



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)

Classification: Training (R5)



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!



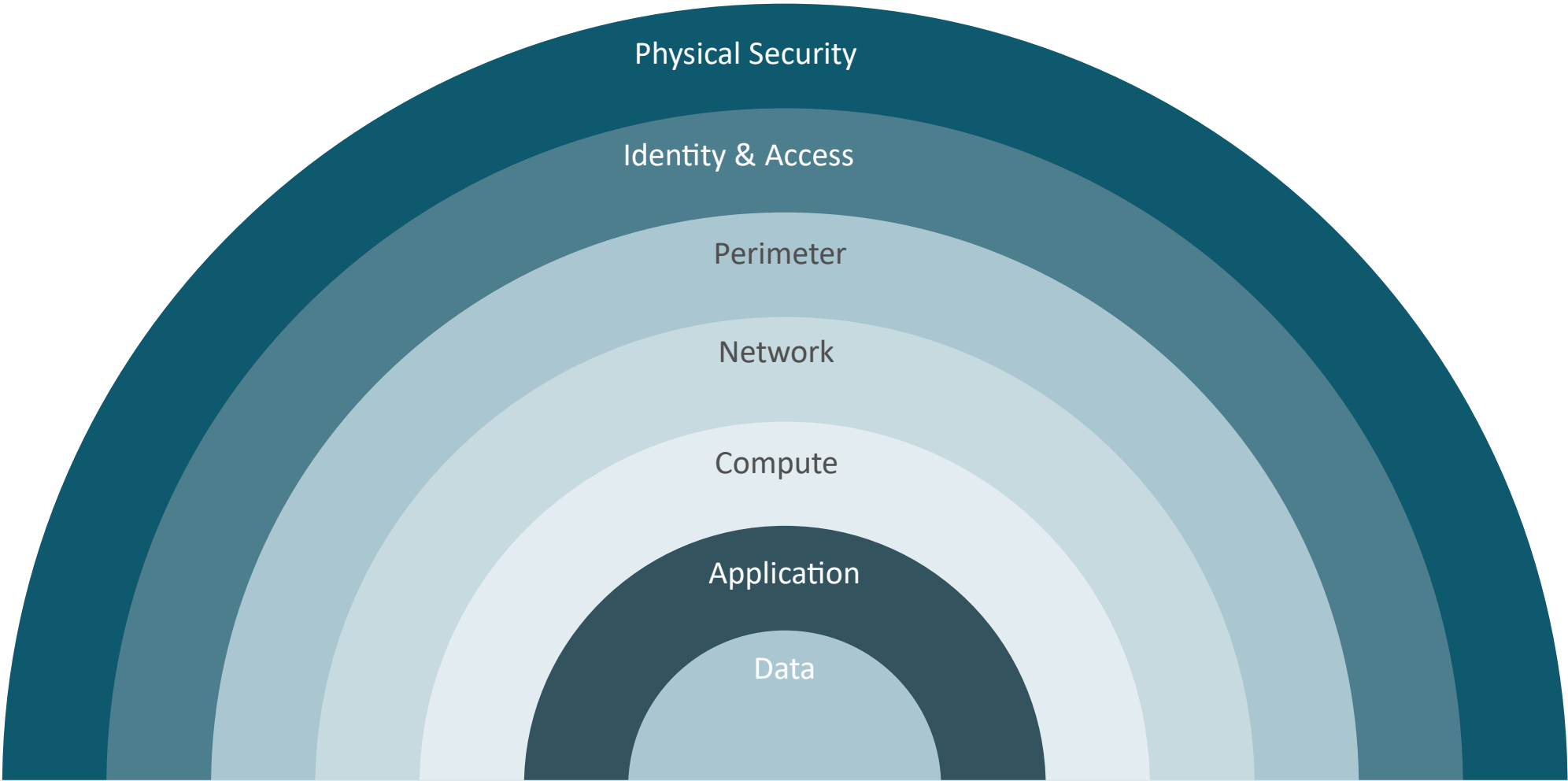
Steven van den Beemt
Cloud Architect @ICT Group





- 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



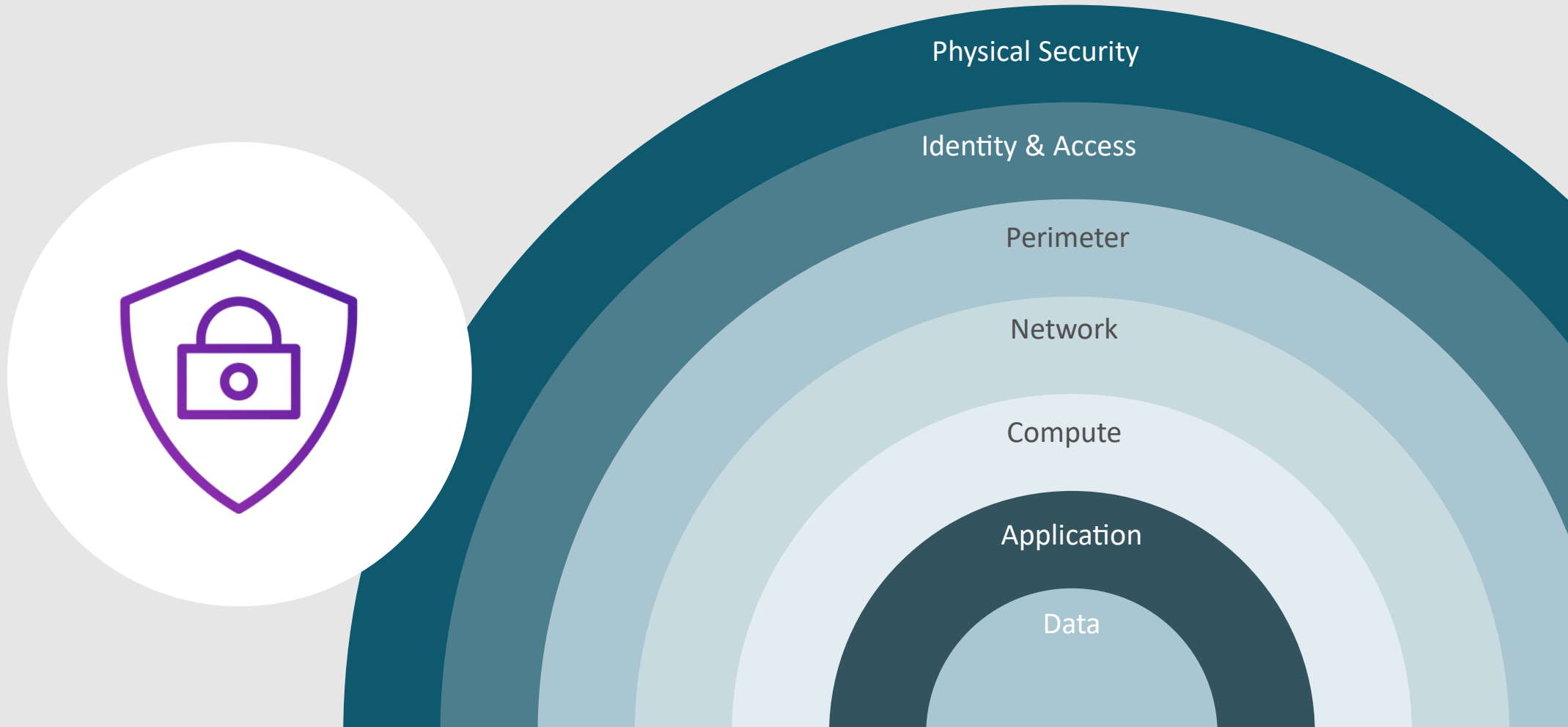
Once upon a time...



Times have changed!



Defense in depth & Zero Trust



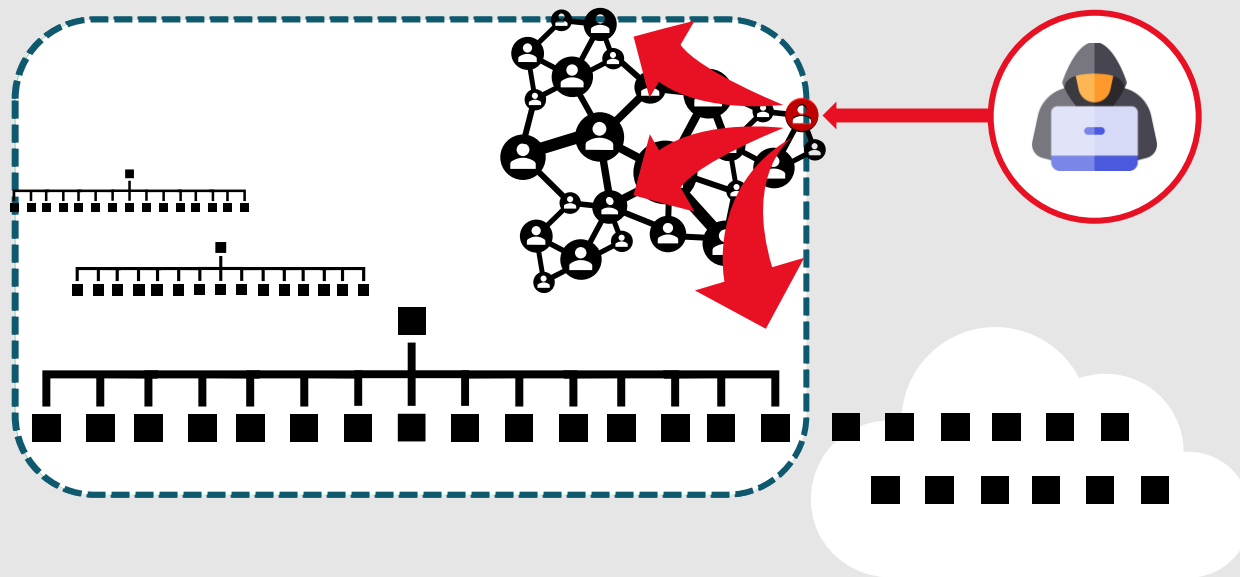


What is Zero Trust?

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



Microsoft Zero Trust Principles

Guidance for technical architecture



Verify explicitly

Always validate all available data points including

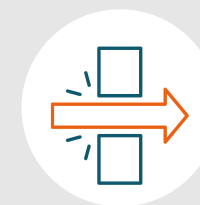
- User identity and location
- Device health
- Service or workload context
- Data classification
- Anomalies



Use least privilege access

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

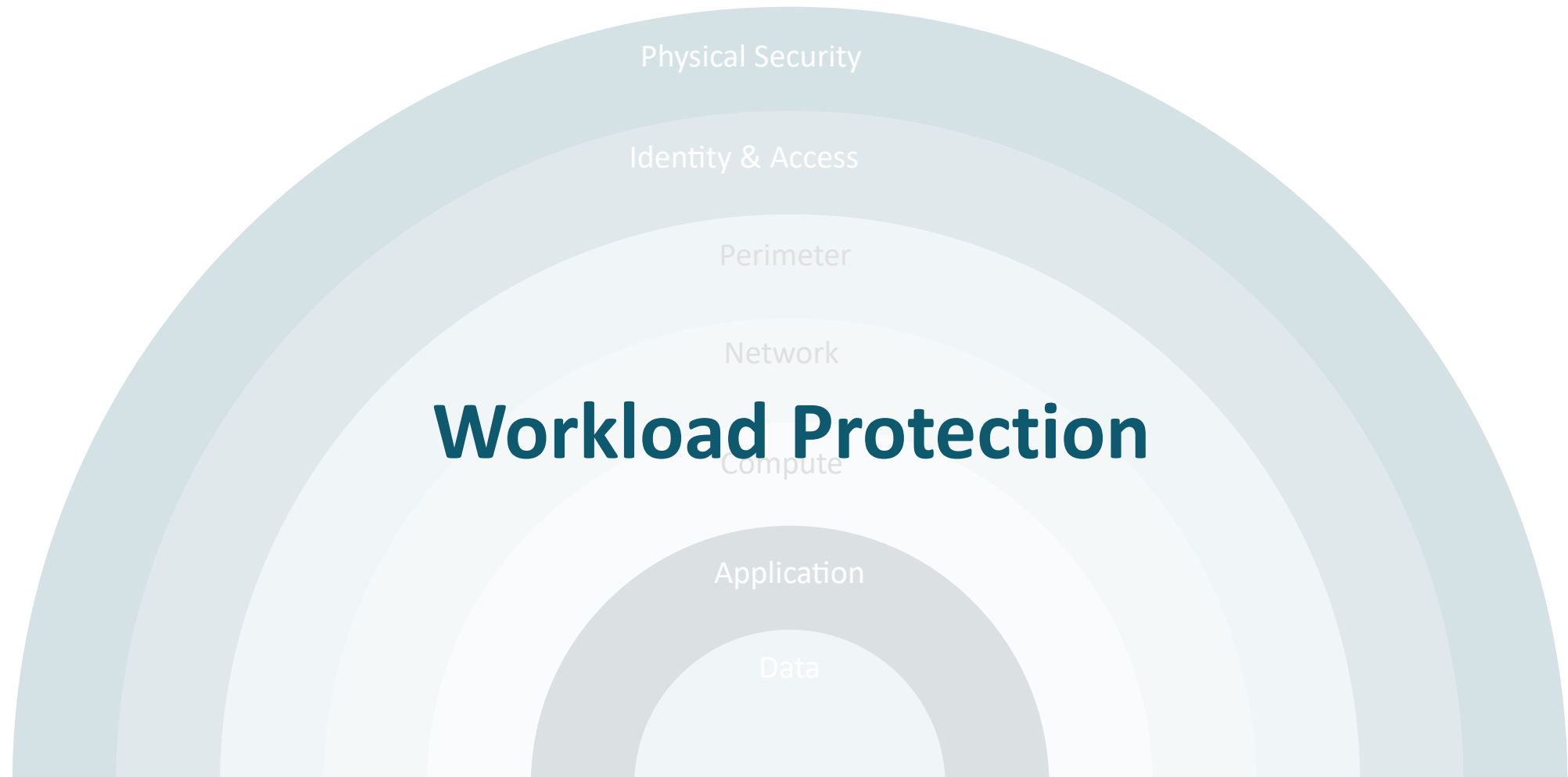
- Just-in-**time** (JIT)
- Just-**enough**-access (JEA)
- Risk-based **adaptive** policies
- Data protection against **out of band** vectors

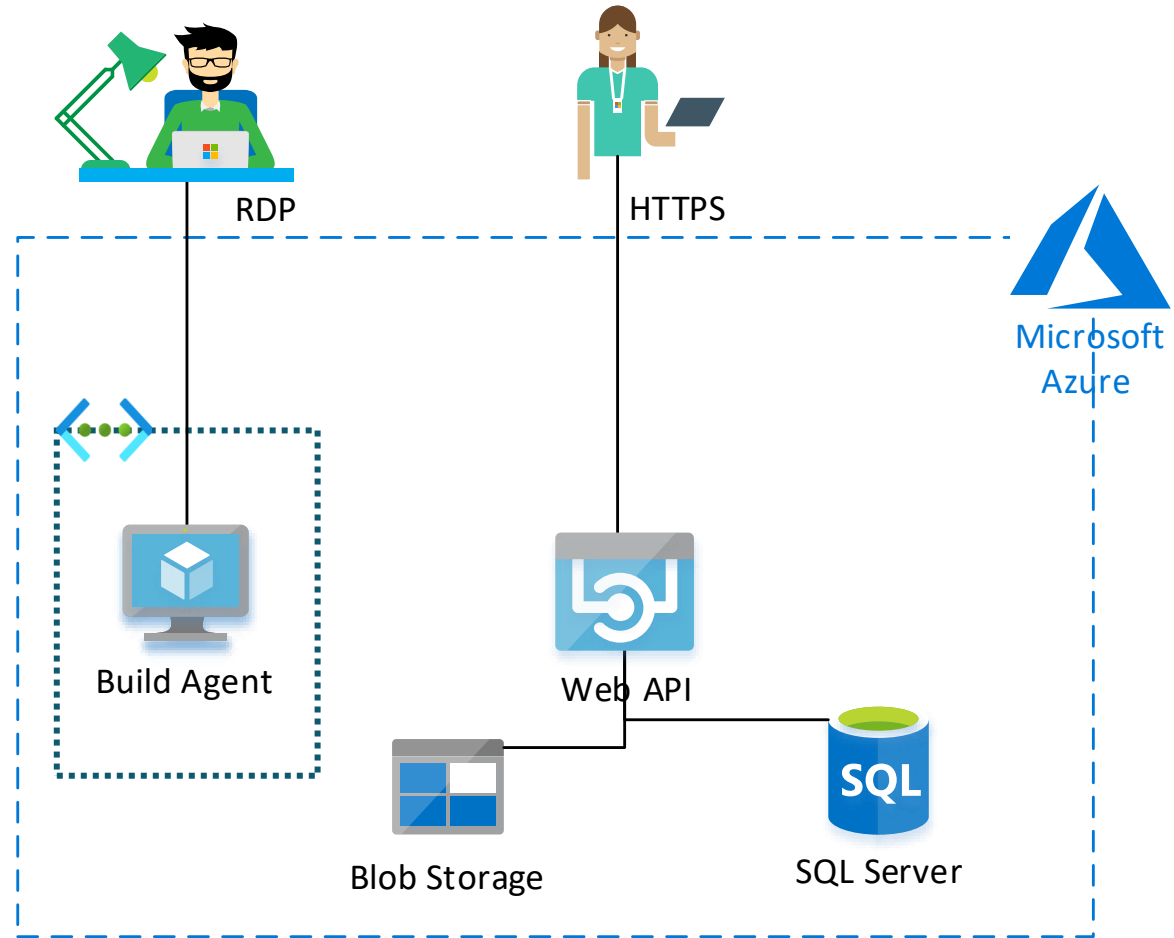


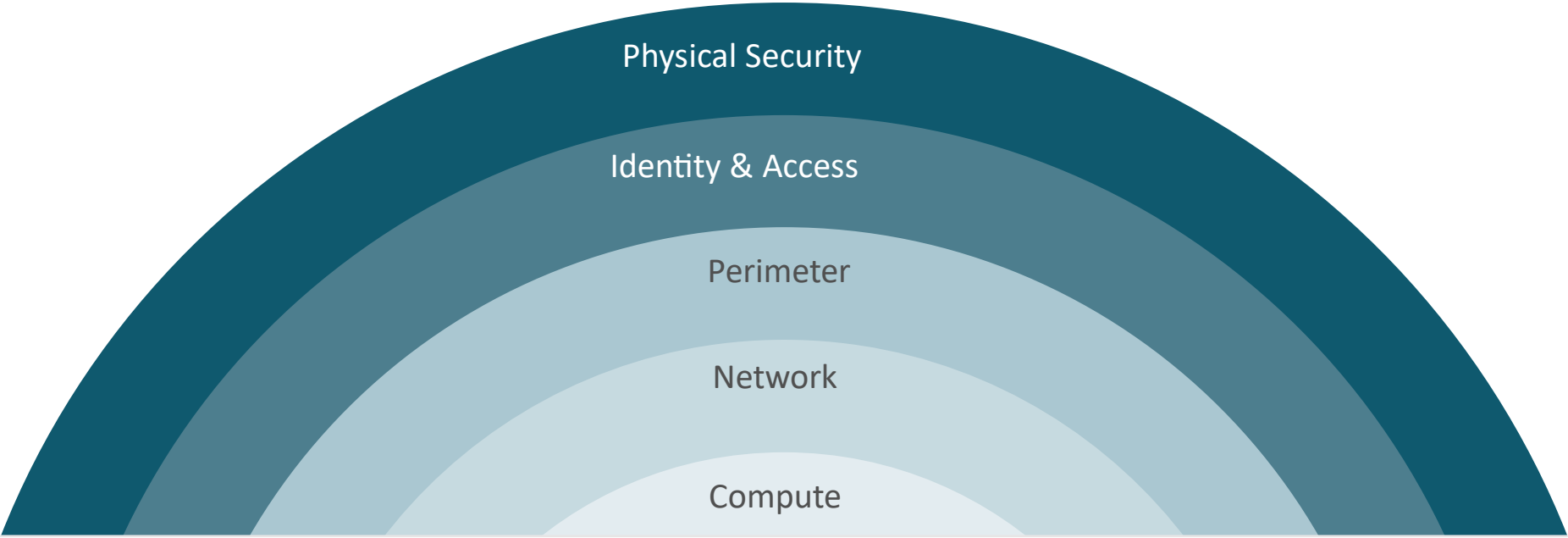
Assume breach

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







Workload Protection

Microsoft Defender for Cloud



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

Home > Microsoft Defender for Cloud | Overview ...
Showing 2 subscriptions

Search << Subscriptions >> What's new

General

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

Security posture

- 6/6 Unassigned recommendation
- 0/0 Overdue recommendations
- 0 Attack paths

Secure score

- Azure 75%
- AWS -
- GCP -

75% SECURE SCORE

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



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 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

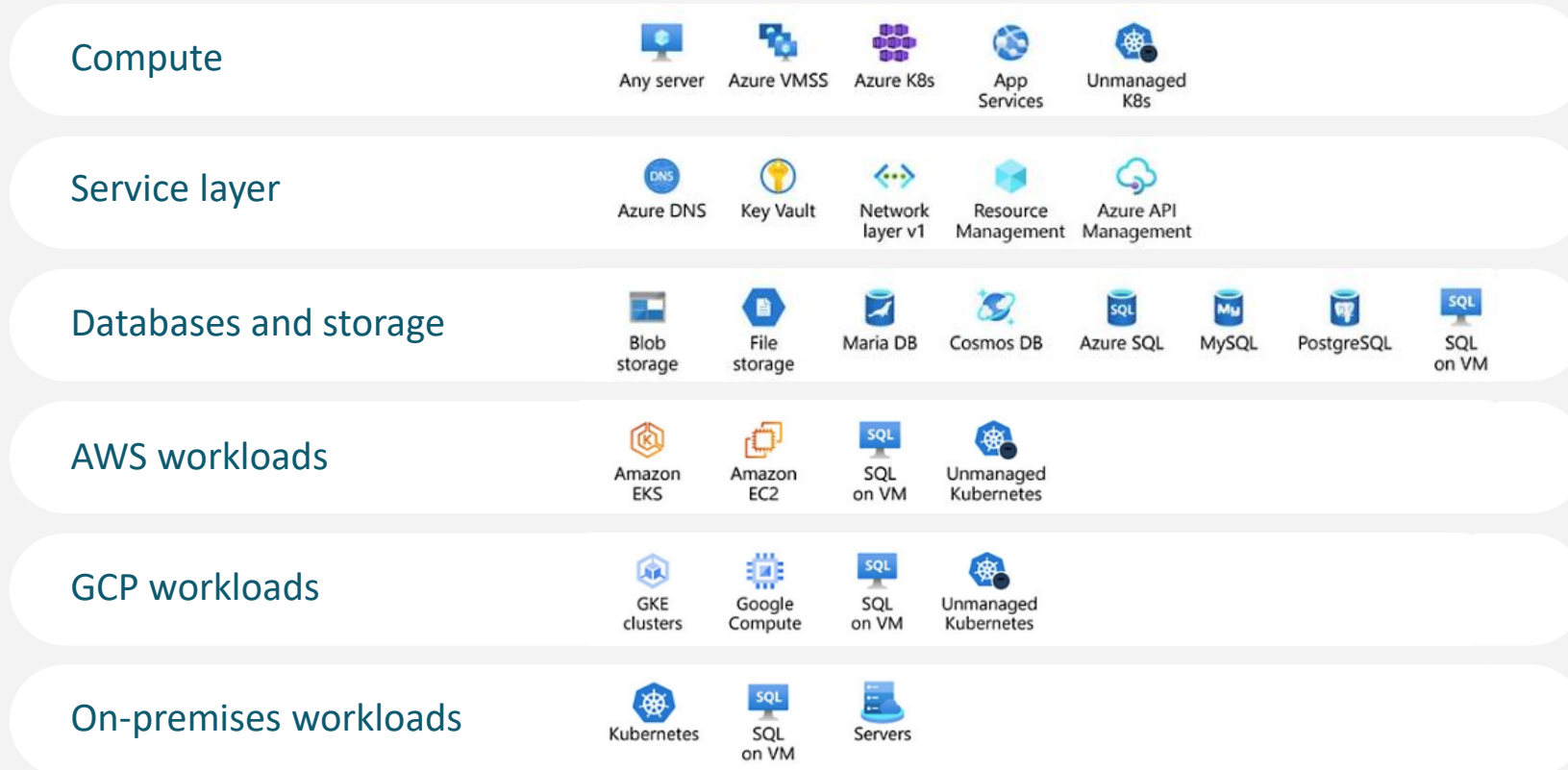
0% For full protection, enable 15 resource plans

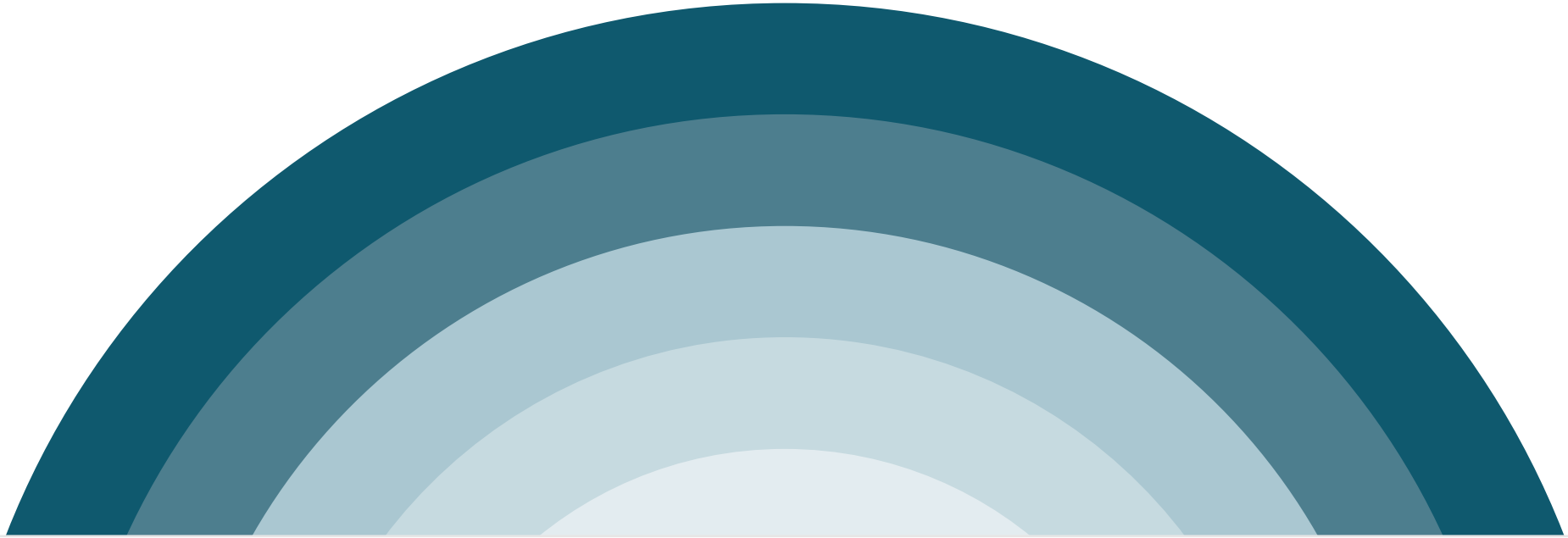
Inventory

Unmonitored VMs

0 All VMs are monitored

Microsoft Defender for Cloud – Workload protection



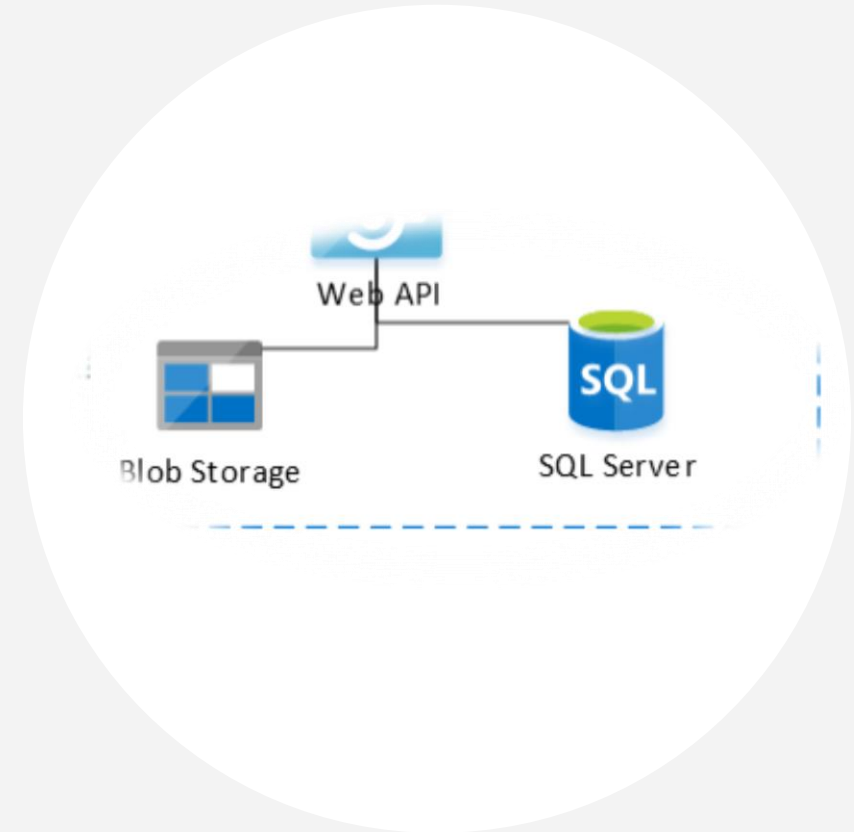


Data Security

Data Security



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





Encryption in-transit (TLS)

TLS 1.2 for most services
TLS 1.3 (very) limited available



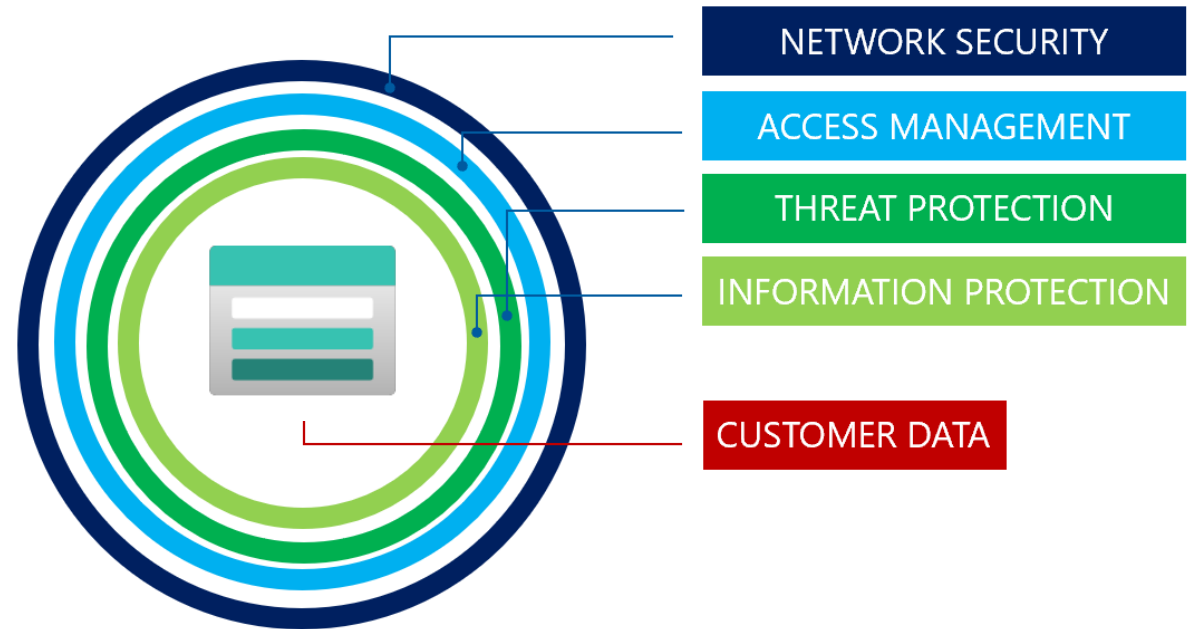
Encryption at-rest (SSE)

Microsoft Managed Key
Customer Managed Key (BYOK)

Protect your storage account



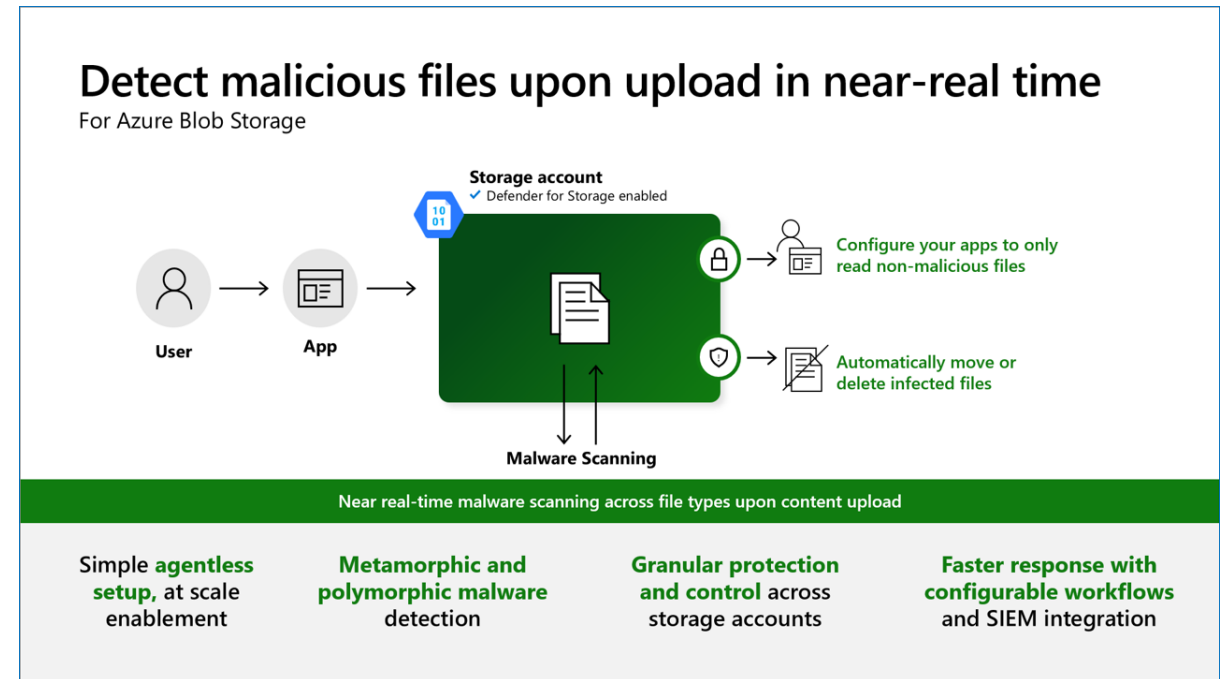
- Control Network Access
- AAD authentication
- Storage account keys / SAS
- Follow least privileged principle
- Microsoft Defender for Storage
- Encryption at-rest (SSE)
- Encryption in-transit (TLS)
- Data protection (soft-delete)
- Immutable Blobs



Microsoft Defender for Storage



- Defender for Storage includes:
 - Activity Monitoring
 - Sensitive data threat detection
(preview feature, new plan only)
 - Malware Scanning
(new plan only)



Microsoft Defender for Storage – DEMO

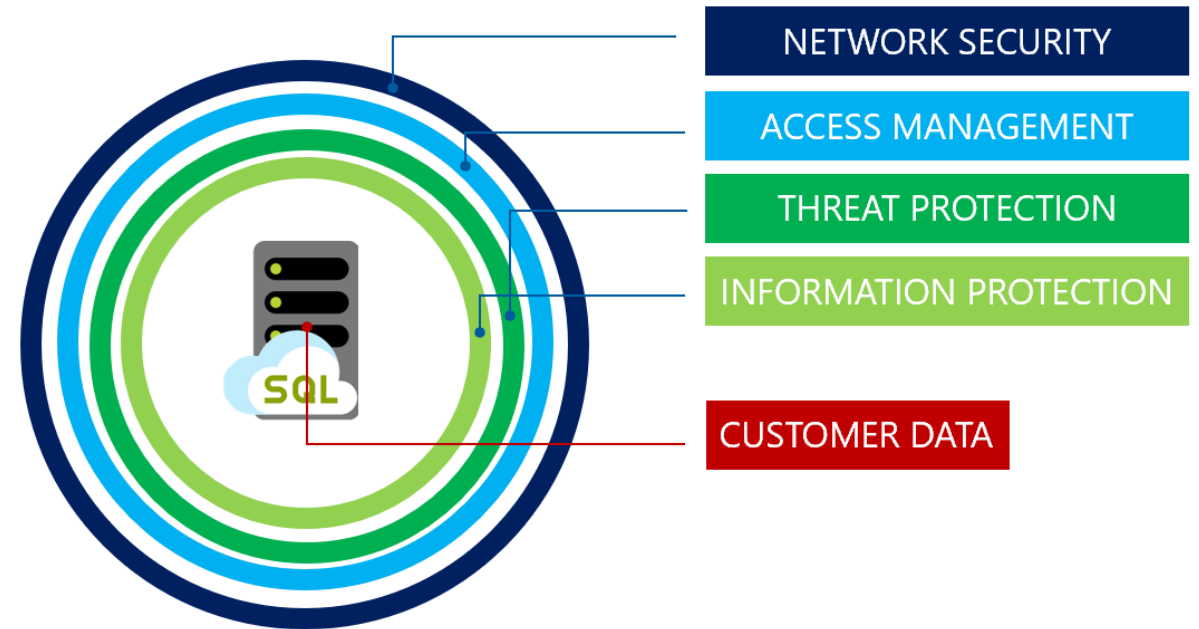


- └ Create Storage Account
 - └ Activate MS Defender For Storage
 - └ Upload files
 - Normal file
 - EICAR file
 - └ See what happens!

Protect your SQL server



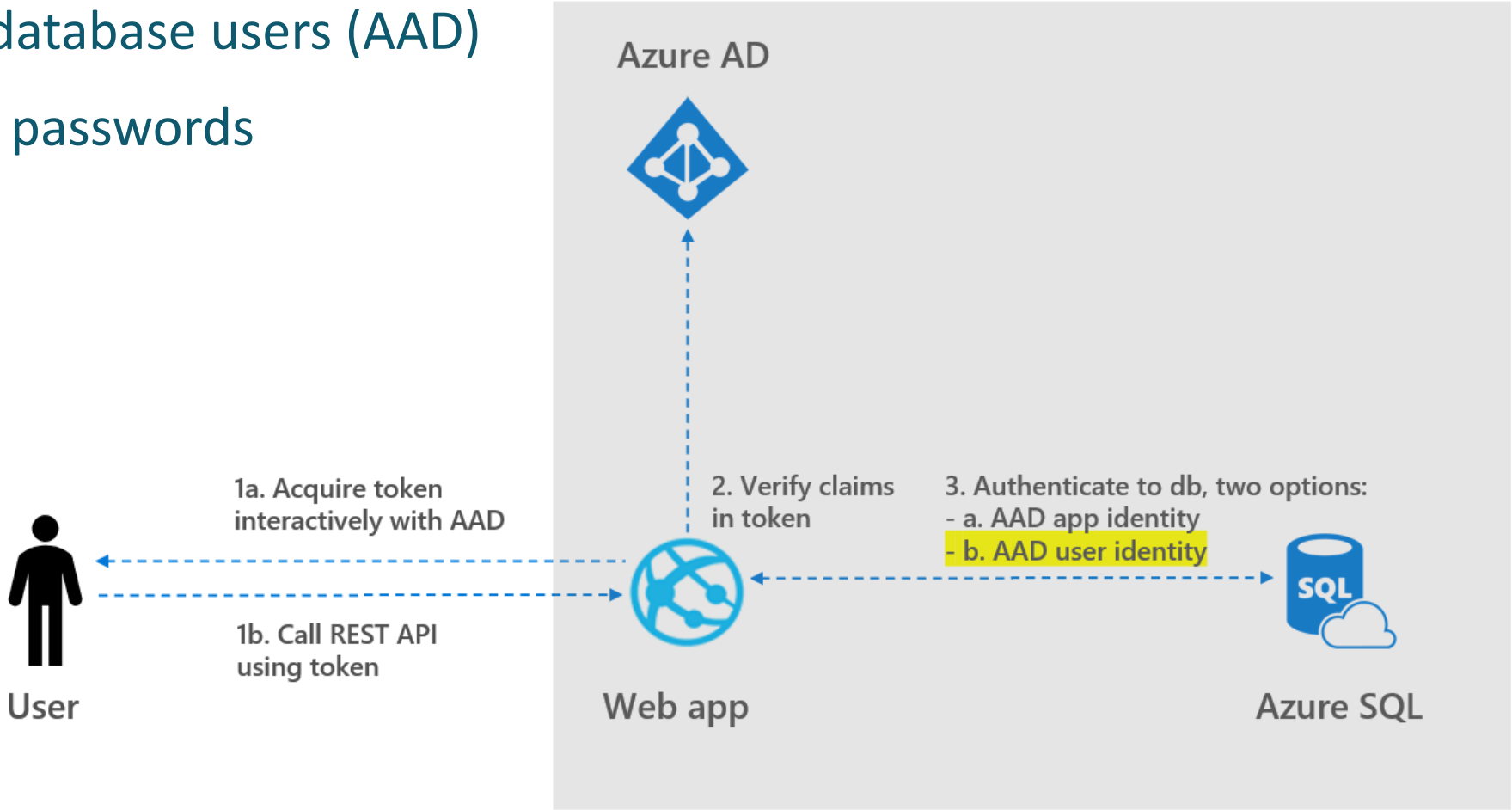
- Control Network Access
- SQL / AAD authentication
- Row Level Security
- Follow least privileged principle
- Enable Auditing
- Microsoft Defender for Cloud
- Transparent Data Encryption (TDE)
- Transport Layer Security (TLS)
- Always Encrypted
- Dynamic Data Masking

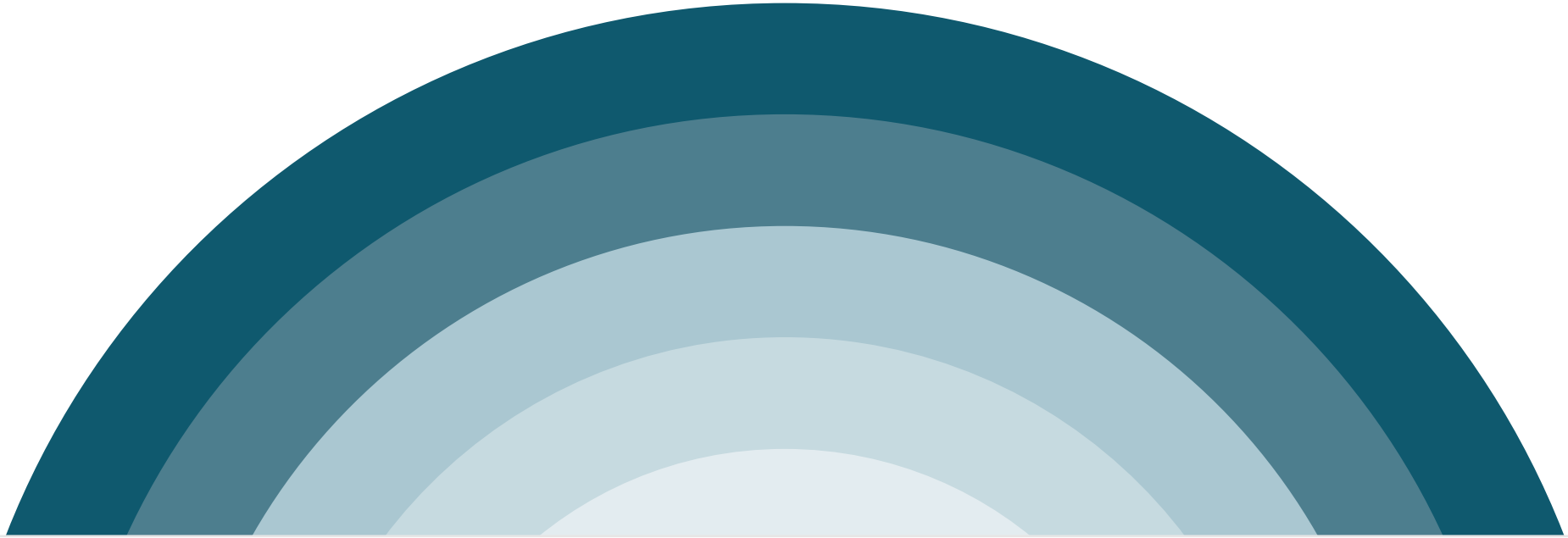


SQL AAD Authentication



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





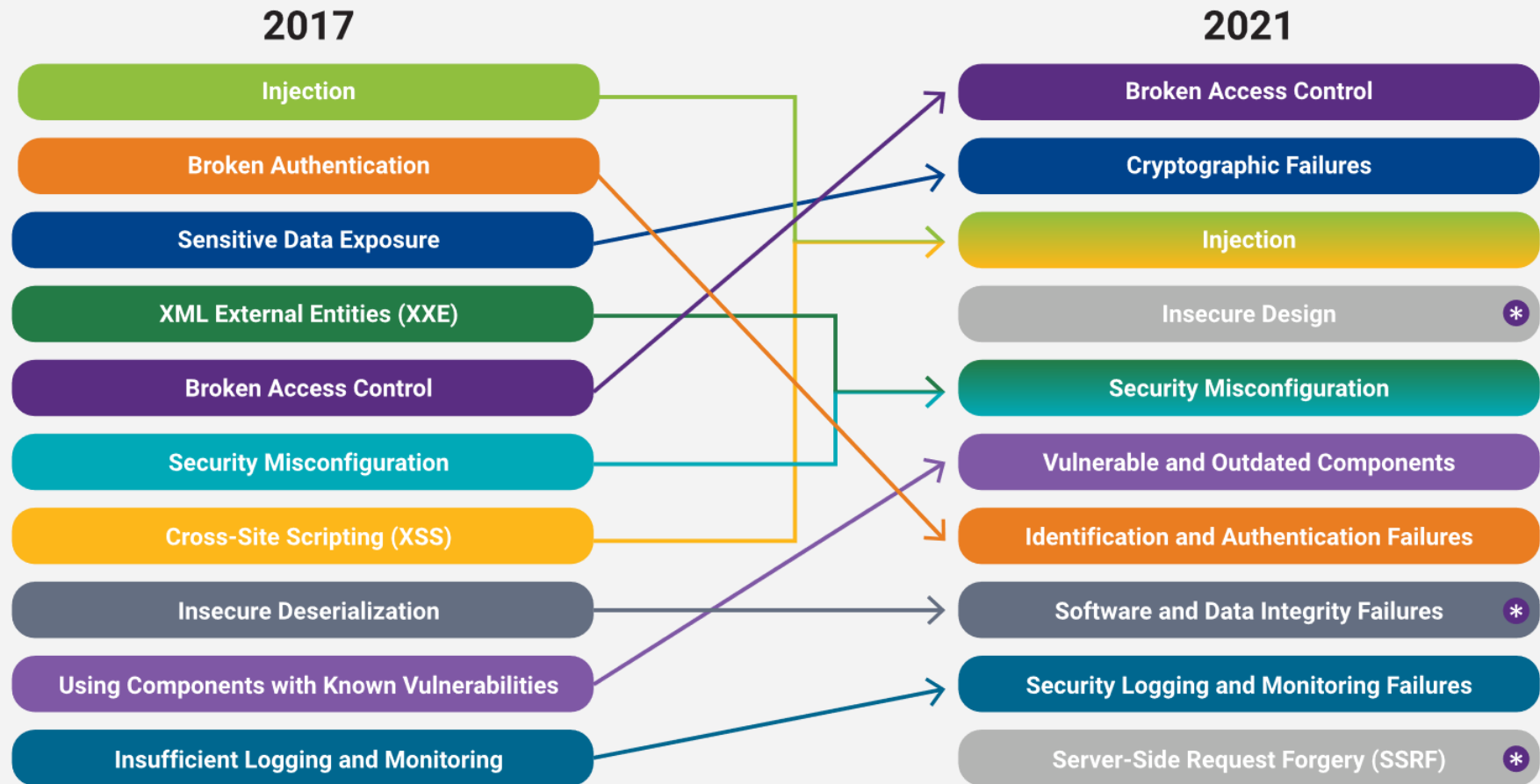
Application Security



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



OWASP TOP-10



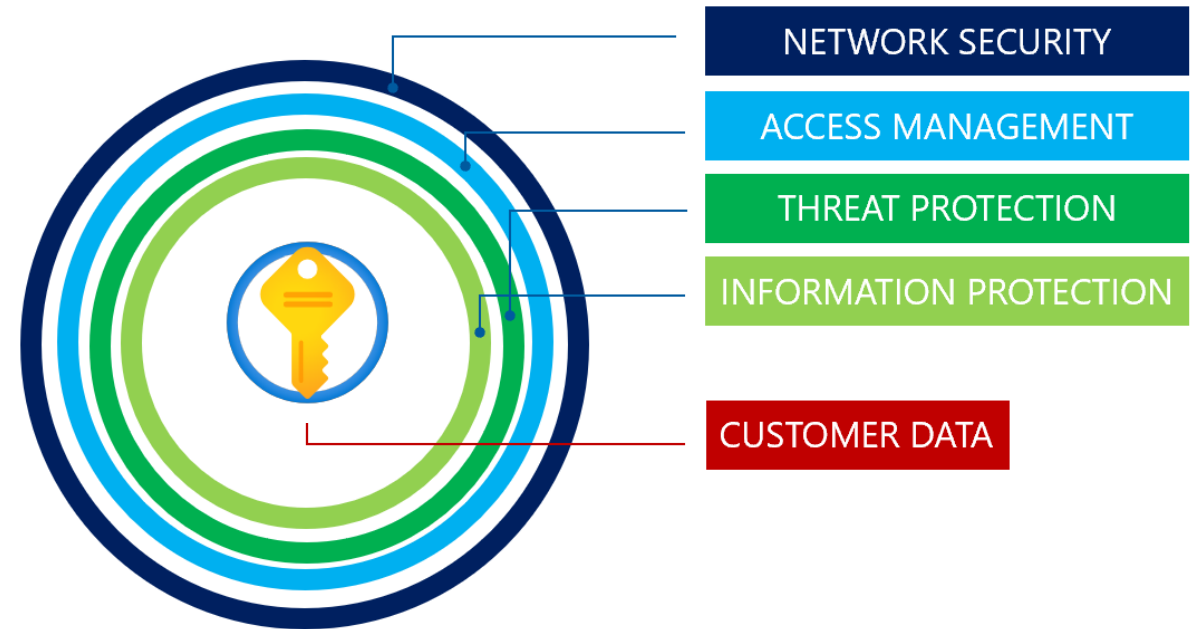
owasp.org/Top10/

* new in 2021

Protect your Key Vault



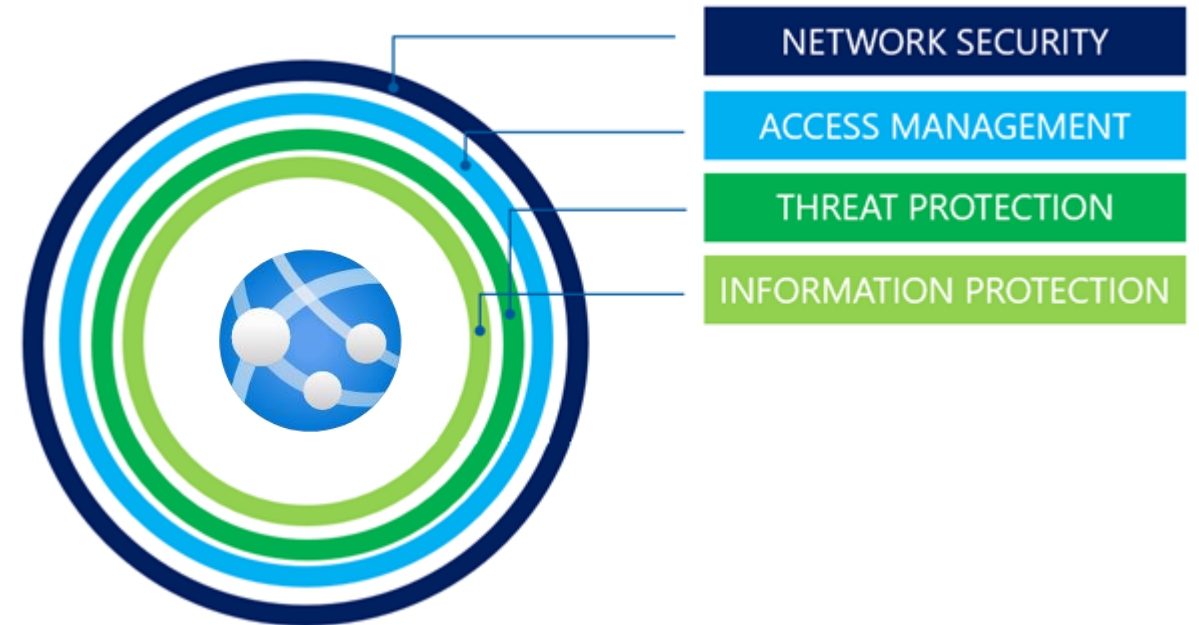
- Control Network Access
- RBAC authorization
- Follow least privileged principle
- Microsoft Defender for Key Vault
- Encryption at-rest & in-transit
- Data protection (soft-delete & purge protection)

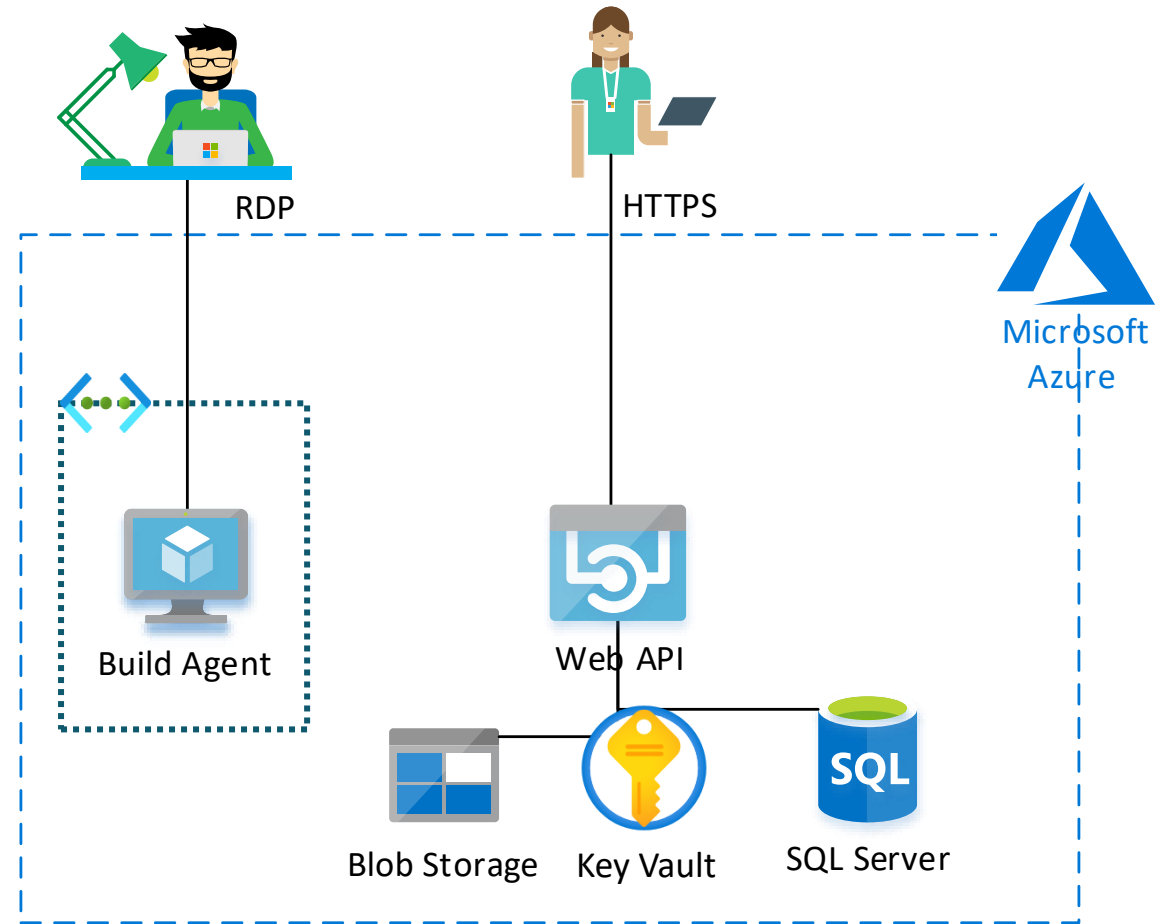


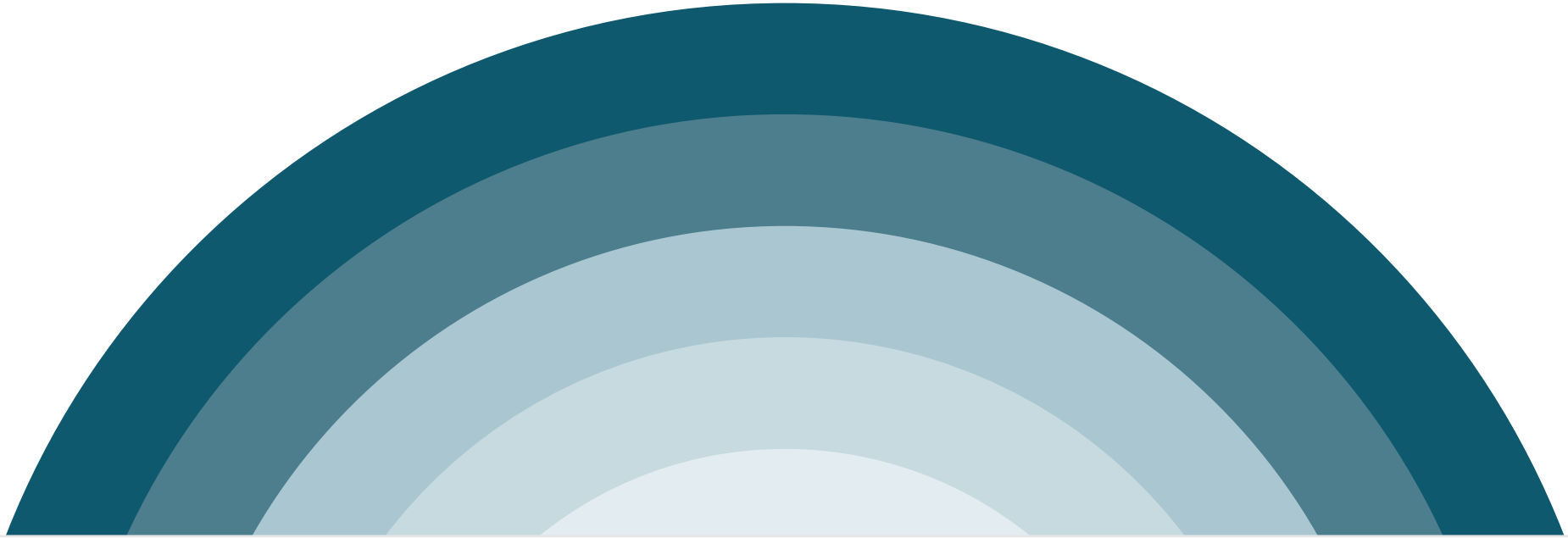
Harden your App Services



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



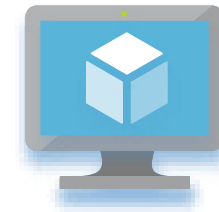




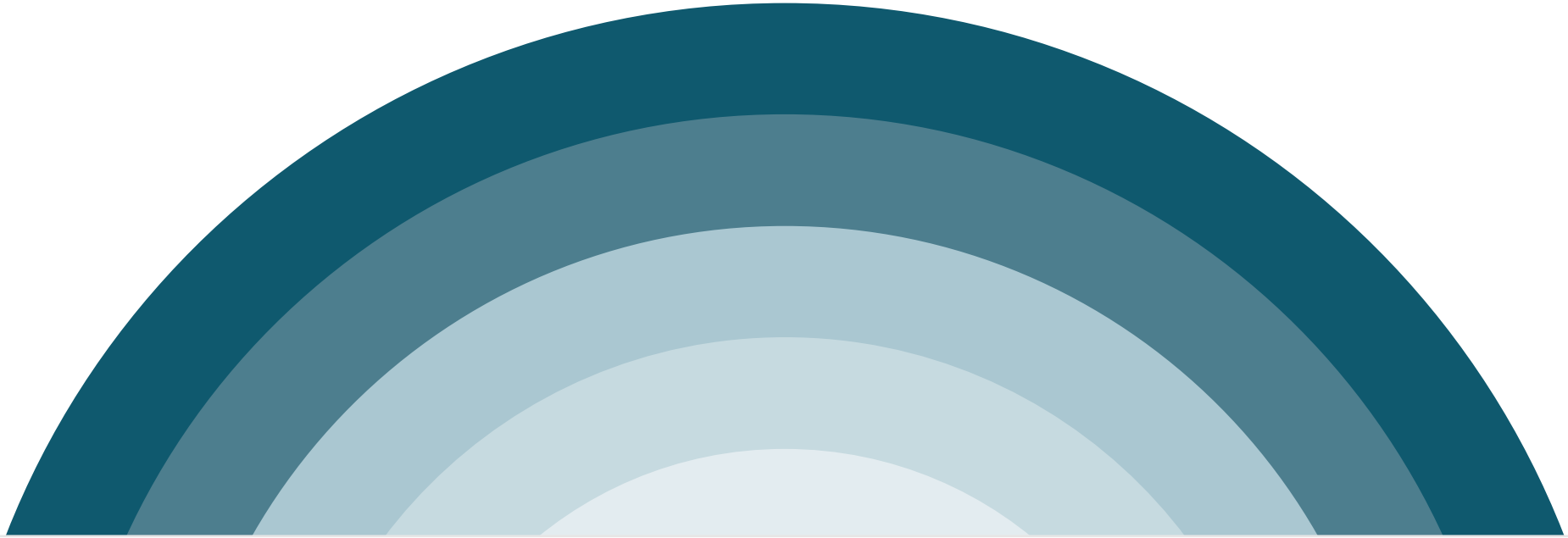
Compute Security



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



Build Agent

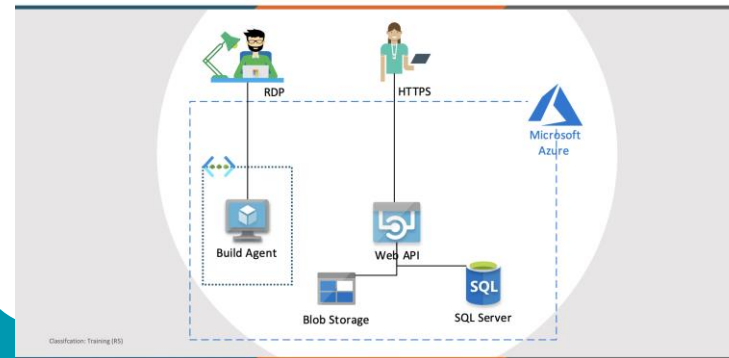


Network Security



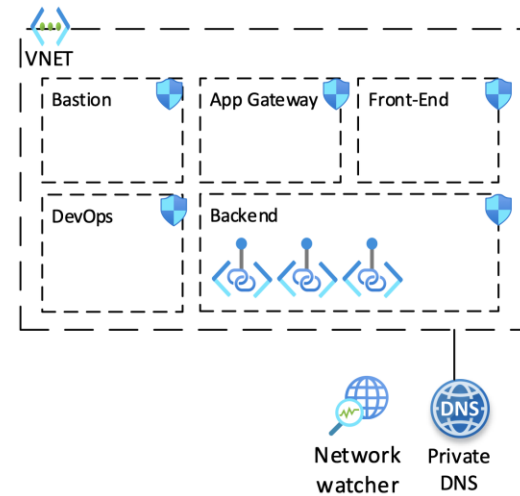
Solution

V 0.1

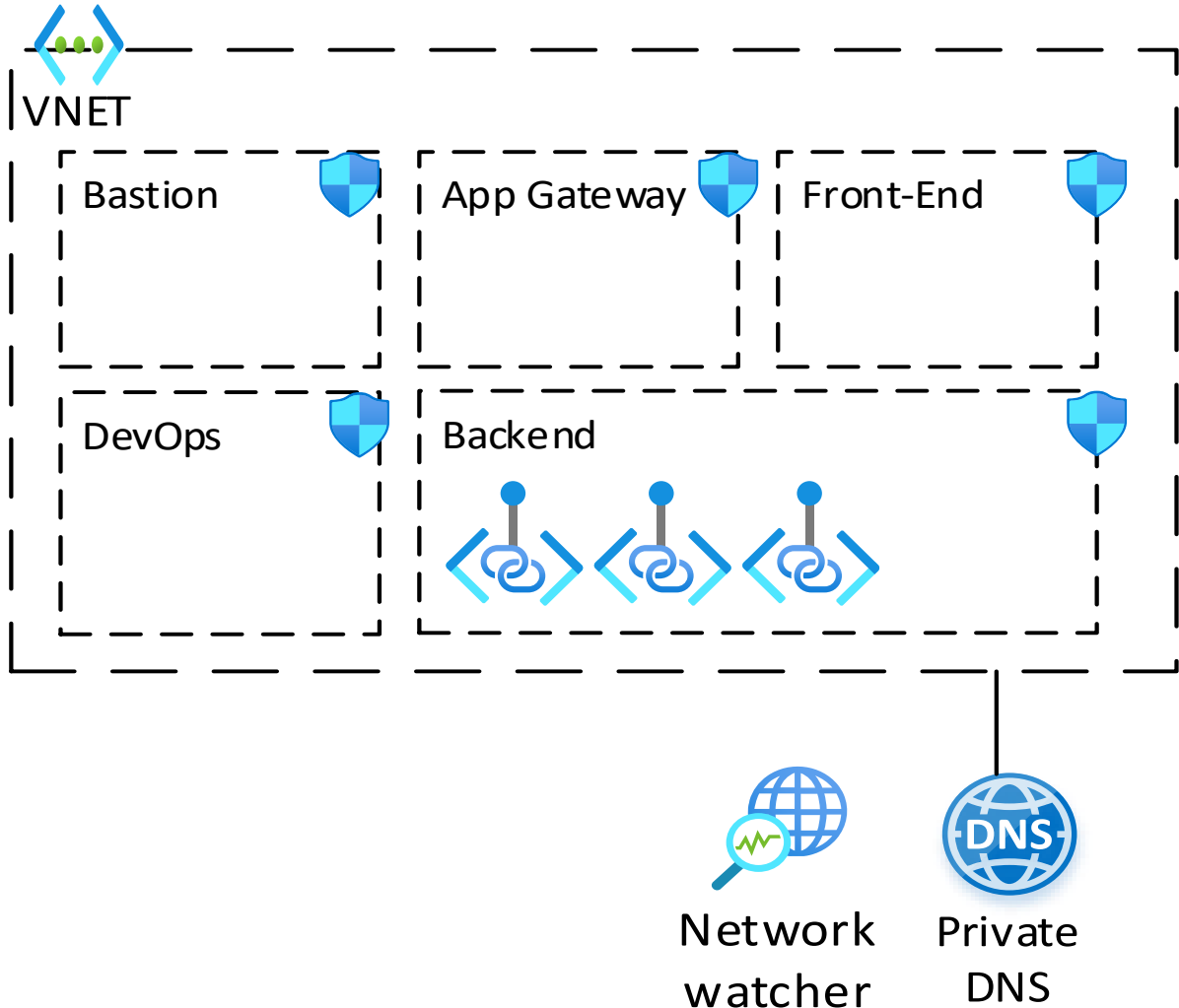


Infrastructure

Infrastructure View



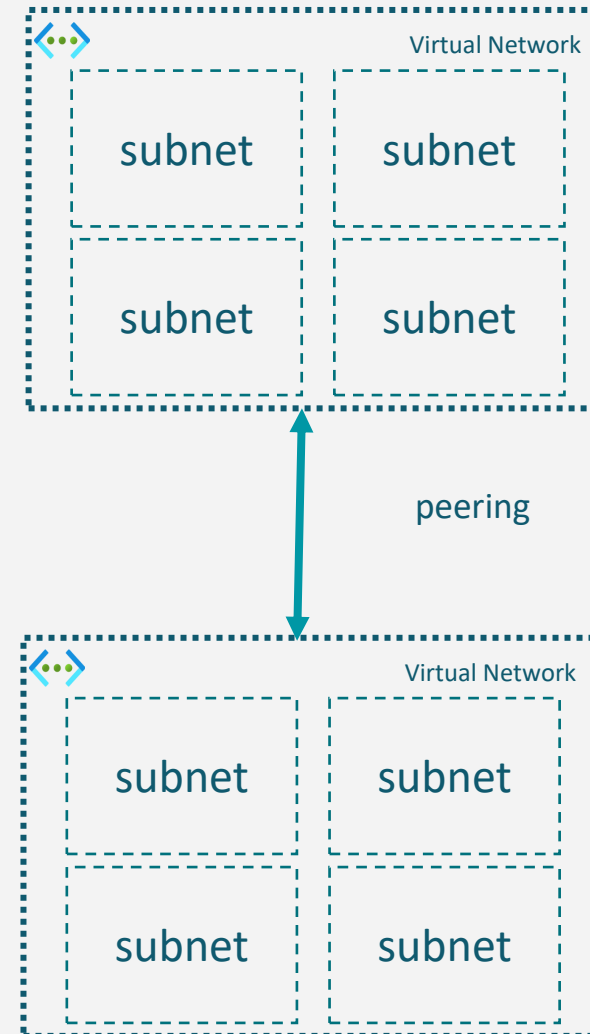
Infrastructure View



Virtual Network



- └ Subnets
- └ VNET Peering
- └ Filter network traffic between subnets
 - NSG
 - NVA
- └ Routing
- └ 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

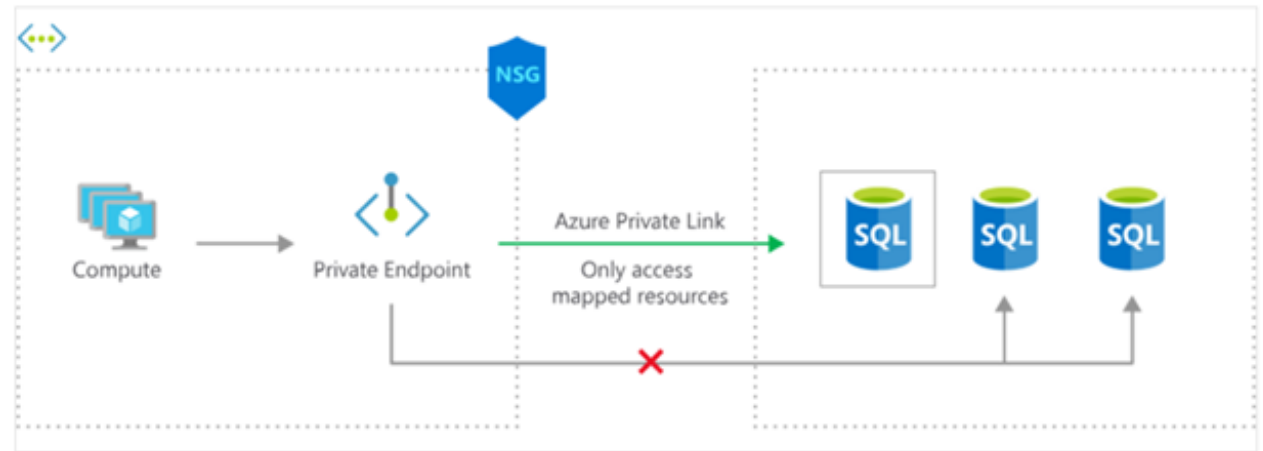
Network security group

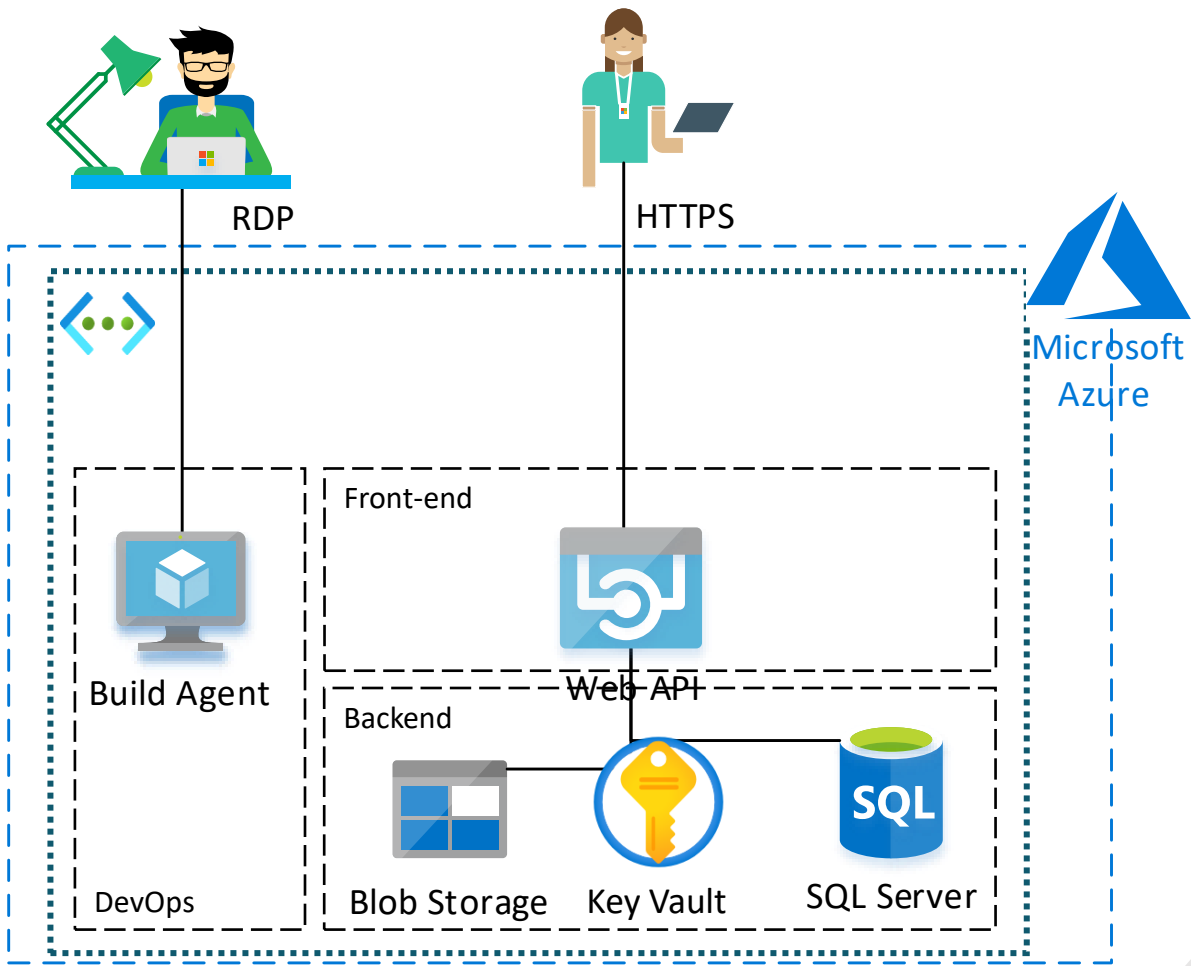
PRIORITY	NAME	PORT	PROTOCOL	SOURCE	DESTINATION	ACTION
65000	AllowVnetOutBound	Any	Any	VirtualNetwork	VirtualNetwork	✓ Allow
65001	AllowInternetOutBound	Any	Any	Any	Internet	✓ Allow
65500	DenyAllOutBound	Any	Any	Any	Any	✗ Deny

How do Private Endpoints work?

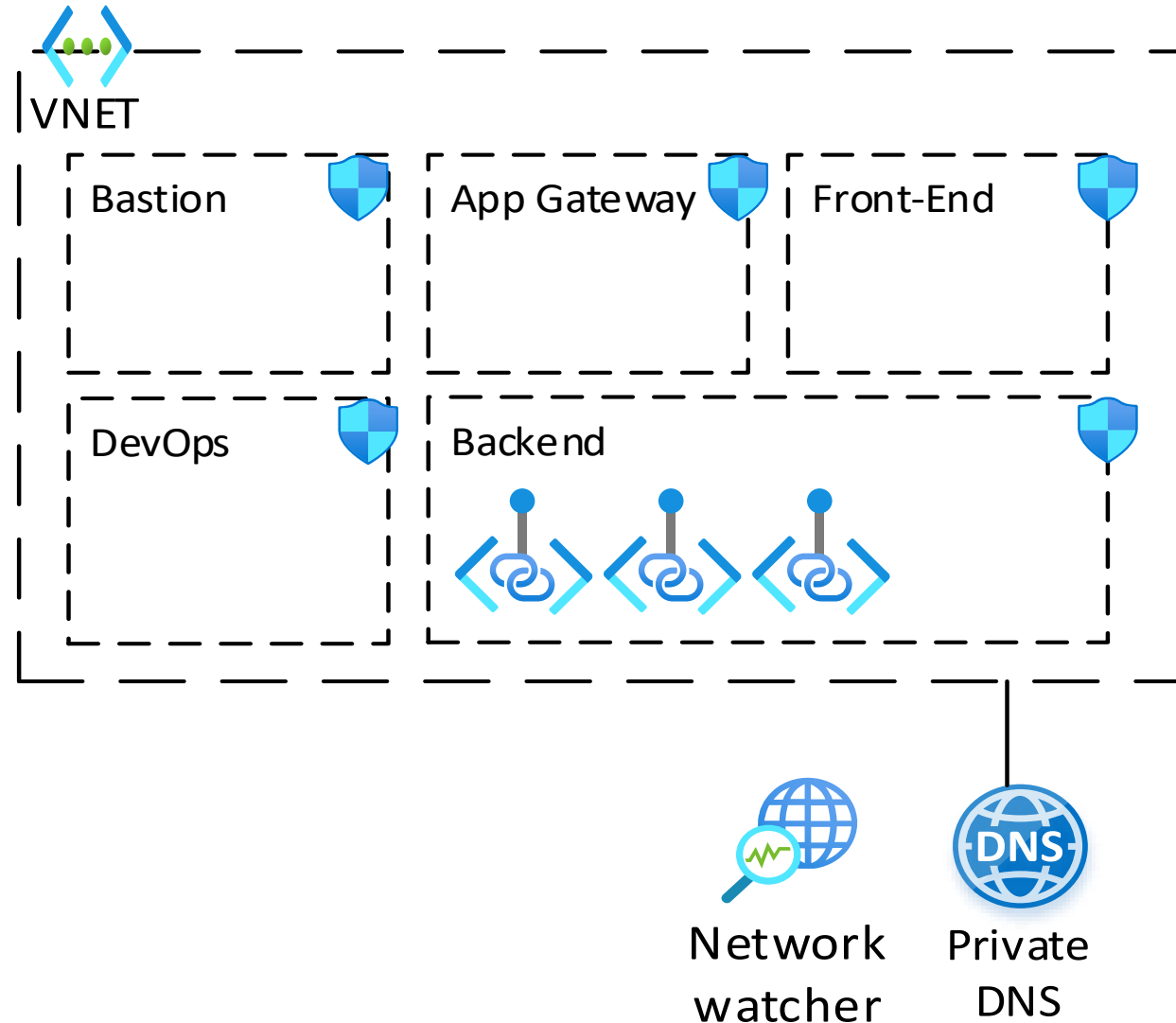


- PE is a special type of NIC that plugs into VNET
- PE uses private IP from subnet
- Traffic remains in VNET
- Relies on DNS





Infrastructure View (V 0.3)





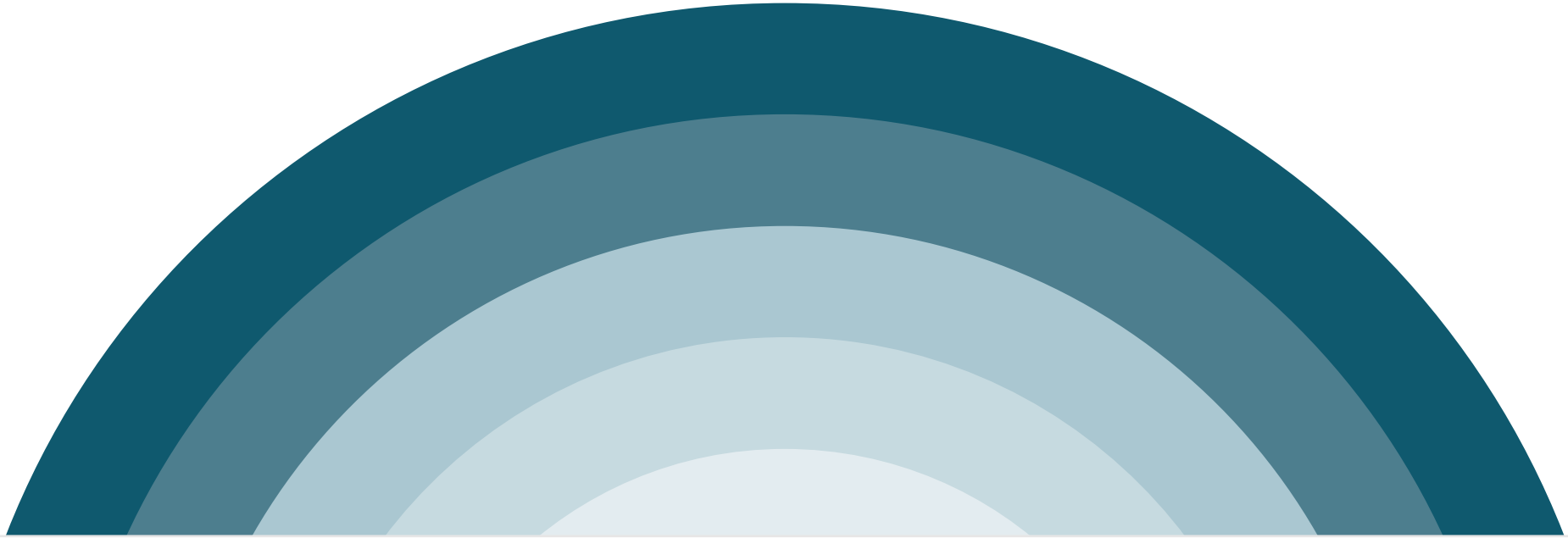
Wait... how can I access my services?



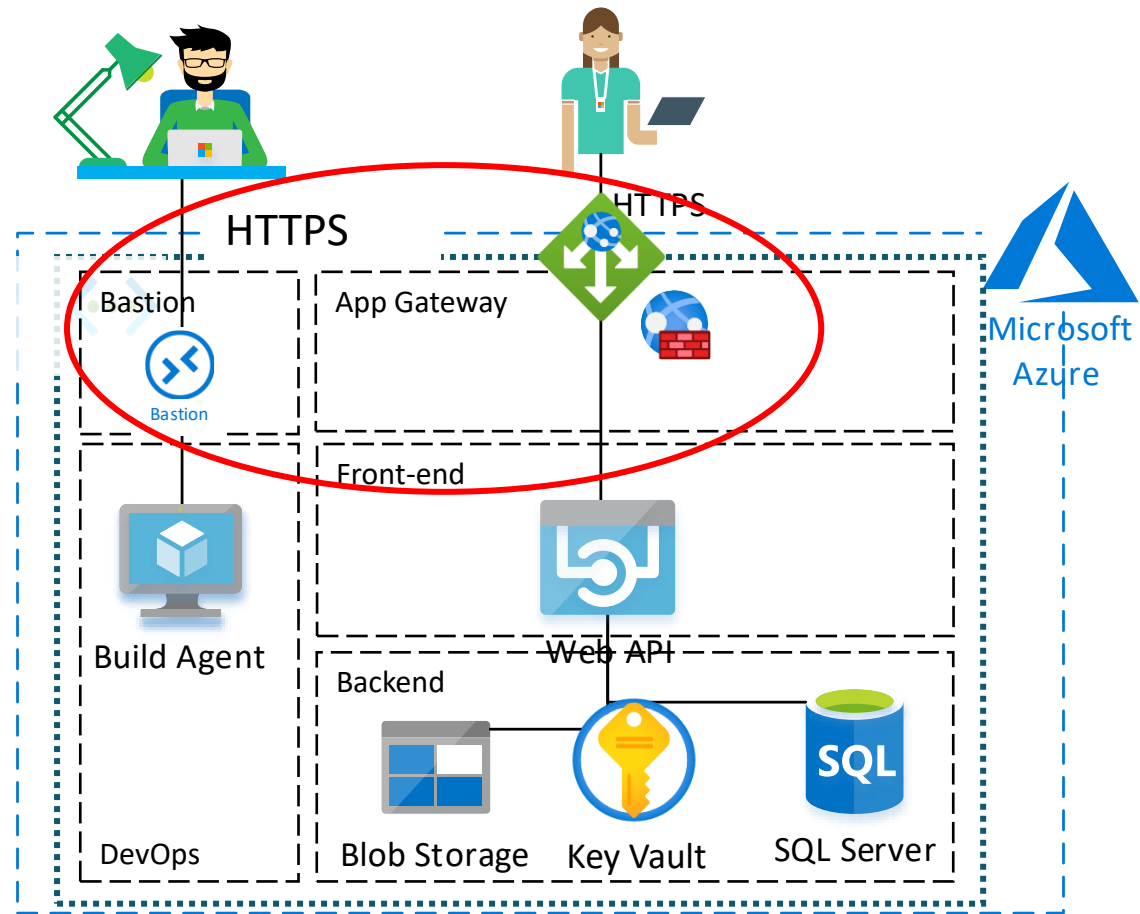
Implications on daily operations



- └ 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



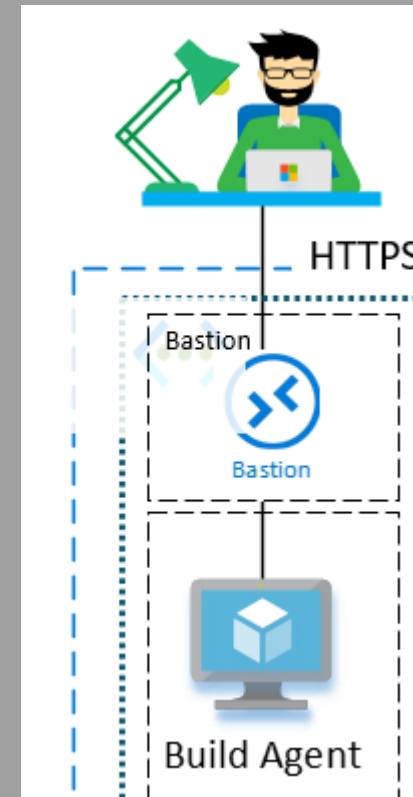
Perimeter Security



Azure Bastion



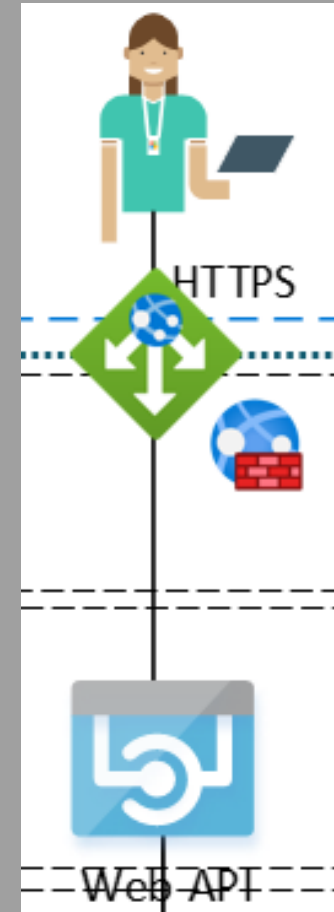
- Provide RDP/SSH access via the browser without the need of a public endpoint / IP
- Reduces attack surface
- Single deployment per virtual network is enough



AGW ↔ WAF ↔ Web API



- Application Gateway
- with integrated Web Application Firewall



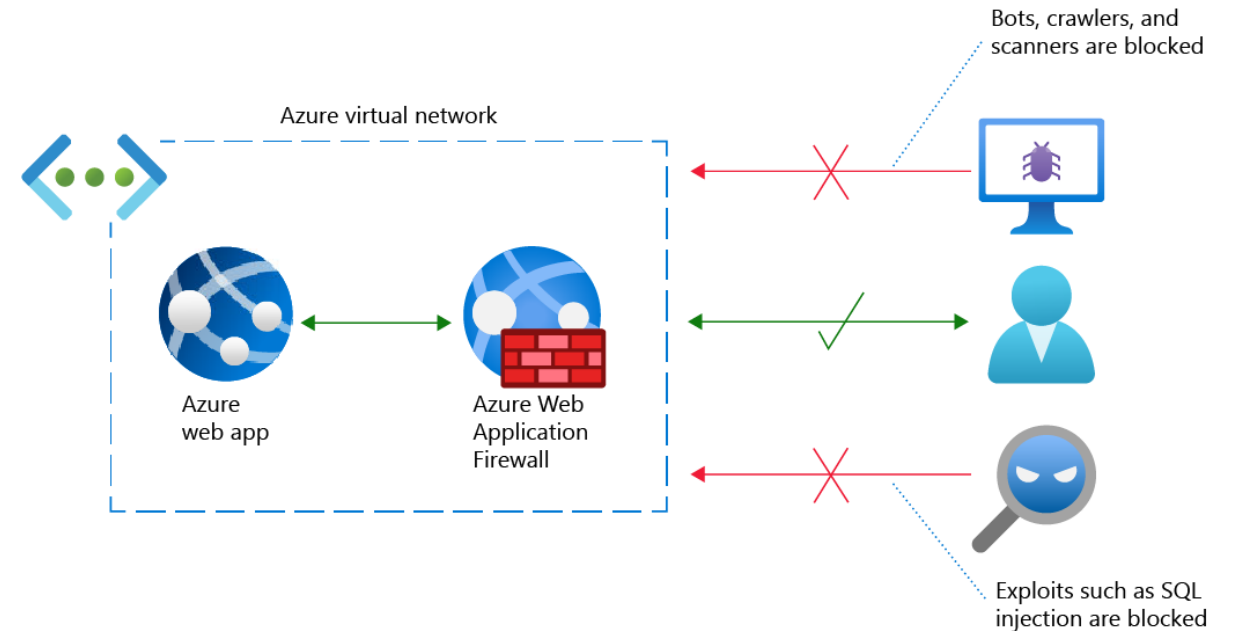
Web Application Firewall (WAF)

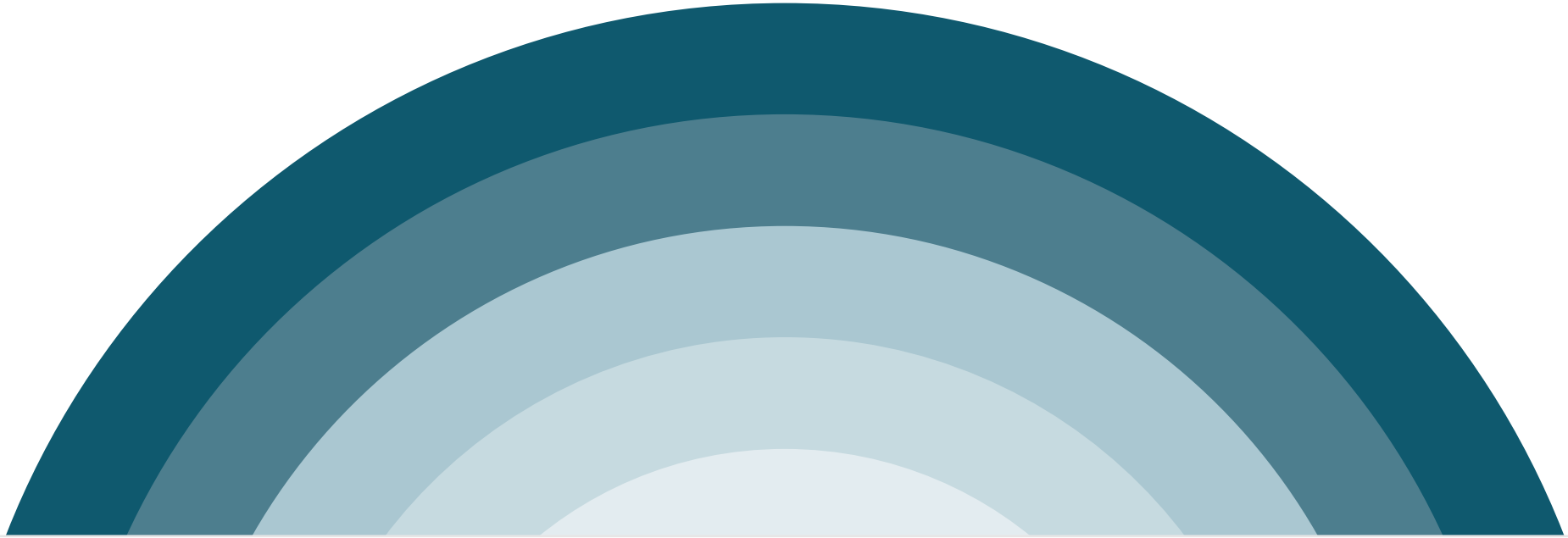


Features:

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

What is the difference with Azure Firewall?





Identity and Access

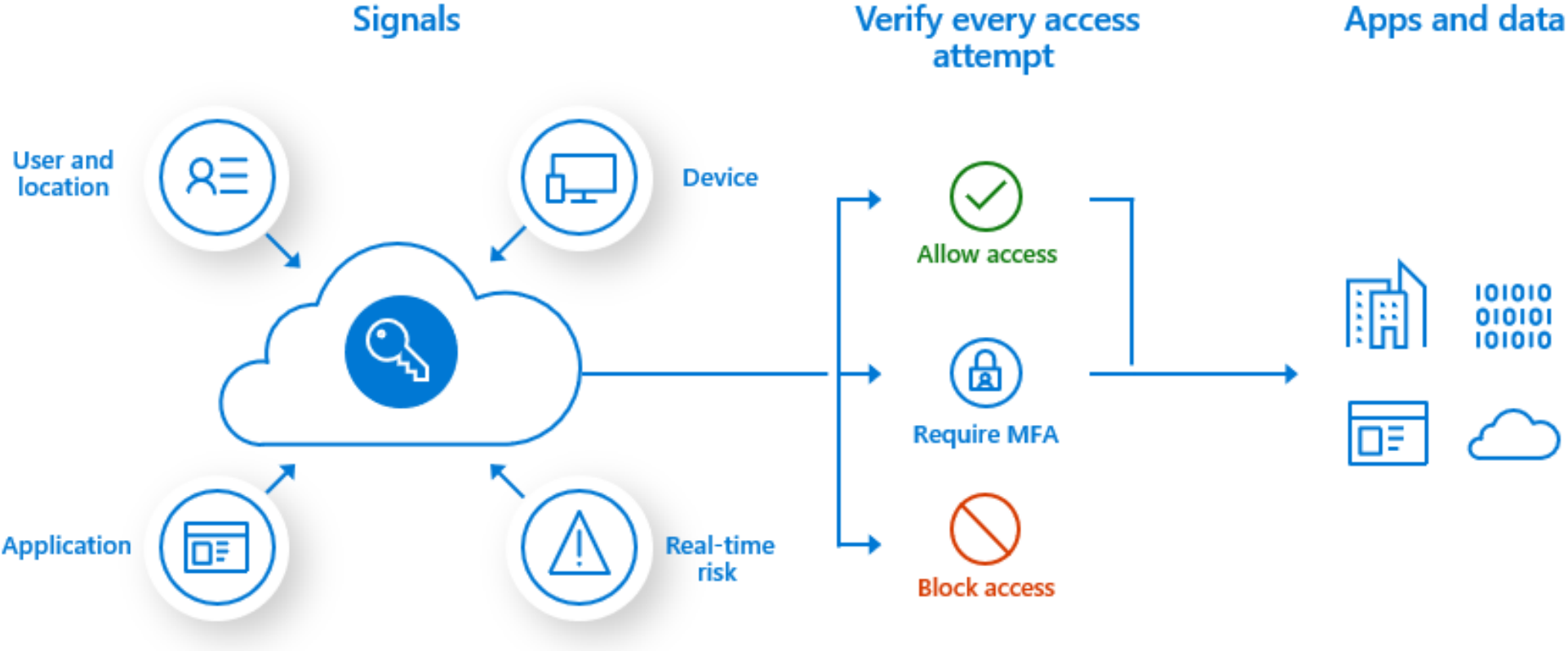
Managed Identity



- 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





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>

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



- └ 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 ...

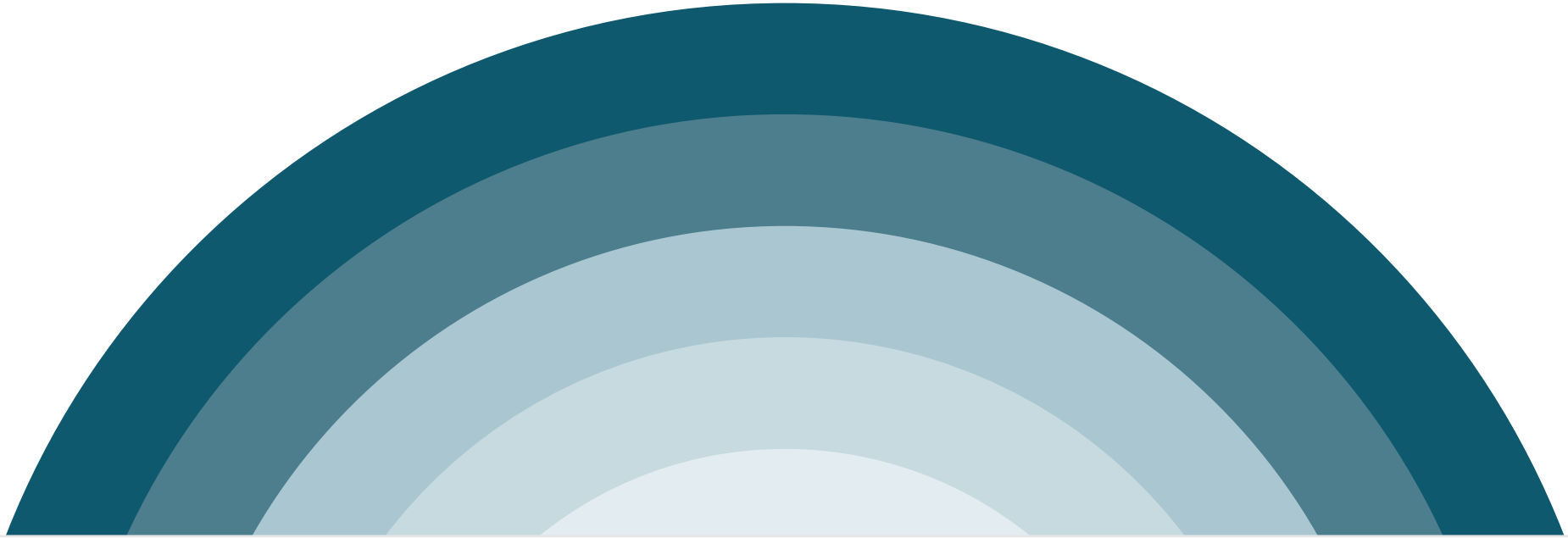
Role **Members** Conditions (optional) Review + assign

 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](#)

```
1 (
2 (
3   !(ActionMatches{'Microsoft.Storage/storageAccounts/blobServices/containers/blobs/read'} AND NOT SubOperationMatches
4   {'Blob.List'})
5 OR
6 (
7   @Resource[Microsoft.Storage/storageAccounts/blobServices/containers/blobs/tags:Malware Scanning scan
8   result<$key_case_sensitive$>] StringEqualsIgnoreCase 'No threats found'
9 )
)
```

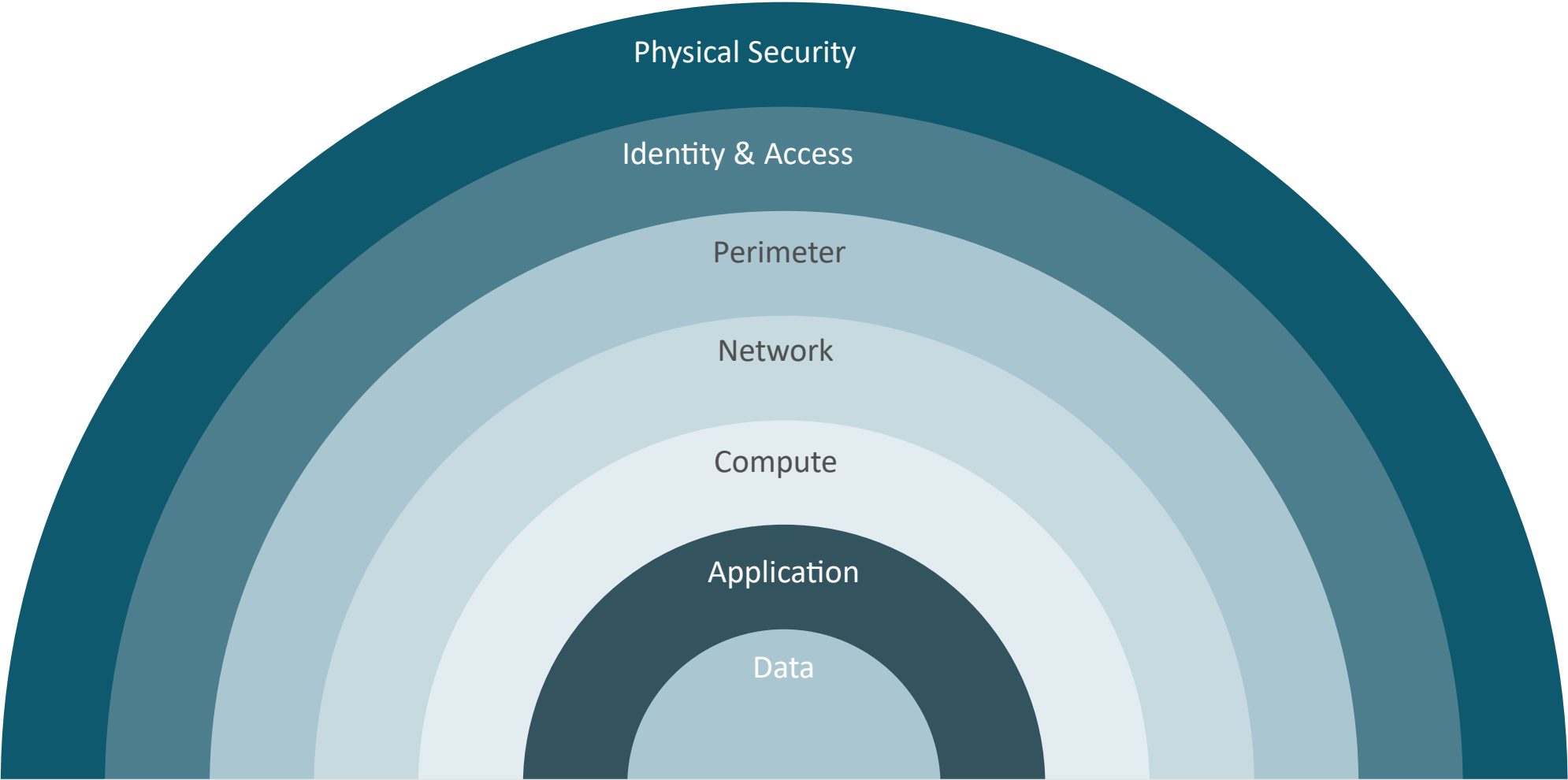


Physical Security



Azure Data Center – Middenmeer (NL)





Questions & Answers

WEBINAR

Building a **Fortress** in Azure



Final info

WEBINAR

Building a **Fortress** in Azure

- ↪ Slides en opname worden vandaag nog gedeeld
- ↪ Februari 2024 nieuw webinar
- ↪ 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

The end

