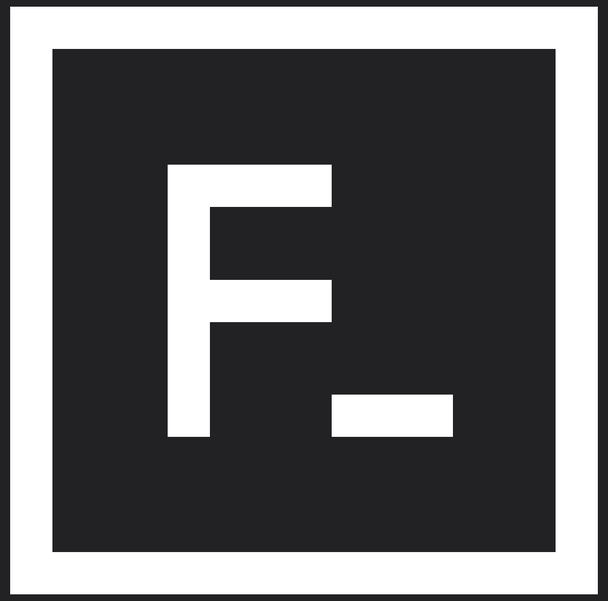
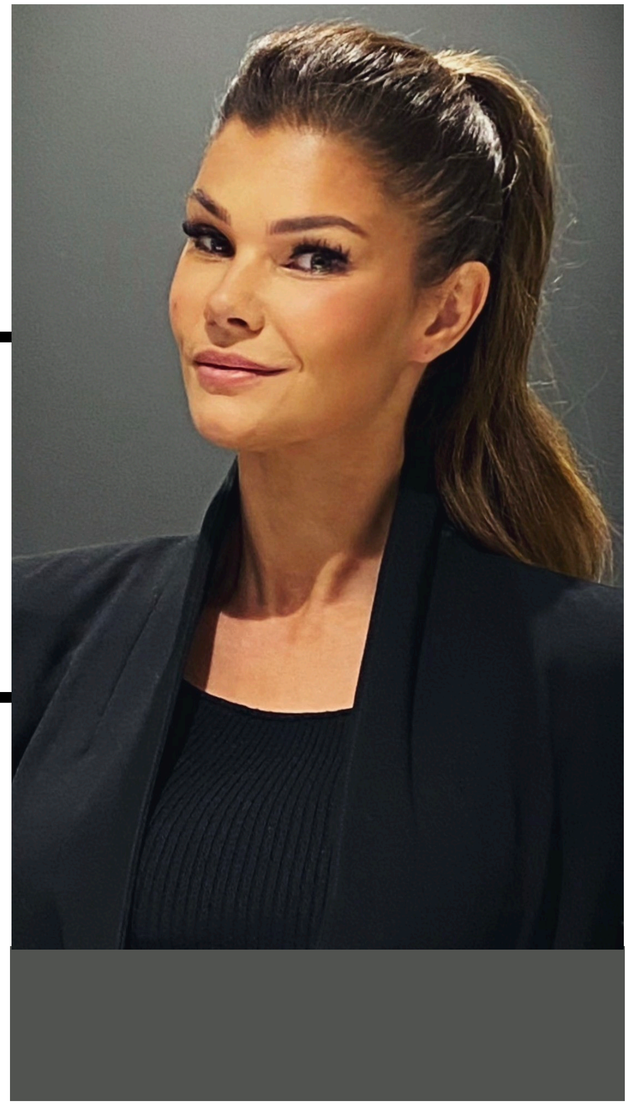
.NET & AZURE COMMUNITY - FORTE DIGITAL
PRESENTATION BY MONICA BEATE TVEDT, DIRECTOR OF TECHNOLOGY





Monica Beate Tvedt

Teknologidirektør

Forte_ Digital

TIDLIGERE

- Agency Director - Head of Microsoft Development, Mixed Reality & Microservices at Sopra Steria
- Head of UMS Innovation Center at Unified Messaging Systems
- Global Head of SaaS Development at Unified Messaging Systems
- Senior Software Engineer Consultant, Webstep @ Sparebanken Vest
- Software Engineer, CellVision
- Gründer

PROSJEKT 2020

- Kunde: **ASKO**
  Rolle: Arkitekt og Front-end lead
- Kunde: **Kværner**
  Rolle: Arkitekt og Mobilspesialist
- Kunde: **COVID-19 Digital Feberpoliklinikk**
  Rolle**:** Løsningsarkitekt

FOREDRAG 2020

Oslo Business Forum 2020, Relevans 2020, Global AI on Tour 2020, Women in Tech 2020, Lørn.Tech.

DIVERSE NTERESSER

Alpint, tennis, programmering, tegne, lese bøker

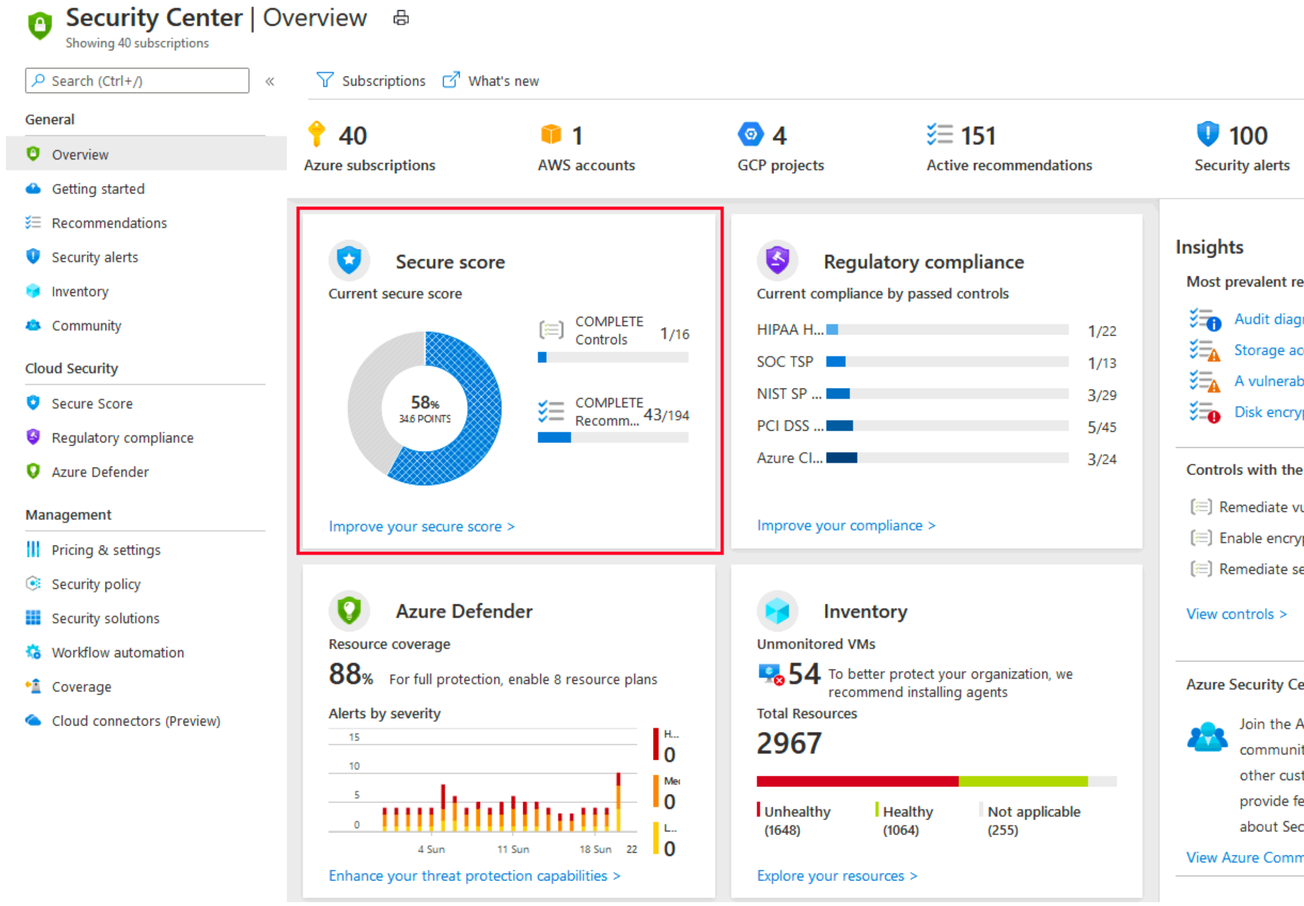
1.0	Security, responsibility, and trust in Azure.
2.0	Configure security policies w/ Exercise 15 min.
3.0	Azure Key Vault.
4.0	Azure Role-based Access control (Azure RBAC).
5.0	Securing Azure SQL Databases - workshop 60 min.
-	-
6.0	Self Study

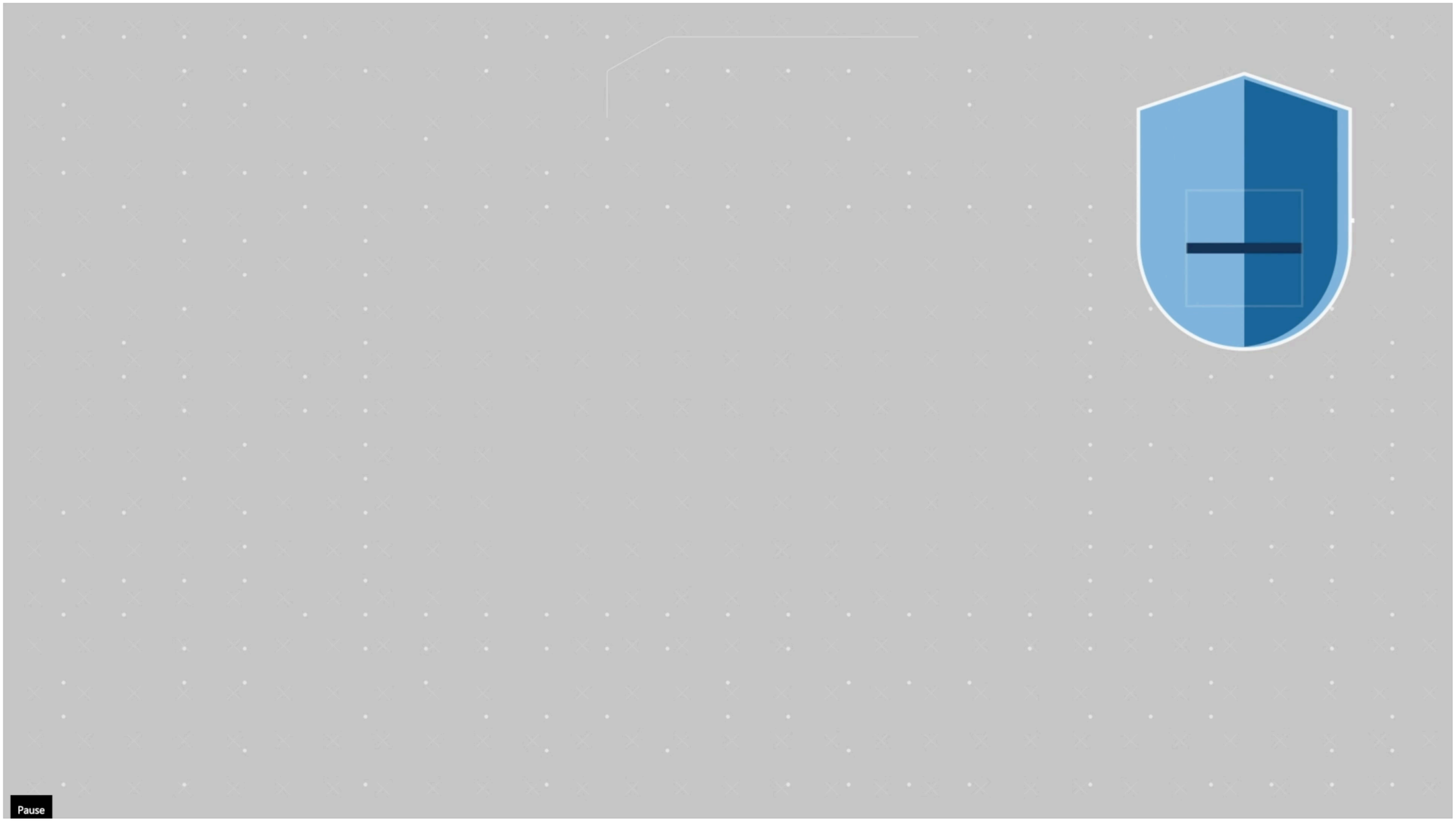
1.0
Security, responsibility, and trust in Azure.

Azure Security Center

Azure Security Center is a unified infrastructure security monitoring service that provides visibility of your security posture across all of your services, both on *Azure* and *on-premises*.

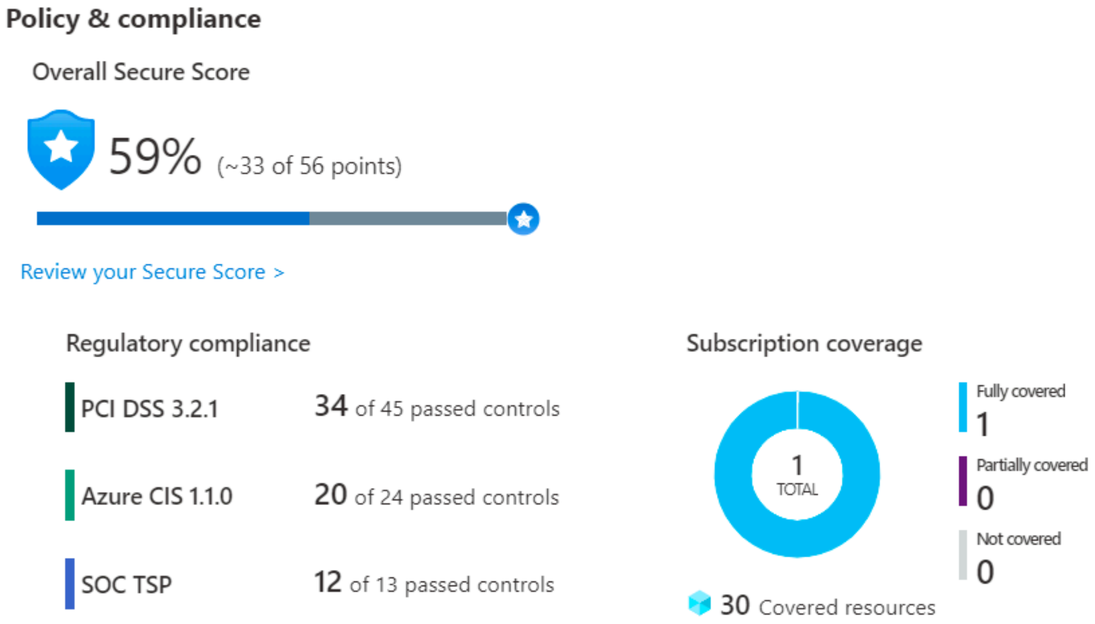
The term *security posture* refers to cybersecurity policies and controls, as well as how well you can predict, prevent, and respond to security threats.




Pause

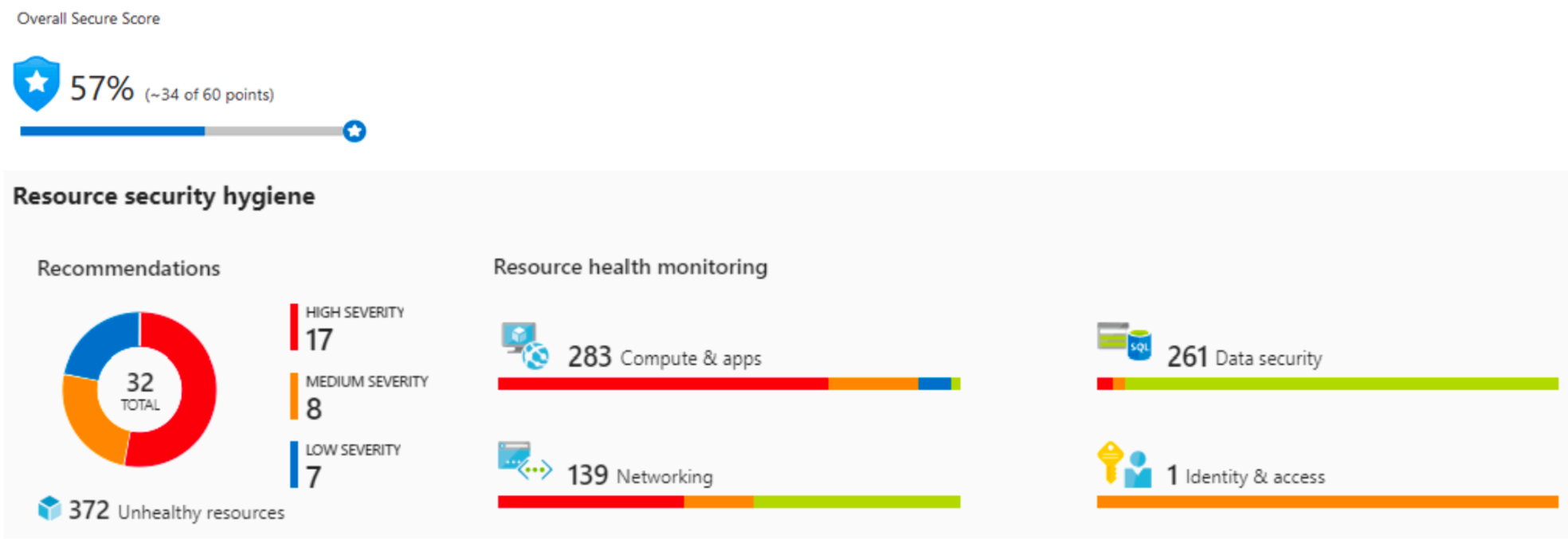
Policy & Compliance

Let's say your company must comply with the Payment Card Industry's Data Security Standard (PCI DSS). This report shows that the company has resources that it needs to remediate.



Resource Security Hygiene

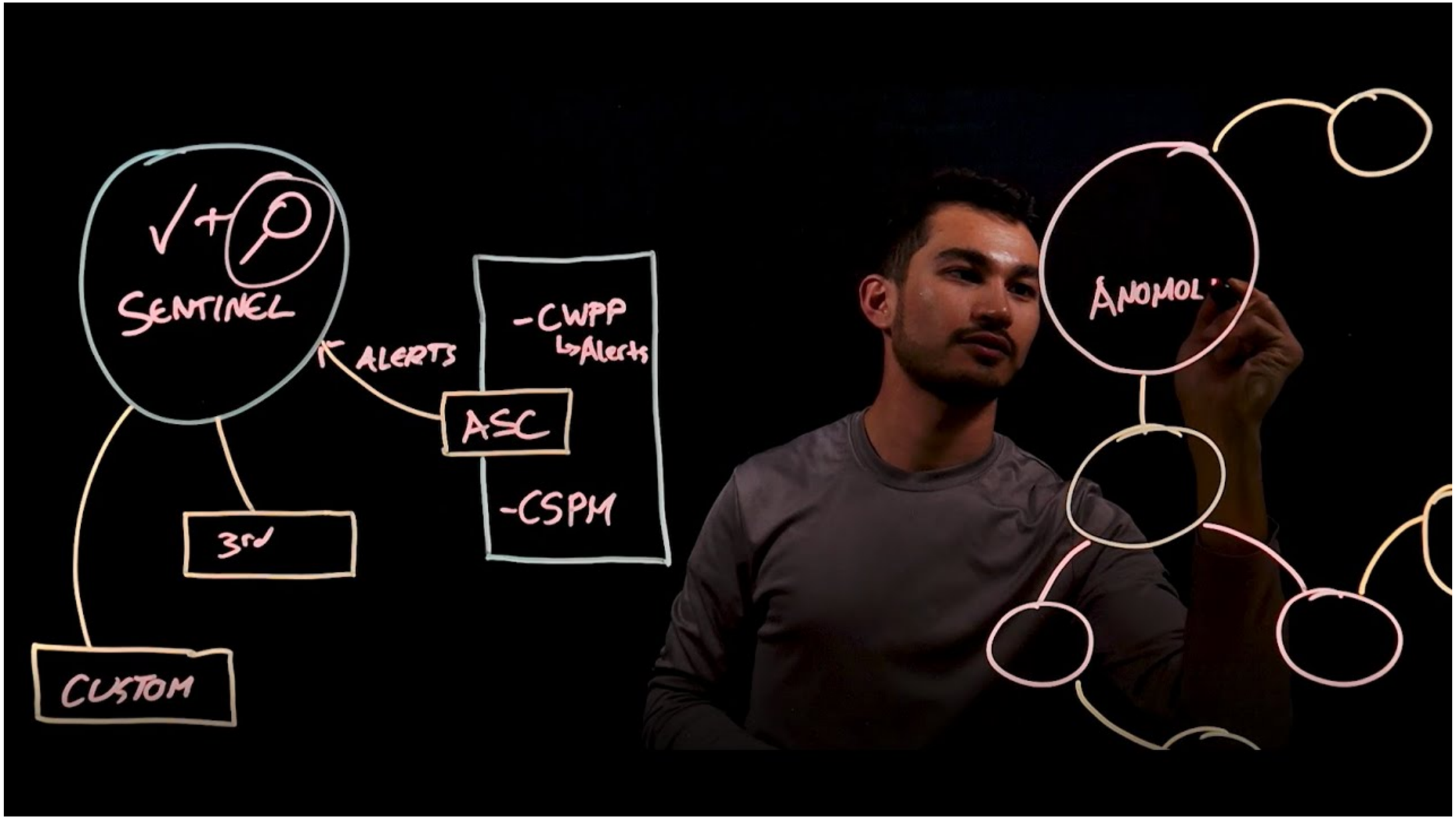
Or your company wants to check the health of its resources from a security perspective.
To help prioritize remediation actions. Your Secure score is based on the percentage of security controls that you satisfy.
The more security controls you satisfy, the higher the score you receive.
Your score improves when you remediate all of the recommendations for a single resource within a control.



Detect and respond to security threats by using Azure Sentinel

Azure Sentinel aggregates security data from many different sources and provides additional capabilities for threat detection and response.

But what's the difference between Sentinel and Security Center?


SENTINEL
ALERTS
-CWPP
Alerts
ASC
-CSPM
3rd
CUSTOM
ANOMOL

Knowledge Check

How can your company enforce having only certain applications run on its VMs?

A. Connect your VMs to Azure Sentinel

B. Create an application control rule in Azure Security Center.

C. Periodically run a script that lists the running processes on each VM. The IT manager can then shut down any applications that shouldn't be running.

Knowledge Check

What's the easiest way for your company to combine security data from all of its monitoring tools into a single report that it can take action on?

A. Collect security data in Azure Sentinel.

B. Build a custom tool that collects security data and displays a report through a web application.

C. Look through each security log daily and email a summary to your team.

Knowledge Check

Which is the best way for a company to safely store its certificates so that they're accessible to cloud VMs?

A. Place the certificates on a network share.

B. Store them on a VM that's protected by a password.

C. Store the certificates in Azure Key Vault.

2.0 Configure security policies.

Classify your data at rest, in process, and in transit

Protect data at rest

Data encryption at rest is a mandatory step toward data privacy, compliance, and data sovereignty.

Best practice:

1. Apply disk encryption to help safeguard your data
2. Use encryption to help mitigate risks related to unauthorized data access.

How to apply:

1. Use Microsoft Azure Disk Encryption. Disk encryption combines the industry-standard BitLocker feature and the Linux DM-Crypt feature to provide volume encryption for the operating system (OS) and the data disks. Azure Storage and Azure SQL Database encrypt data at rest by default, and many services offer encryption as an option.
2. Encrypt your drives before you write sensitive data to them

Classify your data at rest, in process, and in transit

Protect data in transit

Protecting data in transit should be an essential part of your data protection strategy. Because data is moving back and forth from many locations, we generally recommend that you always use SSL/TLS protocols to exchange data across different locations.

Best practice	Solution
Secure access from multiple workstations located on-premises to an Azure virtual network	Use site-to-site VPN.
Secure access from an individual workstation located on-premises to an Azure virtual network	Use point-to-site VPN.
Move large data sets over a dedicated high-speed wide-area network (WAN) link	Use Azure ExpressRoute. If you choose to use ExpressRoute, you can also encrypt the data at the application level by using SSL/TLS or other protocols for added protection.
Interact with Azure Storage through the Azure portal	All transactions occur via HTTPS. You can also use Storage REST API over HTTPS to interact with Azure Storage and Azure SQL Database.

Organizations that fail to protect data in transit are more susceptible to man-in-the-middle attacks, eavesdropping, and session hijacking. These attacks can be the first step in gaining access to confidential data.

Classify an Azure SQL Database

Data discovery and classification (currently in preview) provides advanced capabilities built into Azure SQL Database for discovering, classifying, labeling and protecting sensitive data (such as business, personal data (PII), and financial information) in your databases. Finding and classifying this data can play a pivotal role in your organizational information protection stature.

- **Discovery and recommendations** - The classification engine scans your database and identifies columns containing potentially sensitive data. It then provides you with a more natural way to review and apply the appropriate classification recommendations via the Azure portal.

- **Labeling** - Sensitivity classification labels can be persistently tagged on columns using new classification metadata attributes introduced into the SQL Server Engine. This metadata can then be utilized for advanced sensitivity-based auditing and protection scenarios.

- **Monitor access to sensitive data**

Exercise: ~15 min

Classify an Azure SQL Database

https://docs.microsoft.com/en-us/learn/modules/configure-security-policies-to-manage-data/3-exercise-classify-sql-database

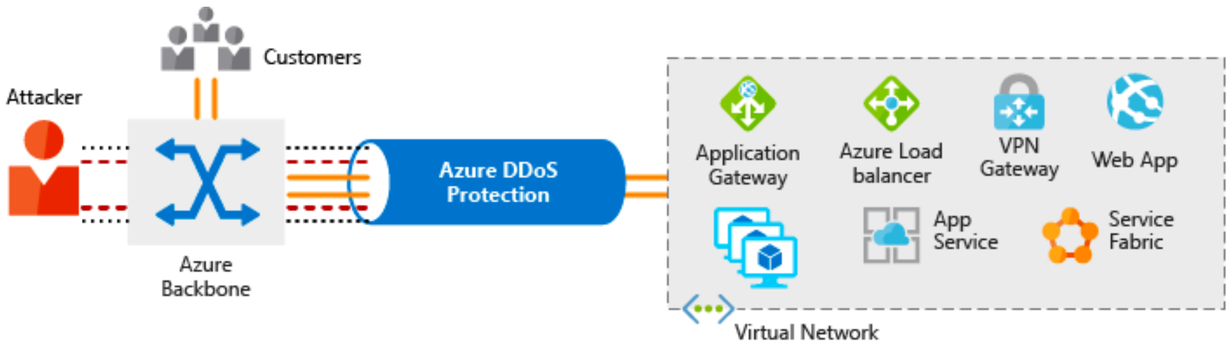
Protect from DDoS attacks by using Azure DDoS Protection

What is a DDoS (Distributed Denial of Service) Attack?

A malicious attempt to disrupt normal traffic by flooding a website with large amounts of fake traffic, making the application slow or unresponsive to legitimate users.

Azure offers **two tiers** of DDoS Protection:

1. DDoS Protection Basic
   - It's Free.
   - Already turned on and protects Azures global network.
2. DDoS Protection Standard
   - Metrics, Alerts, Reporting
   - DDoS Expert Support
   - Starting at $2,994 a month
   - Application and cost protection SLAs

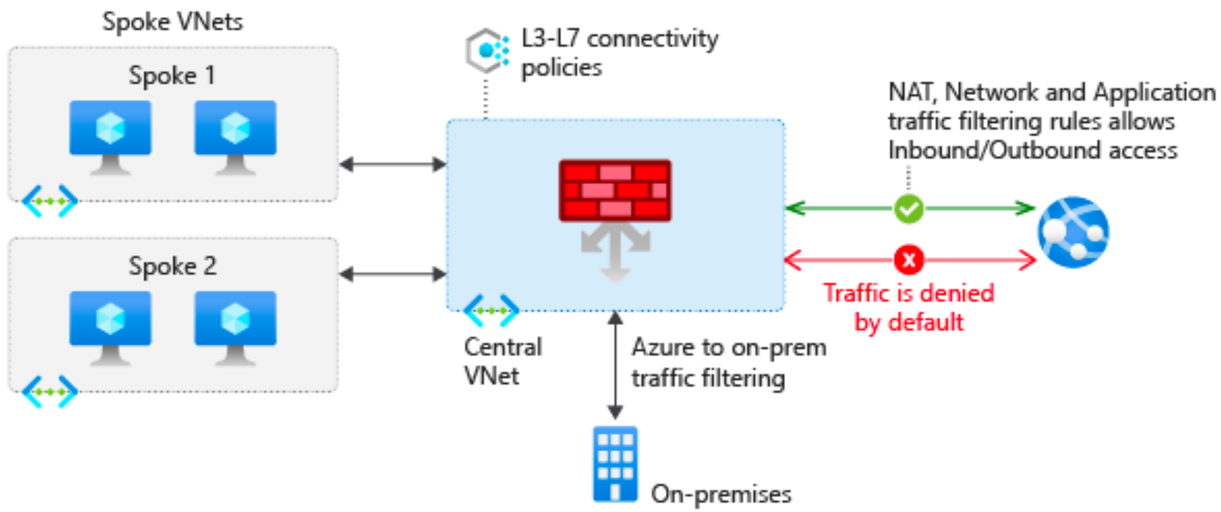


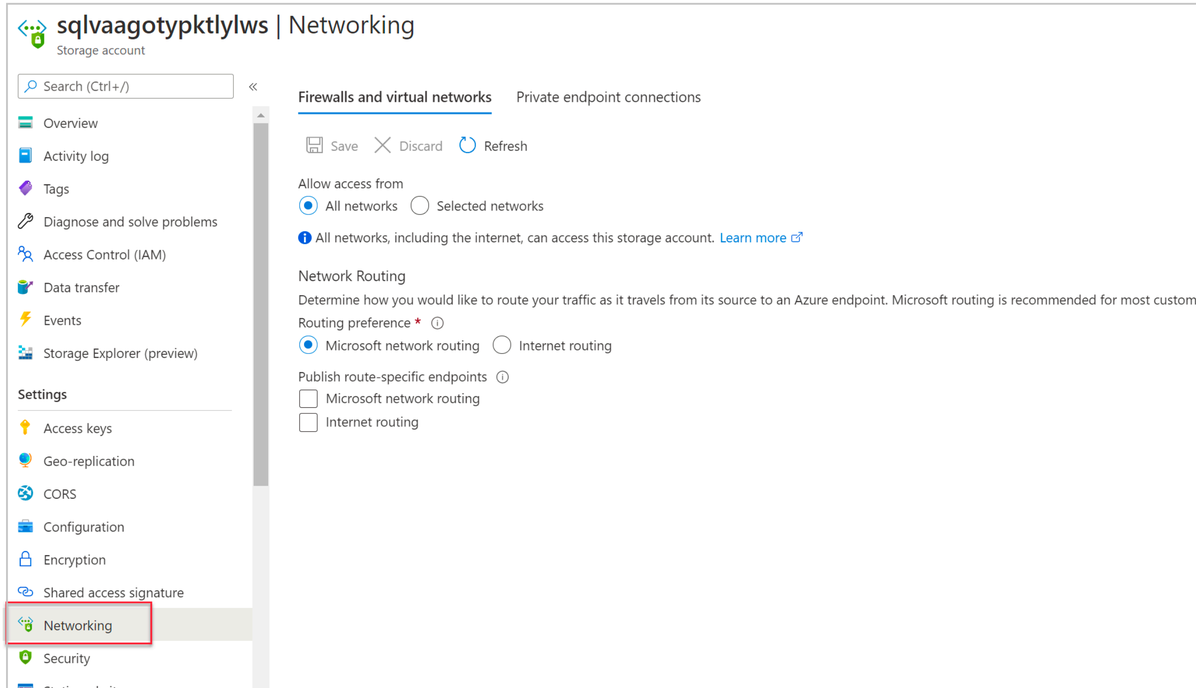
Azure Firewall

Azure Firewall is a managed, cloud-based network security service that protects your Azure Virtual Network resources.

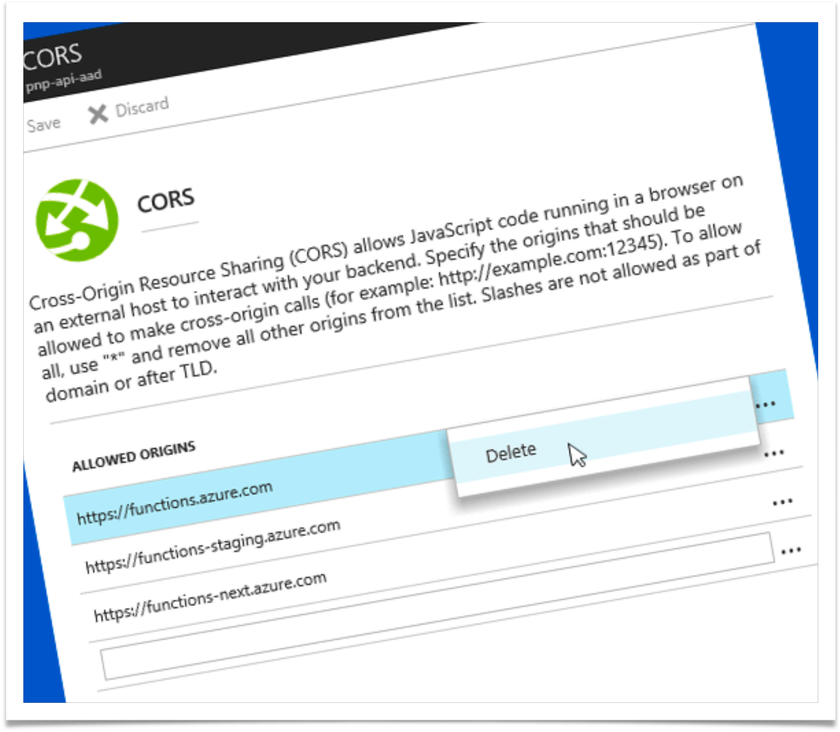
How it works:

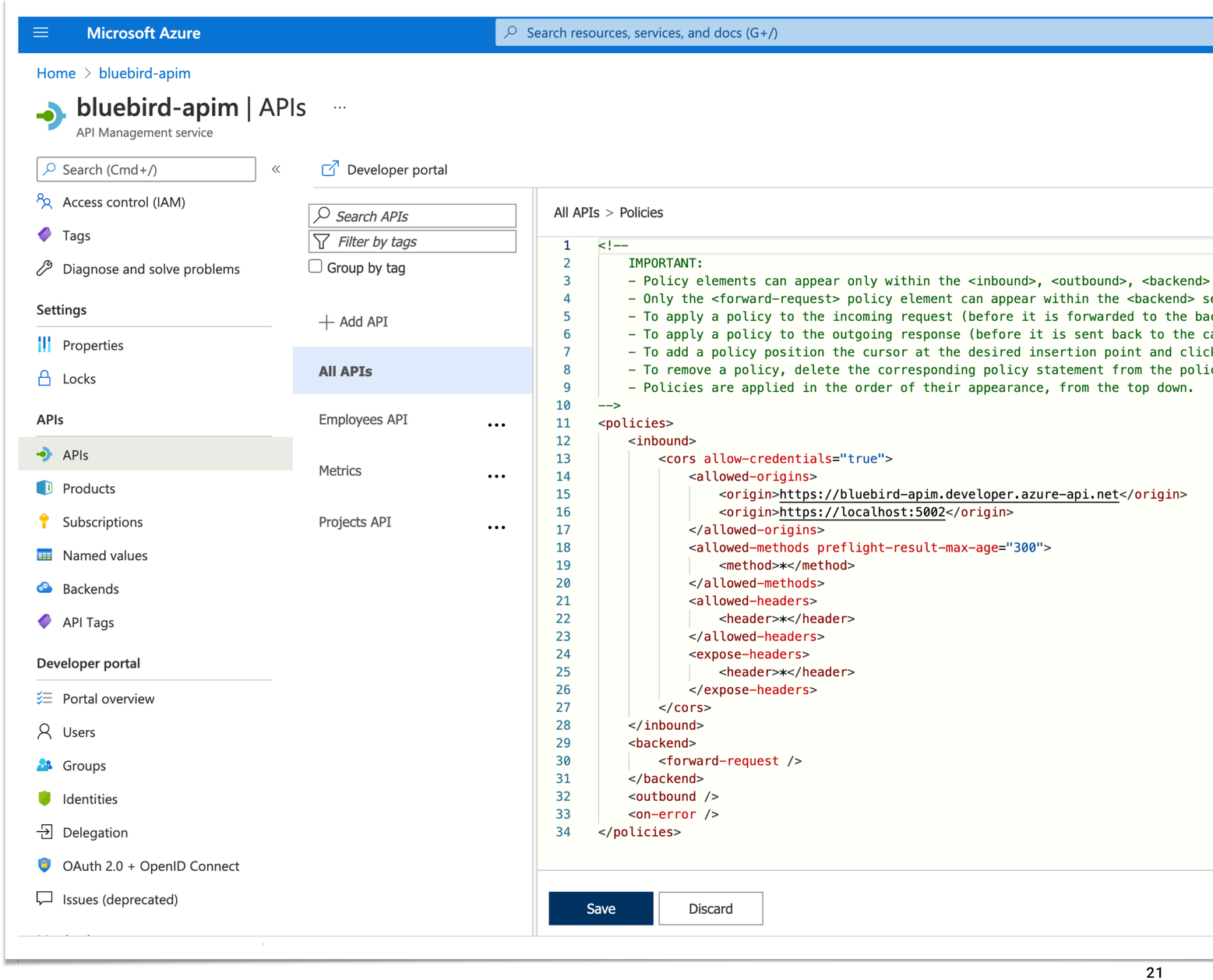
- Centrally create, enforce, and log application and network connectivity policies across subscriptions and virtual networks.
- Uses a static public IP address for your virtual network resources allowing outside firewalls to identify traffic originating from your virtual network.
- High availability is built in, no additional load balancers needed.
- Azure Monitor integration to enable logging and analytics





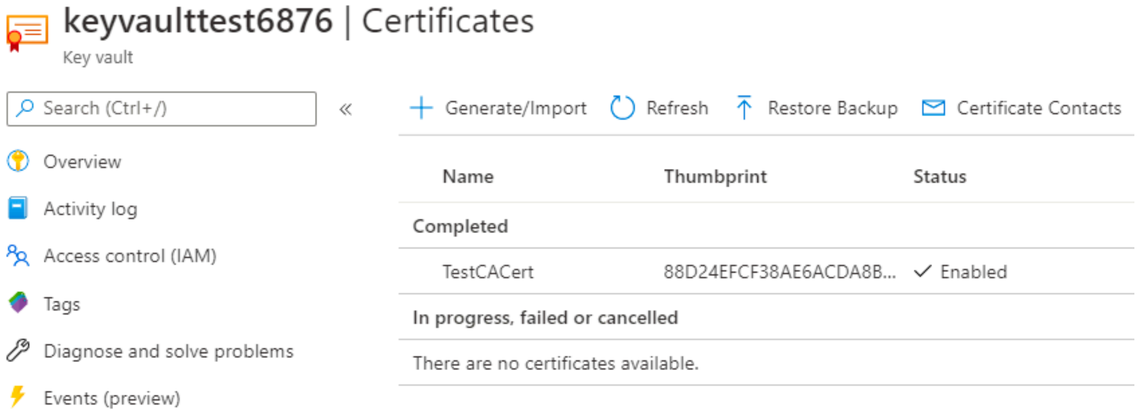
CORS


CORS
pnp-api-aad
Save
Discard
CORS
Cross-Origin Resource Sharing (CORS) allows JavaScript code running in a browser on an external host to interact with your backend. Specify the origins that should be allowed to make cross-origin calls (for example: http://example.com:12345). To allow all, use "*" and remove all other origins from the list. Slashes are not allowed as part of domain or after TLD.
ALLOWED ORIGINS
https://functions.azure.com
Delete
https://functions-staging.azure.com
https://functions-next.azure.com


Microsoft Azure
Search resources, services, and docs (G+/)
Home > bluebird-apim
bluebird-apim | APIs
API Management service
Search (Cmd+/)
Access control (IAM)
Tags
Diagnose and solve problems
Settings
Properties
Locks
APIs
APIs
Products
Subscriptions
Named values
Backends
API Tags
Developer portal
Portal overview
Users
Groups
Identities
Delegation
OAuth 2.0 + OpenID Connect
Issues (deprecated)
Developer portal
Search APIs
Filter by tags
Group by tag
Add API
All APIs
Employees API
Metrics
Projects API
All APIs > Policies
<!--
IMPORTANT:
- Policy elements can appear only within the <inbound>, <outbound>, <backend>
- Only the <forward-request> policy element can appear within the <backend> se
- To apply a policy to the incoming request (before it is forwarded to the bac
- To apply a policy to the outgoing response (before it is sent back to the ca
- To add a policy position the cursor at the desired insertion point and click
- To remove a policy, delete the corresponding policy statement from the polic
- Policies are applied in the order of their appearance, from the top down.
-->
<policies>
<inbound>
<cors allow-credentials="true">
<allowed-origins>
<origin>https://bluebird-apim.developer.azure-api.net</origin>
<origin>https://localhost:5002</origin>
</allowed-origins>
<allowed-methods preflight-result-max-age="300">
<method>*</method>
</allowed-methods>
<allowed-headers>
<header>*</header>
</allowed-headers>
<expose-headers>
<header>*</header>
</expose-headers>
</cors>
</inbound>
<backend>
<forward-request />
</backend>
<outbound />
<on-error />
</policies>
Save
Discard

3.0 Azure Key Vault.

Azure Key Vault



Helps you safeguard cryptographic keys and other secrets used by cloud apps and services.

Secrets Management
Store and tightly control access to tokens, passwords, certificates, API keys, and other secrets.

Key Management
Create and control the encryption keys used to encrypt your data

Certificate Management
Easily provision, manage, and deploy public and private SSL Certificates for use with Azure and internal connected resources.

Hardware Security Module
Secrets and keys can be protected either by software or FIPS 140-2 Level 2 validated HSMs. HSM is a piece of hardware designed to store encryption keys. Keys are stored in-Memory not on disk.

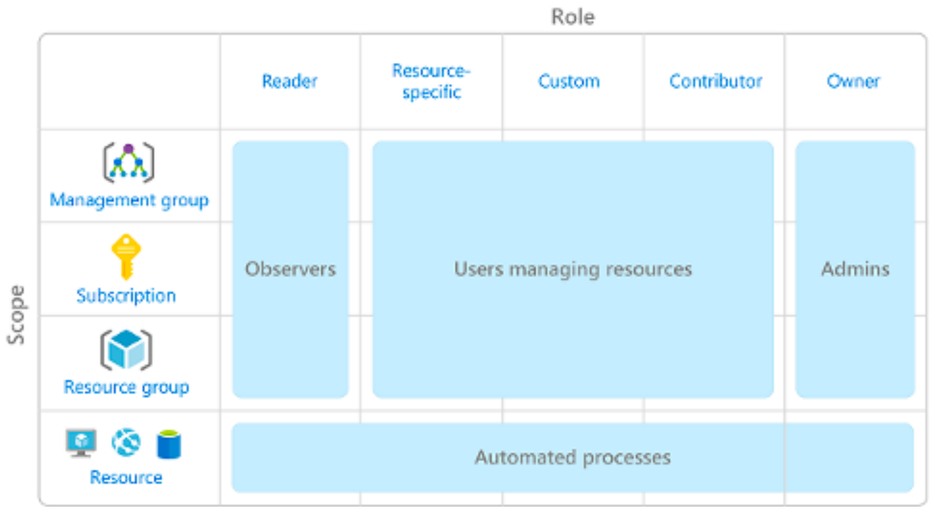
4.0
Azure Role-based Access control (Azure RBAC).

Control access to cloud resources by using Azure role-based access control

When you have multiple IT and engineering teams, how can you control what access they have to the resources in your cloud environment? It's a good security practice to grant users only the rights they need, known as **Least privilege,** to perform their job, and only to the relevant resources.

Azure provides built-in roles that describe common access rules for cloud resources. You can also define your own roles. Each role has an associated set of access permissions that relate to that role. When you assign individuals or groups to one or more roles, they receive all of the associated access permissions.

You can apply Azure RBAC to an individual person or to a group.



When should you use Azure RBAC?

Examples for when you should use Azure RBAC:

- Allow one user to manage VMs in a subscription and another user to manage virtual networks.
- Allow a database administrator group to manage SQL databases in a subscription.
- Allow a user to manage all resources in a resource group, such as virtual machines, websites, and subnets.
- Allow an application to access all resources in a resource group.

5.0
Securing Azure SQL Databases.

Exercise: ~60 min

Secure your Azure SQL Database.
We've will create an Azure SQL Database logical server,
and a virtual machine called *appServer* that we'll use to simulate network connectivity from an application server.

1. Restrict network access - Firewall setup
2. Restrict Database Access - Azure AD permission setup
3. Secure your Data - Add masking rules for sensitive data

https://docs.microsoft.com/en-us/learn/modules/secure-your-azure-sql-database/1-create-database

5.0
Self Study

Microsoft Learn - Secure your cloud data
https://docs.microsoft.com/en-us/learn/paths/secure-your-cloud-data/

Thank you.