BAIT 3273 Cloud Computing

Week 10

Security, Responsibility, and Trust in Azure

Lesson Objectives:

- To understand how security responsibility is shared with Azure
- To understand protection can be provided through identity management, regardless of the network you are in

Introduction

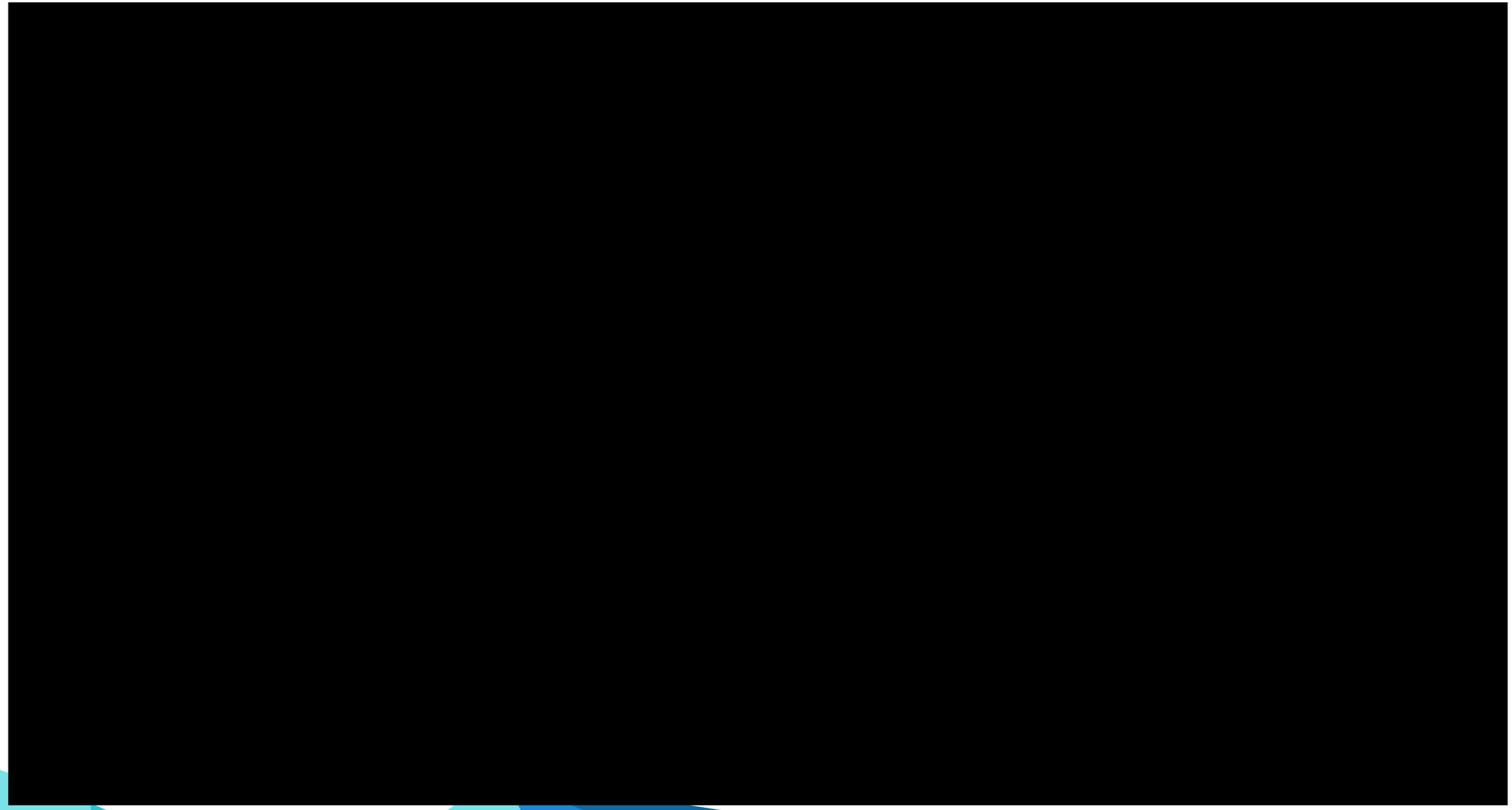
Importance of Security

- Prevent attacks like denial of service attack
- Prevent data breach

Consequences of poor security

- Damages the reputation of your website
- Ruin hard-earned trust between your customers

Introduction

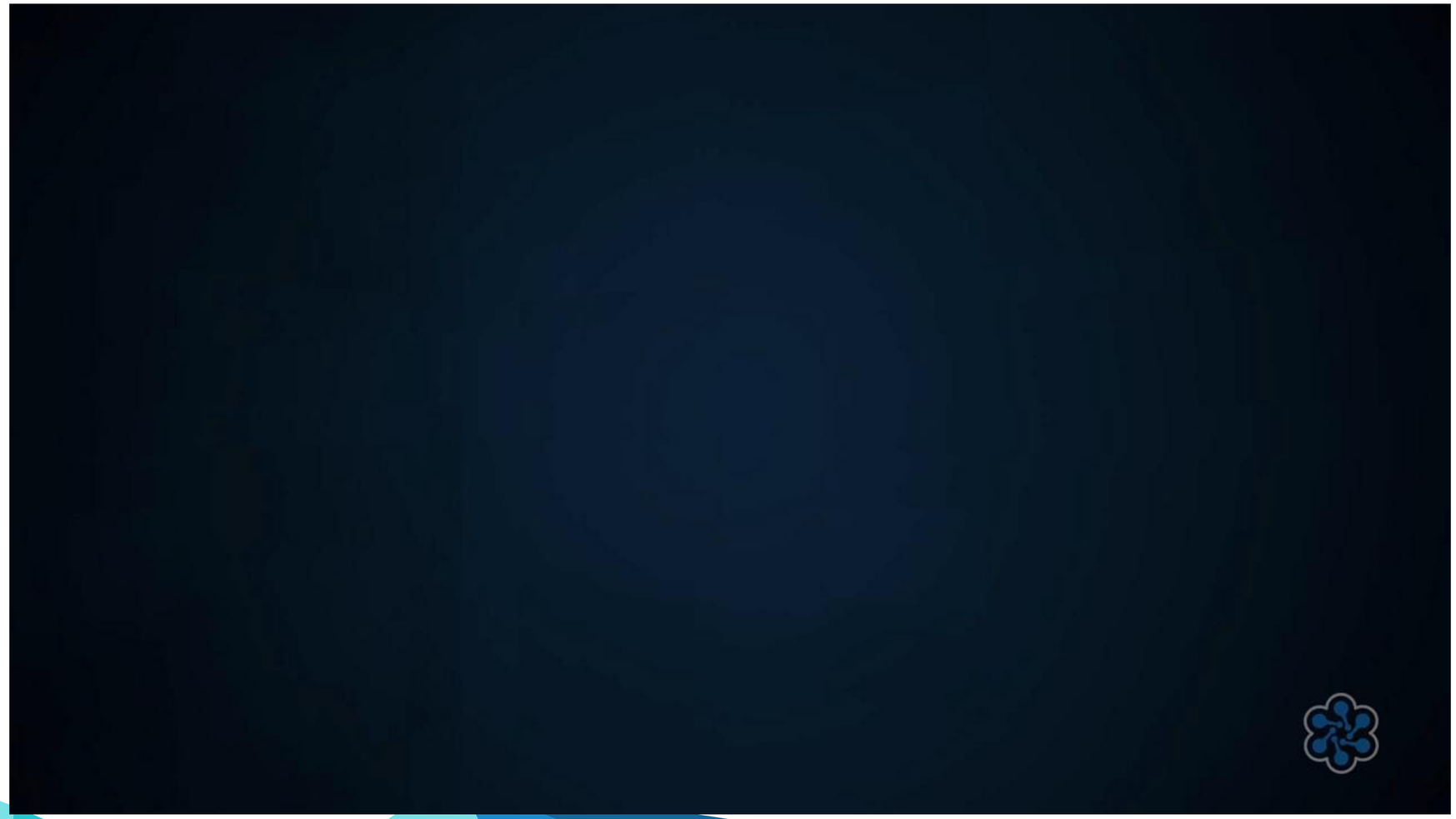


Cloud security is a shared responsibility

- The responsibility of security no longer relies solely on the organization when the computing environments are shifted from customer-controlled datacenters to the cloud.

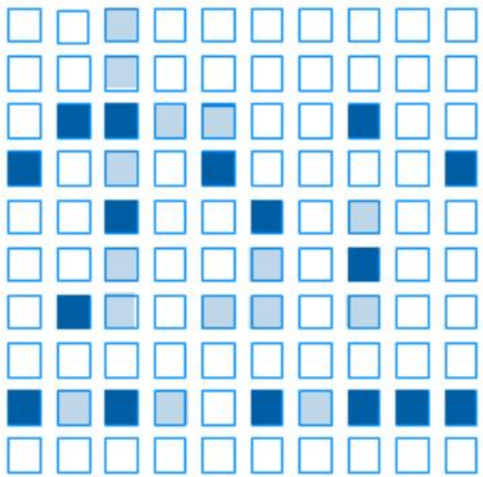
- The cloud providers and customers both share the (ıg the security of operational environment.

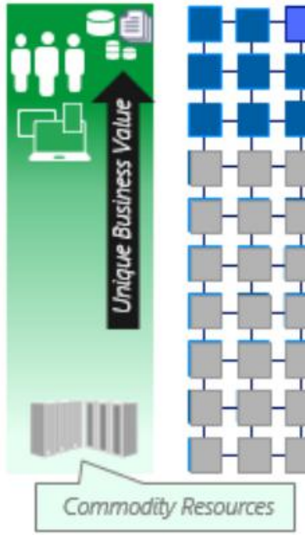
What is shared responsibility



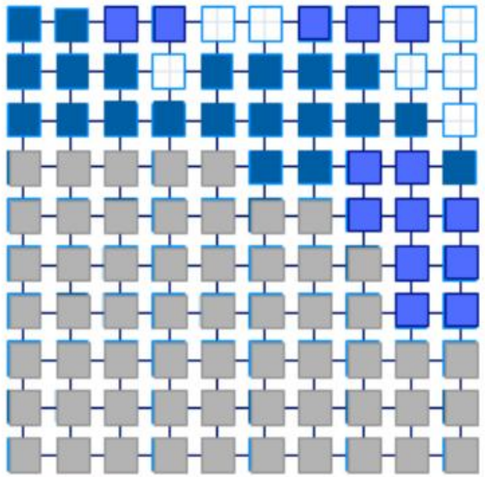
Security Advantages of Cloud Era

TRADITIONAL APPROACH





CLOUD-ENABLED SECURITY



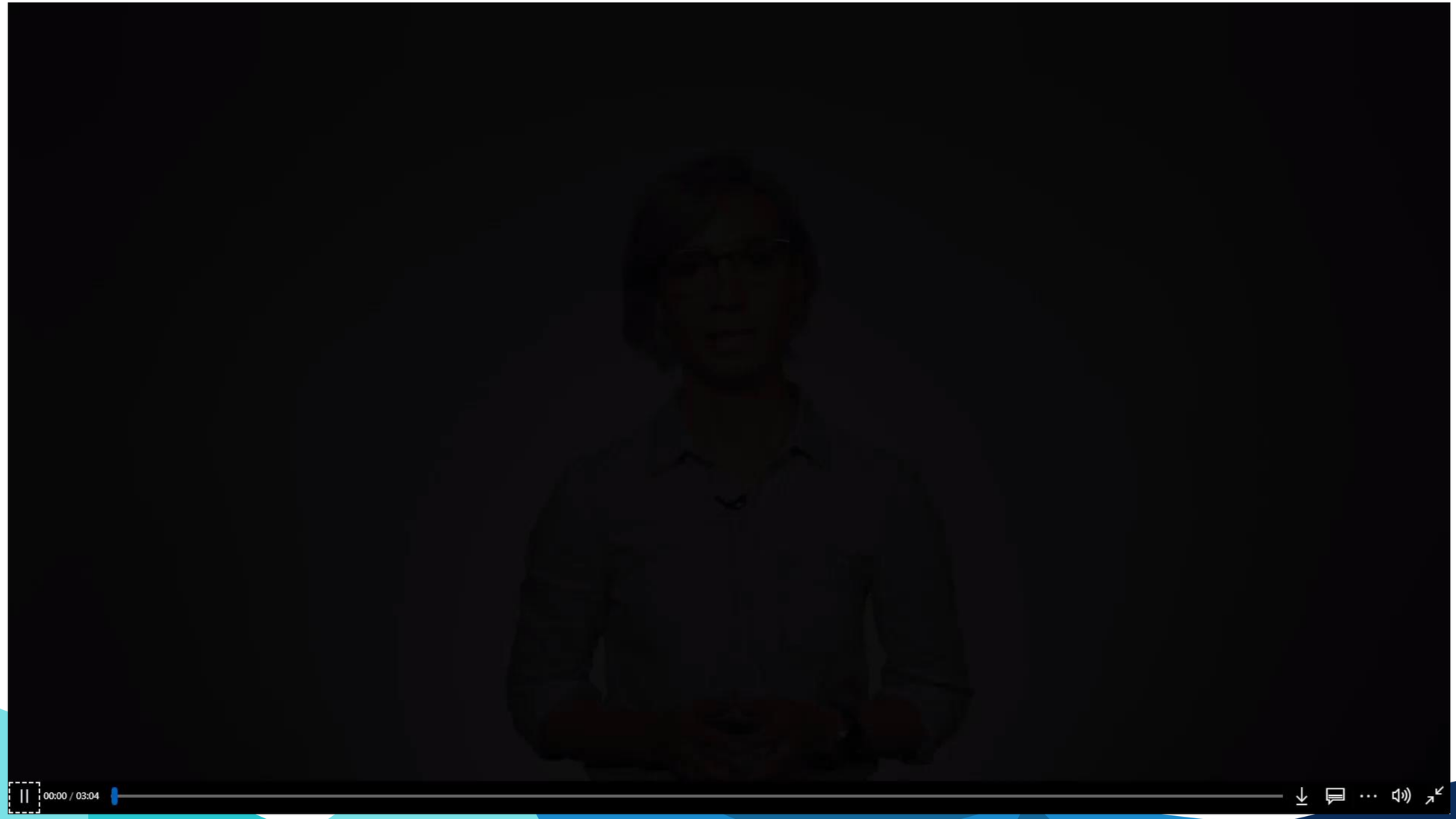
Cloud Technology enables security to:

- Shift commodity responsibilities to provider and re-allocate your resources
- Leverage cloud-based security capabilities for more effectiveness
- Use Cloud intelligence to improve detection/response time

Security is a challenging and under-resourced function

- **Satisfied** responsibility
- Partially met responsibility
- Unmet responsibility
- Cloud Provider responsibility (Trust but verify)

Understand security threats



Infrastructure as a service (IaaS)

- The first shift by customer is from on-premises data centers to
- Customer is still responsible for:
  - Patch and secure operating systems and software
  - Configure the security of network
- Customer benefits from the protection of physical parts of the n

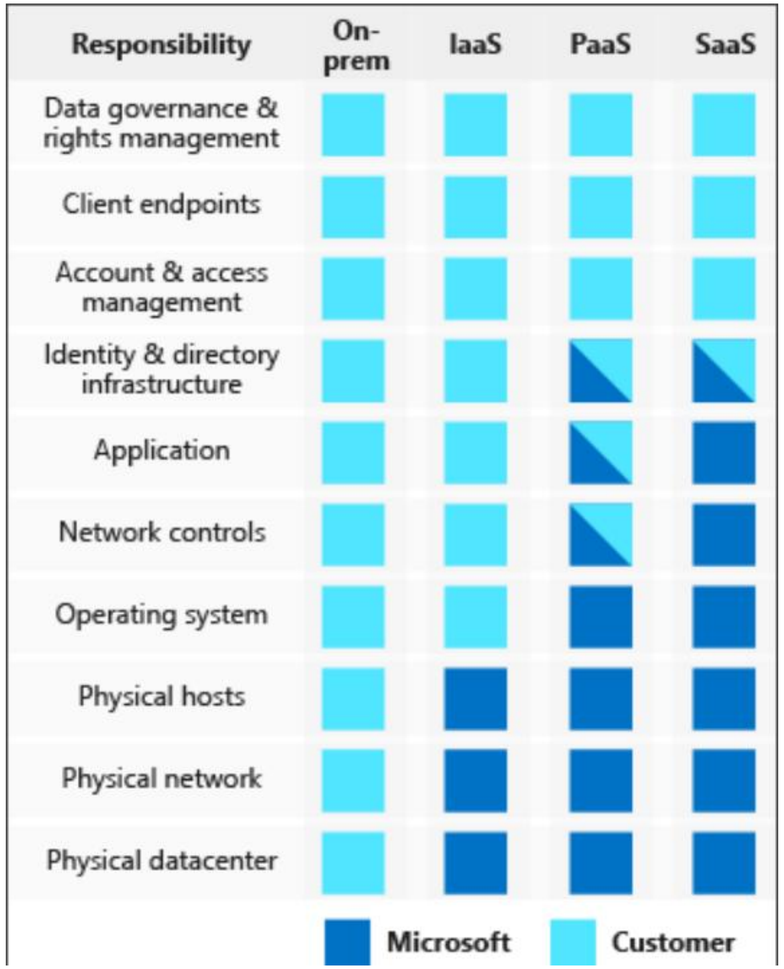
Platform as a service (PaaS)

- Azure takes care of the security for the operating system (OS) and most foundational software like database management systems.
- Azure ensure these systems are updated with latest security patches.
- Can be integrated with Azure Active Directory for access controls.
- Allows user to scale complex, secured systems without building whole infrastructures and subnets.

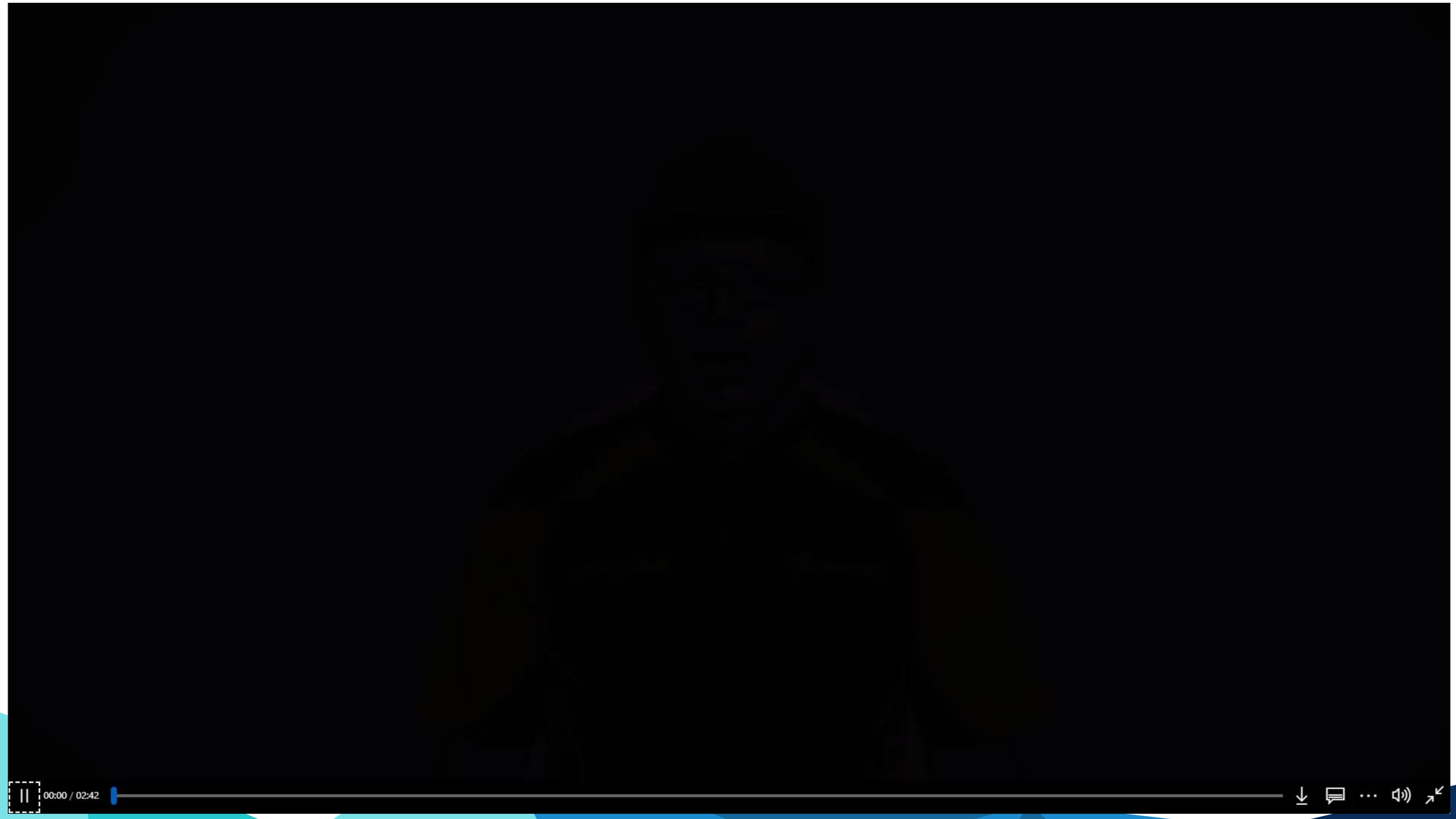
Software as a service (SaaS)

- Outsource almost everything
- Runs with an internet infrastructure
- The software code is configured to be used by the customer but is controlled by the vendor.
    - E.g. Office 365

On-premise vs IaaS vs PaaS vs SaaS

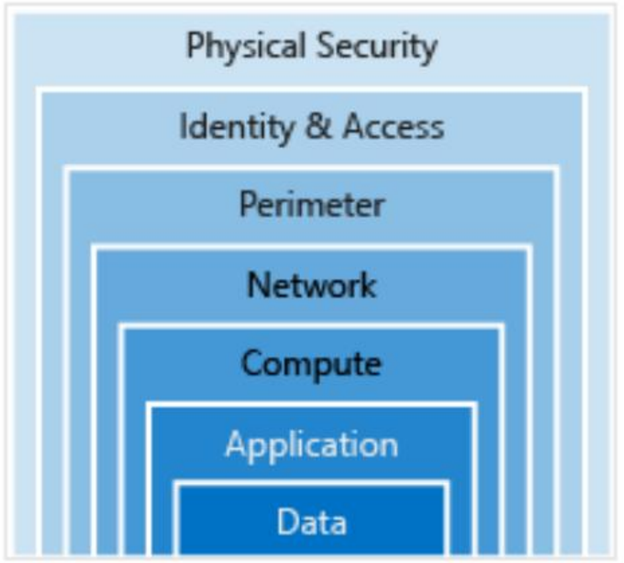


Azure security: you versus the cloud



A layered approach to security

- Microsoft adopted a layered approach to security, both in physical data centers and across Azure services.
- *Defense in depth* is a strategy that employs a series of mechanisms to protect and prevent information from being stolen by unauthorized users.
  - It can be visualized as the data is secured at the center and is being surrounded by a set of concentric rings.
  - Each layer provides additional protections towards the data.



Data

Attackers are usually after the data:

- Stored in a database
- Stored on disk inside virtual machines
- Stored on a SaaS application such as Office 365
- Stored in cloud storage

Those storing and controlling access to data is responsible to ensure that they are secured.

Application

- Ensure applications are secure and free of vulnerabilities.
- Uses a secure storage medium to store sensitive confidential information of application.
- Make security as mandatory design requirement for all application developments.

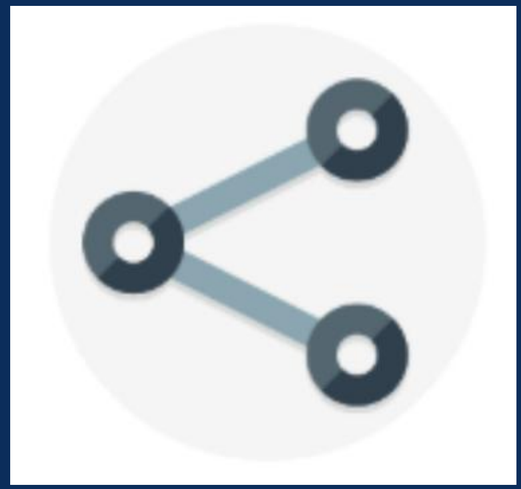
Application development life cycle that integrates security is able to reduce the number of vulnerabilities.

Compute

- Secure access to virtual machines.
- Implement endpoint protection and keeps systems patched and current.

The focus of this layer is ensuring the compute resources of customers are in secure state where customers have controls to minimize security risks.

Networking



- Restrict communication between resources.
- Deny by default.
- Regulate inbound internet access and limit outbound, where appropriate.
- Enforce secure connectivity to on-premises networks.

The focus of this layer is on regulating the network connectivity across all the customer resources and allow only what is required.

Perimeter

- Filter large-scale attacks through distributed denial of service (DDoS) protection.
- Use perimeter firewalls to determine any malicious attacks against the network and alert the customers.

In this layer, it is concerned with protecting the customer resources from network-based attacks.

Identity and access

- Administer access to infrastructure and change control.
- Use single sign-on and multi-factor authentication.
- Examine events and changes.

The focus of this layer is about:

- Security of identities
- Access granted
- Logging changes

Physical security

- First line of defense.
- Physical building security that controls the access to computing hardware within the data center.

Physical security provide safeguards against access to assets.

Defense in Depth Security

Azure Security Center

- A monitoring service that provides threat protection across all services both in Azure, and on-premises.
- Security Center can:
  - Provide security recommendations
  - Monitor security settings
  - Continuously monitor all services
  - Detect and block malware
  - Analyze and identify potential attacks
  - Provide just-in-time access control for ports

Azure Security Center Available Tiers

Free

- Available as part of Azure subscription.
- Limited to assessments and recommendations of Azure resour

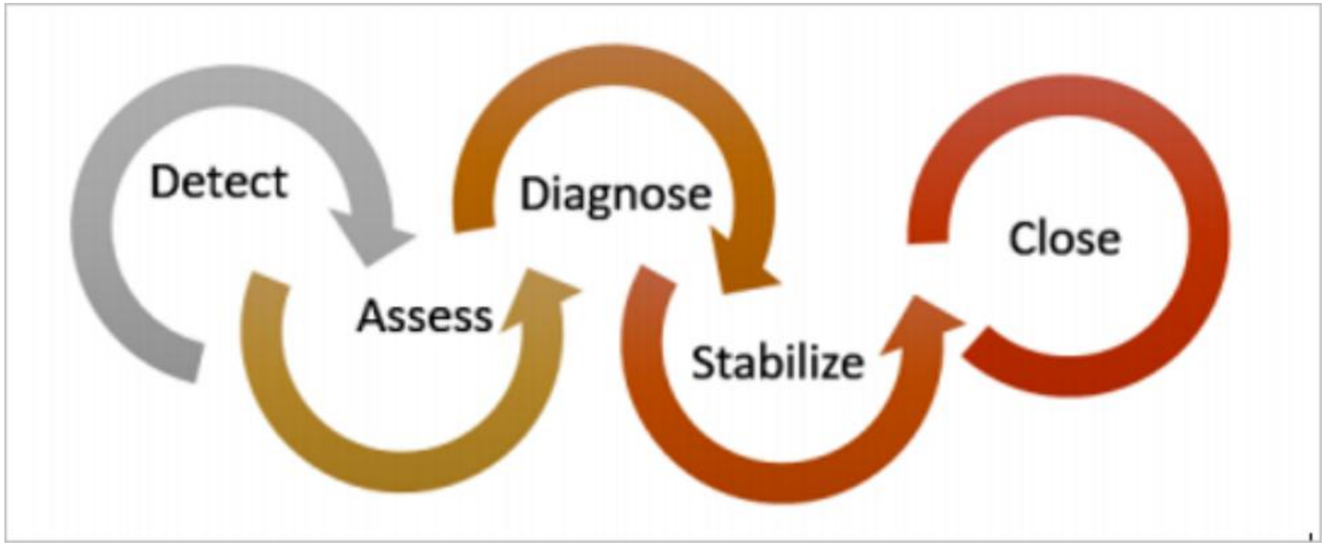
Standard

- Includes a full suite of security-related services.
- E.g. threat detection etc.

cenarios of using Azure Security Cente

1. Use Security Center for incident response

- Azure Security Center can be used in different stages:
  - Detect
  - Assess
  - Diagnose

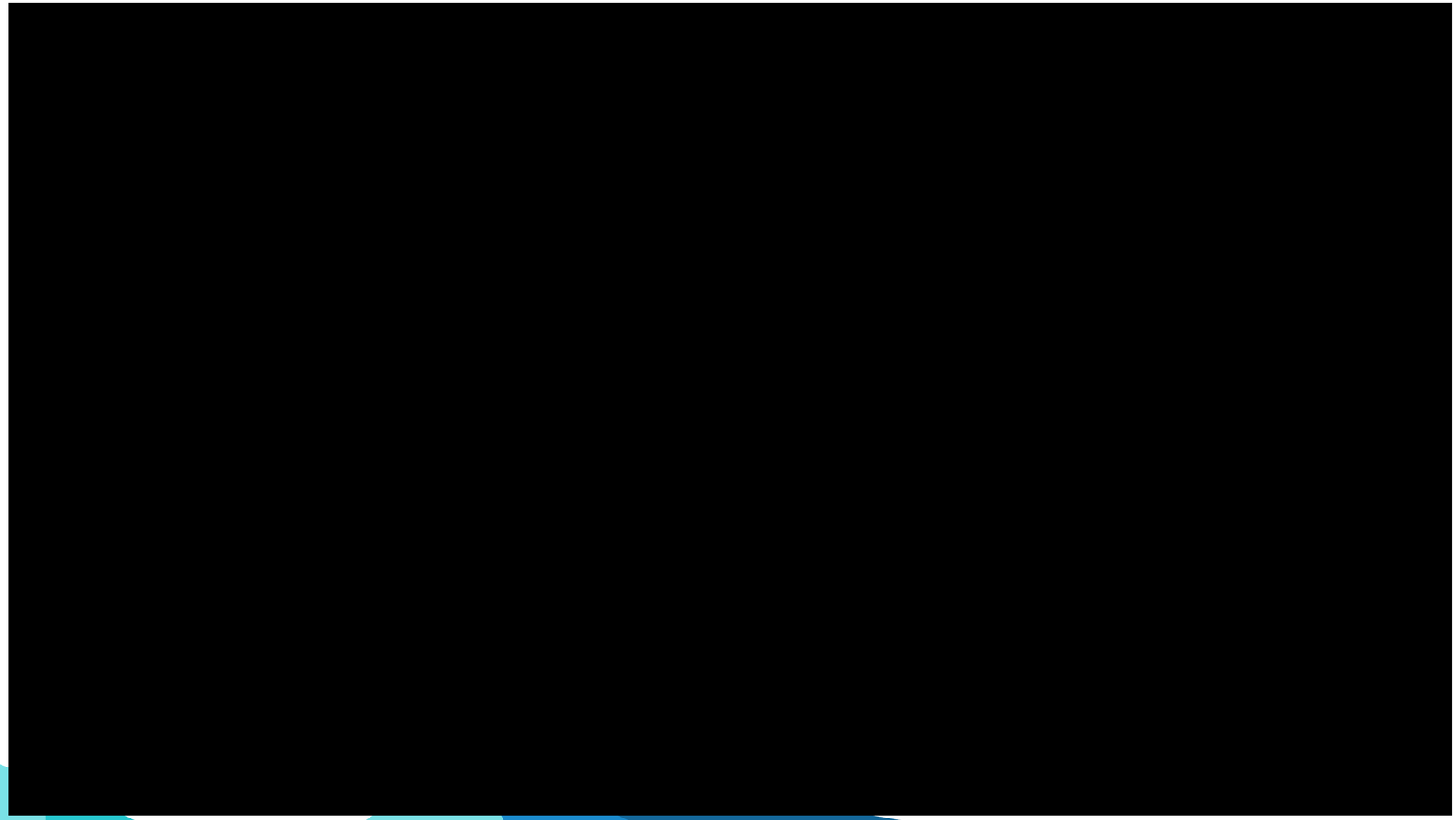


cenarios of using Azure Security Cente

2. Use Security Center recommendations to enhance security

- Define policies according to company's security requirements.
- Security Center analyses the security state and creates recommendations based on security policy.

Azure Security Center



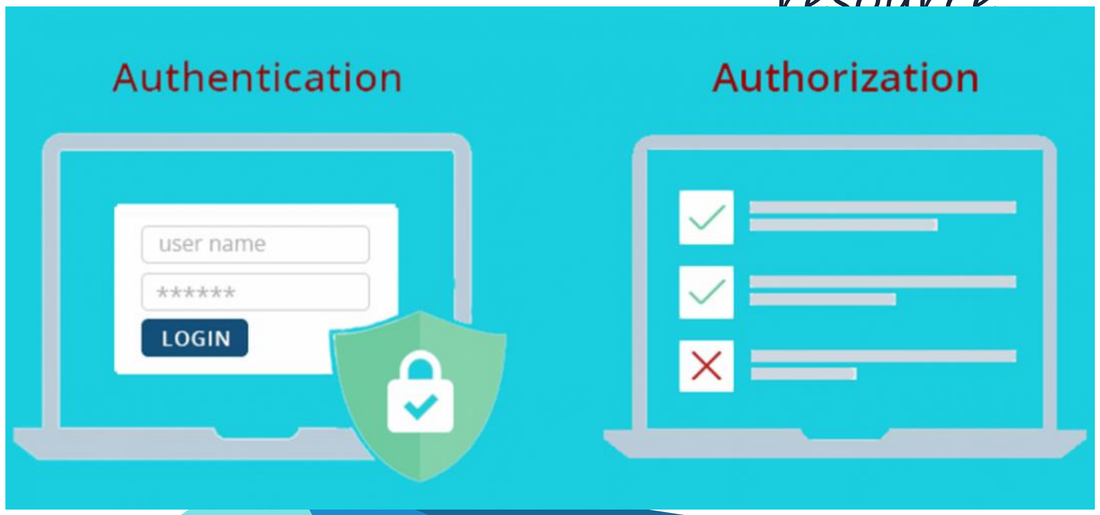
Identity and access

Authentication

- The process of establishing the identity of a person or service that is looking to access a resource.

Authorization

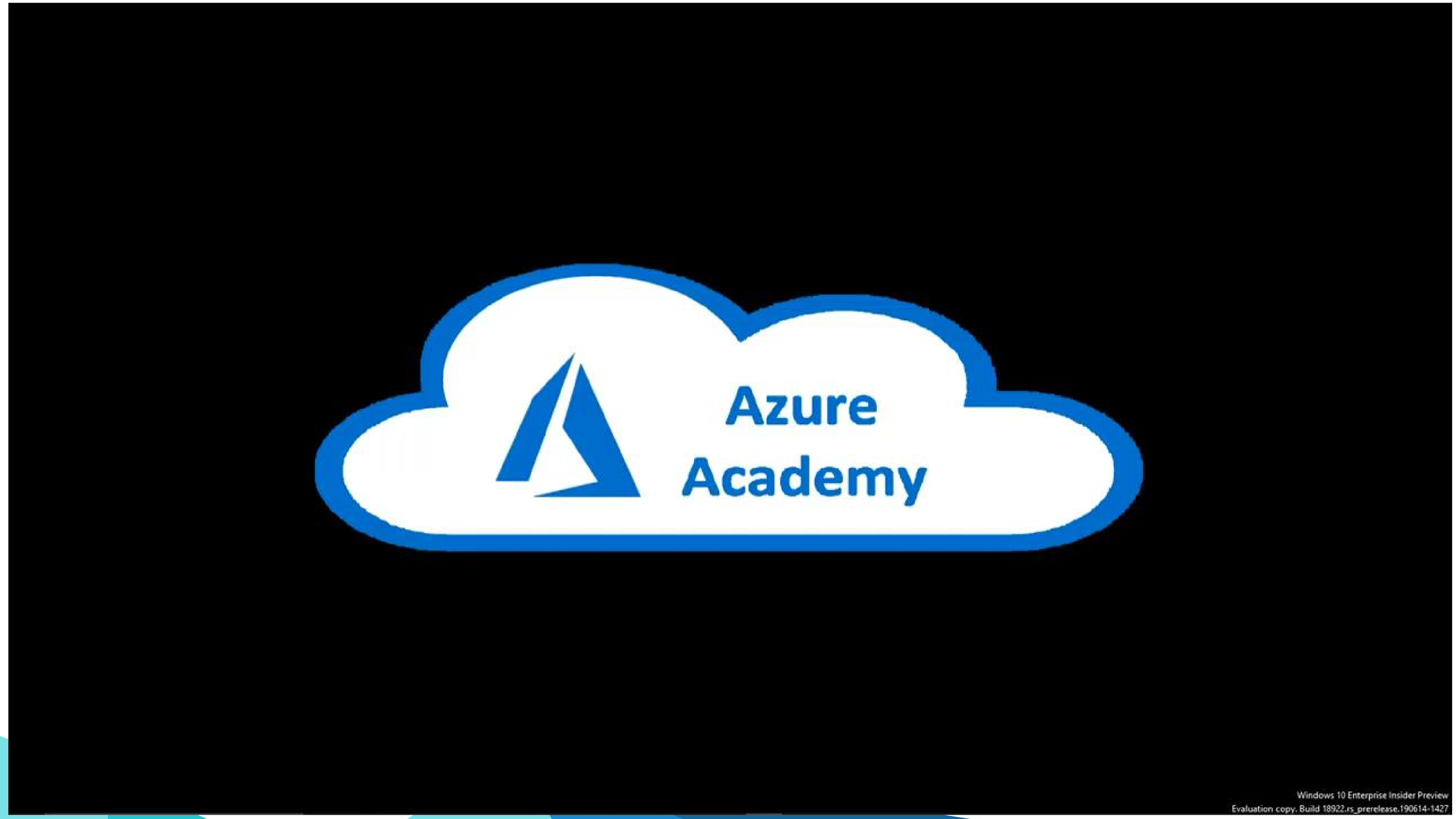
- The process of establishing the level of access that an authenticated person or service has towards a resource



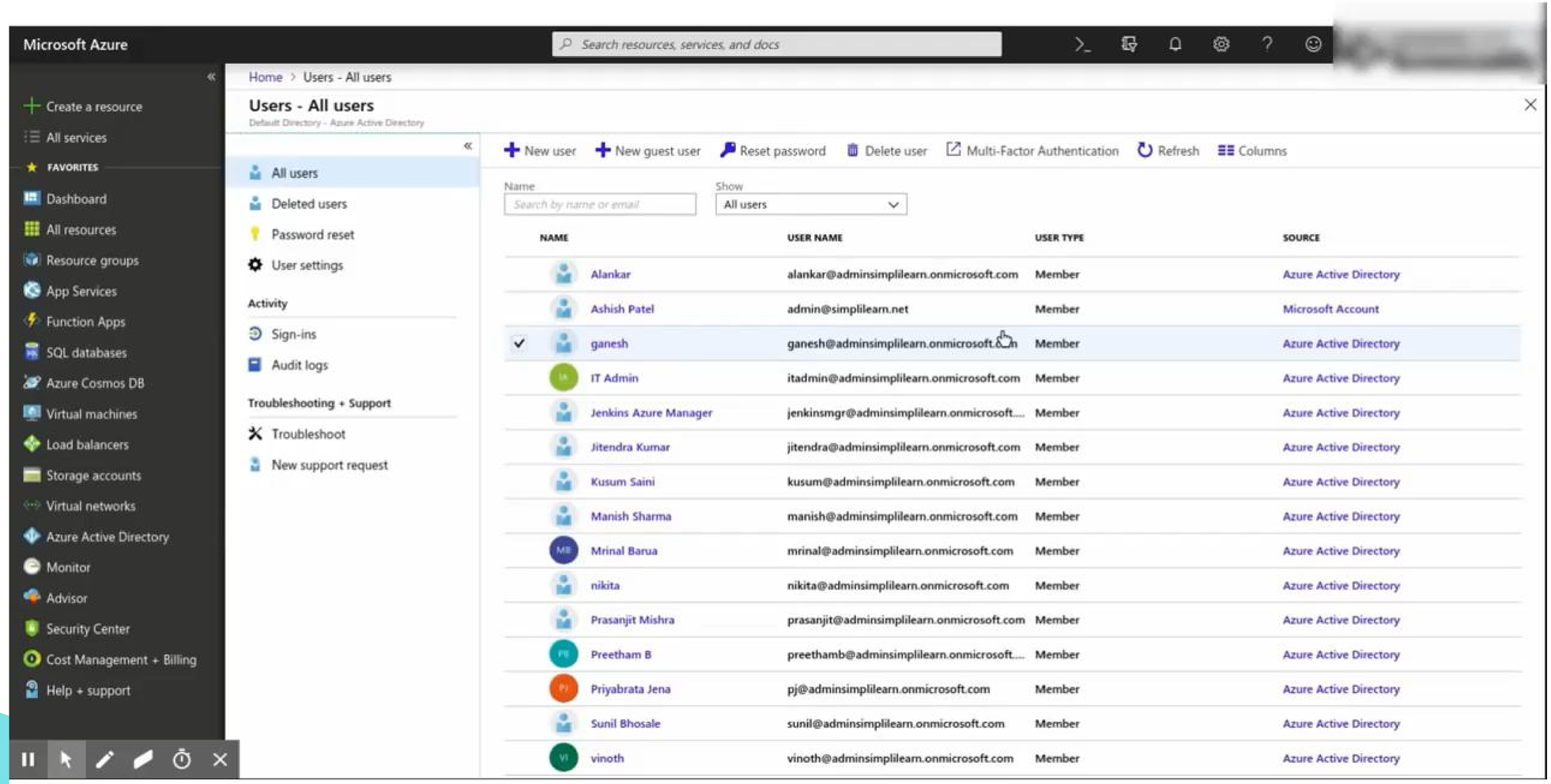
What is Azure Active Directory?

- A cloud-based identity service.
- Support synchronizing with existing on-premises Active Directory or can be used stand-alone.
- Azure Active Directory services:
  - Authentication
  - Single-Sign-On (SSO)
  - Application Management
  - Business to business (B2B) identity services
  - Business-to-Customer (B2C) identity services
  - Device Management

Azure Active Directory



Azure Active Directory Demo



simplilearn

Single sign-on

- Users only need to remember a single ID and password to access multiple applications.
- Reduces the effort required to modify or disable accounts.

Multi-factor authentication

- Multi-factor authentication (MFA) further enhance the security for identities by requiring additional elements for authentication.

- Categories of elements:
  - *Something you know – e.g. security question*
  - *Something you possess – e.g. mobile app*
  - *Something you are – e.g. biometric property*

Azure Multi-factor authentication

Providing identities to services

Service principals

- *Identity* – a thing that can be authenticated.
- *Principal* – An identity acting with certain roles or claims.
- Service principal is an identity that is adopted by a service or applic

Managed identities

- Can be created in an instant given that it is supported by the Azure service.
- The authentication of service and account management are taken care by Azure infrast

Role-based access control

- Roles determine the users access to an Azure service instance.
  - E.g. “Read-only” or “Contributor”

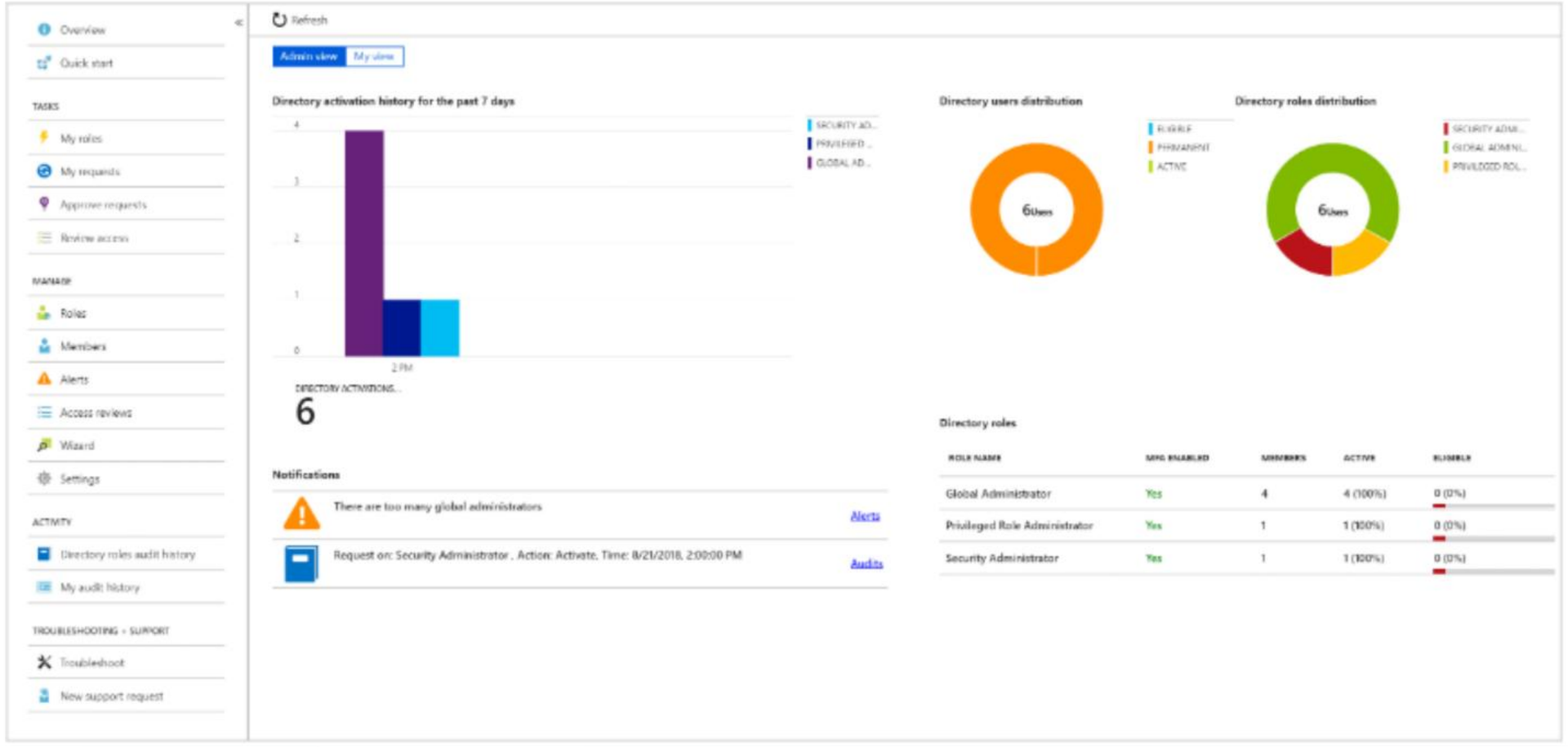
- Identities can be either mapped to roles directly or through group membership.

- Roles can be granted at the individual service instance level.

Role-based access control

Privileged Identity Management

- An additional, paid-for offering
- Provides oversight such as role assignments, self-service etc.



Summary

- Identity enable us to maintain a security perimeter
- Single sign-on and appropriate role-based access configuration ensure the resource is accessible by certain people only.

Thanks!