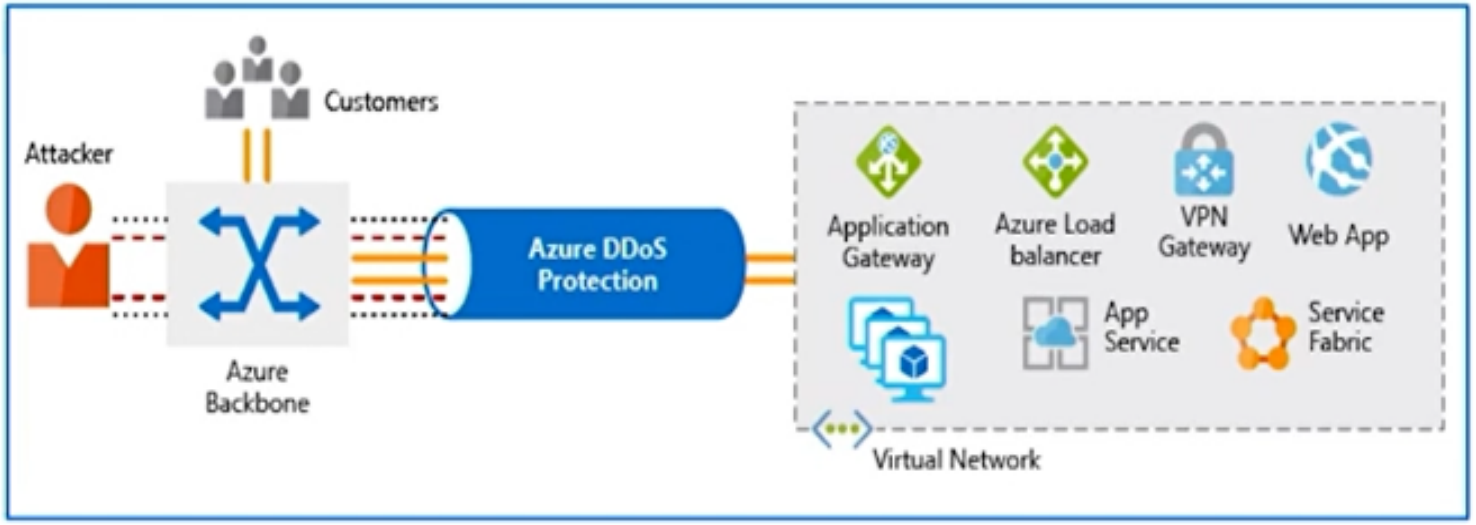
Azure DDoS protection

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

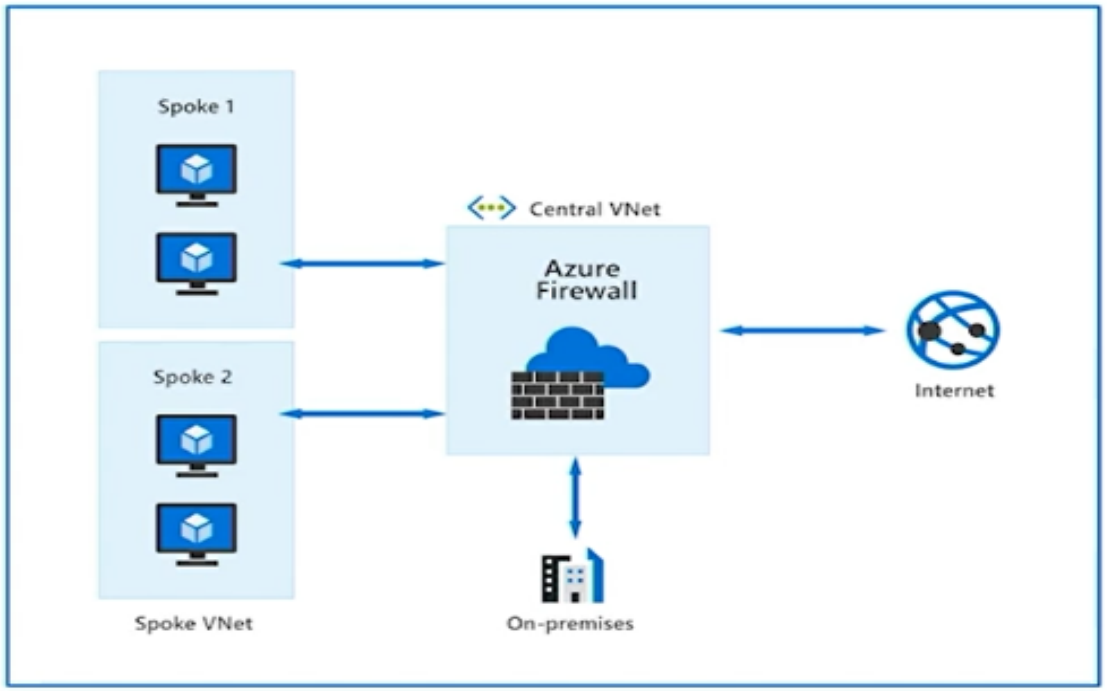


Microsoft Access & Identity Solutions

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

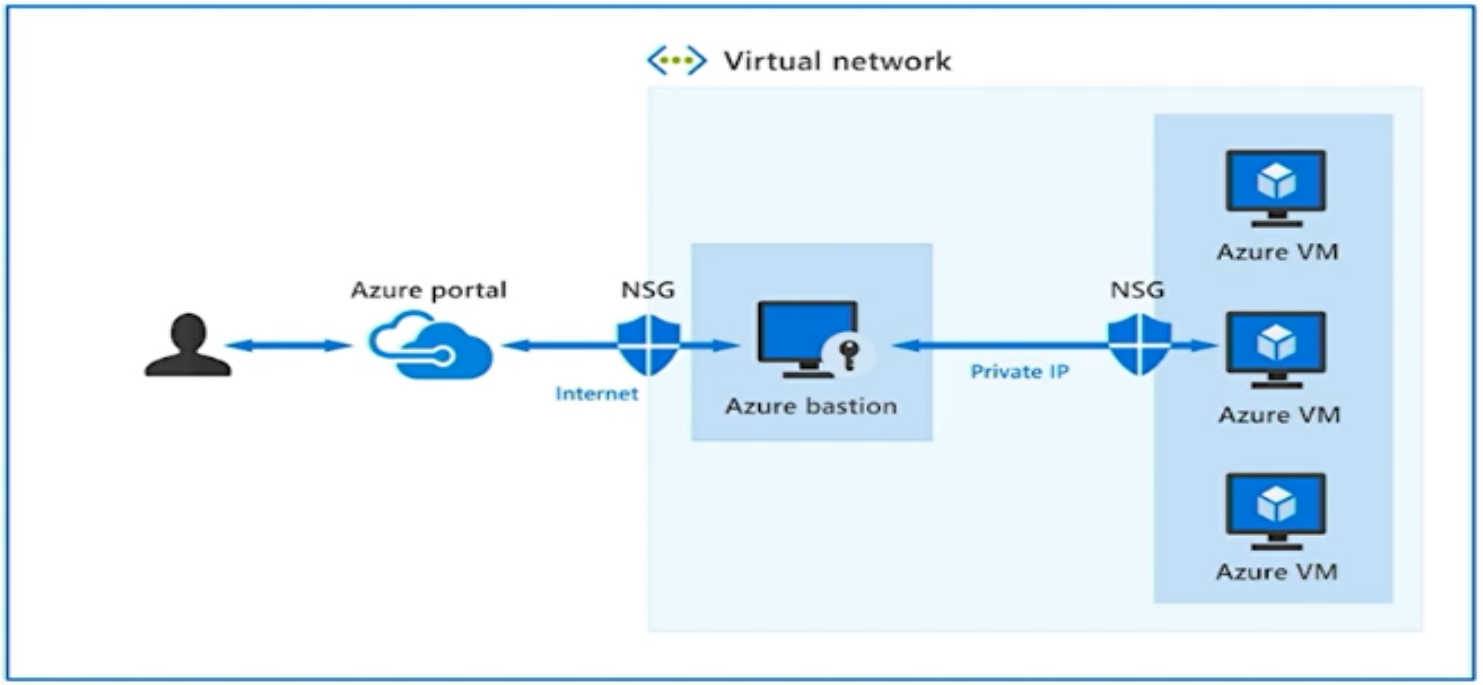


Microsoft Access & Identity Solutions

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.

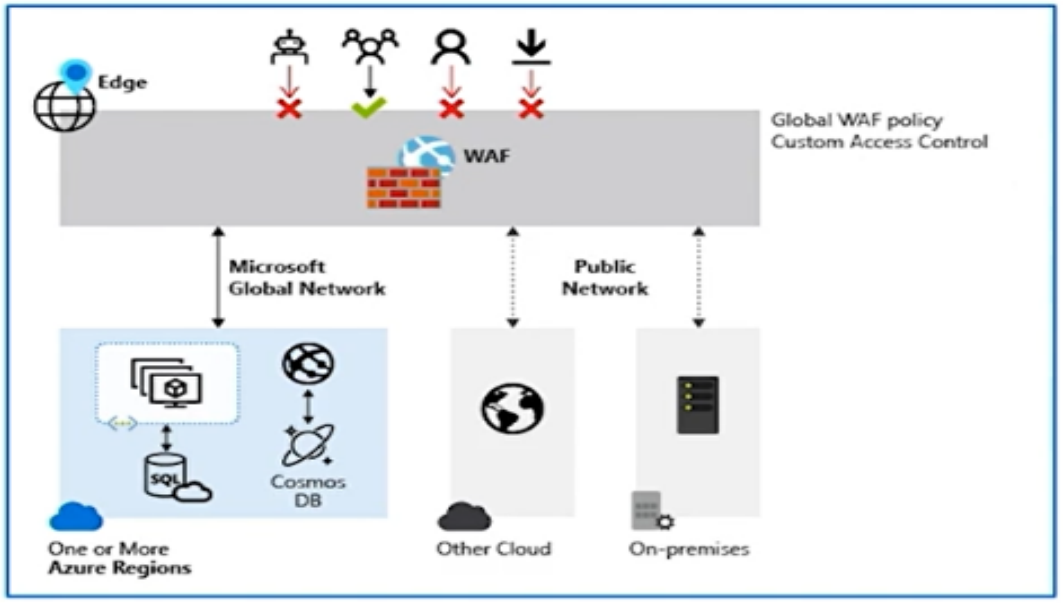


Microsoft Access & Identity Solutions

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	What is Azure Key Vault?
Azure Storage Service Encryption	Secrets management
Azure Disk Encryption	Key management
Transparent data encryption (TDE)	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

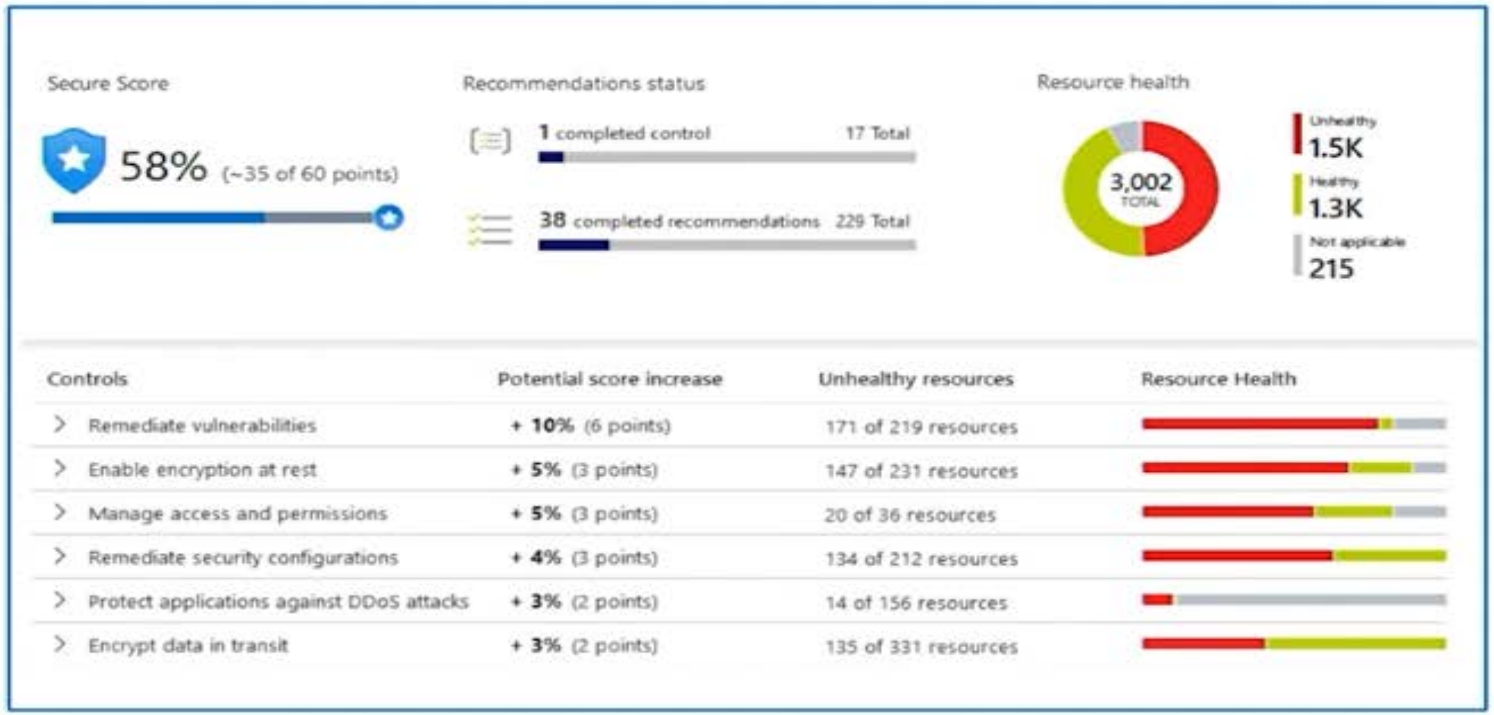
Strengthen security posture across your machines, data services, and applications.

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.



Vidyatech

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

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.

Microsoft Security Solutions

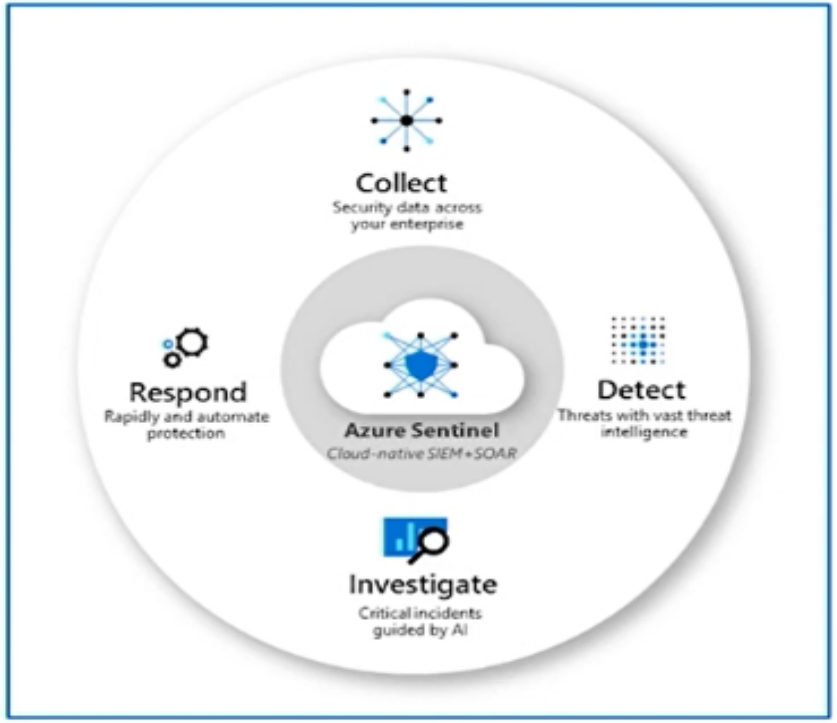
Sentinel provides integrated threat protection (Slide 1)

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.

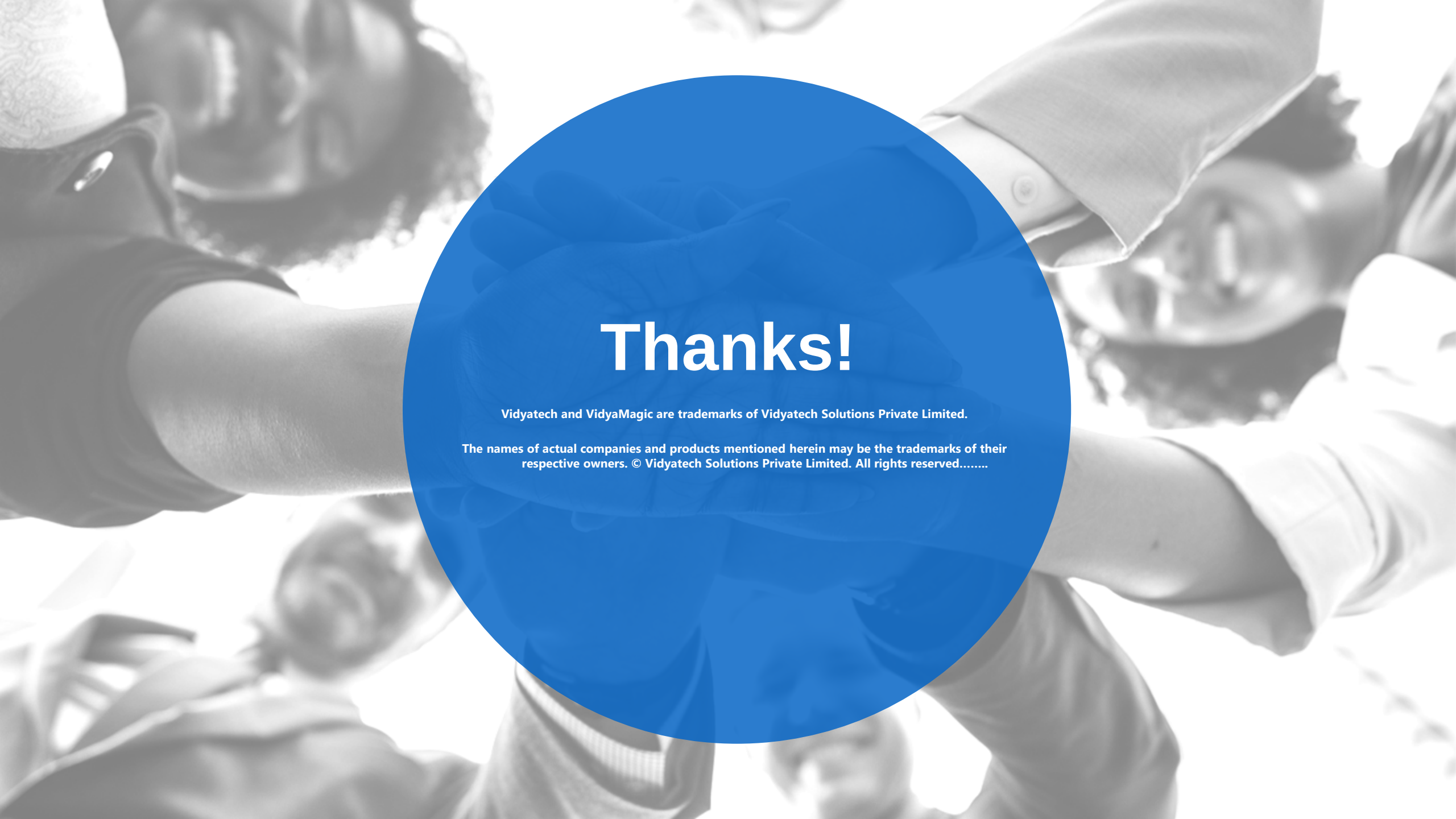
Security automation and orchestration: Integrate with Azure Logic Apps, to create workflows

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!