WEBINAR

Building a Fortress in Azure

Versterk je Azure oplossing met de 'Defense in Depth' strategie

28/11/2023 | Steven van den Beemt

Classification: Training (R5)

Algemene informatie en ‘huisregels’ van het fort

WEBINAR

Building a **Fortress** in Azure

- De webinar wordt opgenomen
- Slides en opname worden achteraf gedeeld
- Q&A bewaren we tot het eind
- Graag je microfoon uitgeschakeld houden
- Camera’s aan: optioneel, liefst wel tijdens Q&A
- Eet smakelijk!

Hello World!

Steven van den Beemt

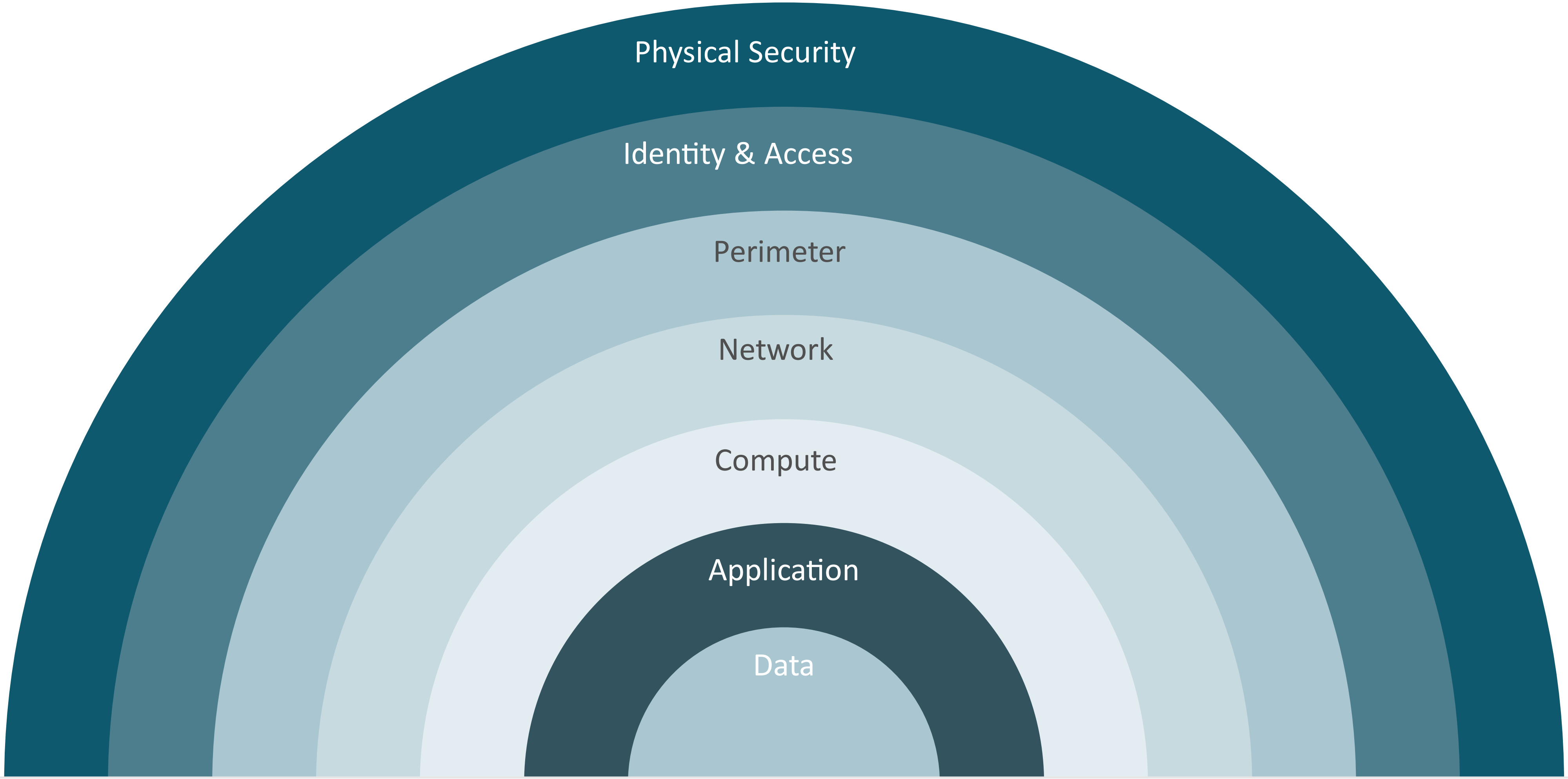
Cloud Architect @ICT Group

Microsoft CERTIFIED
AZURE SOLUTIONS ARCHITECT
EXPERT
Microsoft CERTIFIED
CYBERSECURITY ARCHITECT
EXPERT
Microsoft CERTIFIED
DEVOPS ENGINEER
EXPERT
MICROSOFT CERTIFIED TRAINER
Microsoft
MCT
Trainer
2023 - 2024

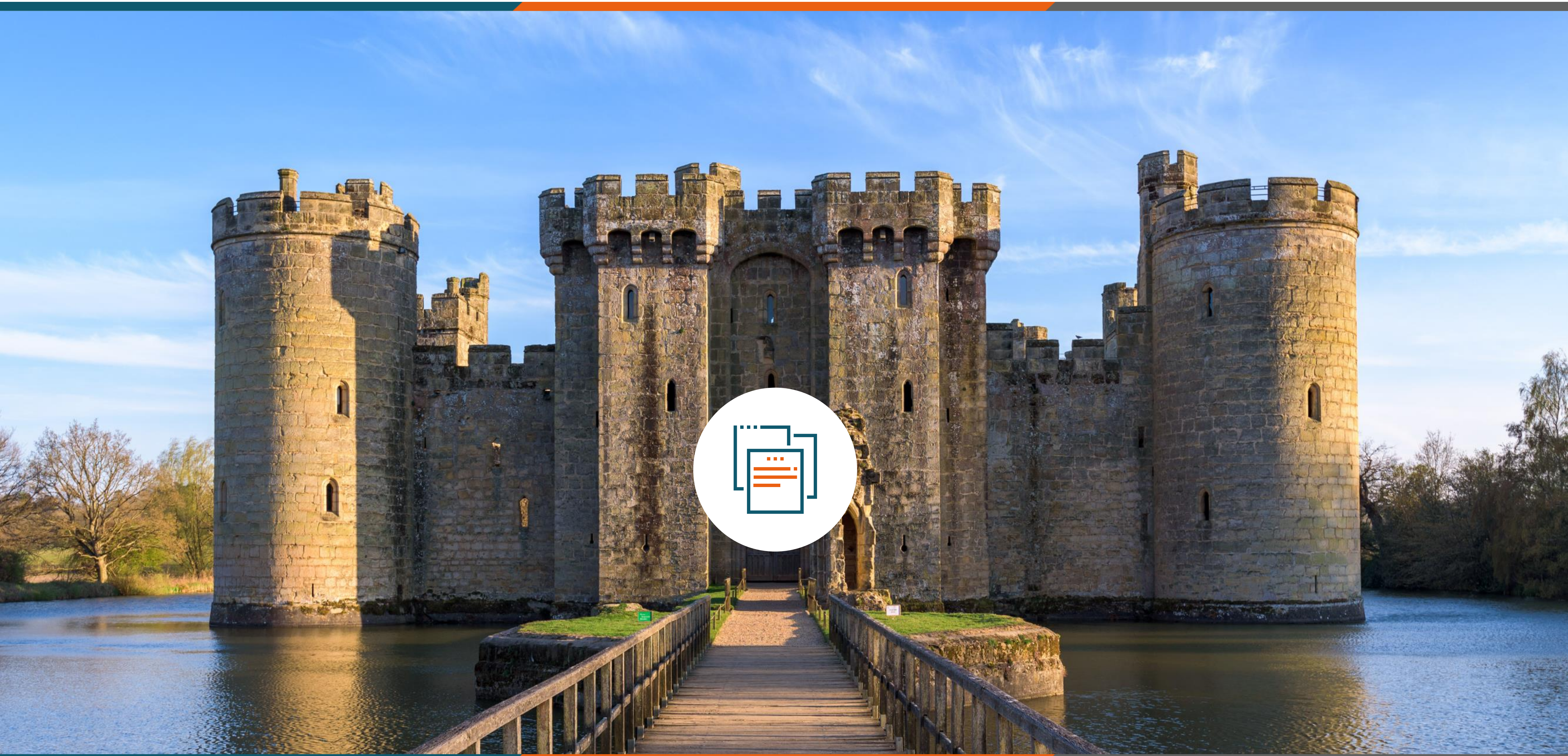
Goal

- You will learn how the defense in depth model can increase the security of your solution.
- You will learn the principles of the zero trust model.
- You will learn which controls Azure offers to make your solution more secure.
- You gain inspiration for your own projects!

Defense in depth

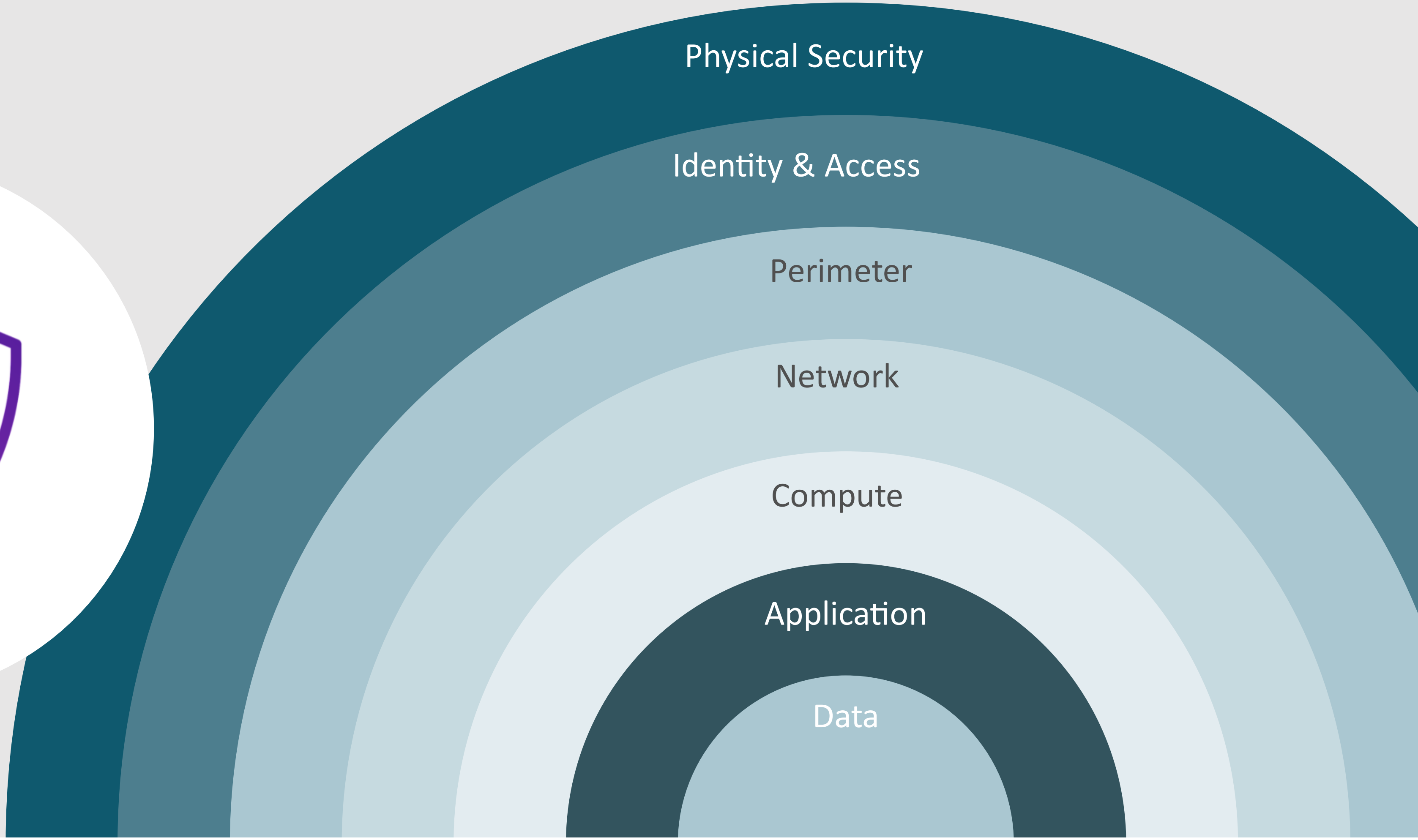


Once upon a time...



Times have changed!

Defense in depth & Zero Trust



Physical Security

Identity & Access

Perimeter

Network

Compute

Application

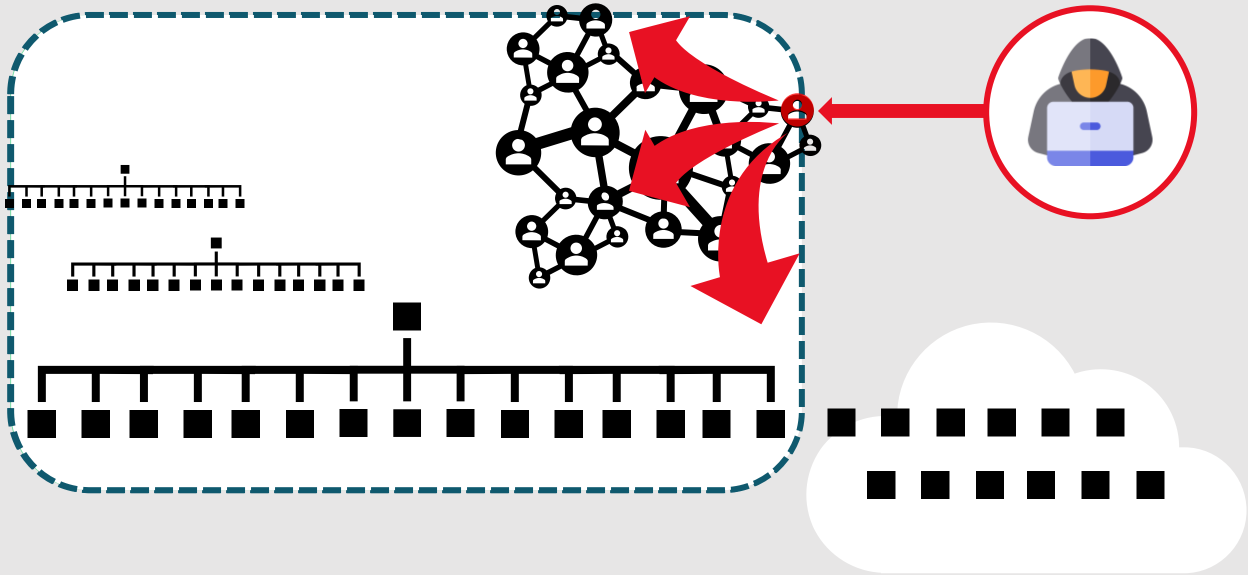
Data

What is **Zero Trust?**

Why are we having a Zero Trust conversation?

Keep Assets away from Attackers

Zero Trust



IT Security is Complex

- Many Devices, Users, & Connections

“Trusted network” security strategy

- Initial attacks were network based
- *Seemingly* simple and economical
- Accepted lower security within the network

Assets increasingly leave the network

- BYOD, WFH, Mobile, and SaaS

Attackers shift to identity attacks

- Phishing and credential theft
- Security teams often overwhelmed

Classification: Training (R5)

Microsoft Zero Trust Principles

Guidance for technical architecture

Verify explicitly

Always validate all available data points including

- User identity and location
- Device health
- Service or workload context
- Data classification
- Anomalies

Use least privilege access

To help secure both data and productivity, limit user access using

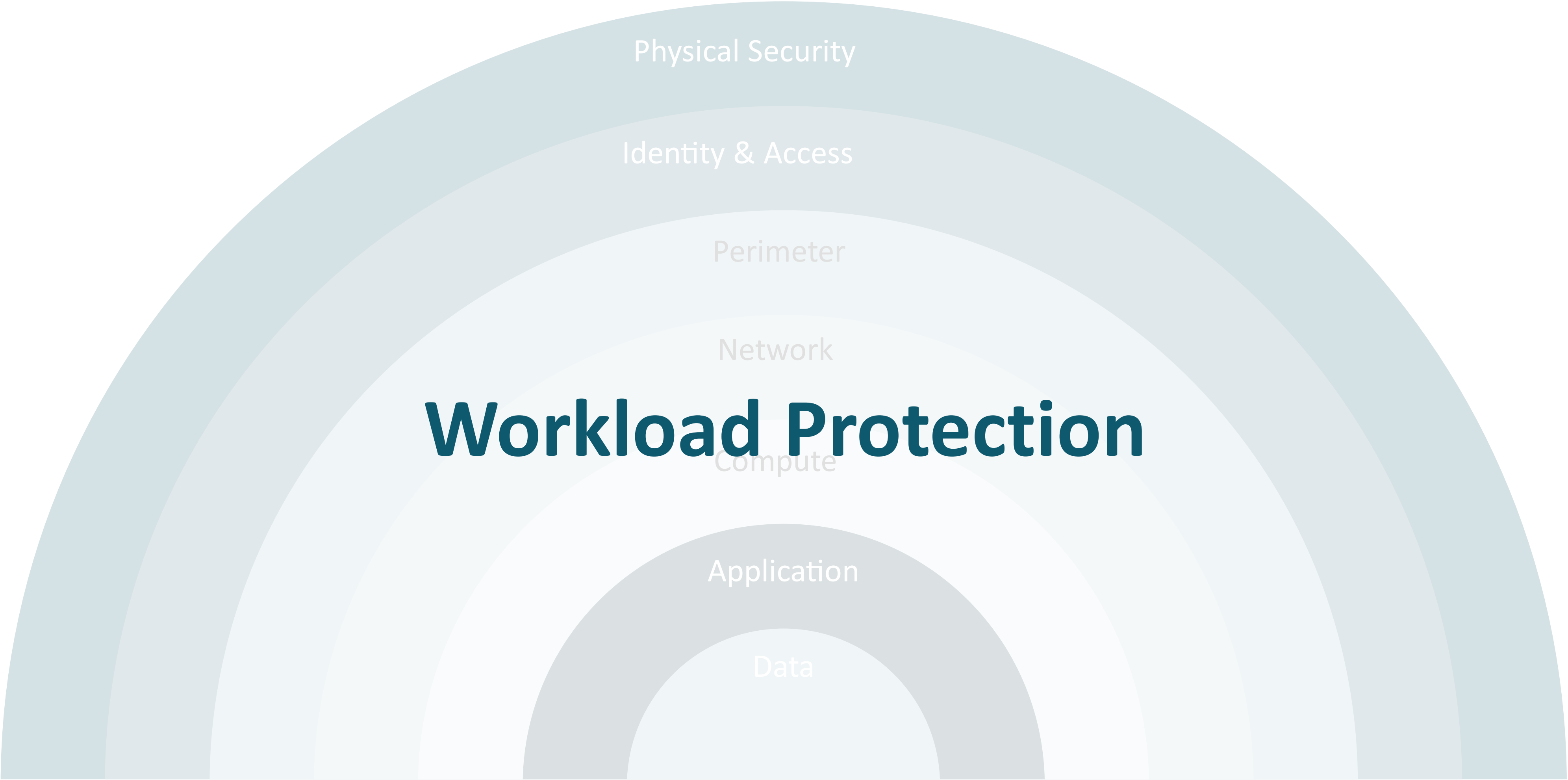
- Just-in-**time** (JIT)
- Just-**enough**-access (JEA)
- Risk-based **adaptive** polices
- Data protection against **out of band** vectors

Assume breach

Minimize blast radius for breaches and prevent lateral movement by

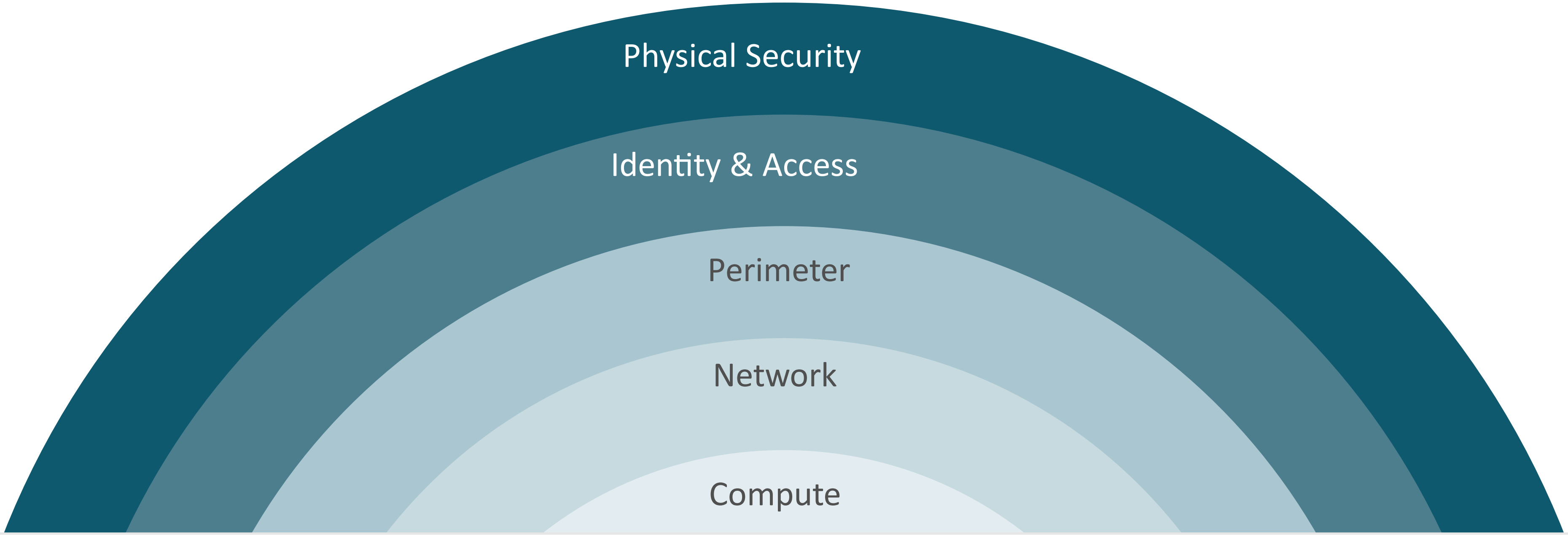
- **Segmenting access** by network, user, devices, and app awareness.
- **Encrypting** all sessions end to end.
- **Use analytics** for threat detection, posture visibility and improving defenses

Agenda



Workload Protection

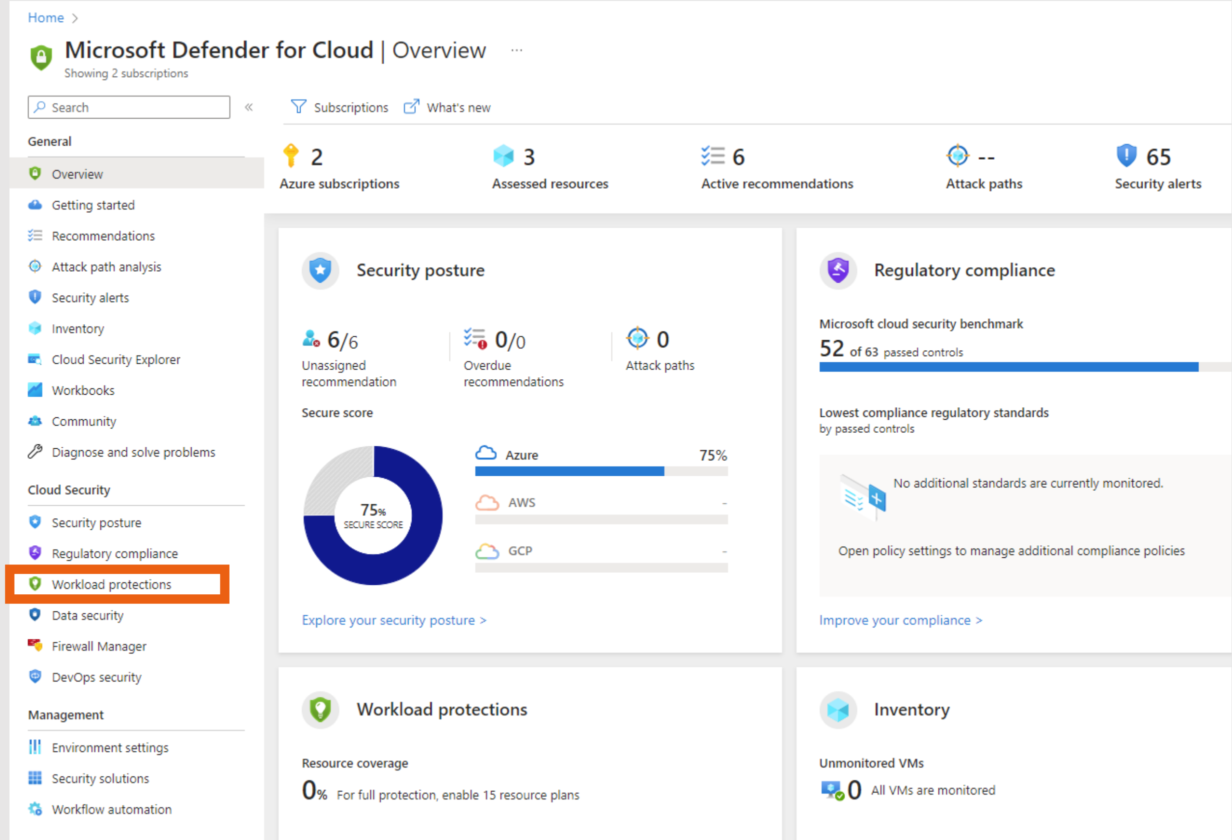
Classification: Training (R5)



Workload Protection

Microsoft Defender for Cloud

- Microsoft Defender for Cloud
  - Regulatory Compliance
  - Security Posture Management
  - **Workload Protection**



Microsoft Defender for Cloud | Overview

Showing 2 subscriptions

2 Azure subscriptions

3 Assessed resources

6 Active recommendations

-- Attack paths

65 Security alerts

Security posture

6/6 Unassigned recommendation

0/0 Overdue recommendations

0 Attack paths

Secure score

75% SECURE SCORE

Azure	75%
AWS	-
GCP	-

Explore your security posture >

Regulatory compliance

Microsoft cloud security benchmark

52 of 63 passed controls

Lowest compliance regulatory standards by passed controls

No additional standards are currently monitored.

Open policy settings to manage additional compliance policies

Improve your compliance >

Workload protections

Resource coverage

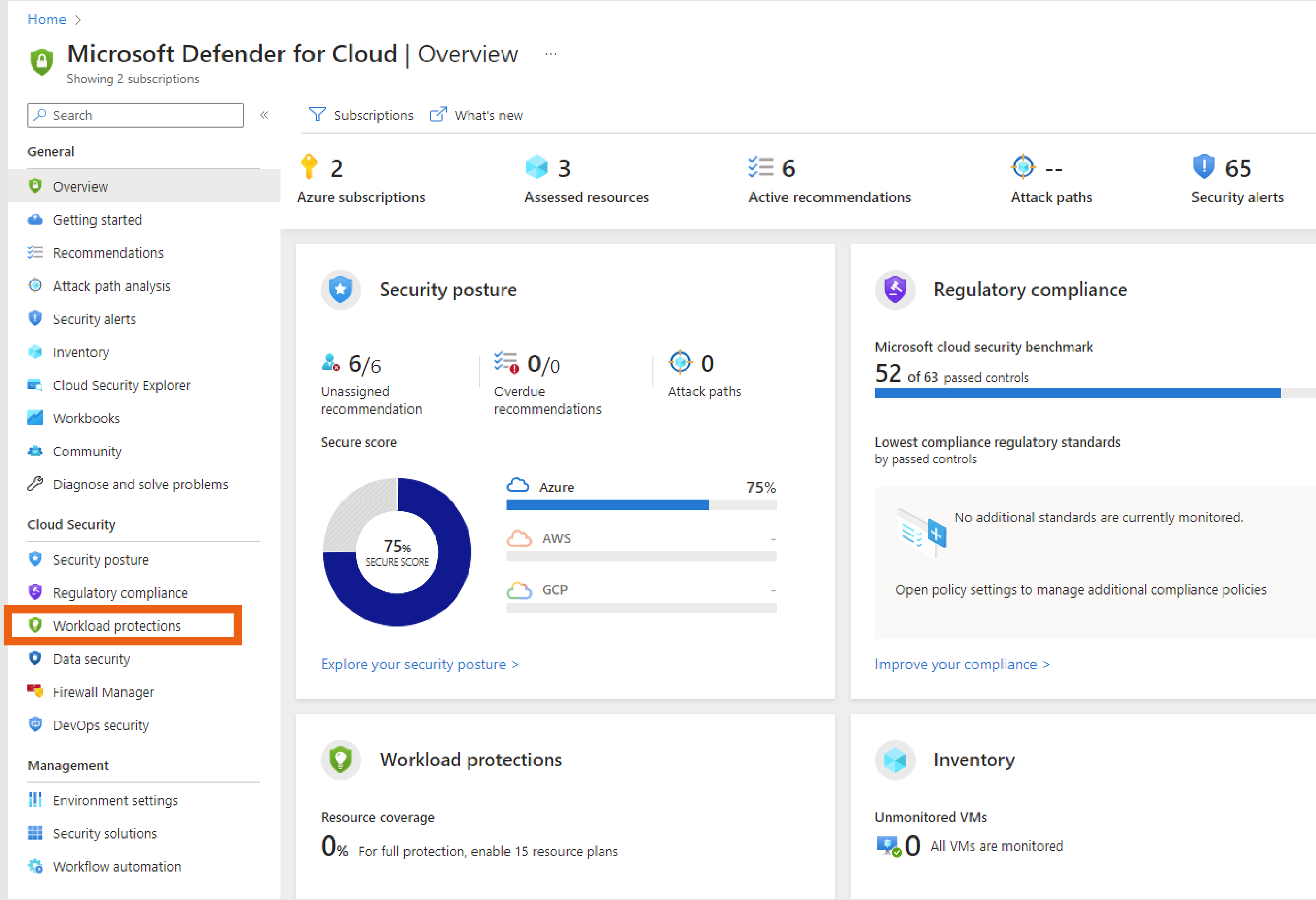
0% For full protection, enable 15 resource plans

Inventory

Unmonitored VMs

0 All VMs are monitored

Classification: Training (R5)



Home >

Microsoft Defender for Cloud | Overview

Showing 2 subscriptions

Search

Subscriptions What's new

General

- Overview
- Getting started
- Recommendations
- Attack path analysis
- Security alerts
- Inventory
- Cloud Security Explorer
- Workbooks
- Community
- Diagnose and solve problems

Cloud Security

- Security posture
- Regulatory compliance
- Workload protections
- Data security
- Firewall Manager
- DevOps security

Management

- Environment settings
- Security solutions
- Workflow automation

2	3	6	--	65
Azure subscriptions	Assessed resources	Active recommendations	Attack paths	Security alerts

Security posture

6/6 Unassigned recommendation

0/0 Overdue recommendations

0 Attack paths

Secure score

75% SECURE SCORE

Azure	75%
AWS	-
GCP	-

Explore your security posture >

Regulatory compliance

Microsoft cloud security benchmark

52 of 63 passed controls

Lowest compliance regulatory standards
by passed controls

No additional standards are currently monitored.

Open policy settings to manage additional compliance policies

Improve your compliance >

Workload protections

Resource coverage

0% For full protection, enable 15 resource plans

Inventory

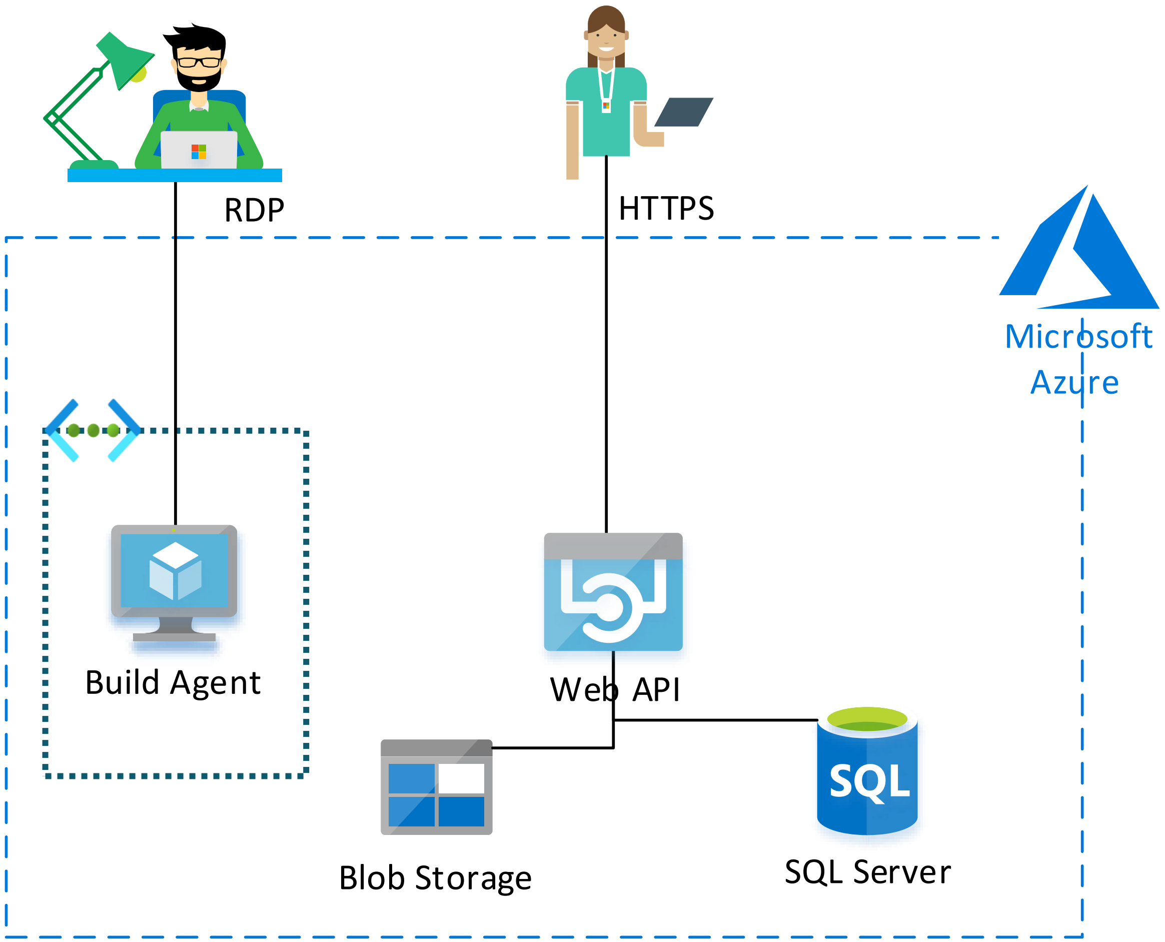
Unmonitored VMs

0 All VMs are monitored

Microsoft Defender for Cloud – Workload protection

Compute	Any server	Azure VMSS	Azure K8s	App Services	Unmanaged K8s			
Service layer	Azure DNS	Key Vault	Network layer v1	Resource Management	Azure API Management			
Databases and storage	Blob storage	File storage	Maria DB	Cosmos DB	Azure SQL	MySQL	PostgreSQL	SQL on VM
AWS workloads	Amazon EKS	Amazon EC2	SQL on VM	Unmanaged Kubernetes				
GCP workloads	GKE clusters	Google Compute	SQL on VM	Unmanaged Kubernetes				
On-premises workloads	Kubernetes	SQL on VM	Servers					

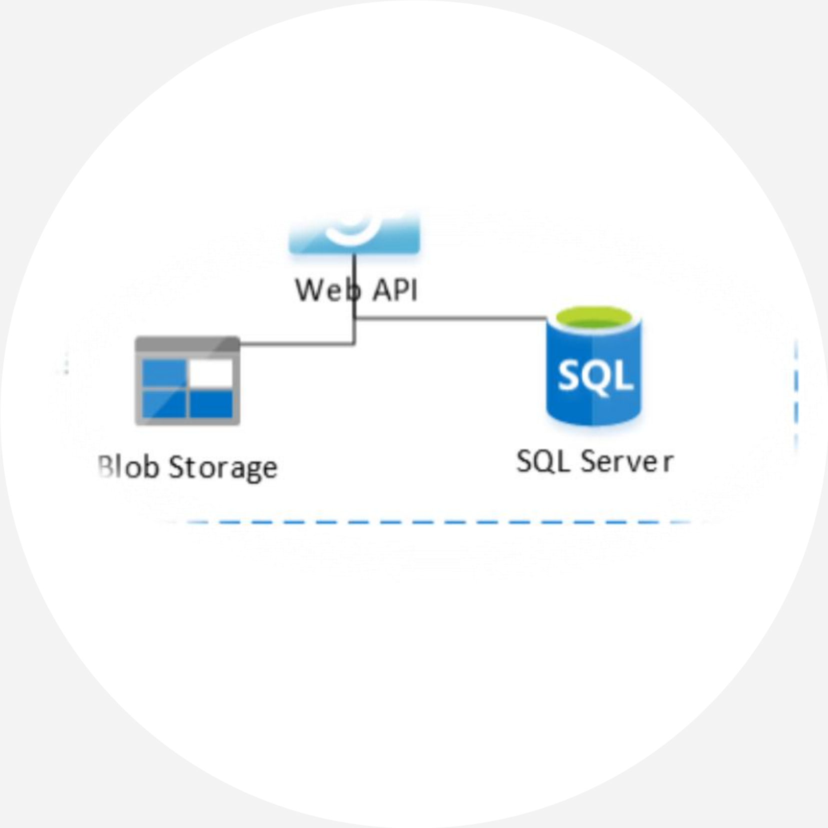
V 0.1


RDP
HTTPS
Microsoft Azure
Build Agent
Web API
Blob Storage
SQL
SQL Server

Data Security

Data Security

- Encryption
- Azure services will discuss:
  - Storage Accounts
  - SQL databases



Classification: Training (R5)

Encryption

Encryption in-transit (TLS)

TLS 1.2 for most services

TLS 1.3 (very) limited available

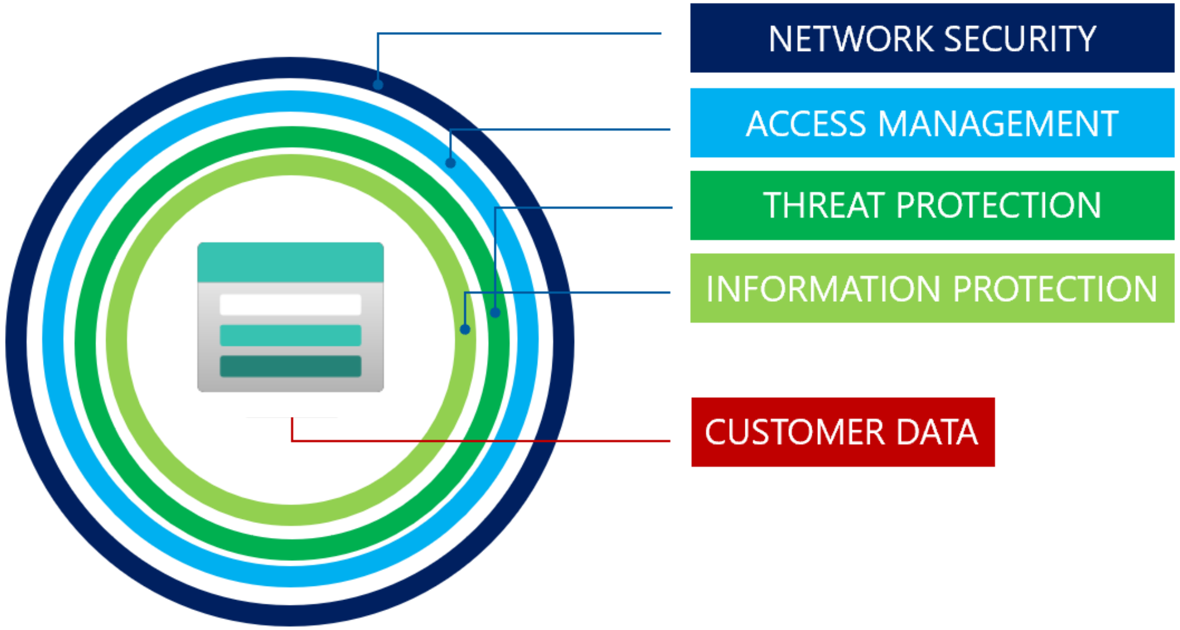
Encryption at-rest (SSE)

Microsoft Managed Key

Customer Managed Key (BYOK)

Protect your storage account

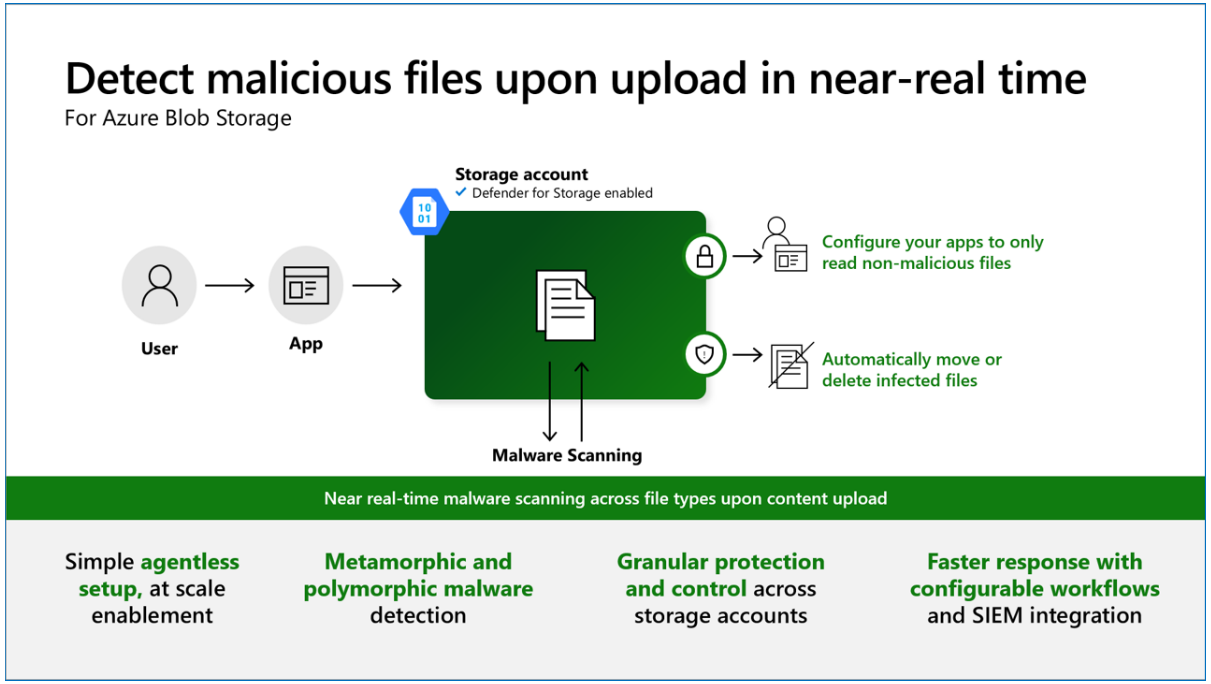
- Control Network Access
- AAD authentication
- Storage account keys / SAS
- Follow least privileged principle
- Microsoft Defender for Storage
- Encryption at-rest (SSE)
- Encryption in-transit (TLS)
- Data protection (soft-delete)
- Immutable Blobs



Microsoft Defender for Storage

- Defender for Storage includes:
  - Activity Monitoring
  - Sensitive data threat detection

  (preview feature, new plan only)
  - Malware Scanning (new plan only)



Detect malicious files upon upload in near-real time

For Azure Blob Storage

Storage account
✓ Defender for Storage enabled
User
App
Malware Scanning
Configure your apps to only read non-malicious files
Automatically move or delete infected files

Near real-time malware scanning across file types upon content upload

Simple agentless setup, at scale enablement

Metamorphic and polymorphic malware detection

Granular protection and control across storage accounts

Faster response with configurable workflows and SIEM integration

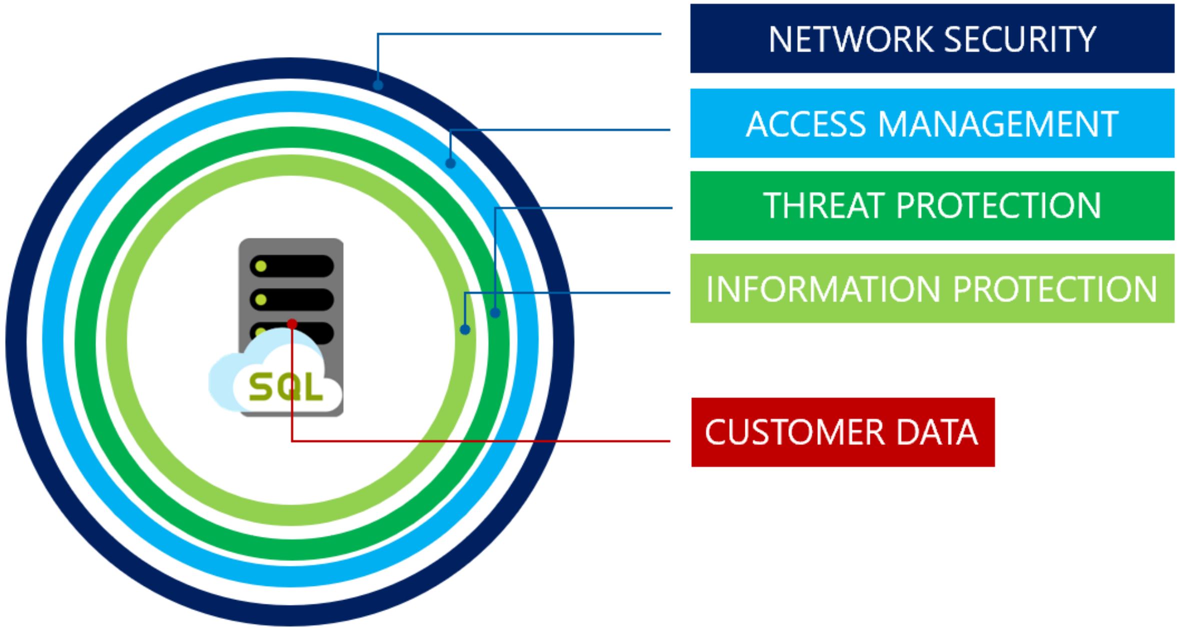
Classification: Training (R5)

Microsoft Defender for Storage – DEMO

- Create Storage Account
  - Activate MS Defender For Storage
  - Upload files
    - Normal file
    - EICAR file
  - See what happens!

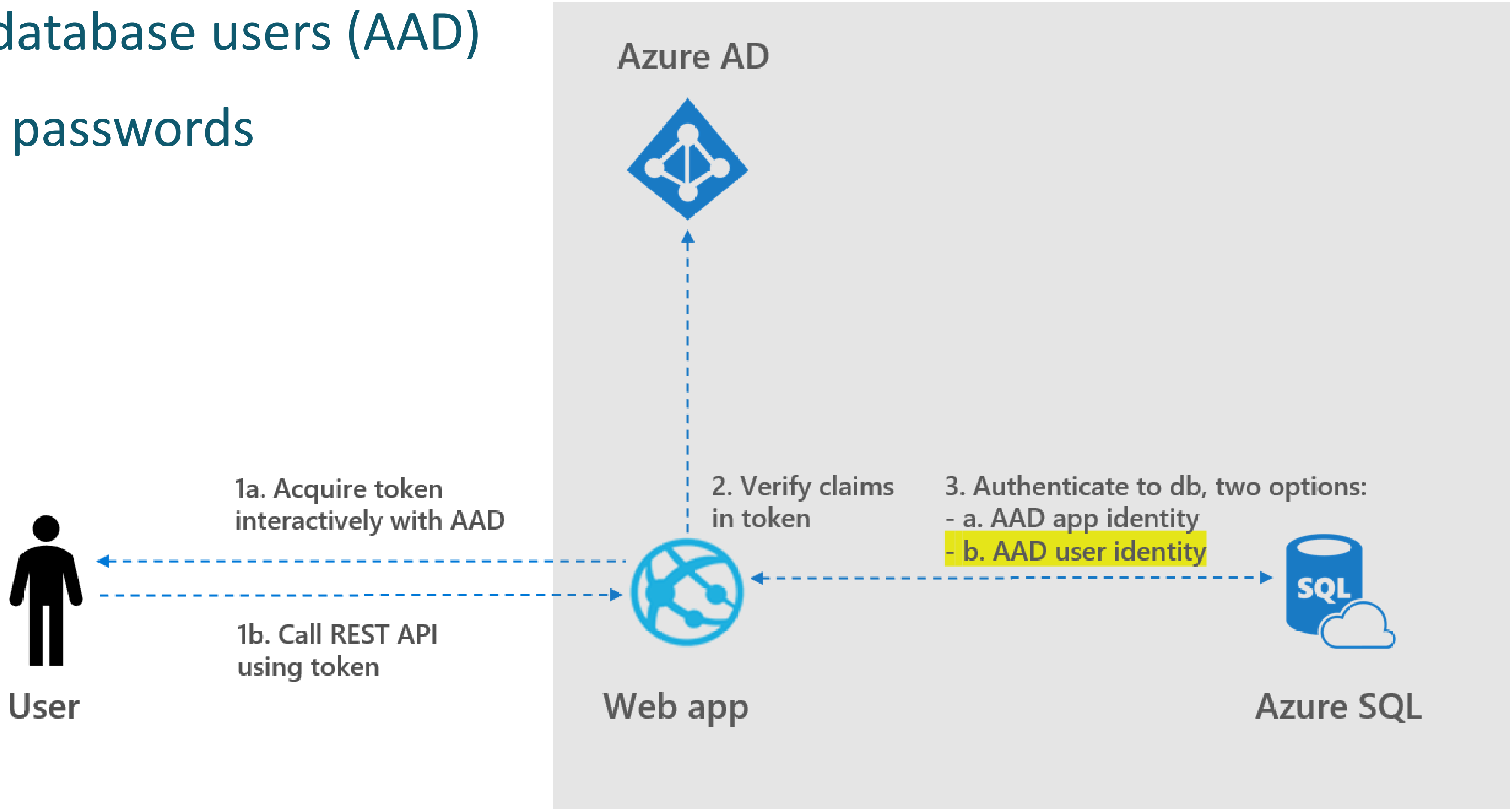
Protect your SQL server

- Control Network Access
- SQL / AAD authentication
- Row Level Security
- Follow least privileged principle
- Enable Auditing
- Microsoft Defender for Cloud
- Transparent Data Encryption (TDE)
- Transport Layer Security (TLS)
- Always Encrypted
- Dynamic Data Masking



SQL AAD Authentication

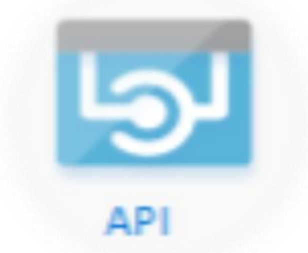
- Central manage database users (AAD)
- Eliminate storing passwords


Azure AD
1a. Acquire token interactively with AAD
1b. Call REST API using token
2. Verify claims in token
3. Authenticate to db, two options:
- a. AAD app identity
- b. AAD user identity
SQL
User
Web app
Azure SQL

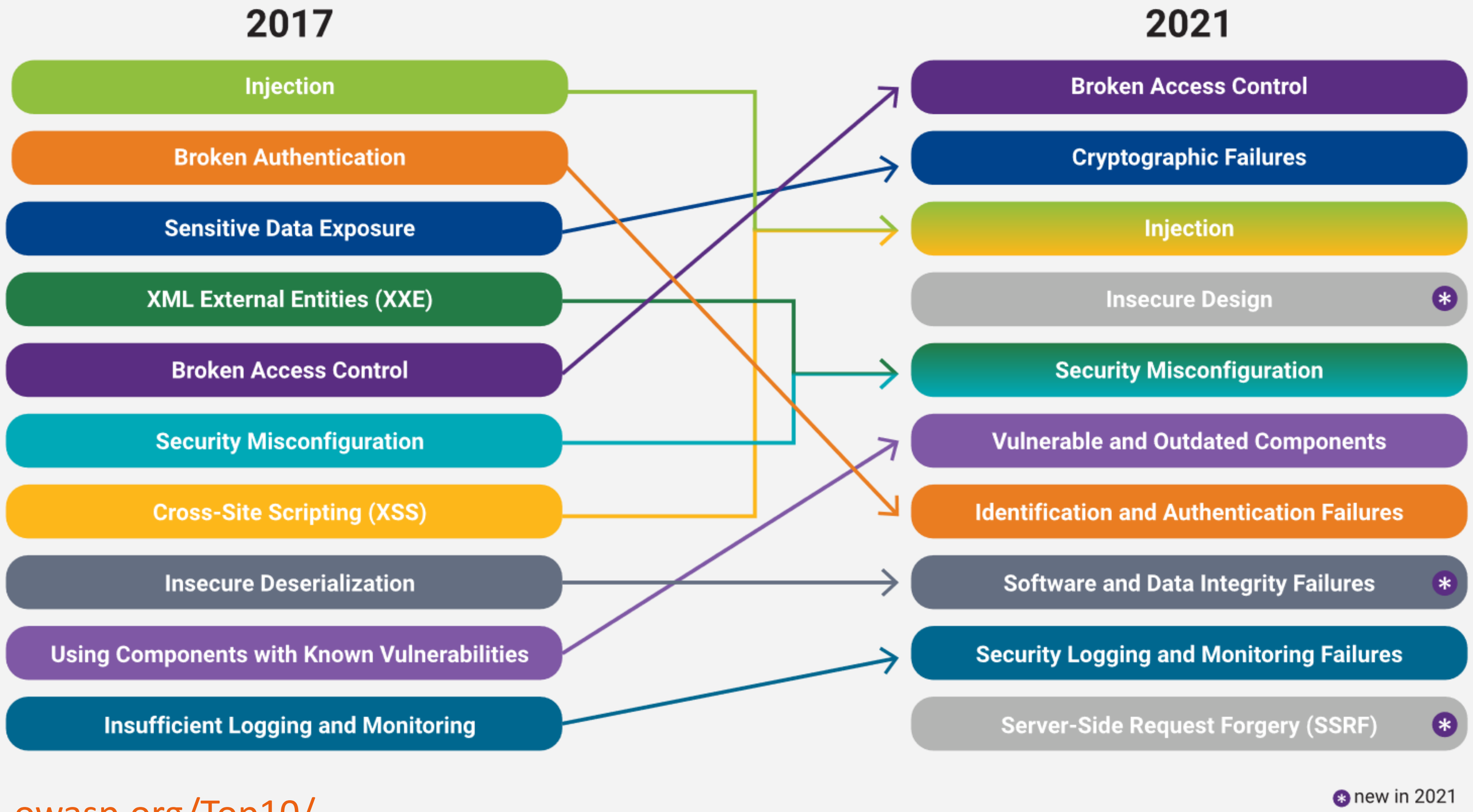
Application Security

Application Security

- **How can we secure our applications?**
  - Address OWASP
  - Secure Programming
  - Secret Management
  - Hardening of App Services
  - Authentication and Authorization



OWASP TOP-10



2017

- Injection
- Broken Authentication
- Sensitive Data Exposure
- XML External Entities (XXE)
- Broken Access Control
- Security Misconfiguration
- Cross-Site Scripting (XSS)
- Insecure Deserialization
- Using Components with Known Vulnerabilities
- Insufficient Logging and Monitoring

2021

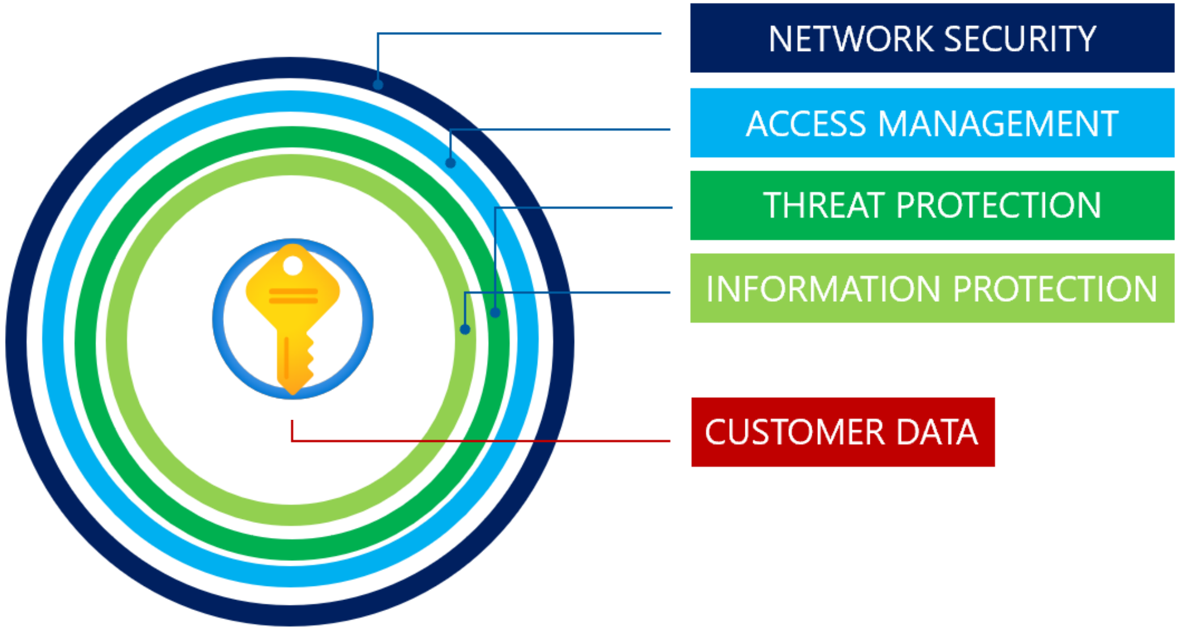
- Broken Access Control
- Cryptographic Failures
- Injection
- Insecure Design *
- Security Misconfiguration
- Vulnerable and Outdated Components
- Identification and Authentication Failures
- Software and Data Integrity Failures *
- Security Logging and Monitoring Failures
- Server-Side Request Forgery (SSRF) *

* new in 2021

owasp.org/Top10/

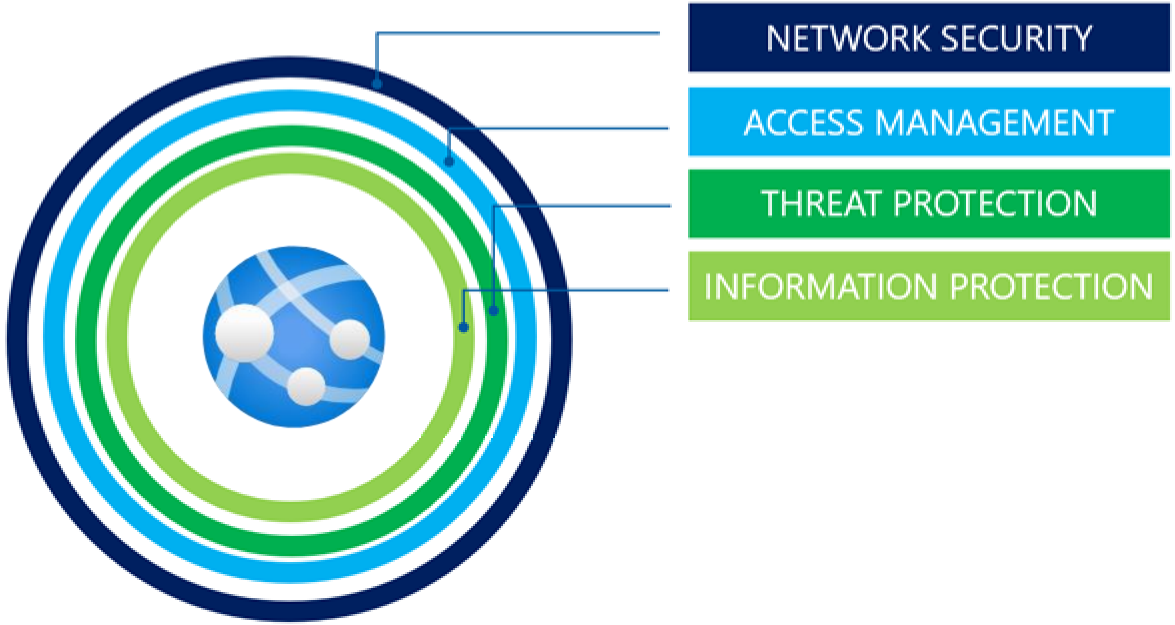
Protect your Key Vault

- Control Network Access
- RBAC authorization
- Follow least privileged principle
- Microsoft Defender for Key Vault
- Encryption at-rest & in-transit
- Data protection (soft-delete & purge protection)

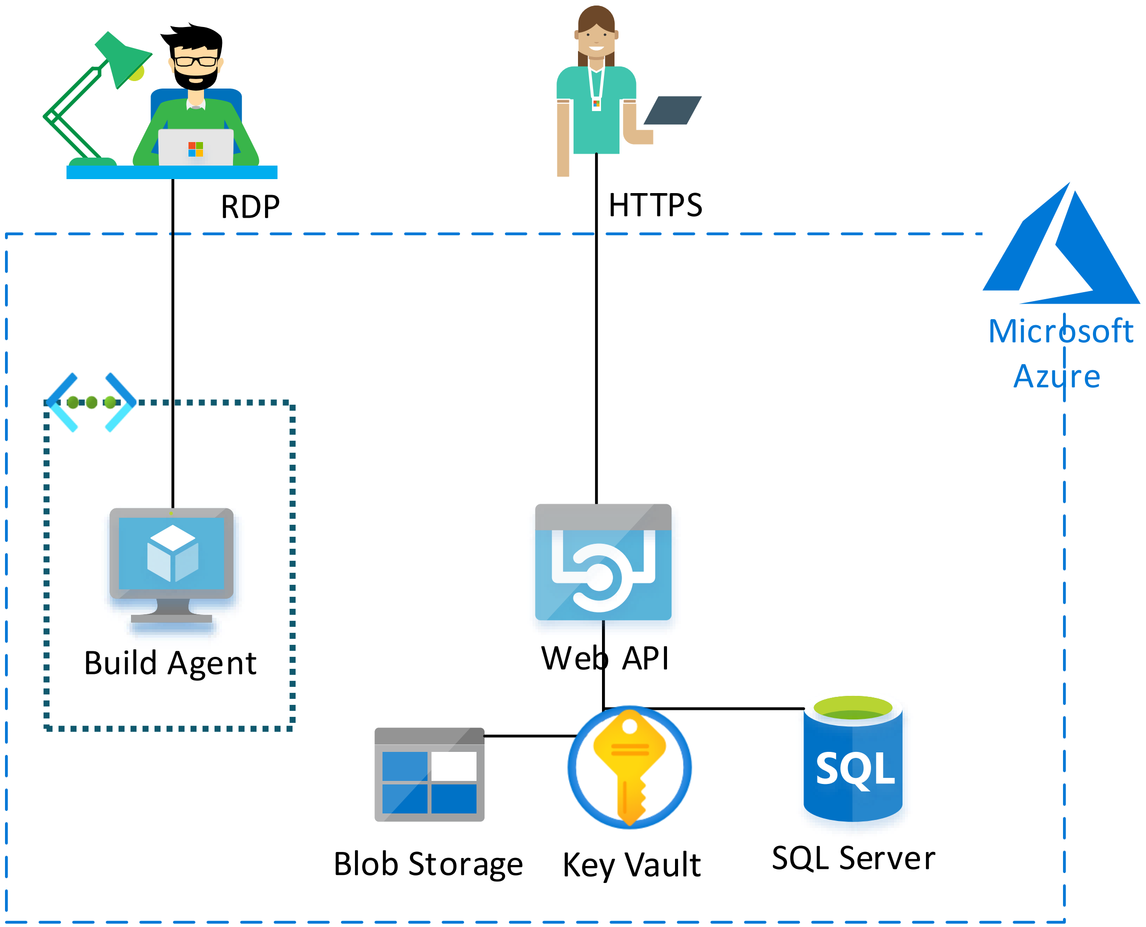


Harden your App Services

- Control Network Access
  - Disable FTP State
  - Disable SCM
- Managed Identity
- SSO
- Enable Auditing
- Microsoft Defender for Cloud
- Encryption in-transit (TLS)
- HTTPS only



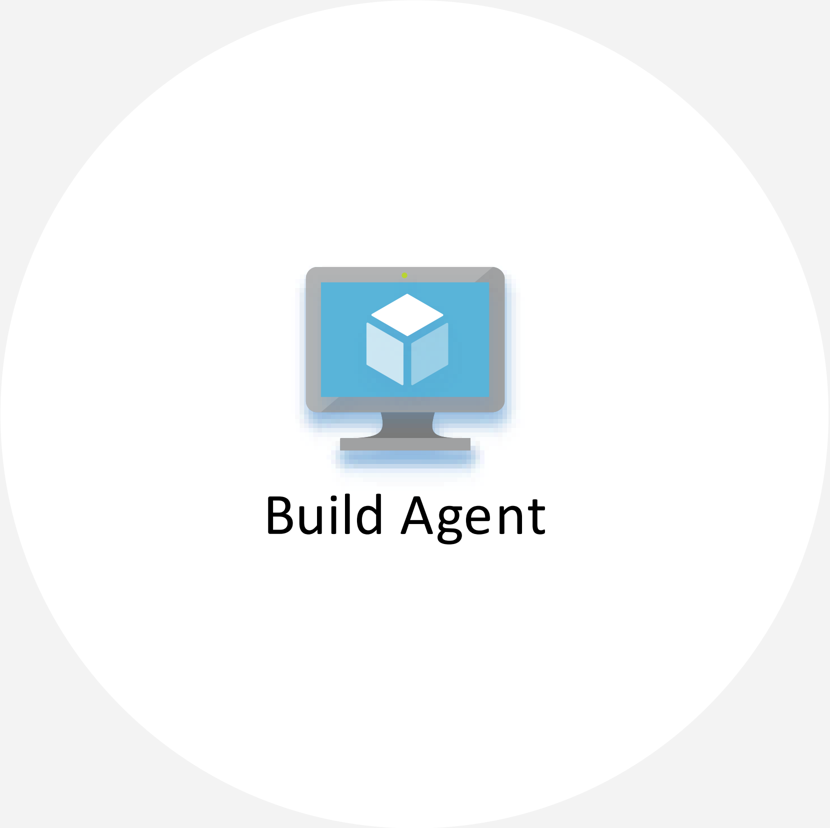
V 0.2


RDP
HTTPS
Microsoft Azure
Build Agent
Web API
Blob Storage
Key Vault
SQL
SQL Server

Compute Security

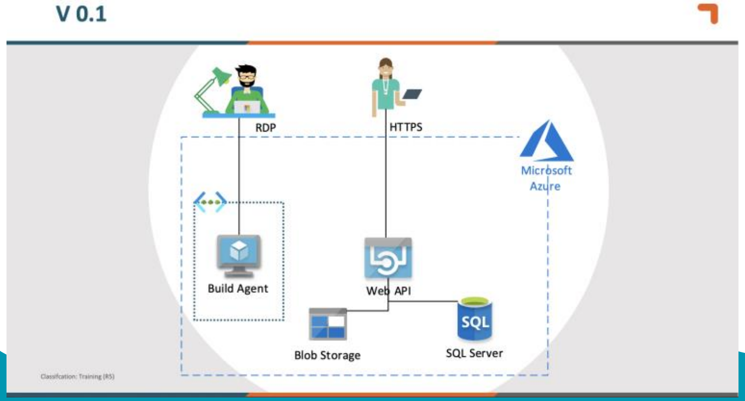
Compute Security

- Microsoft Defender for Servers
- VM Endpoint protection
- Just-in-Time VM access



Network Security

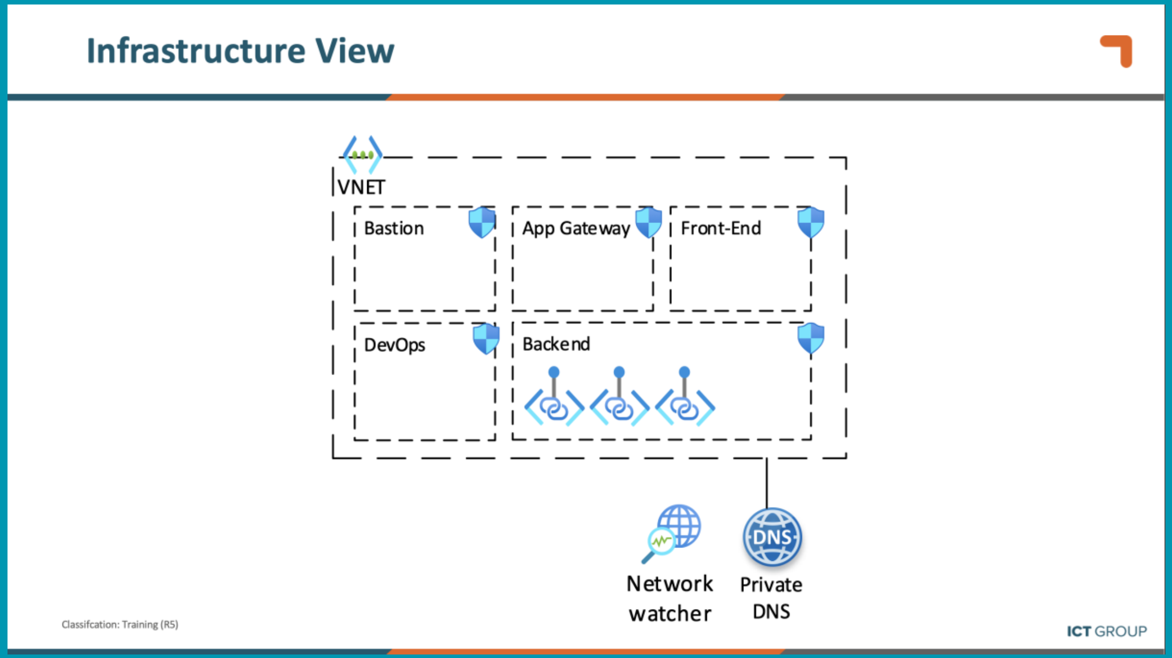
Solution



V 0.1

Classifcation: Training (R5)

Infrastructure



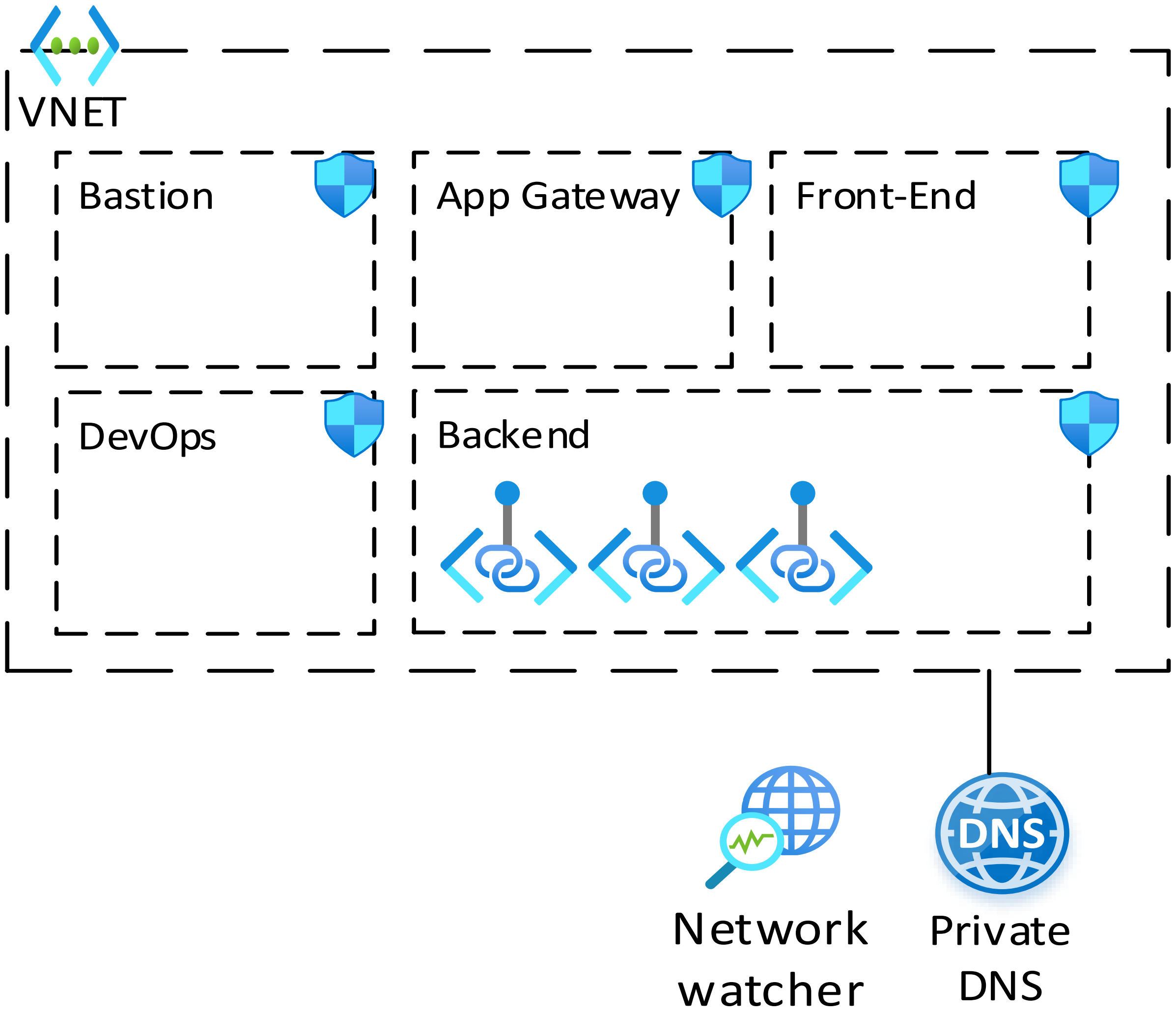
Infrastructure View

Classifcation: Training (R5)

ICT GROUP

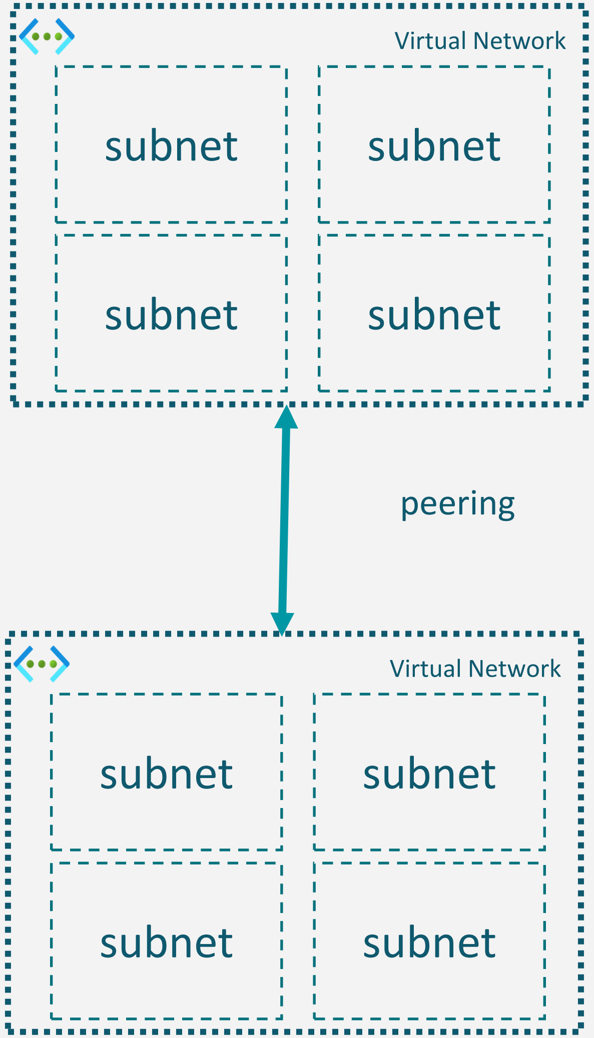
Classification: Training (R5)

Infrastructure View



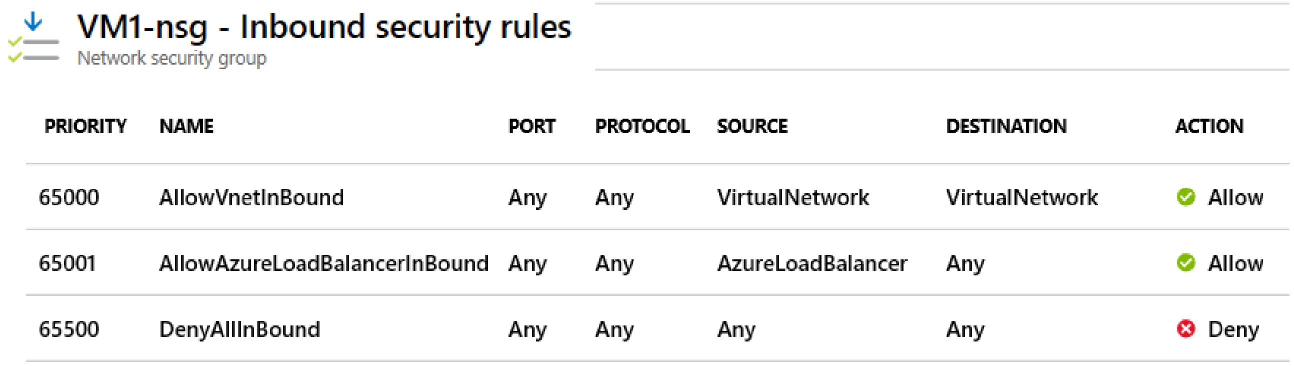
Virtual Network

- Subnets
- VNET Peering
- Filter network traffic between subnets
  - NSG
  - NVA
- Routing
- DNS
- Address space / IP planning



Network Security Groups

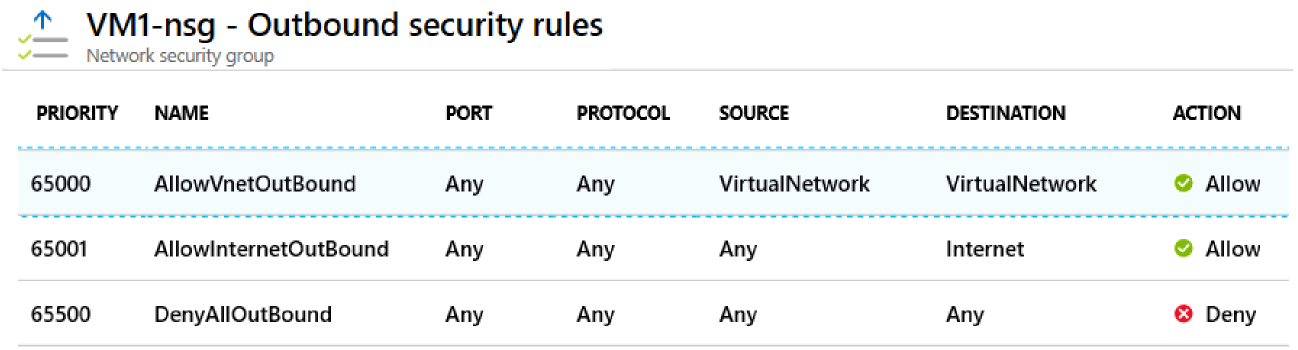
- Limit network traffic to resources in a virtual network
- Can be assigned on subnets and Network Interface Cards (NIC)



VM1-nsg - Inbound security rules

Network security group

PRIORITY	NAME	PORT	PROTOCOL	SOURCE	DESTINATION	ACTION
65000	AllowVnetInBound	Any	Any	VirtualNetwork	VirtualNetwork	✓ Allow
65001	AllowAzureLoadBalancerInBound	Any	Any	AzureLoadBalancer	Any	✓ Allow
65500	DenyAllInBound	Any	Any	Any	Any	✗ Deny



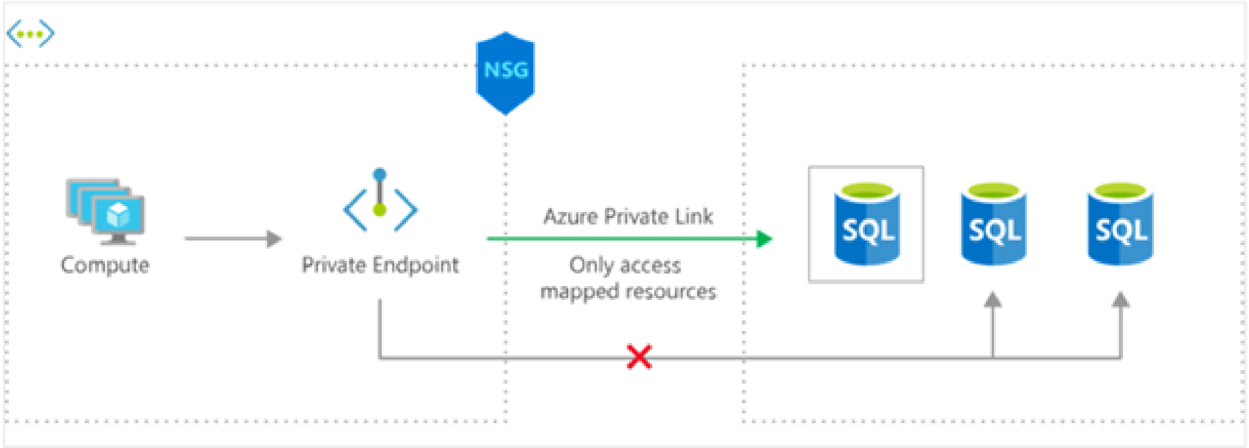
VM1-nsg - Outbound security rules

Network security group

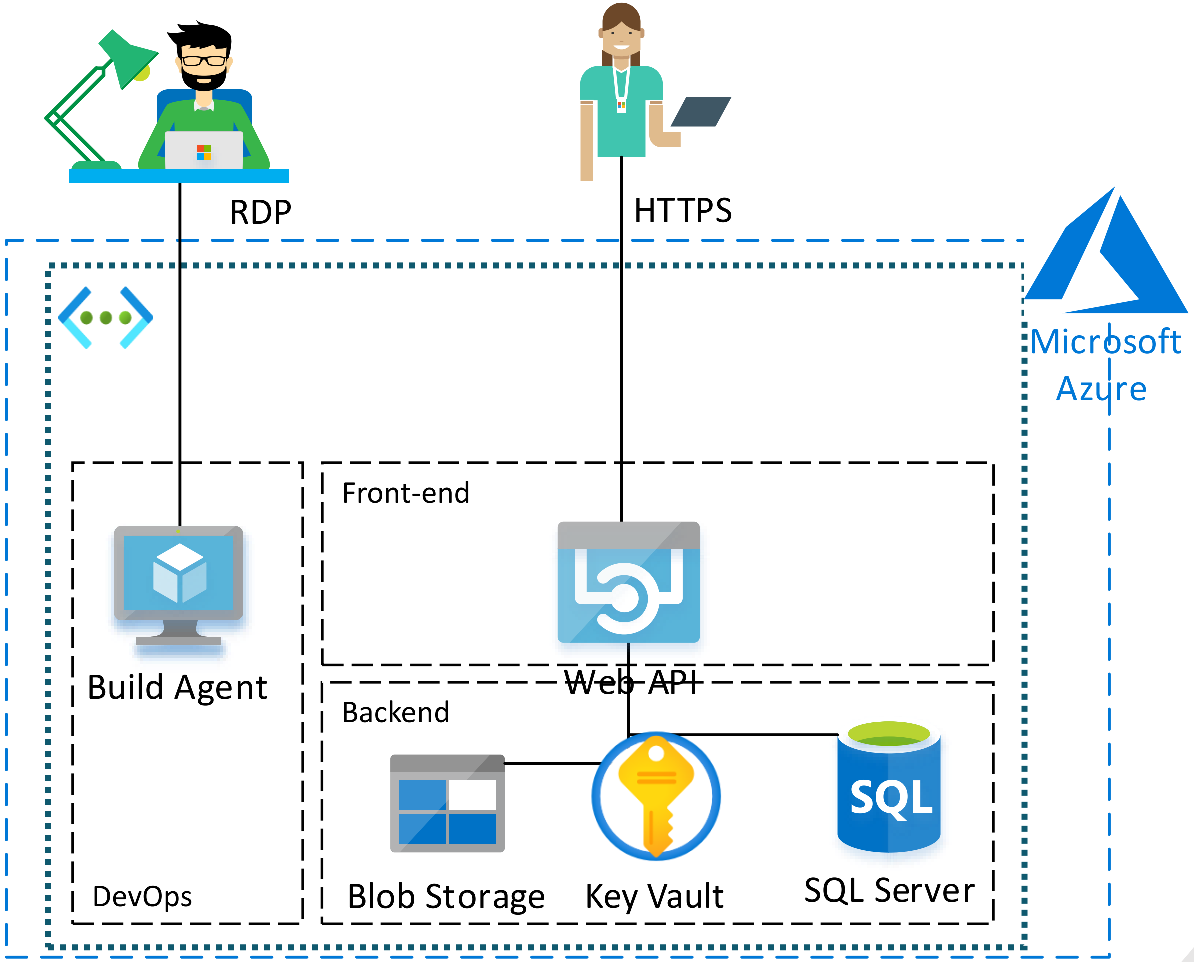
PRIORITY	NAME	PORT	PROTOCOL	SOURCE	DESTINATION	ACTION
65000	AllowVnetOutBound	Any	Any	VirtualNetwork	VirtualNetwork	✓ Allow
65001	AllowInternetOutBound	Any	Any	Any	Internet	✓ Allow
65500	DenyAllOutBound	Any	Any	Any	Any	✗ Deny

How do Private Endpoints work?

- PE is a special type of NIC that plugs into to VNET
- PE uses private IP from subnet
- Traffic remains in VNET
- Relies on DNS

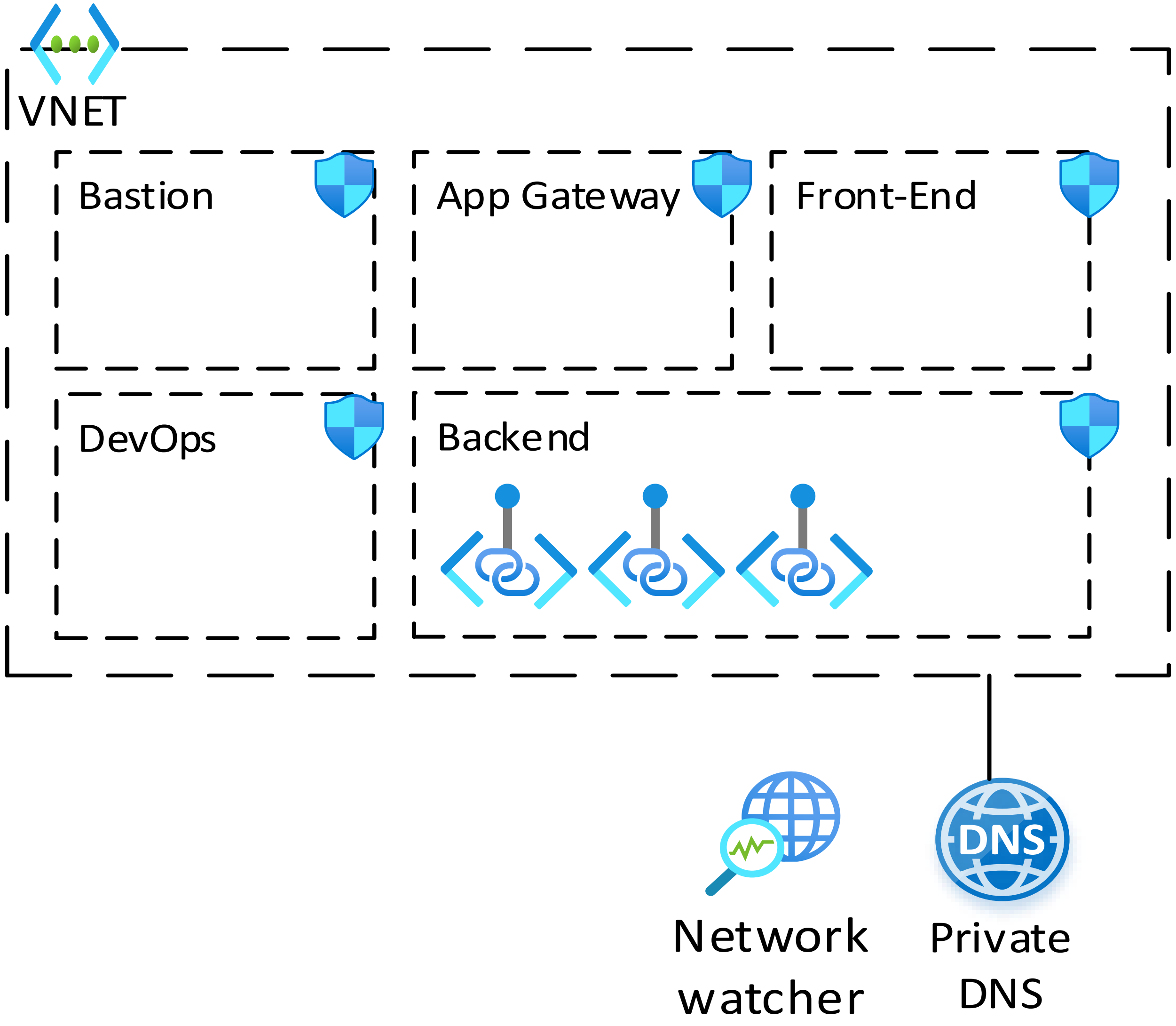


V 0.3



Classification: Training (R5)

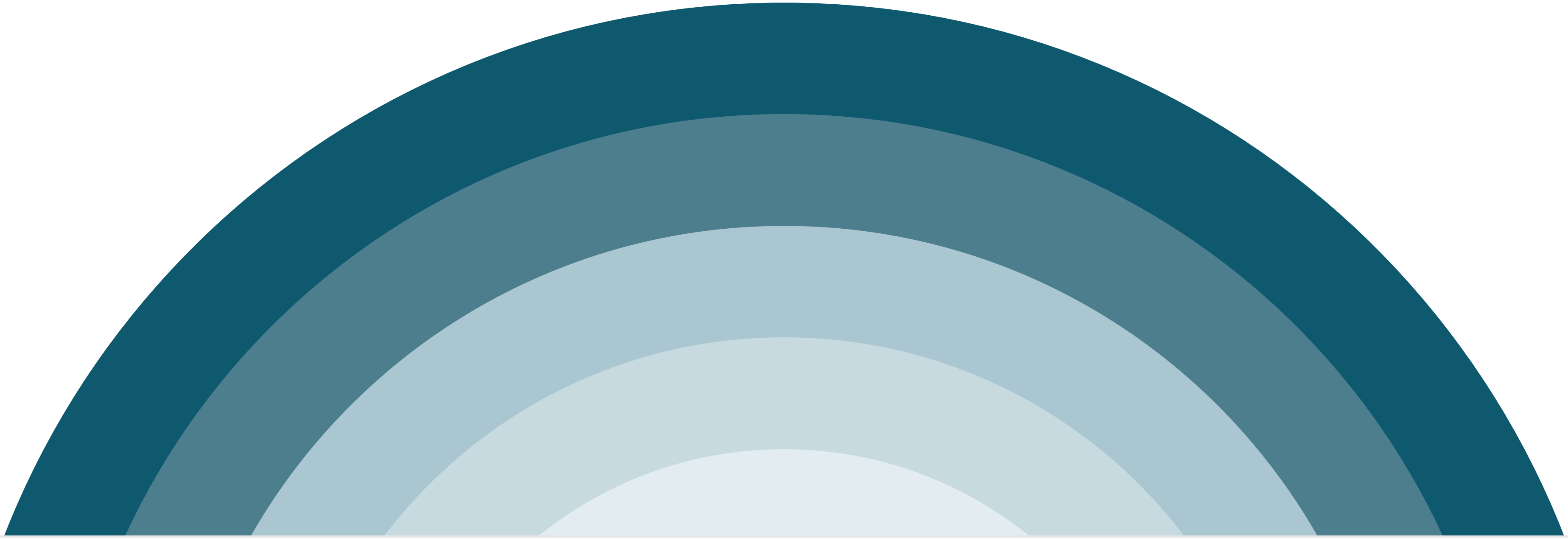
Infrastructure View (V 0.3)



Wait… **how can I access my services?**

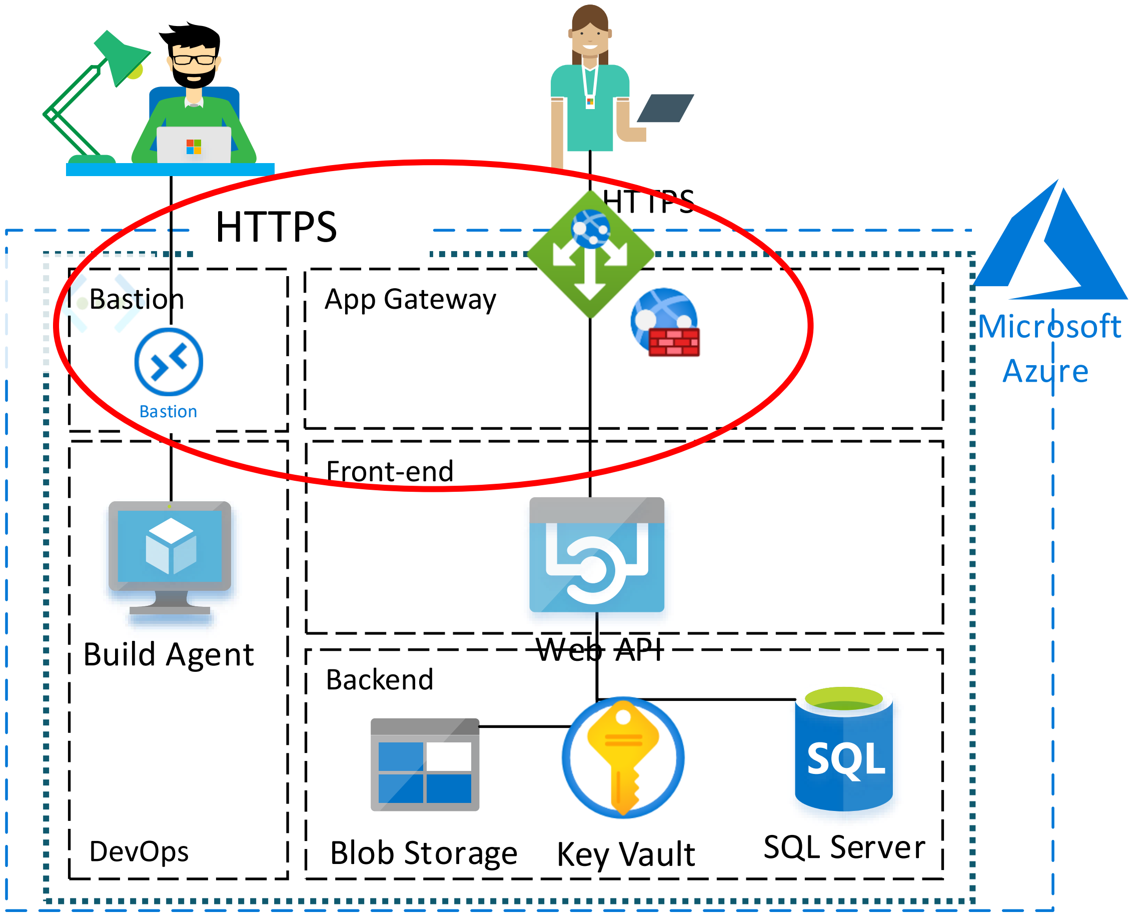
Implications on daily operations

- Q: How can I deploy from a build agent to my environment?
  - A: Use a self-hosted build agent
  - A2: Temporarily whitelist your azure hosted build agent
- Q: How can I access my VM using RDP / SSH?
  - A: VPN
  - A2: Azure Bastion
- Q: How can I access resources using Private Endpoints?
  - A: VPN
  - A2: Azure Bastion + steppingstone VM
- Q: How can I access resources other resources?
  - A: Add your IP to the firewall whitelist



Perimeter Security

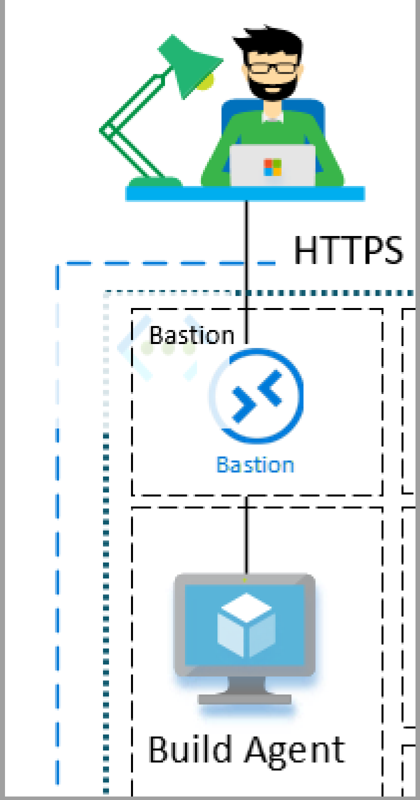
V 0.4



Classification: Training (R5)

Azure Bastion

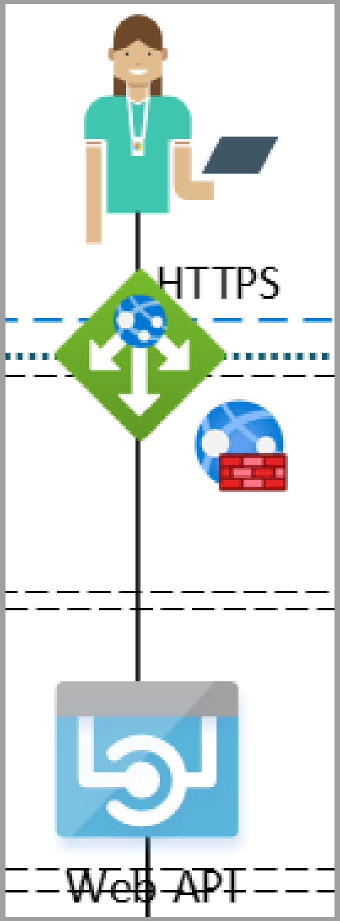
- Provide RDP/SSH access via the browser without the need of a public endpoint / IP
- Reduces attack surface
- Single deployment per virtual network is enough



Classification: Training (R5)

AGW <–> WAF <–> Web API

- Application Gateway
- with integrated Web Application Firewall

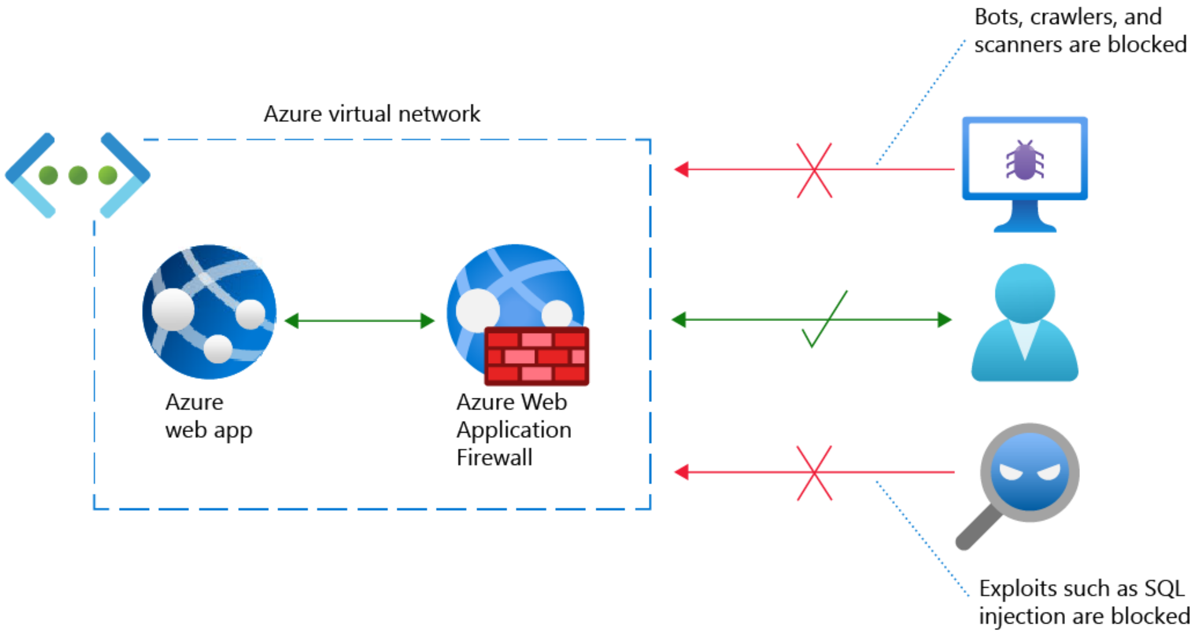


Web Application Firewall (WAF)

Features:

- Custom Access Control
- Rate Limiting
- Preconfigured managed rules sets
- OWASP Top 10 protection

What is the difference with Azure Firewall?

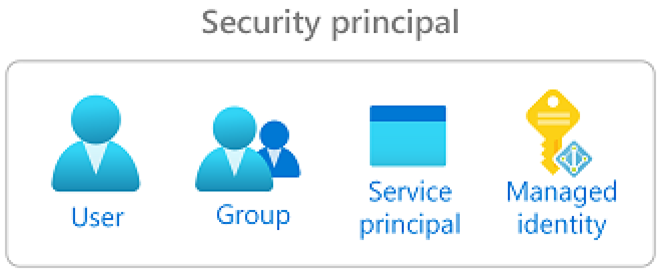


Bots, crawlers, and scanners are blocked
Azure virtual network
Azure web app
Azure Web Application Firewall
Exploits such as SQL injection are blocked

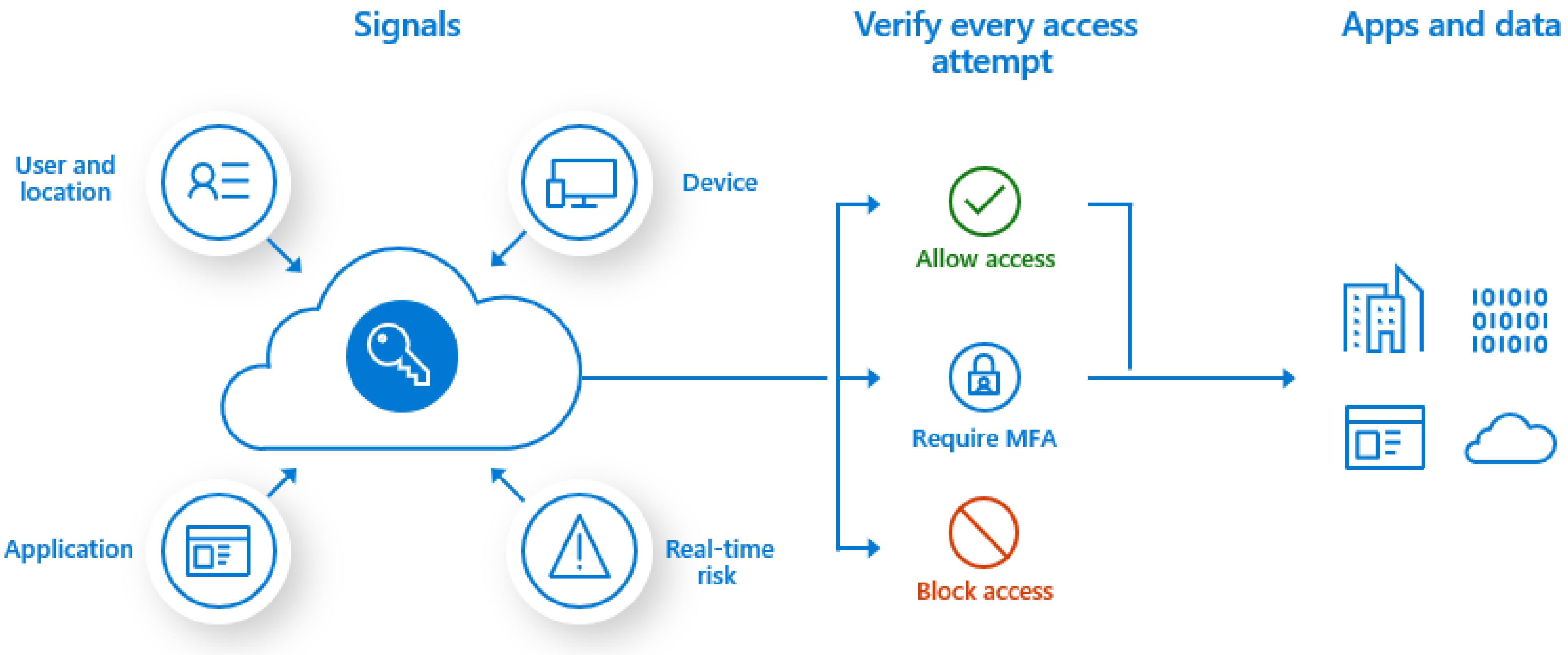
Identity and Access

Managed Identity

- Managed Identity
  - System-Assigned Managed Identity
    - Part of resource
    - Shared life-cycle with parent resource
    - Linked to 1 resource
  - User-assigned Managed identity
    - Stand-alone resource
    - Independent life-cycle
    - Can be shared among other resources



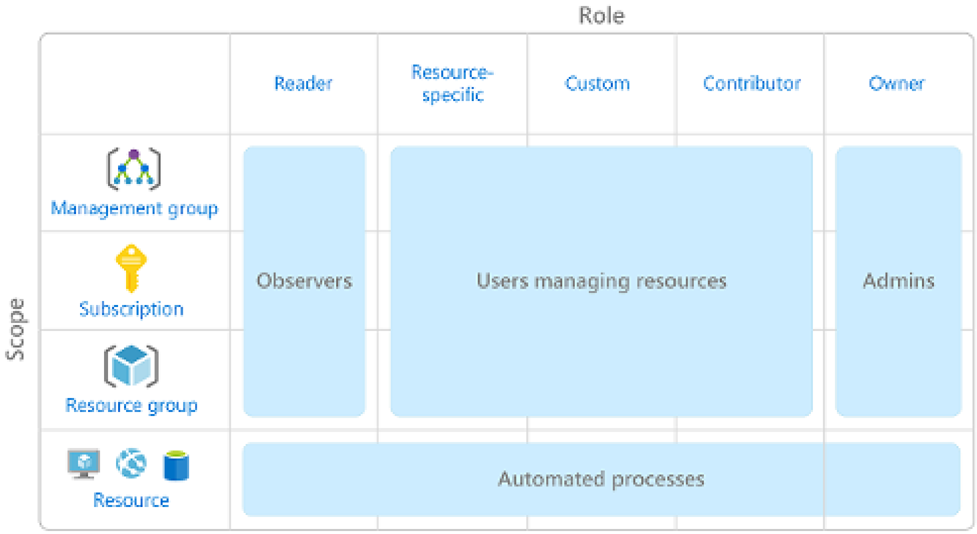
Conditional Access



Classification: Training (R5)

RBAC

- Most common Azure roles for **Control Plane**:
  - Owner
  - Contributor
  - Reader
- When it comes to the **Data Plane**:
  - Storage Blob Data Reader / Writer / Owner
  - Key Vault Administrator / Key Vault Secret User (etc)
- Complete list: https://docs.microsoft.com/en-us/azure/role-based-access-control/built-in-roles



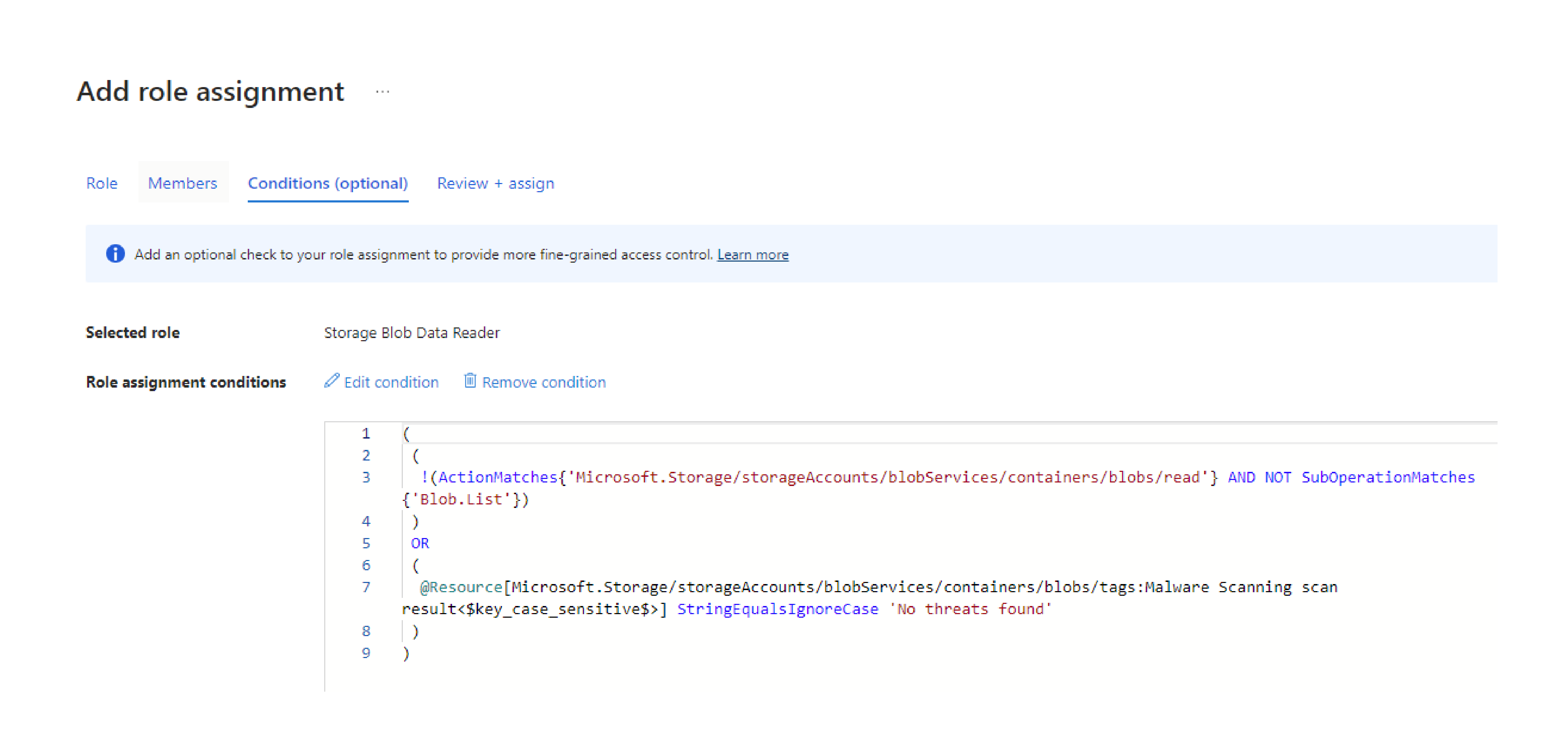
	Reader	Resource-specific	Custom	Contributor	Owner
Management group	Observers	Users managing resources			Admins
Subscription					
Resource group					
Resource	Automated processes				

ABAC

- Attribute Based Access Control (ABAC)
- Role Assignment conditions based on attributes
- **Why use conditions?**
  - Provide more fine-grained access control
    - E.g. Constrain roles an Owner can assign
  - Use attributes that have specific business meaning
    - E.g. use Tag and allow only access to Blob with Tag Value ‘Project X’

Role Assignment Conditions – DEMO

- Assign the Storage Blob Data Reader role only if Blob doesn’t contain any threats



Add role assignment

Role | Members | Conditions (optional) | Review + assign

Add an optional check to your role assignment to provide more fine-grained access control. Learn more

Selected role Storage Blob Data Reader

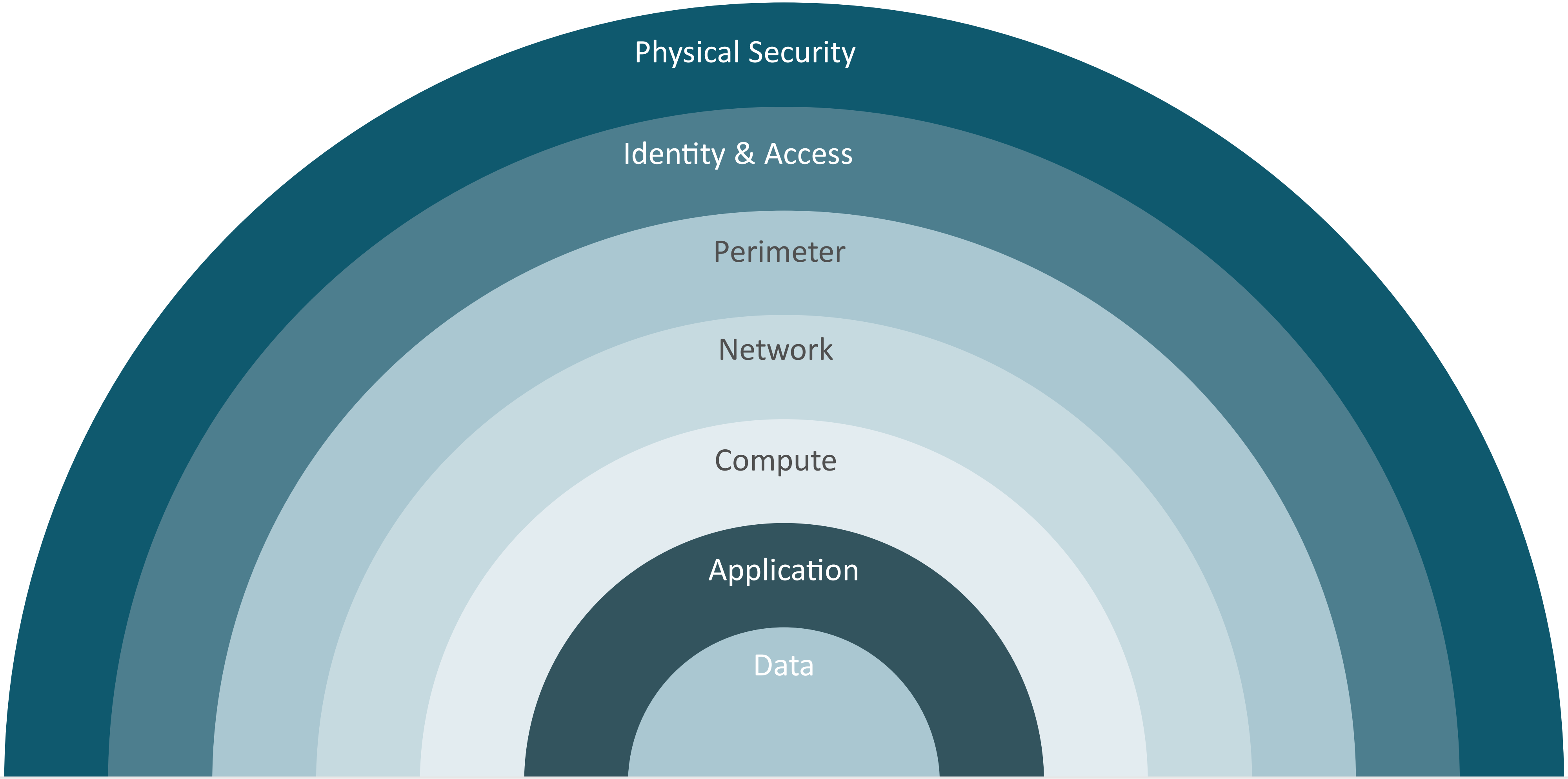
Role assignment conditions Edit condition Remove condition

```
(
 (
  !(ActionMatches{'Microsoft.Storage/storageAccounts/blobServices/containers/blobs/read'} AND NOT SubOperationMatches{'Blob.List'})
 )
 OR
 (
  @Resource[Microsoft.Storage/storageAccounts/blobServices/containers/blobs/tags:Malware Scanning scan result<$key_case_sensitive$>] StringEqualsIgnoreCase 'No threats found'
 )
)
```

Physical Security

Azure Data Center – Middenmeer (NL)

Wrap-up


Physical Security
Identity & Access
Perimeter
Network
Compute
Application
Data

Questions & Answers

WEBINAR

Building a **Fortress**
in Azure

Final info

WEBINAR

Building a **Fortress**
in Azure

- Slides en opname worden vandaag nog gedeeld
- Next topic? Waar zou jij over willen leren
- Feedback? help ons verbeteren!
- Updates over volgend webinar & survey worden gedeeld per mail
- Volg ons op LinkedIn

Next up!

WEBINAR

Building an integration platform in Azure

Integreer data tussen systemen en deel data met externe partijen

Q1 2024

The end