

Becoming an Azure SQL DBA



Learning pathway session

② Security, Compliance, Threats, Connectivity

November 6

2:00 PM-3:00 PM

345-346

Learning Pathway: Becoming an Azure SQL DBA

Advancing the Role of the On-Premises SQL Server DBA

Wednesday Nov 6th

- ① High Availability
and BCDR

11:15am – 12:15pm

Room 345-346

Thursday Nov. 7th

- ③ Performance Monitoring, Tuning
and Alerting

11:30am – 12:30pm

Room 345-346

- ② Security, Compliance, Threats,
Connectivity

2:00pm – 3:00pm

Room 345-346

- ④ New Opportunities from Basics to
Microsoft Copilot

2:00pm – 3:00pm

Room 345-346



Niko Neugebauer

Product Manager
Microsoft

Niko is a Senior Product Manager at Microsoft working on building Azure SQL platform features.

In his previous roles for over 20 years he helped customers successfully build, migrate and optimize Microsoft Data solutions in OLTP & OLAP markets.

 @nikoneugebauer

 aka.ms/sqlmi-videos

 www.linkedin.com/in/nikoneugebauer/



Pam Lahoud

Principal PM Manager
Microsoft

Pam Lahoud is a Principal PM Manager in Azure Data, based in Redmond, WA, USA. She has been with Microsoft since 2006 and currently leads the Databases in Fabric CAT team. She is passionate about SQL Server performance and has focused on performance tuning and optimization, particularly from the developer perspective, throughout her career. She is a SQL 2008 MCM with over 25 years of experience working with SQL Server, and co-author of the book “Learn T-SQL Querying”.

 @SQLGoddess

 <https://aka.ms/LearnTSQLQuerying>

 <https://www.linkedin.com/in/pam-lahoud>



Dr. Dani Ljepava

Product Manager
Microsoft

Dani is a Senior Product Manager at Microsoft working on building Azure SQL platform features.

Experience in SQL team includes hybrid environments, data mobility, high availability, backup and restore, monitoring, intelligent performance features, and development of data mobility features for SQL Server 2016-2022. Involved with building Azure SQL Managed Instance since the service launch in 2018.

 @danimir

 aka.ms/sqlmi-videos

 <https://www.linkedin.com/in/danimir>



Erin Stellato

Principal Product Manager
Microsoft

Erin Stellato is a Principal Program Manager on the SQL Experiences team, helping advance tools that customers use daily with Azure SQL. She is passionate about data and chocolate, but not always in that order. She previously worked as a consultant and was a Data Platform MVP and has been an active member of the SQL Server community as both a volunteer and speaker.

 @erinstellato

 <https://www.sqlskills.com/about/erin-stellato/>

 www.linkedin.com/in/erinstellato

Azure SQL

The family of SQL cloud databases



SQL Server on Azure Virtual Machines



Azure SQL Managed Instance



Azure SQL Database

Migration

Best for: Migrating (“lift and shift”) 3rd party apps to customer-managed Azure virtual machines.

Best for: Migrating custom apps at-scale to a Microsoft-managed, SQL Server-compatible instance.

Innovation

Best for: Developing highly-scalable, AI-ready applications with SQL’s reliability and security at commercial open-source database costs.



Azure SQL enabled by Azure Arc

Run Azure SQL on premises and in multicloud environments

Your first step on the journey to Azure.

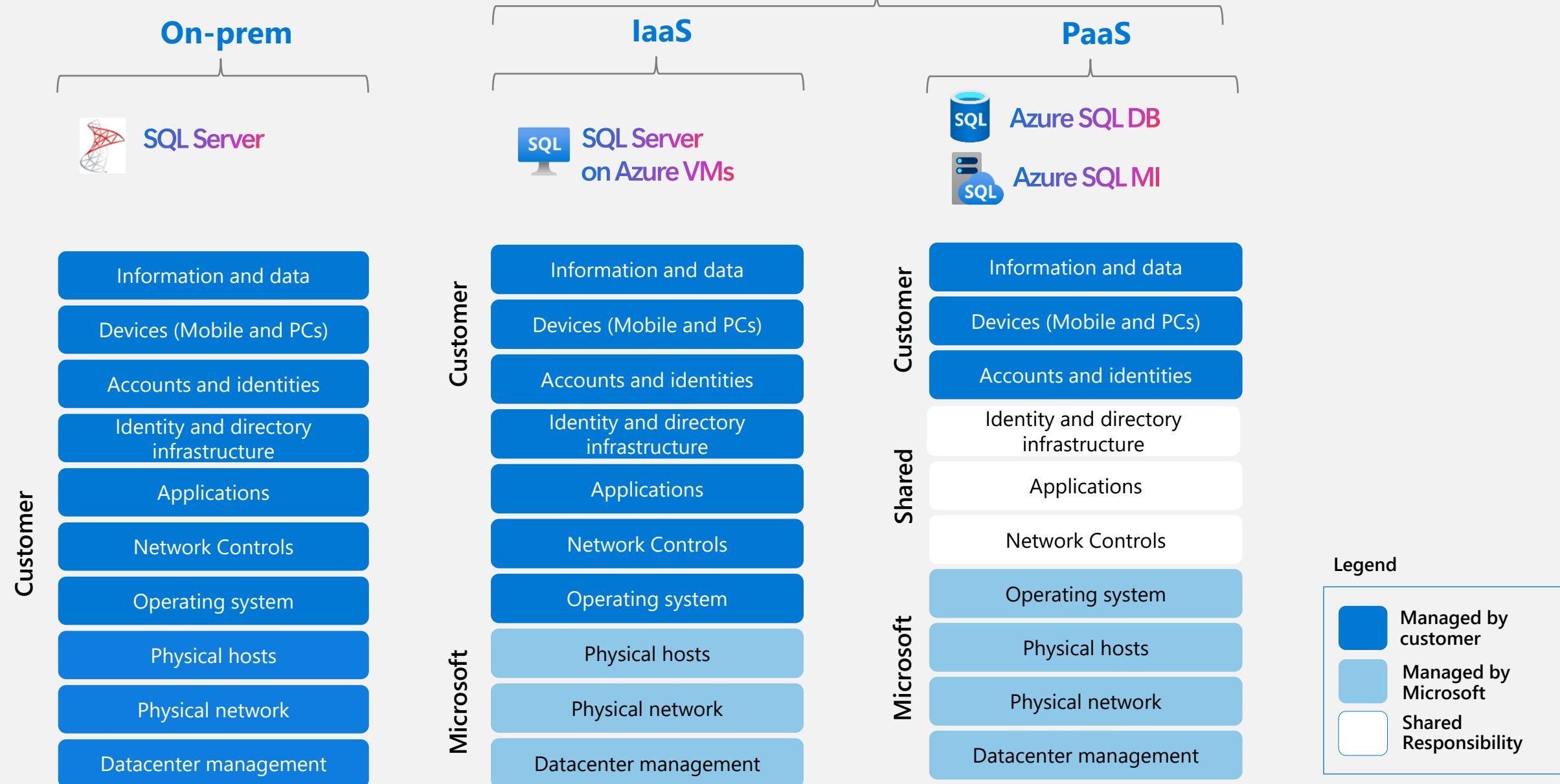
Azure is the cloud that knows SQL Server best

In Azure SQL we have a shared responsibility model

Azure SQL DBA working together with Microsoft



Shared responsibility on Azure SQL



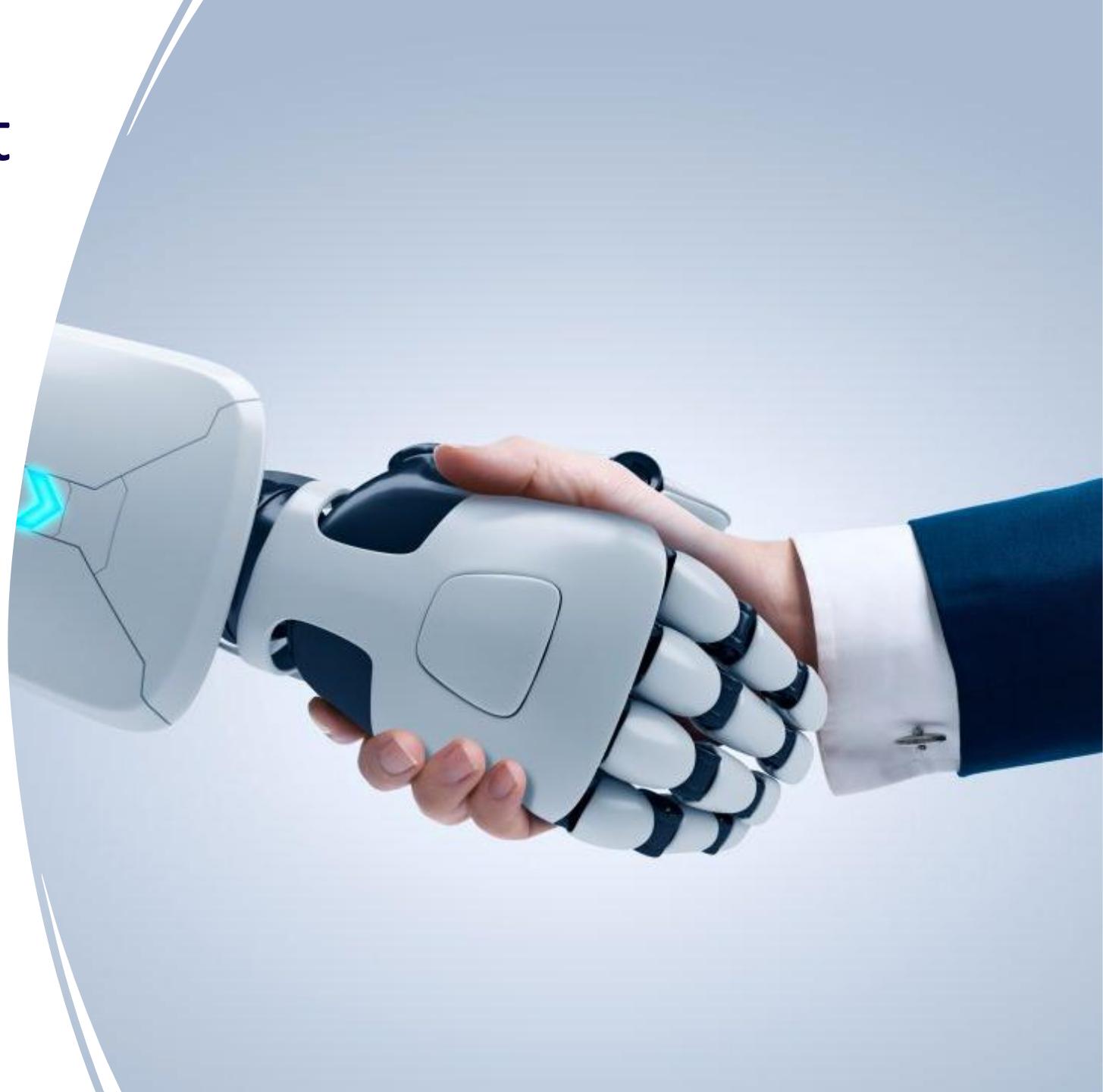
The checklists are still relevant as ever!

- Trip Planning
- Exterior Inspection
- Cockpit Preparation
- Engine Start-up
- System Checks
- Disaster Recovery Planning
- Final Checks



Some of the tasks that
DBA and the Platform
need to do together

- Networking
- Security and
Compliance



Azure SQL DBAs responsibilities



Security

- Managing Access (Identity, Login, Roles, Permissions)
- Client and server-side security
- Network traffic protection
- Monitoring the access (choose and configure monitoring software, configure alerts)



Compliance

- Ensuring database and apps are compliant
- Selecting the right technology
- Setting up & Running the Audit
- SMK or CMK
- Implementing company-specific protocols

Shared Responsibility: Networking



DBA responsibility

- Implementing security best practices and company policies regarding networking, firewall rules, encryption, access control
- Using Network Security Groups, Azure Firewalls



Azure responsibility

- Ensuring platform security and compliance certifications
- Adding new security protocols, solutions & services

Shared Responsibility: Security & Compliance



DBA responsibility

- Implementing security best practices and company policies regarding networking, encryption, access control
- Making choices for TDE (SMK vs CMK)
- Creating and updating Logins, Users
- Managing Groups & permissions
- Configuring & running Audit
- Reporting on SLA



Azure responsibility

- Ensuring platform security and compliance certifications
- Innovating with new security options and services

Reminder: Authorization is not a shared responsibility

Direction

- Scenario-oriented roles
 - Performance Monitoring
 - Security Auditing
 - Database documentation
 - Server configuration
- Granular permissions
 - DMVs, CVs, DMFs
 - Aligned with policies and RBAC

User accounts

- Created in SQL metadata
- Logins
 - Server-level principal
 - Local or external (i.e., Azure AD mapped)
- Users
 - Database-level principal
 - Linked to logins or contained

Roles

- Server or database level

Permissions

- Assigned directly
- Assigned with roles (Preferable)

Essential Azure Services

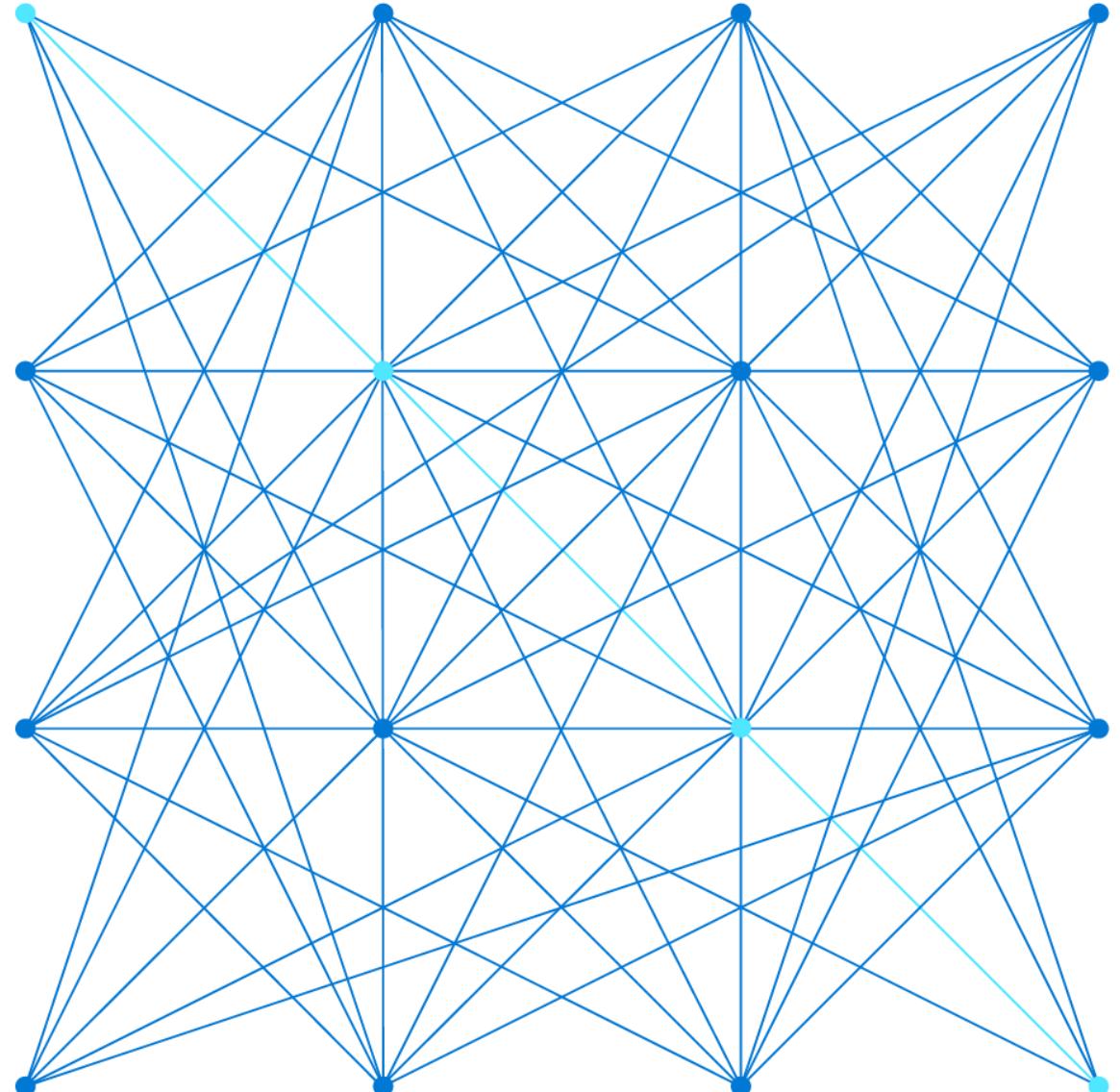
Azure Virtual Network (vNet)

Azure Subnet

Azure Blob Storage

Azure Key Vault

Azure Entra



Virtual network (VNets)

Applies to Azure SQL VM & Azure SQL MI only

Basic building block of Azure networking

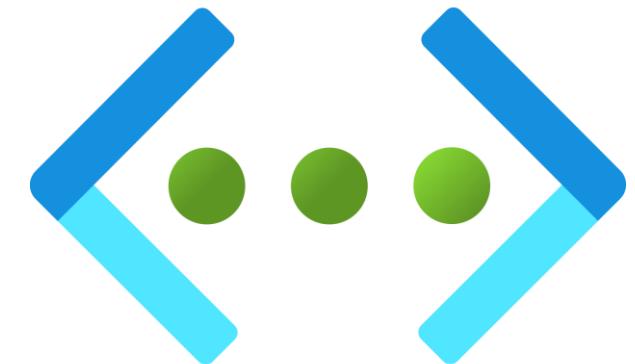
Has an assigned IP address space; can be partitioned into subnets

Connectivity

Devices in a VNet can communicate with each other by default

Inbound connectivity via public IP address, public load balancer

Outbound connectivity open by default



Domain Name resolution

Azure-provided domain name resolution

Can also use custom domain name servers

Virtual networks: Subnets

Applies to Azure SQL VM & Azure SQL MI only

Subnets are subsets of virtual network's address space, with configurable traffic routing and security rules

Traffic routing

Routing table

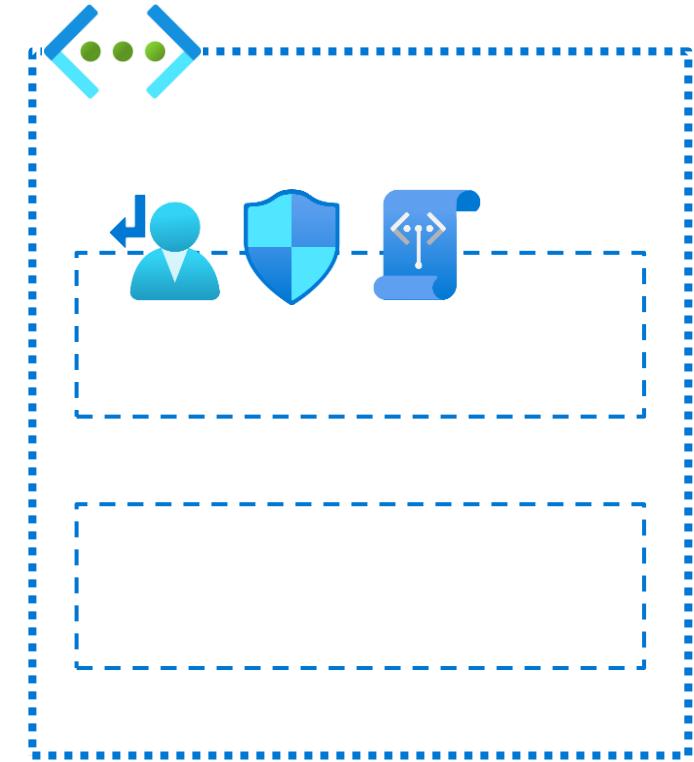
Service endpoints

Traffic filtering

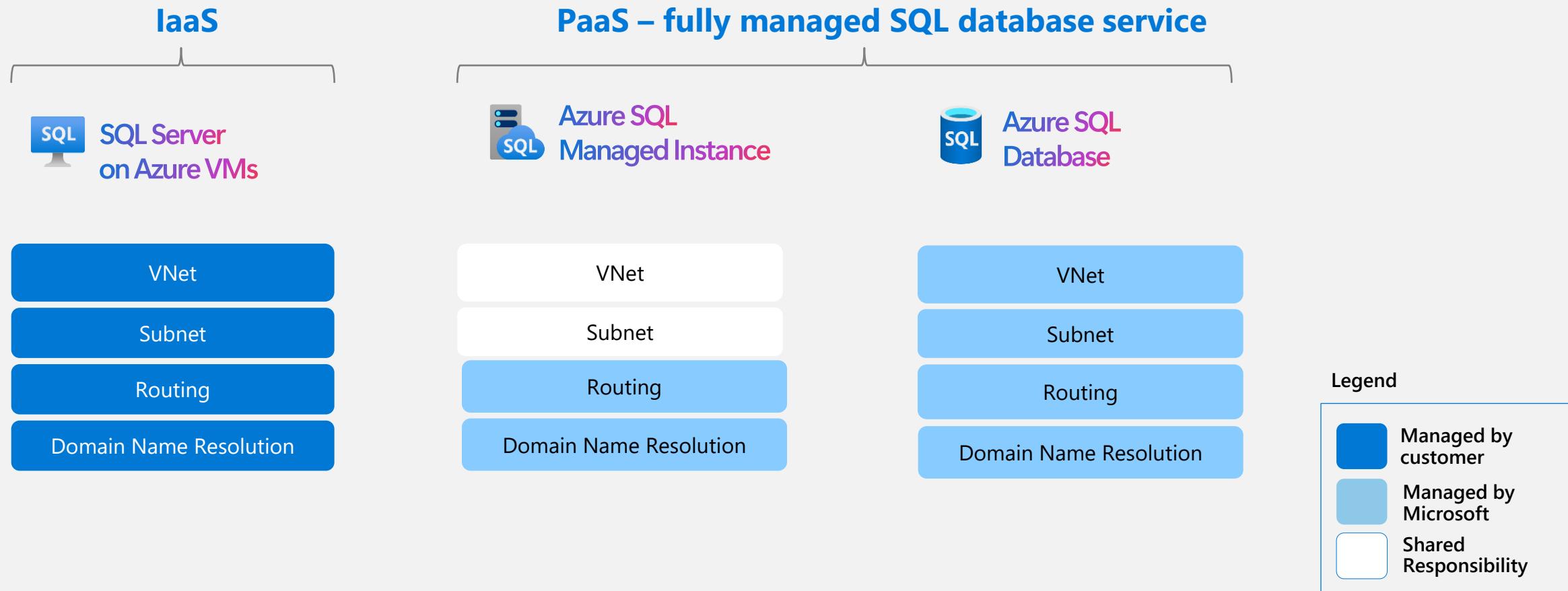
Network security groups (NSGs), allow/deny rules

Network virtual appliances

Service endpoint policies



Shared responsibility for Network Management



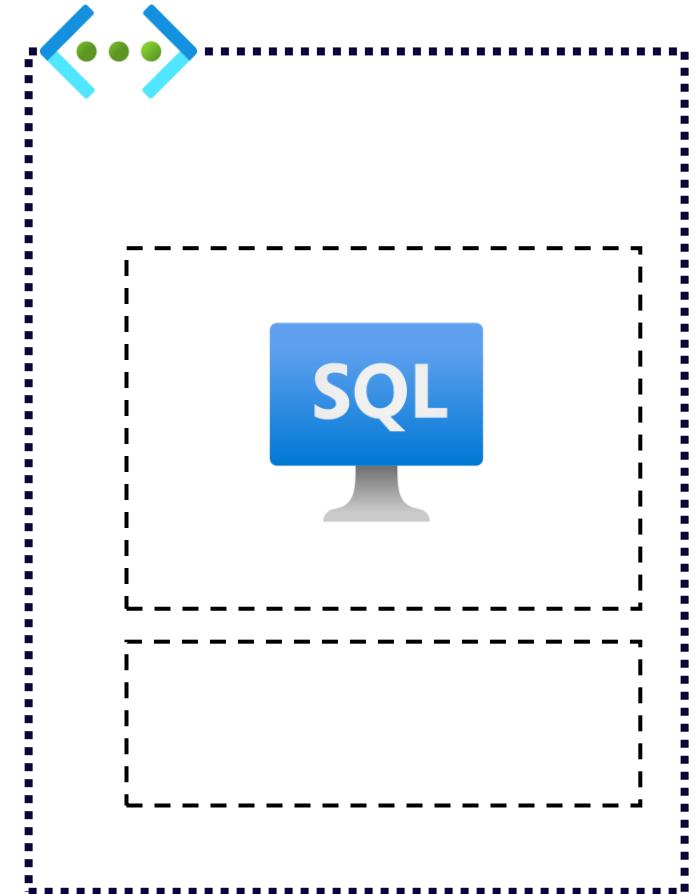
How SQL Server on Azure VM integrates into your virtual network

SQL Server on Azure VM is placed in the subnet of your choice under your specific needs and definitions, just like you would do that on-premises.

Similar deployment process as when doing that on-premises, customer can place as many different Azure SQL VMs in the same subnet as they desire and as subnetwork can place with the given networking ip configuration.

You can move your VM where you need to.

Consider it to be a **basic building block of your solution.**



How Azure SQL Managed Instance integrates into your virtual network

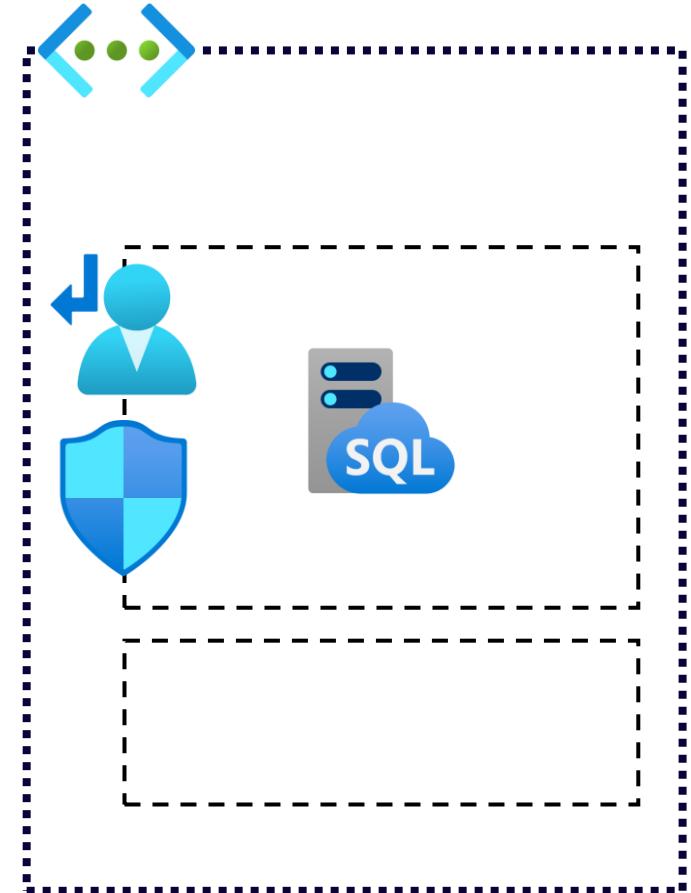


SQL Managed Instance deploys in a dedicated subnet

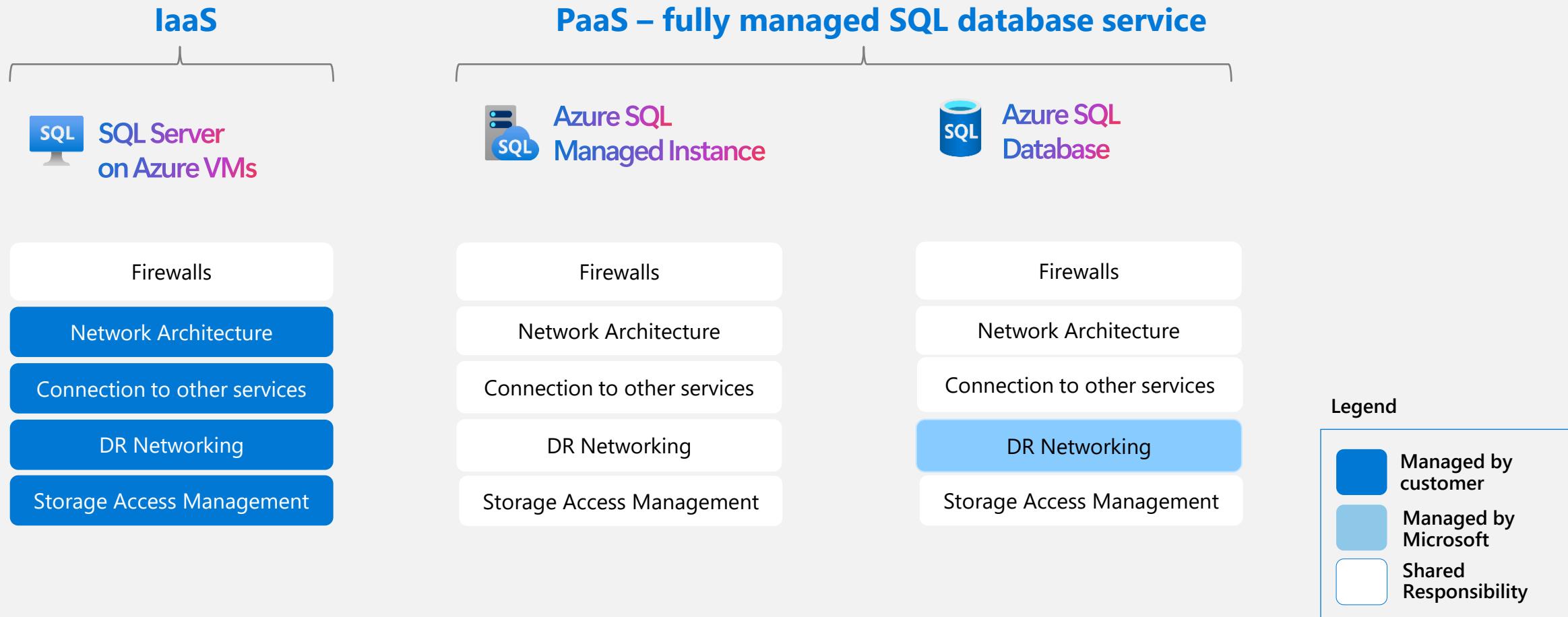
- **Filtering rules** installed on the subnet's NSG.
Some are configured by default; customer can add additional ones later.
- **Routes** configured on the subnet's route table
- NSG and route table **protected** against disruption of service
- **IP addresses** consumed from the subnet's range

When deployed:

- This subnet is **reserved** for SQL MI only (one or more instances)
- Customer can still deploy resources in other subnets
- Azure SQL Managed Instance's subnet range cannot be changed.
- Instance can still be moved from one subnet to another.



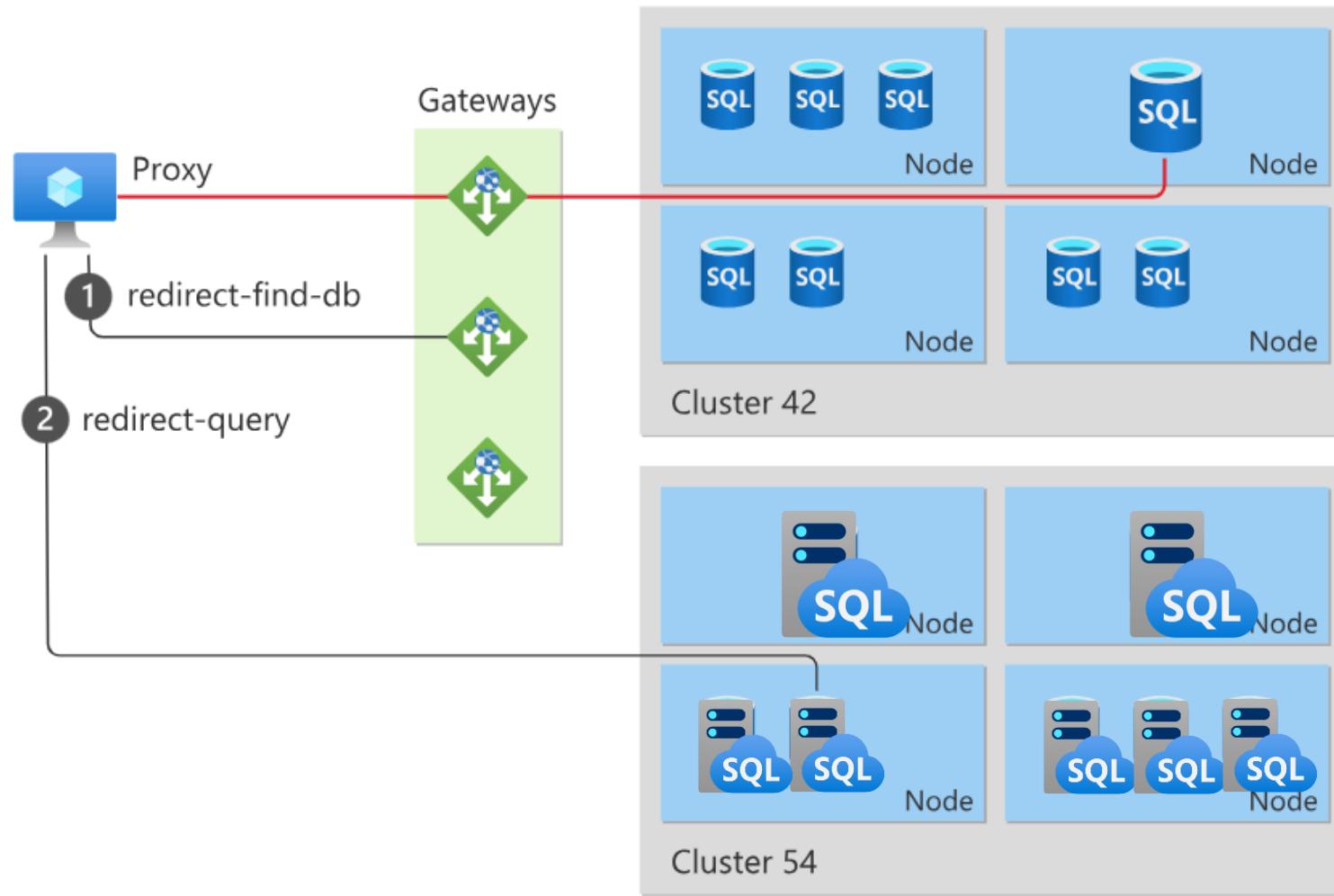
Shared responsibility for Networking & Security



Architecture of Connectivity: Inbound & Outbound

for Azure SQL DBA

Redirect & Proxy connection types/policies explained:



Architecture of Connectivity: Inbound and Outbound

For **SQL Server on Azure VMs**, the connection policies possibilities are endless – you just need to build and maintain them.



**SQL Server on Azure
Virtual Machines**

For **Azure SQL Database** the possible connection types(aka policies) are:

- Default (uses Proxy or Redirect, depending on location)
- Proxy
- Redirect



Azure SQL Database

On **Azure SQL Managed Instance** you have the following connection types:

- Proxy (default)
- Redirect



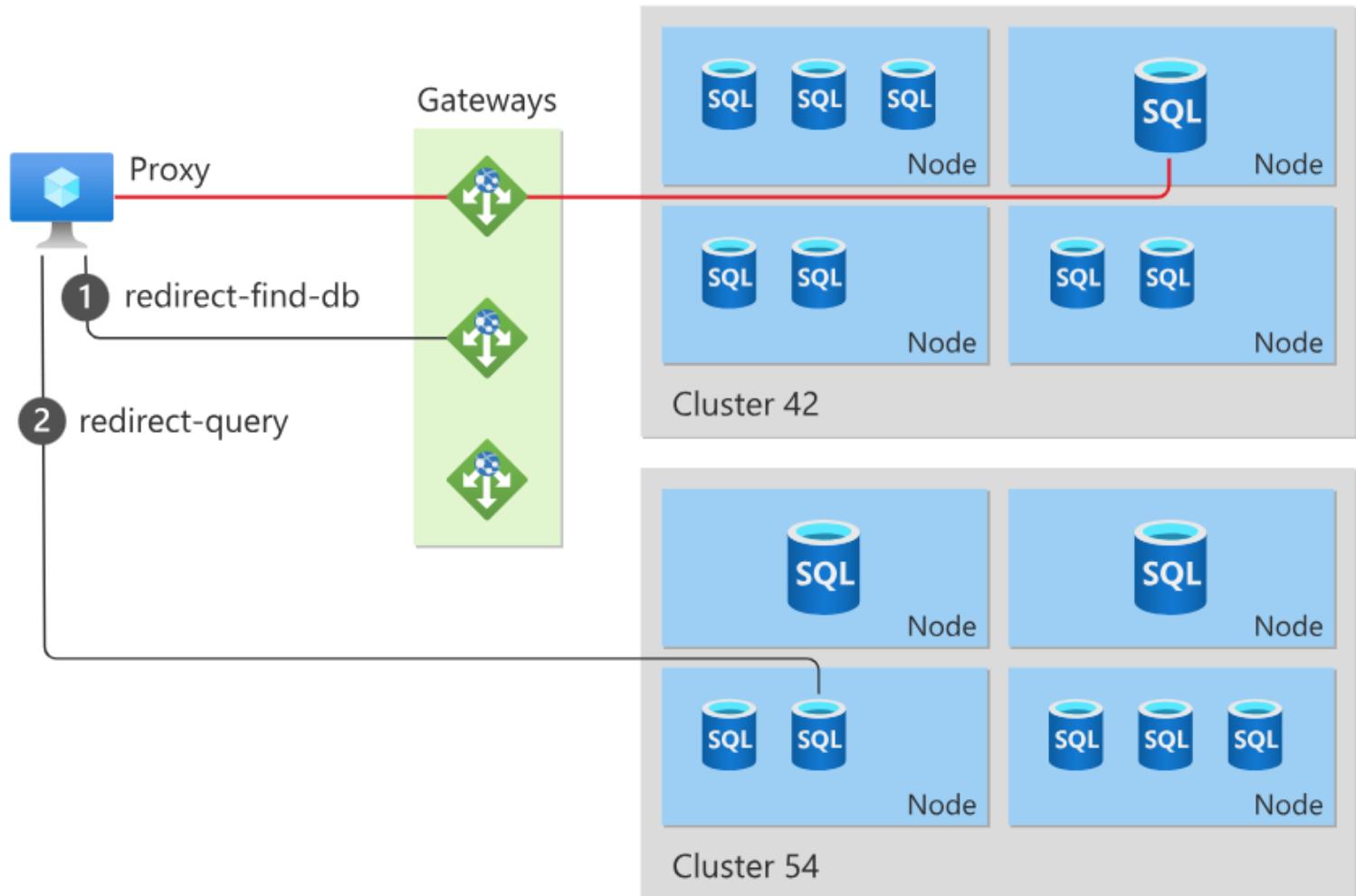
**Azure SQL
Managed Instance**

Connecting to Azure SQL DB:

Connecting **within Azure**, use **Redirect** policy by default.

Connecting **outside of Azure**, Your connection will have policy of **Proxy** be default.

Connection types available:
Public endpoint
Private endpoints



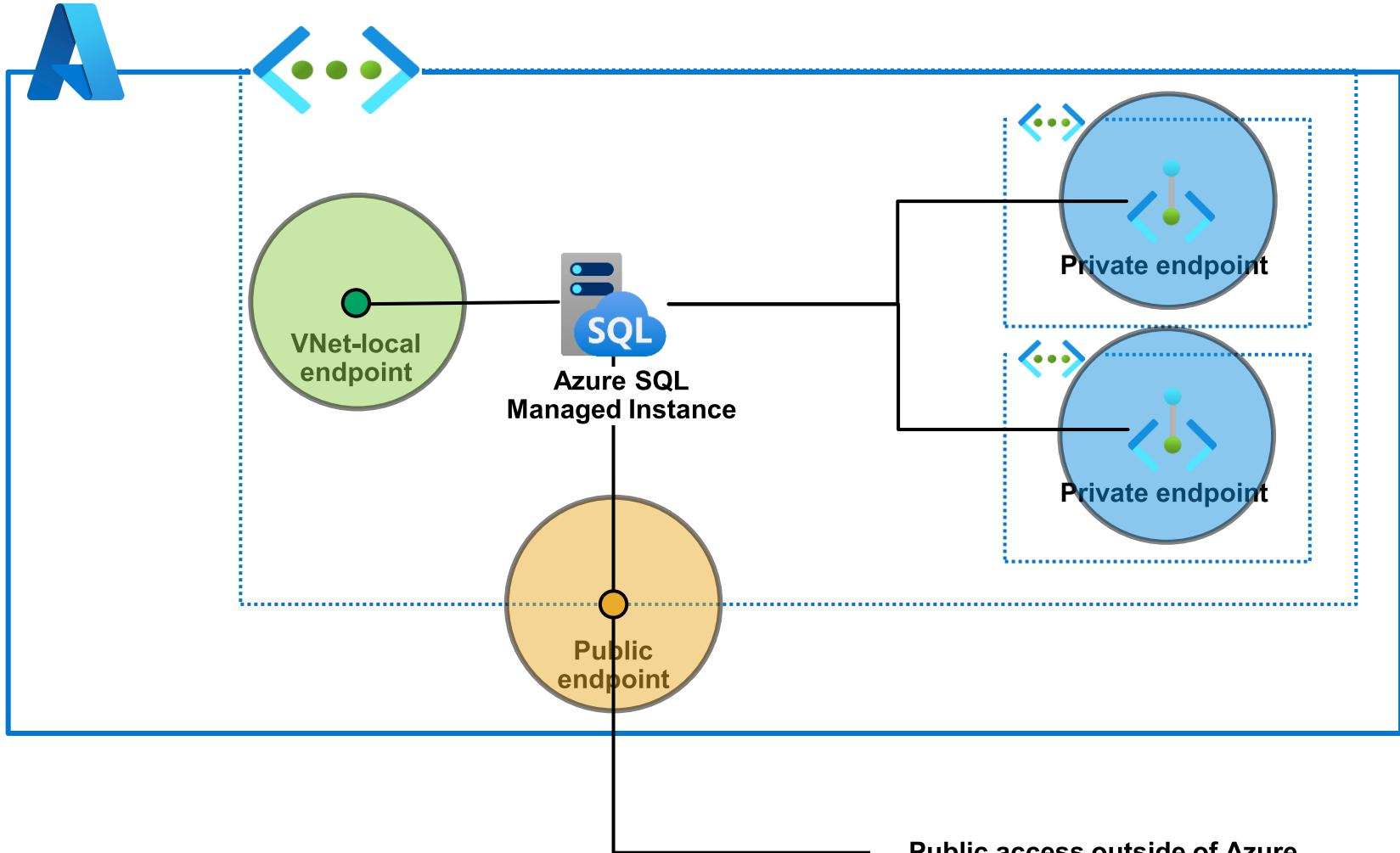
Connecting to Azure SQL Managed Instance

There are 3 connection endpoints configurable:

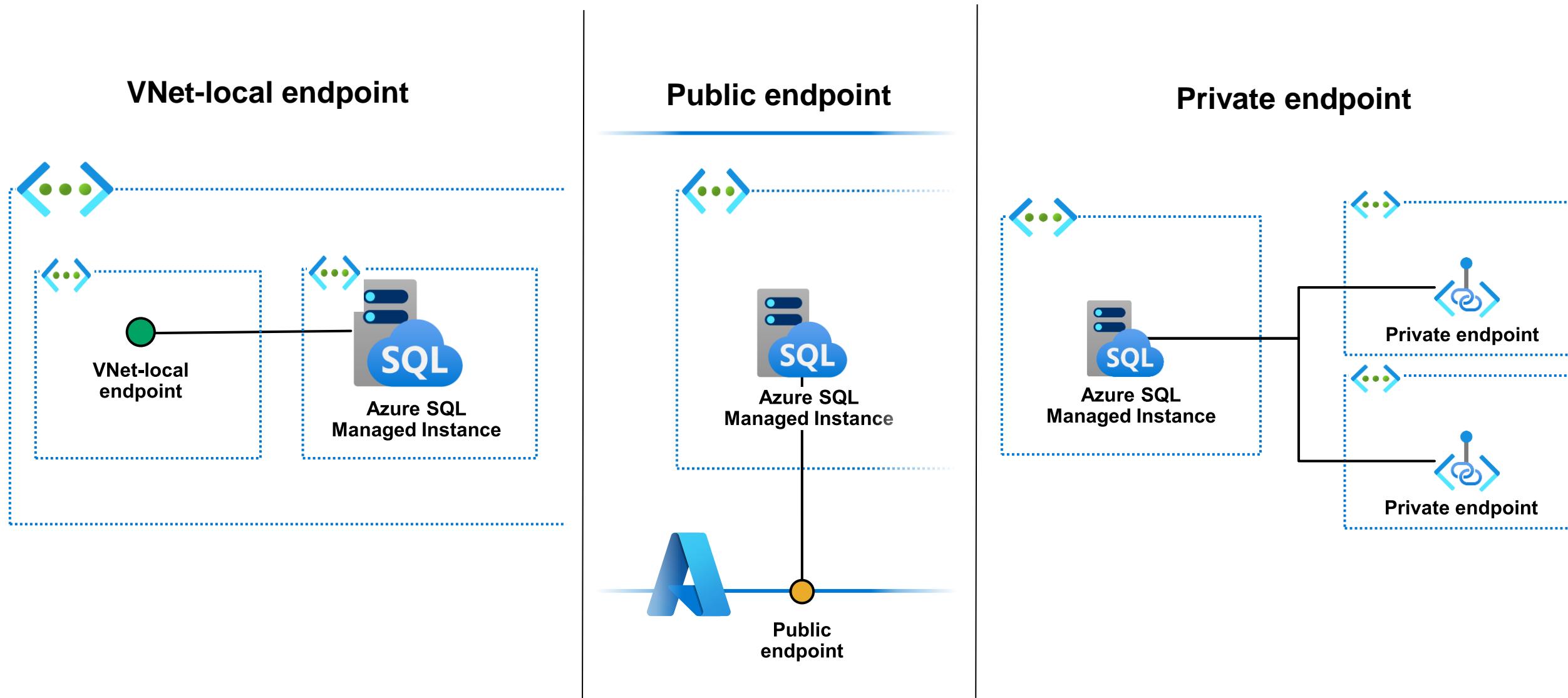
- VNet-local endpoint
- Public endpoint
- Private endpoints

Connection types supported:

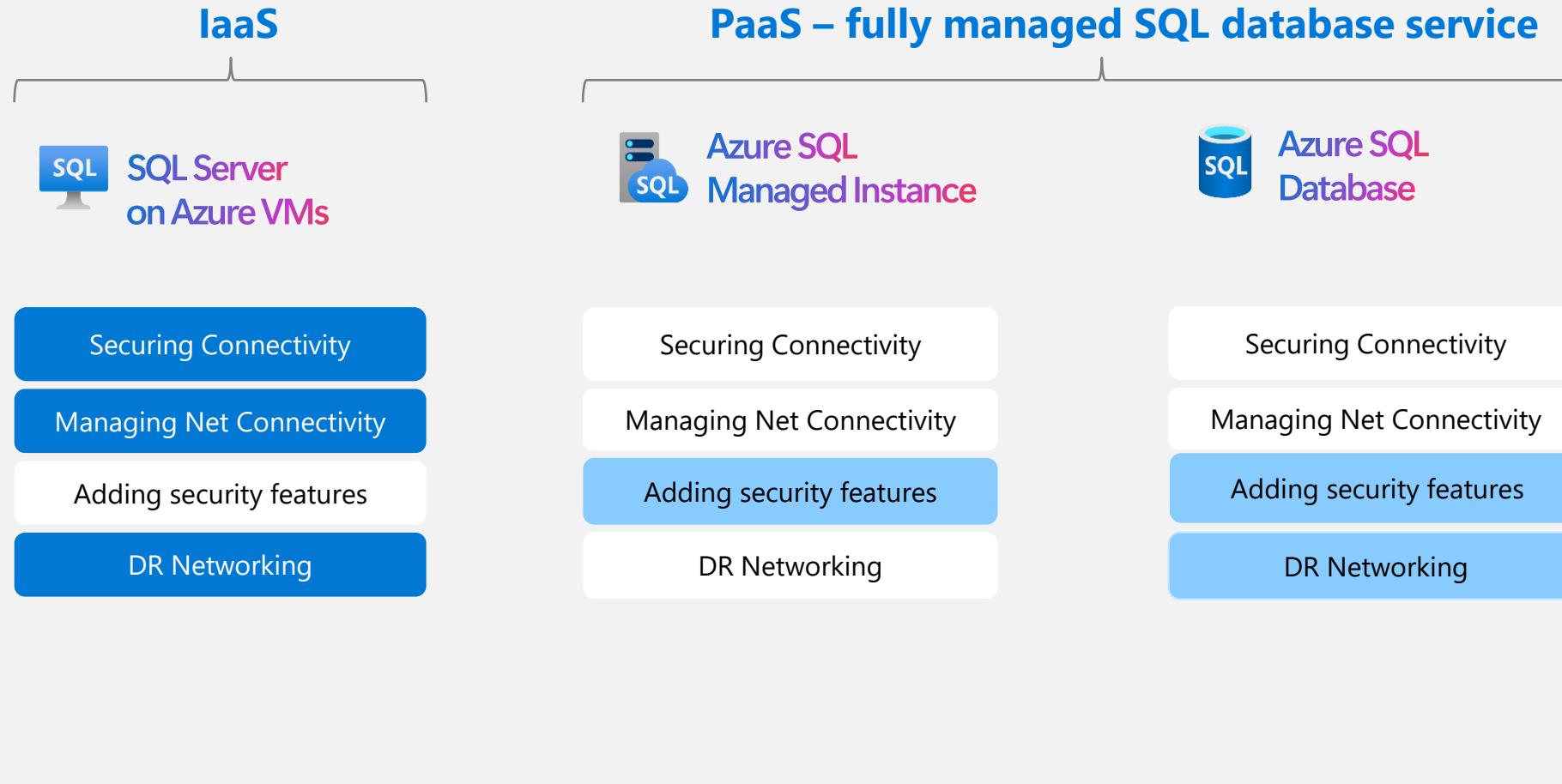
- Proxy: all
- Redirect: only **vNet local endpoint**



Connecting to Azure SQL Managed Instance



Shared responsibility for Networking & Security



Outbound Connectivity

for Azure SQL DBA

Outbound connectivity tools for Azure SQL Database



The connectivity for Azure SQL DB has several opportunities to achieve the needed goal

By using a combination of

- **Restrict outbound networking**
- **Managed Identities (System-managed or User-managed)**
- **Federated Identity**
- **Azure Firewall**
- **Private Link (Private Endpoints)**

Customer can configure secure outbound connections to the desired destination.

Outbound connectivity tools for Azure SQL Managed Instance



The connectivity for Azure SQL MI has several opportunities.

By using a combination of

- **Managed Identities (System-managed or User-managed)**
- **SQL Trust Groups**
- **Firewalls**
- **Private Endpoints**
- **Network Peering**

Customer can configure secure outbound connections to the desired destination.

▼ Security

- Networking
- Microsoft Defender for Cloud
- Transparent data encryption
- Private endpoint connections
- SQL trust groups
- Identity

Managed Identity for Azure SQL PaaS

Used for authenticating Azure SQL to other resources

Common scenarios

- [AKV | Managed HSM] TDE with Customer-Managed Key (CMK)
- [Storage] Auditing, BULK INSERT / OPENROWSET
- [Azure AD] Authentication – Retrieving user and group information

SQL MI specific scenarios

- [Storage] BACKUP / RESTORE
- [SQL] Linked server

The screenshot shows the Azure portal interface for managing identities. At the top, there are 'Save' and 'Feedback' buttons. Below that, the 'System assigned managed identity' section is shown, which describes how it enables authentication to cloud services without storing credentials in code. It includes a 'Status' toggle switch set to 'On'. The 'System-Assigned Service Principal' section follows, describing its use for Kerberos authentication, also with an 'On' status. The 'User assigned managed identity' section is described as enabling authentication to cloud services using standalone Azure resources, with an 'Off' status. Below these, a table lists 'Name', 'resource group', 'subscription', and a sorting icon. A note states 'No user assigned managed identities assigned to this resource. Select 'Add' to add more.' Under the 'Primary identity' section, it says to designate one identity as primary for the server, with a 'Learn more' link. A dropdown menu for selecting the primary identity is shown.

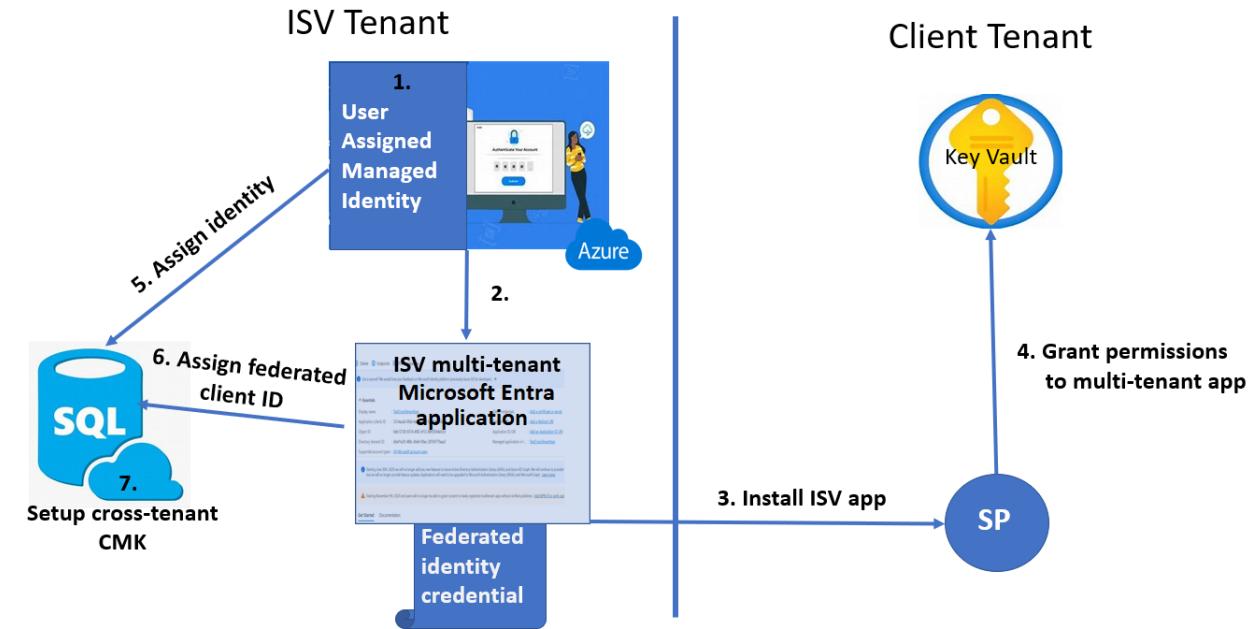
Federated Identity for Azure SQL Database



For cross-tenant resource access, such as using a customer-managed key from a key vault in another Microsoft Entra tenant, you may select a federated client identity to use with the selected managed identity.

You can configure TDE with CMK for Azure SQL Database for keys stored in key vaults that are configured in different Microsoft Entra tenants. Microsoft Entra ID introduces a feature called workload identity federation, and it allows Azure resources from one Microsoft Entra tenant the capability to access resources in another Microsoft Entra tenant.

Cross Tenant Support Setup for TDE/CMK



Server trust groups (aka SQL trust groups)



Est. trust among SQL instances

Based on certificate exchange

Cross-instance use cases

- Distributed transactions
- Service broker
- Linked servers Entra Id Authentication

uth-demo-env > aadauthdemosqlmi

aadauthdemosqlmi | SQL trust groups

SQL managed instance

Search (Ctrl+ /)

+ New Group Heart Feedback

Cloud Overview

Log Activity log

User Access control (IAM)

Tags

Problem Diagnose and solve problems

Cloud Quick start

Settings

Compute Compute + storage

Use SQL Trust Groups to enable a group of resources to communicate across multiple SQL instances.

1 SQL trust group

Search to filter SQL trust group...

Name	Status
------	--------

Cloud LinkedServers	Enabled
--	---------



Common Azure SQL MI connectivity scenarios

- **Backup to and restore from Azure Storage**

Private endpoint to your storage account in another subnet; or

Connect directly to Azure Storage account, using a service endpoint policy to block others

- **Hybrid connectivity via Managed Instance Link**

Peer networks and allow inbound and outbound on ports 5022, 11xxx

- **Failover groups**

Configure SQL Managed Instance as a member of a failover group during creation

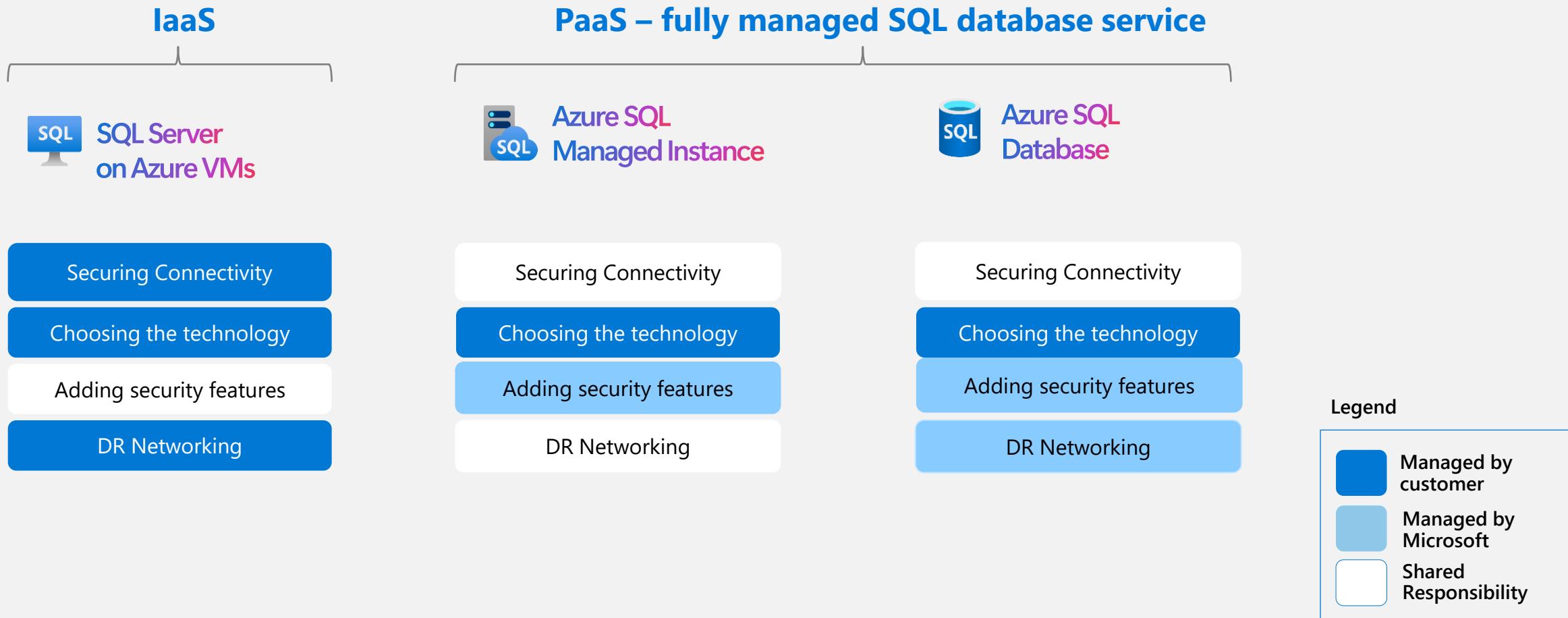
Peer networks and allow inbound from other, outbound to other on ports 5022, 11xxx

- **Distributed transactions**

Set up a Server Trust Group

Peer networks and allow inbound and outbound on ports 5024, 11xxx

Shared responsibility for Outbound Connectivity



Restricting Network Access

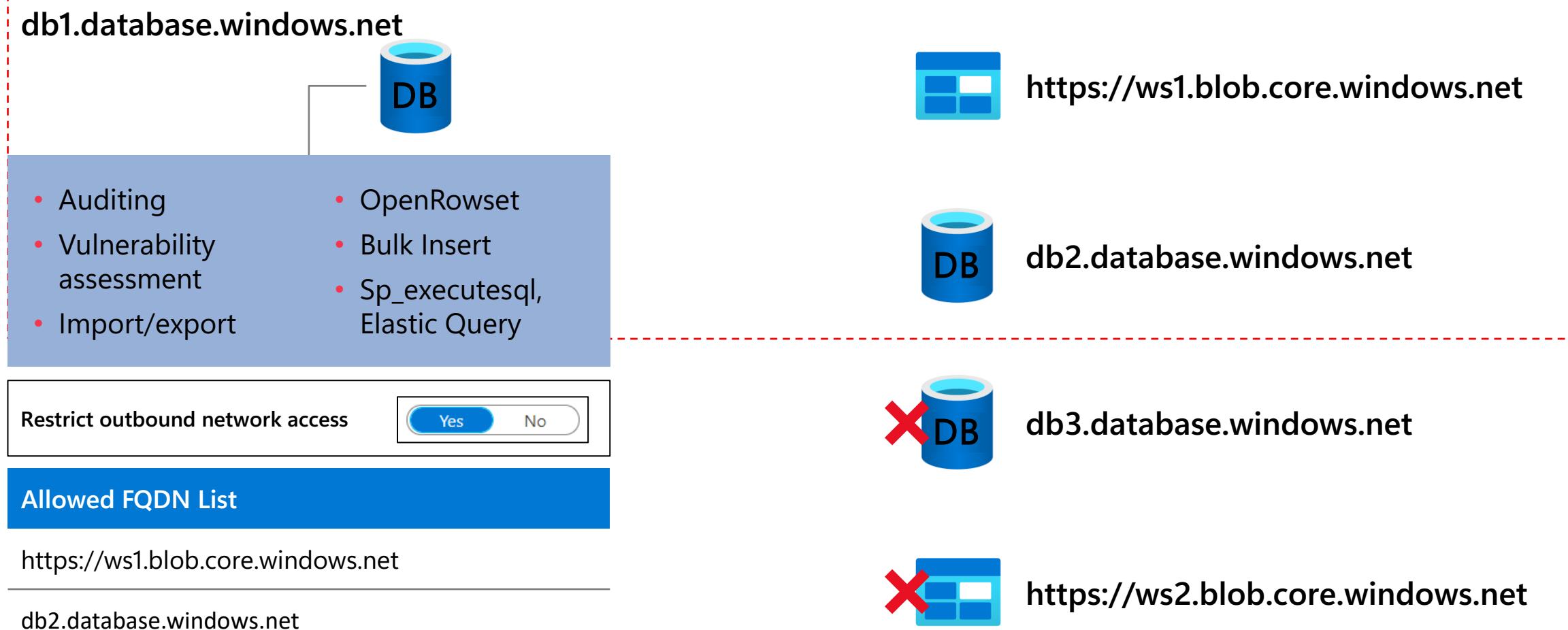
for Azure SQL DBA

Restricting networking access on Azure SQL

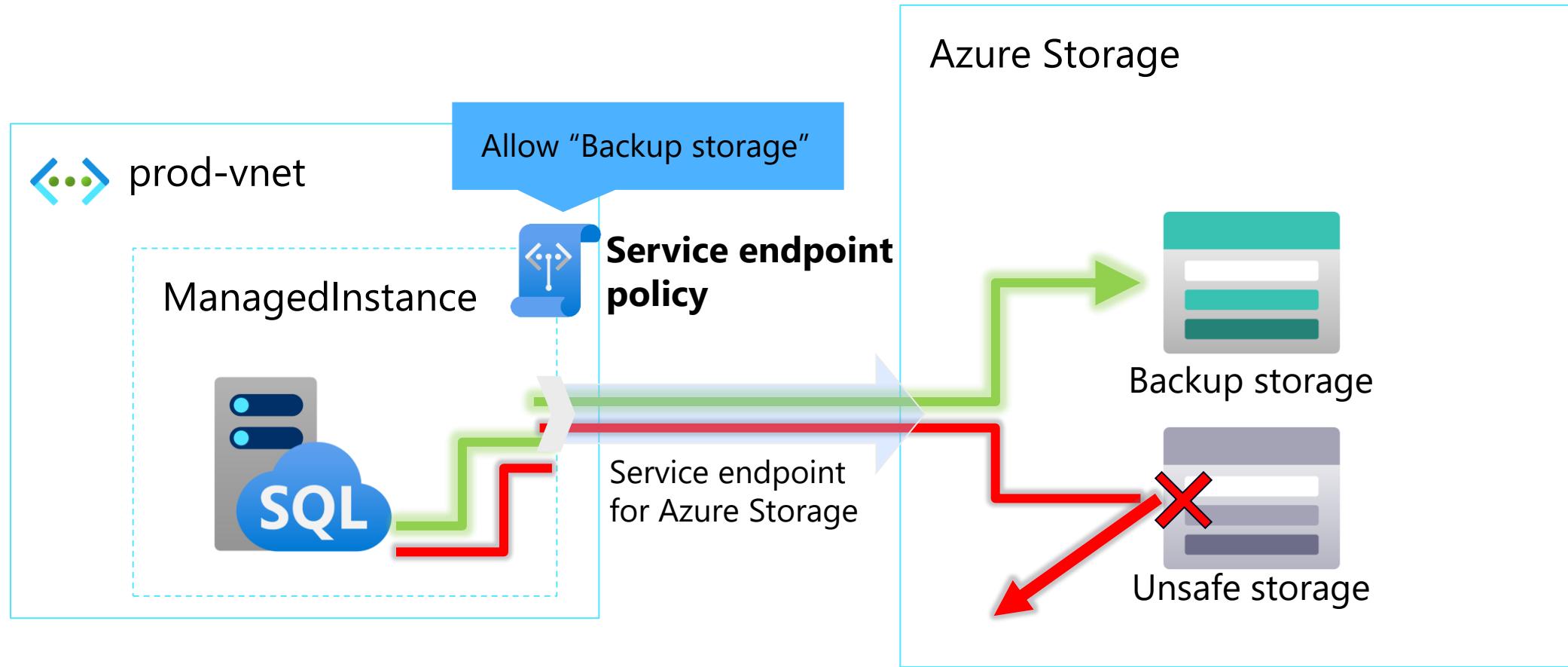
Let's take a dive into available solutions for restricting networking access on Azure SQL

- Azure SQL DB Firewall Rules
- Service Endpoint Policies
- Network Security Groups
- Azure Firewall
- Azure Virtual Network Manager
- Other Network Configurations (proxy, appliances, etc)

Outbound firewall rules for Azure SQL DB



Service endpoint policies control traffic to Azure (Preview)



Network Security Group (NSG)

The screenshot shows the Azure portal interface for managing a Network Security Group (NSG). The left sidebar contains a navigation menu with items such as Overview, Activity log, Access control (IAM), Tags, Diagnose and solve problems, Settings (Inbound security rules, Outbound security rules, Network interfaces, Subnets, Properties, Locks), Monitoring (Alerts, Diagnostic settings, Logs, NSG flow logs), and a search bar at the top.

Inbound Security Rules

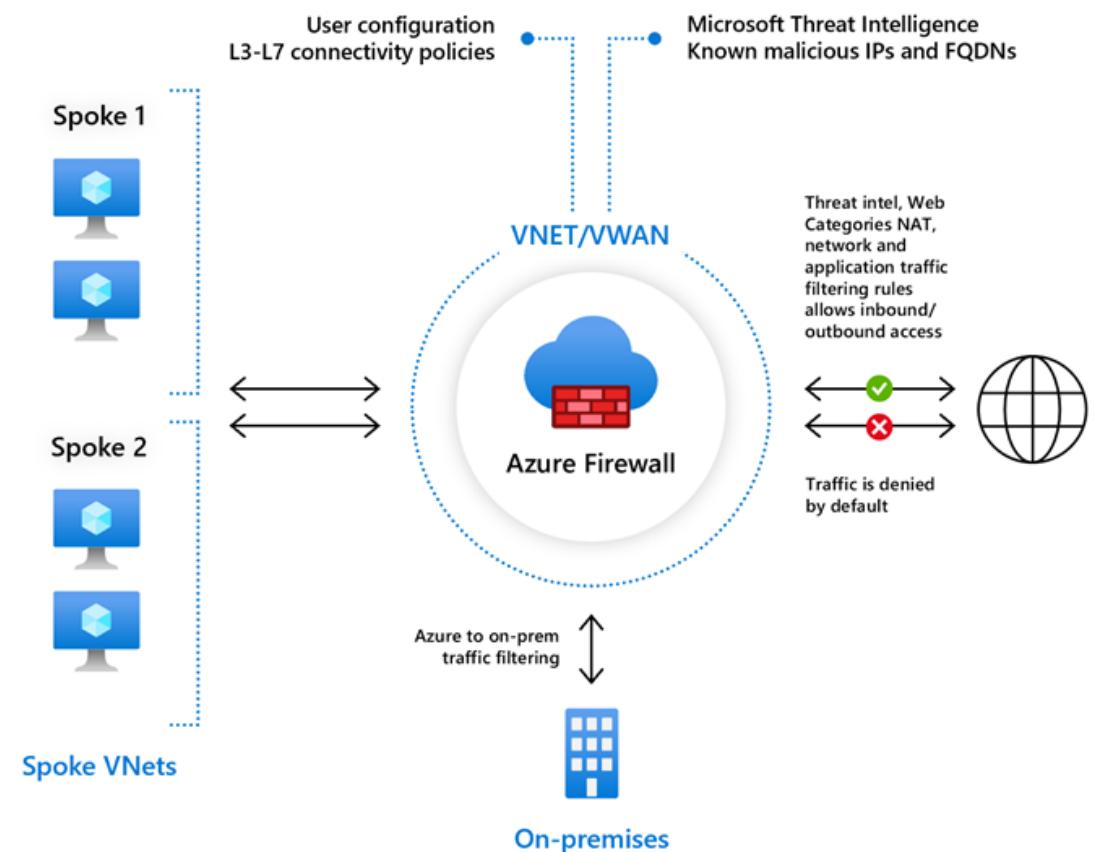
Rule ID	Name	Source	Destination	Protocol	Subnet	Action	Operations
100	Microsoft.Sql-managedIn...	Any	Any	AzureLoadBalancer	10.0.0.0/24	Allow	
101	Microsoft.Sql-managedIn...	Any	Any	10.0.0.0/24	10.0.0.0/24	Allow	
1000	allow_tds_inbound	1433	Tcp	VirtualNetwork	10.0.0.0/24	Allow	
1100	allow_redirect_inbound	11000-11999	Tcp	VirtualNetwork	10.0.0.0/24	Allow	
1200	allow_geodr_inbound	5022	Tcp	VirtualNetwork	10.0.0.0/24	Allow	
1300	public_endpoint_inbound	3342	Tcp	Internet	10.0.0.0/24	Allow	
4096	deny_all_inbound	Any	Any	Any	Any	Deny	
65000	AllowVnetInBound	Any	Any	VirtualNetwork	VirtualNetwork	Allow	
65001	AllowAzureLoadBalancerIn...	Any	Any	AzureLoadBalancer	Any	Allow	
65500	DenyAllInBound	Any	Any	Any	Any	Deny	

Outbound Security Rules

Rule ID	Name	Source	Destination	Protocol	Subnet	Action	Operations
100	Microsoft.Sql-managedIn...	443	Tcp	10.0.0.0/24	AzureActiveDirectory	Allow	
101	Microsoft.Sql-managedIn...	443	Tcp	10.0.0.0/24	OneDsCollector	Allow	
102	Microsoft.Sql-managedIn...	Any	Any	10.0.0.0/24	10.0.0.0/24	Allow	
103	Microsoft.Sql-managedIn...	443	Any	10.0.0.0/24	Storage.eastus2euap	Allow	
104	Microsoft.Sql-managedIn...	443	Any	10.0.0.0/24	Storage.centraluseuap	Allow	

Azure Firewall

- Network and application-level filtering
- Threat intelligence feeds directly from Microsoft Cyber Security: alert and deny known malicious traffic
- Built-in HA
- SNAT and DNAT
- FQDN based filtering when set as a DNS proxy



Azure Virtual Network Manager

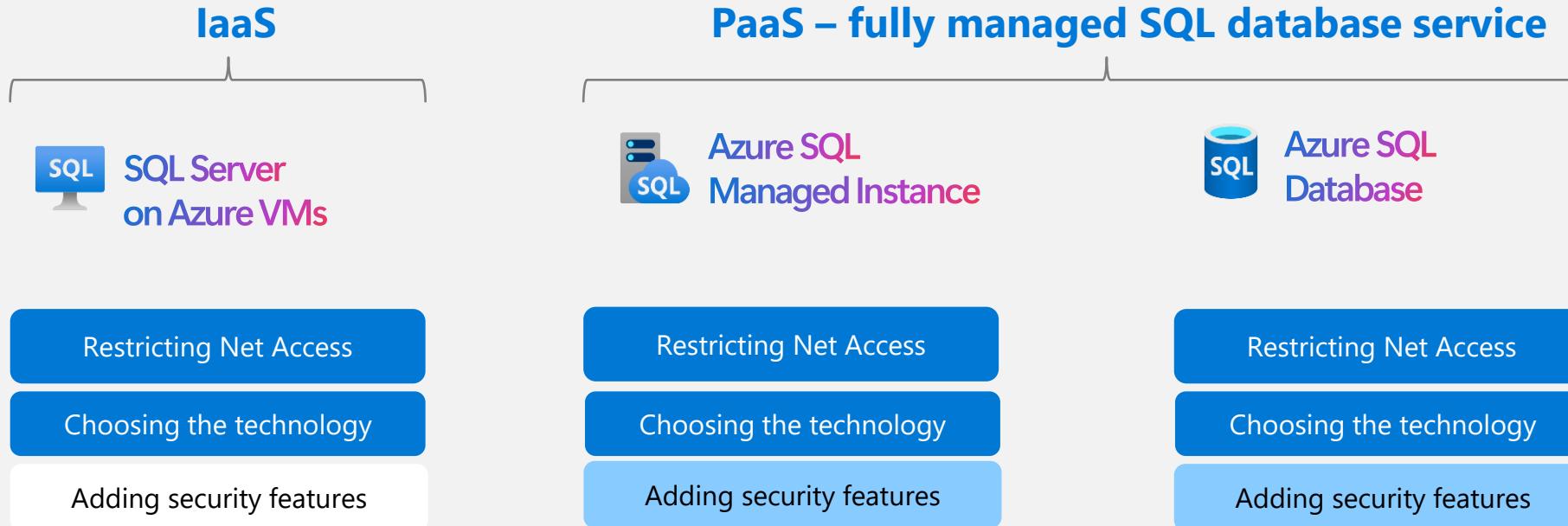


- Management service to group, deploy, manage virtual networks globally across subscriptions
- Define network groups to logically segment (zone) your architecture
- Define connectivity configurations to establish mesh or hub-and-spoke topologies
- Define security admin rules to specify inbound/outbound rules at the global level
- Can be configured to not apply “deny” rules on Azure SQL Managed Instance VNets

The screenshot shows the Azure Virtual Network Manager interface for a specific virtual network named 'vnet-sqlmiao02'. The left sidebar includes links for Overview, Activity log, Access control (IAM), Tags, Diagnose and solve problems, Settings (with sub-options like Address space, Connected devices, Subnets, Bastion, DDoS protection, Firewall, Microsoft Defender for Cloud, and Network manager), DNS servers, Peerings, and Service endpoints. The main content area displays a table titled 'Connectivity configurations' under the 'Security admin configurations' tab. The table has columns for Priority, Rule name, Network manager, Action, Direction, Protocol, Source, Source port, Destination, and Destination port. There are 108 rows listed, each with a green checkmark in the 'Action' column indicating they are all set to 'Allow'. The table also includes a 'Refresh' button and a 'Search' bar.

Priority	Rule name ↑	Network manager	Action	Direction	Protocol	Source	Source port	Destination	Destinatio...
1	GenevaRunners2	NRMS-ZeroTrust-Co...	Allow	Inbound	Any	40.114...	1-65535	*	1-65535
2	GenevaRunners	NRMS-ZeroTrust-Co...	Allow	Inbound	Any	168.61...	1-65535	*	1-65535
3	HealthMonitoringAddresses	NRMS-ZeroTrust-Co...	Allow	Inbound	Any	191.23...	1-65535	*	1-65535
9	EV2	NRMS-ZeroTrust-Co...	Allow	Inbound	Any	52.225...	1-65535	*	1-65535
20	ManagedVPN	NRMS-ZeroTrust-Co...	Allow	Inbound	Any	20.120...	1-65535	*	1-65535
100	ActionGroup	NRMS-ZeroTrust-Co...	Allow	Inbound	Any	Action...	1-65535	*	1-65535
101	ApiManagement	NRMS-ZeroTrust-Co...	Allow	Inbound	Any	ApiMa...	1-65535	*	1-65535
102	ApplicationInsightsAvailability	NRMS-ZeroTrust-Co...	Allow	Inbound	Any	Applic...	1-65535	*	1-65535
103	AppServiceManagement	NRMS-ZeroTrust-Co...	Allow	Inbound	Any	AppSe...	1-65535	*	1-65535
104	AzureActiveDirectoryDomainServ...	NRMS-ZeroTrust-Co...	Allow	Inbound	Any	Azure...	1-65535	*	5896...
105	AzureCognitiveSearch	NRMS-ZeroTrust-Co...	Allow	Inbound	Tcp	Azure...	1-65535	*	80, 44...
106	AzureConnectors	NRMS-ZeroTrust-Co...	Allow	Inbound	Any	Azure...	1-65535	*	1-65535
107	AzureDatabricks	NRMS-ZeroTrust-Co...	Allow	Inbound	Any	Azure...	1-65535	*	22, 5557
108	AzureDataExplorerManagement	NRMS-ZeroTrust-Co...	Allow	Inbound	Any	Azure...	1-65535	*	443

Shared responsibility for Restricting Network Access

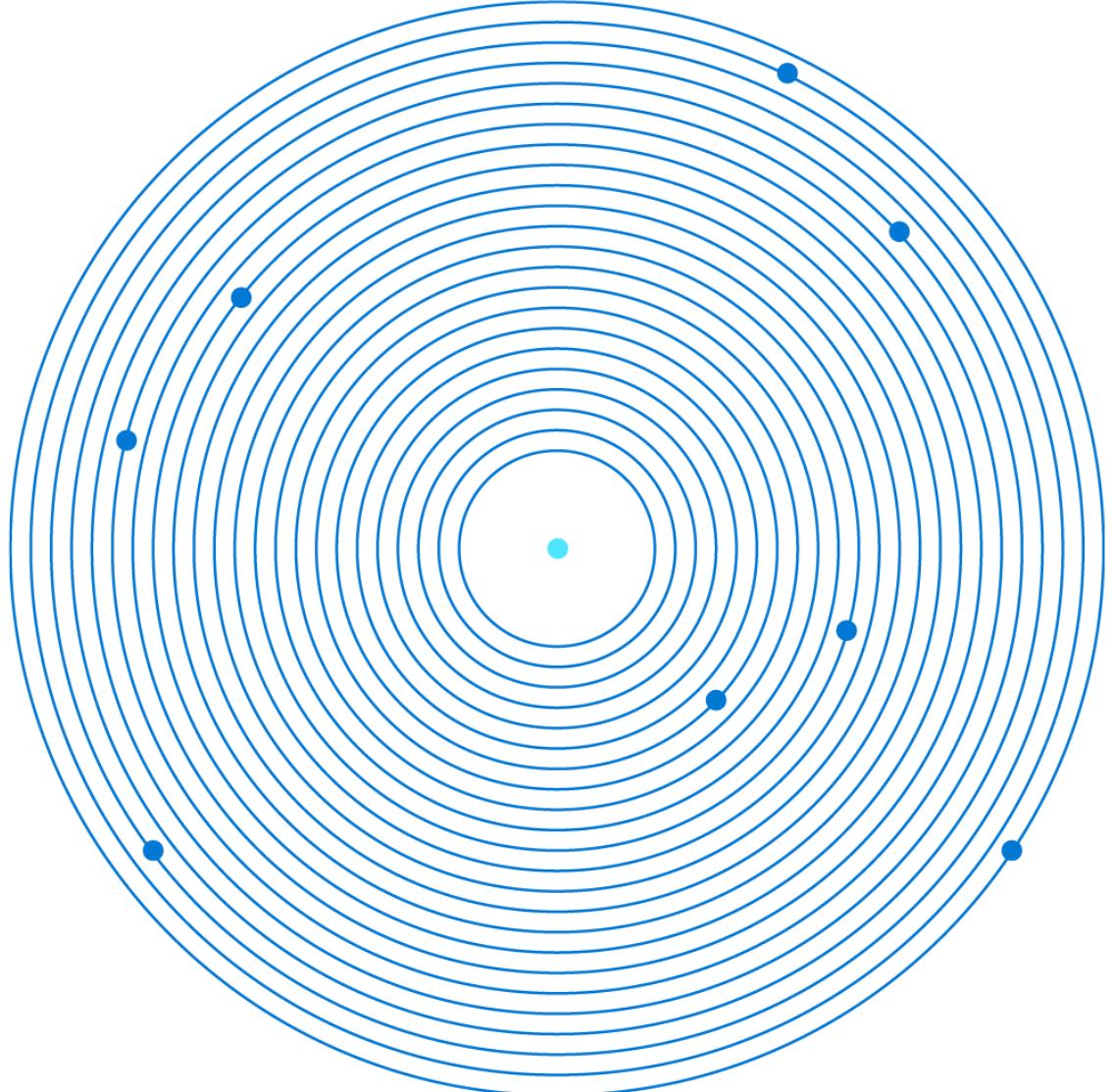


Legend

	Managed by customer
	Managed by Microsoft
	Shared Responsibility

Azure SQL Authentication

what is required to securely connect to, and access,
your Azure SQL resources



Transport Layer Security -TLS



Secure data in motion being sent over the network between a client and server.

It protects data between the client and server against snooping and man-in-the-middle attacks

For cloud databases it always enforces encryption for connections regardless of connection string setting.

The minimal TLS version setting allows customers to choose which version of TLS their SQL database uses. The latest TLS version is 1.3

TLS in Azure SQL Database



TLS is REQUIRED

From the 31st of August 2025, you won't be able to set Azure SQL Database TLS connectivity minimum version below 1.2

The screenshot shows the 'Networking' section of the Azure portal for a SQL server named 'mydocsamplesqlserver'. The 'Networking' tab is selected and highlighted with a red box. The 'Connectivity' tab is also highlighted with a red box. Under 'Connection Policy', the 'Default' option is selected. In the 'Encryption in transit' section, it states that the server supports TLS 1.3, 1.2, and 1.1. A dropdown menu for 'Minimum TLS version' is open, showing options: TLS 1.3 (selected), TLS 1.0, TLS 1.1, and TLS 1.2. The 'TLS 1.3' option is also highlighted with a red box.

mydocsamplesqlserver | Networking

Search (Ctrl+ /)

Feedback

Security

Networking

Microsoft Defender for Cloud

Transparent data encryption

Identity

Auditing

Public access Private access Connectivity

Connection Policy

Configure how clients communicate with your SQL database server. [Learn more](#)

Connection policy

Default - Uses Redirect policy for all client connections originating inside of Azure and Proxy for all client connections originating outside Azure

Proxy - All connections are proxied via the Azure SQL Database gateways

Redirect - Clients establish connections directly to the node hosting the database

Encryption in transit

This server supports encrypted connections using Transport Layer Connections (TLS). Any login attempts from clients using a TLS version less than the Minimum TLS Version shall be rejected. For information on TLS version and certificates, refer to connecting with TLS/SSL. [Learn more](#)

Minimum TLS version

TLS 1.3

TLS 1.0

TLS 1.1

TLS 1.2

TLS 1.3

TLS in Azure SQL Managed Instance



TLS is REQUIRED

**TLS 1.2 is enforced on outbound connections
since Jan 2020**

**TLS 1.3 is not yet supported on Azure SQL MI, but
we are working on it.**

From the 31st of August 2025, you won't be able to set
Azure SQL Database TLS connectivity minimum version
below 1.2

> Data management

∨ Security

Networking

Microsoft Defender for
Cloud

Transparent data
encryption

Private endpoint
connections

SQL trust groups

Endpoint

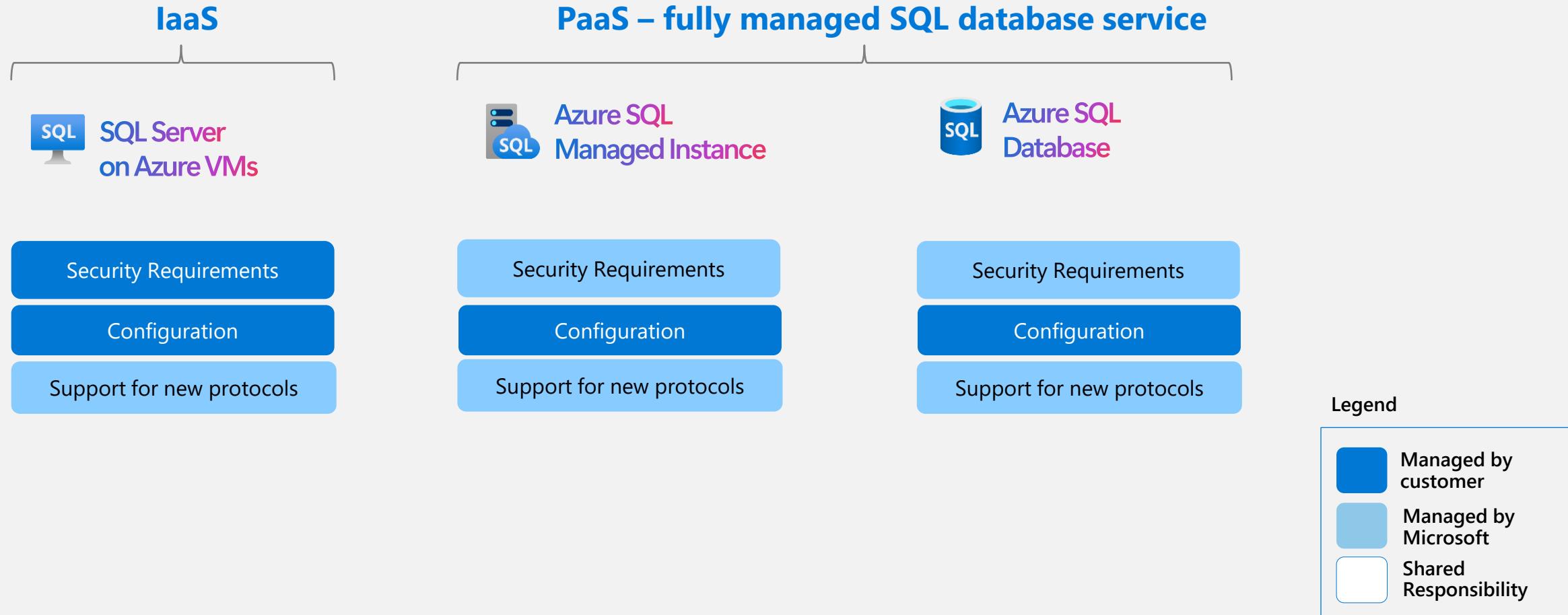
Minimum TLS version ⓘ

1.0 1.1 1.2

Connection type (VNet-local endpoint)

Proxy (Default)

Shared responsibility for Communication protocol

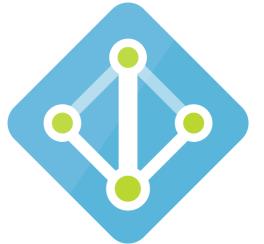


Authentication Modes

for Azure SQL DBA

Azure SQL Authentication Modes

- SQL Authentication (supported in all Azure SQL, **NOT RECOMMENDED**)
- Windows Authentication
- Mixed Authentication Mode
- Microsoft Entra
(supported in Azure SQL PaaS, SQL Server 2022+ on Azure VMs)
- Windows Authentication for Entra on Azure SQL Managed Instance



Overall, customers are highly recommended to use either Entra or Windows Authentication, avoiding SQL Authentication wherever possible.

Strengthen Your Security with Microsoft Entra Authentication

- Secure your data from unauthorized access
- Ensure the highest level of identity protection
- Centrally manage identities of database users and other Microsoft services in one central location



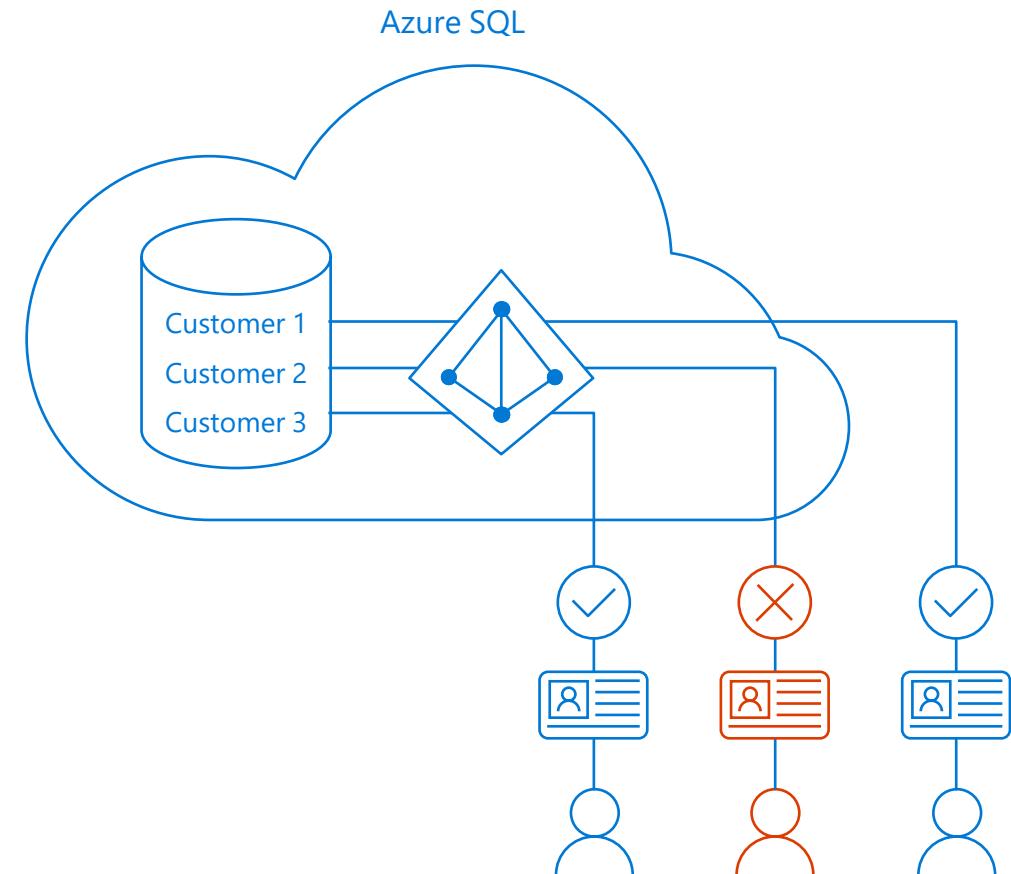
Microsoft Entra Authentication with Azure SQL

- **Overview**

- Manage user identities in one location
- Enable access to Azure SQL and other Microsoft services with Microsoft Entra Authentication user identities and groups

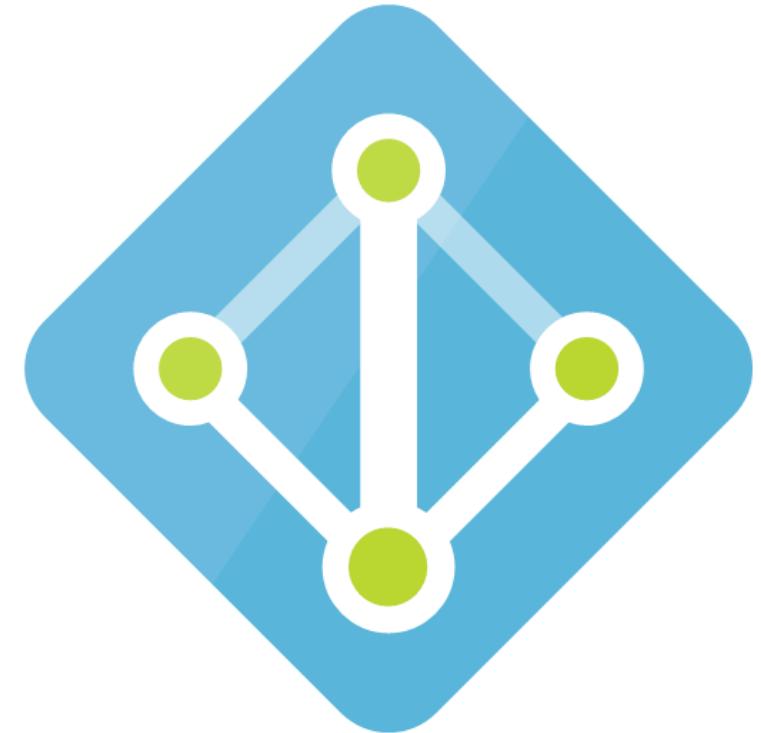
- **Benefits**

- Limits proliferation of user identities across databases
- Allows password rotation in a single place
- Enables management of database permissions by using external Microsoft Entra ID groups
- Eliminates the need to store passwords



Entra ID Only Authentication for Azure SQL DB & Azure SQL MI

- Disables SQL Authentication
- Including built-in Server Admin account
- Blocks changing Server Admin password
- Can be set at creation-time
- Could be enforced with Azure Policy

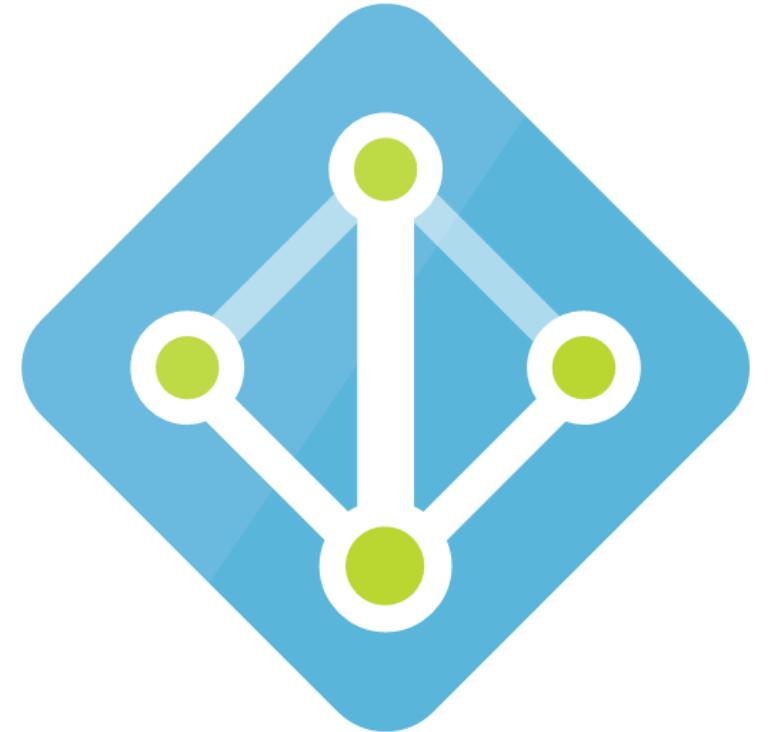


Windows Authentication for Entra ID

Windows Authentication is additional Single-Sign-On authentication option for Entra ID users.

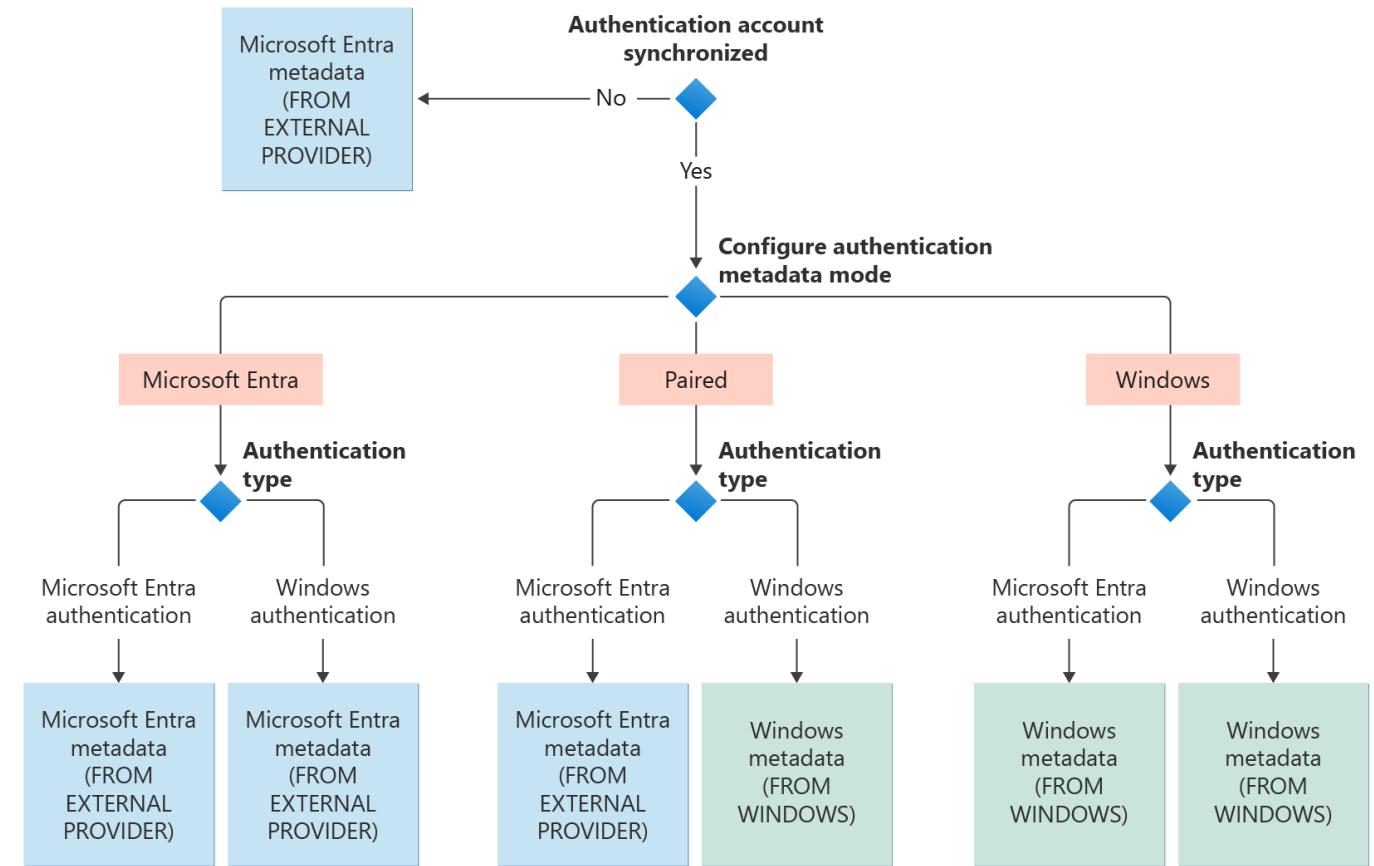
Compared to the previous options, it brings the following benefits:

- Works with legacy drivers, that don't have built-in Entra ID support
- Works on both Domain Joined, and Entra Directory Joined machines
- Works in double hop scenarios (i.e., IIS impersonation)
- Support for MFA and Conditional Access in making

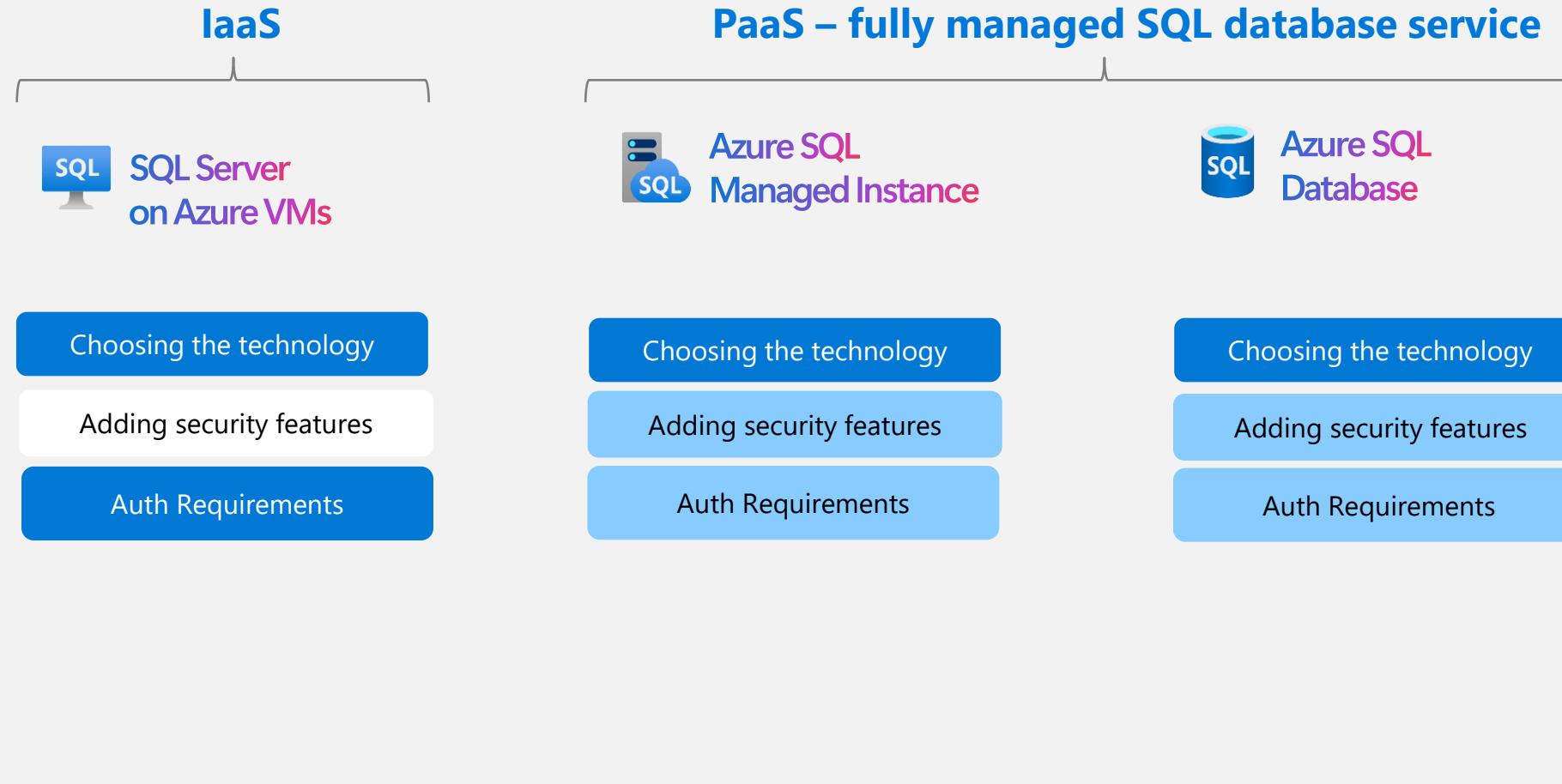


Native Window principals for Azure SQL Managed Instance (Preview)

- The **Windows authentication metadata mode** is a new mode that allows users to use Windows authentication or Microsoft Entra authentication (using a Windows principal metadata) with Azure SQL Managed Instance.
- This mode is available for SQL Managed Instance only. The Windows authentication metadata mode isn't available for Azure SQL Database.



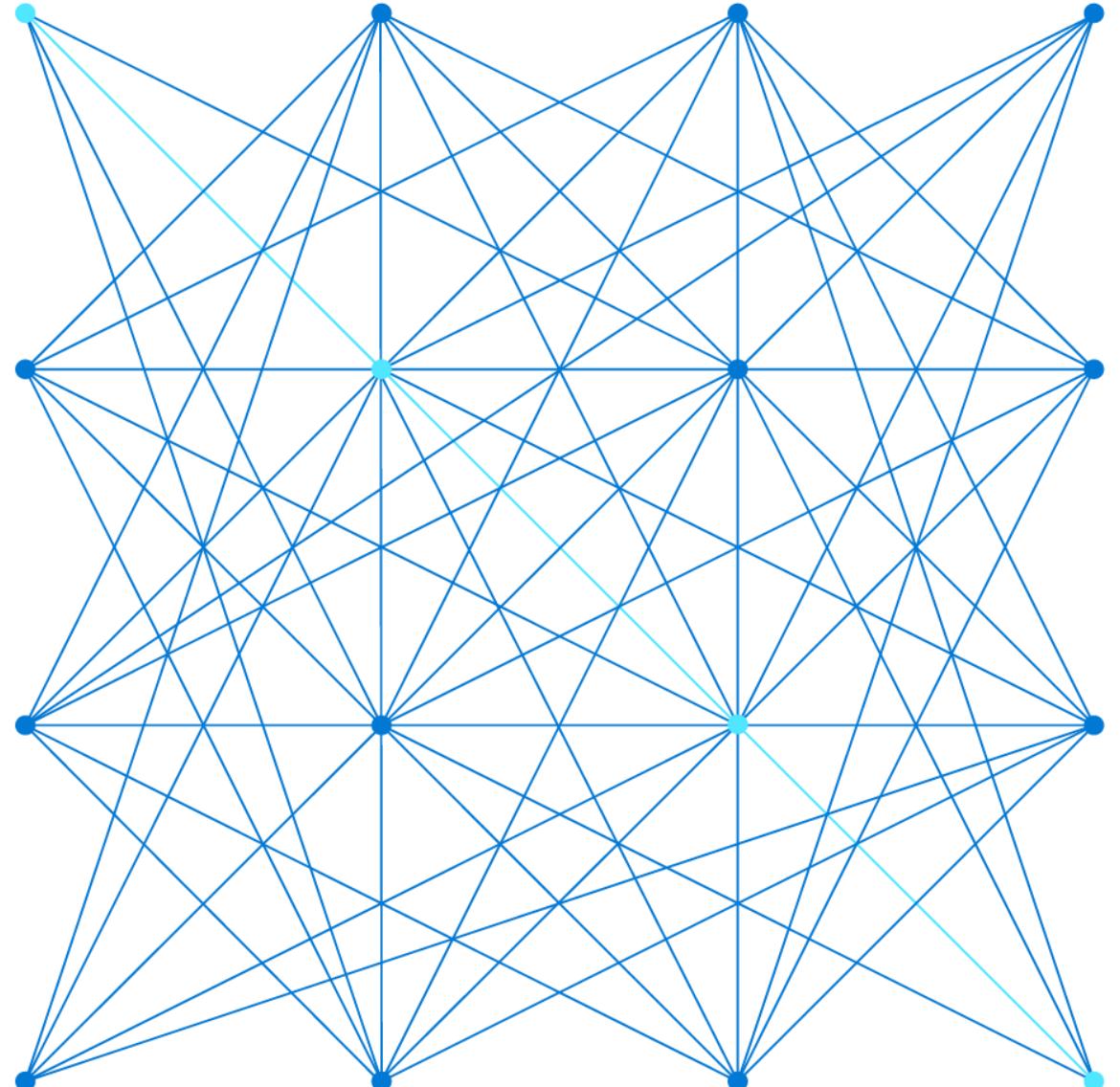
Shared responsibility for Authentication



Legend

- Managed by customer
- Managed by Microsoft
- Shared Responsibility

Compliance and Security in Azure SQL



Azure - Compliance Offerings

The details for the public cloud as well as for the Government cloud can be found in our [Service Trust Portal](#).

Regulatory Compliance in Azure Policy (preview)

Regulatory Compliance in Azure Policy provides built-in initiative definitions to view a list of the **controls** and **compliance domains** based on responsibility (*Customer, Microsoft, Shared*).

For Microsoft-responsible controls, we provide additional details of our audit results based on third-party attestation and our implementation details to achieve that compliance

[Regulatory Compliance in initiative definitions - Azure Policy](#)

Azure Policy Regulatory Compliance controls for Azure SQL Database & SQL Managed Instance

The list of the available policies can be found at
[Azure Policy Regulatory Compliance controls - Azure SQL](#)

PCI DSS v4.0

To review how the available Azure Policy built-ins for all Azure services map to this compliance standard, see [Azure Policy Regulatory Compliance details for PCI DSS v4.0](#). For more information about this compliance standard, see [PCI DSS v4.0](#).

Domain	Control ID	Control title	Policy (Azure portal)	Policy version (GitHub)
Requirement 10: Log and Monitor All Access to System Components and Cardholder Data	10.2.2	Audit logs are implemented to support the detection of anomalies and suspicious activity, and the forensic analysis of events	Auditing on SQL server should be enabled 	2.0.0 
Requirement 10: Log and Monitor All Access to System Components and Cardholder Data	10.3.3	Audit logs are protected from destruction and unauthorized modifications	Auditing on SQL server should be enabled 	2.0.0 
Requirement 11: Test Security of Systems and Networks Regularly	11.3.1	External and internal vulnerabilities are regularly identified, prioritized, and addressed	SQL databases should have vulnerability findings resolved 	4.1.0 
Requirement 03: Protect Stored Account Data	3.3.3	Sensitive authentication data (SAD) is not stored after authorization	An Azure Active Directory administrator should be provisioned for SQL servers 	1.0.0 
Requirement 03: Protect Stored Account Data	3.5.1	Primary account number (PAN) is secured wherever it is stored	Transparent Data Encryption on SQL databases should be enabled 	2.0.0 
Requirement 05: Protect All Systems and Networks from Malicious Software (malware)	5.2.1	Malicious software (malware) is prevented, or detected and addressed	SQL databases should have vulnerability findings resolved 	4.1.0 

HIPAA HITRUST 9.2

To review how the available Azure Policy built-ins for all Azure services map to this compliance standard, see [Azure Policy Regulatory Compliance - HIPAA HITRUST 9.2](#). For more information about this compliance standard, see [HIPAA HITRUST 9.2](#).

Domain	Control ID	Control title	Policy (Azure portal)	Policy version (GitHub)
03 Portable Media Security	0301.09o1Organizational.123-09.o	0301.09o1Organizational.123-09.o 09.07 Media Handling	Transparent Data Encryption on SQL databases should be enabled 	2.0.0 
03 Portable Media Security	0304.09o3Organizational.1-09.o	0304.09o3Organizational.1-09.o 09.07 Media Handling	SQL managed instances should use customer-managed keys to encrypt data at rest 	2.0.0 
03 Portable Media Security	0304.09o3Organizational.1-09.o	0304.09o3Organizational.1-09.o 09.07 Media Handling	SQL servers should use customer-managed keys to encrypt data at rest 	2.0.1 
07 Vulnerability Management	0709.10m1Organizational.1-10.m	0709.10m1Organizational.1-10.m 10.06 Technical Vulnerability Management	SQL databases should have vulnerability findings resolved 	4.1.0 
07 Vulnerability Management	0709.10m1Organizational.1-10.m	0709.10m1Organizational.1-10.m 10.06 Technical Vulnerability Management	Vulnerability assessment should be enabled on SQL Managed Instance 	1.0.1 
07 Vulnerability Management	0709.10m1Organizational.1-10.m	0709.10m1Organizational.1-10.m 10.06 Technical Vulnerability Management	Vulnerability assessment should be enabled on SQL Managed Instance 	3.0.0 

[Australian Government ISM PROTECTED](#)

[Canada Federal PBMM](#)

[CIS Microsoft Azure Foundations Benchmark 1.1.0](#)

[CIS Microsoft Azure Foundations Benchmark 1.3.0](#)

[CIS Microsoft Azure Foundations Benchmark 1.4.0](#)

[CIS Microsoft Azure Foundations Benchmark 2.0.0](#)

[CMMC Level 3](#)

[FedRAMP High](#)

[FedRAMP Moderate](#)

[HIPAA HITRUST 9.2](#)

[IRS 1075 September 2016](#)

[ISO 27001:2013](#)

[Microsoft Cloud for Sovereignty Baseline Confidential Policies](#)

[Microsoft cloud security benchmark](#)

[NIST SP 800-171 R2](#)

[NIST SP 800-53 Rev. 4](#)

[NIST SP 800-53 Rev. 5](#)

[NL BIO Cloud Theme](#)

[PCI DSS 3.2.1](#)

[PCI DSS v4.0](#)

[Reserve Bank of India - IT Framework for NBFC](#)

[Reserve Bank of India IT Framework for Banks v2016](#)

[RMIT Malaysia](#)

[SWIFT CSP-CSCF v2021](#)

[UK OFFICIAL and UK NHS](#)

[Next steps](#)

Azure Policy & RBAC

for Azure SQL DBA

Azure Policy and Azure RBAC

RBAC



- Azure RBAC focuses on managing user actions at different scopes.
- If control of an action is required, then Azure RBAC is the correct tool to use.
- Even if an individual has access to perform an action, if the result is a non-compliant resource, Azure Policy still blocks the create or update.

Azure Policy



- Azure Policy evaluates state by examining properties on resources that are represented in Resource Manager and properties of some Resource Providers.

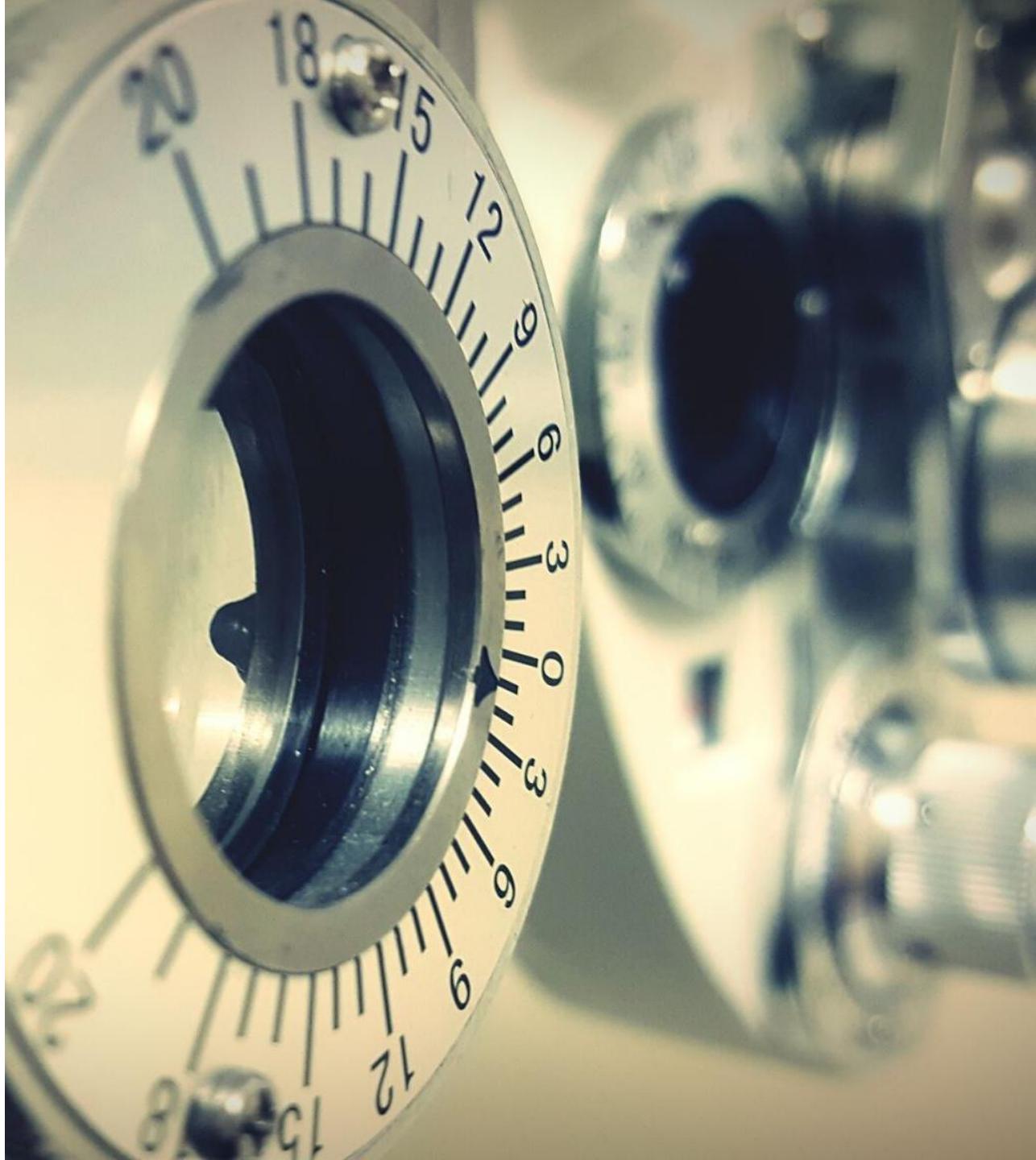
The combination of Azure RBAC and Azure Policy provides full scope control in Azure.

Transparent Data Encryption

for Azure SQL DBA

The benefits of Transparent Data Encryption (TDE)

- Protects data-at-rest
- Entire database is encrypted on disk (not in memory)
- Enabled by default
- No application or schema changes are required
- Backups, data, and log files are unusable without the encryption key
- Supports both service-managed and customer-managed keys



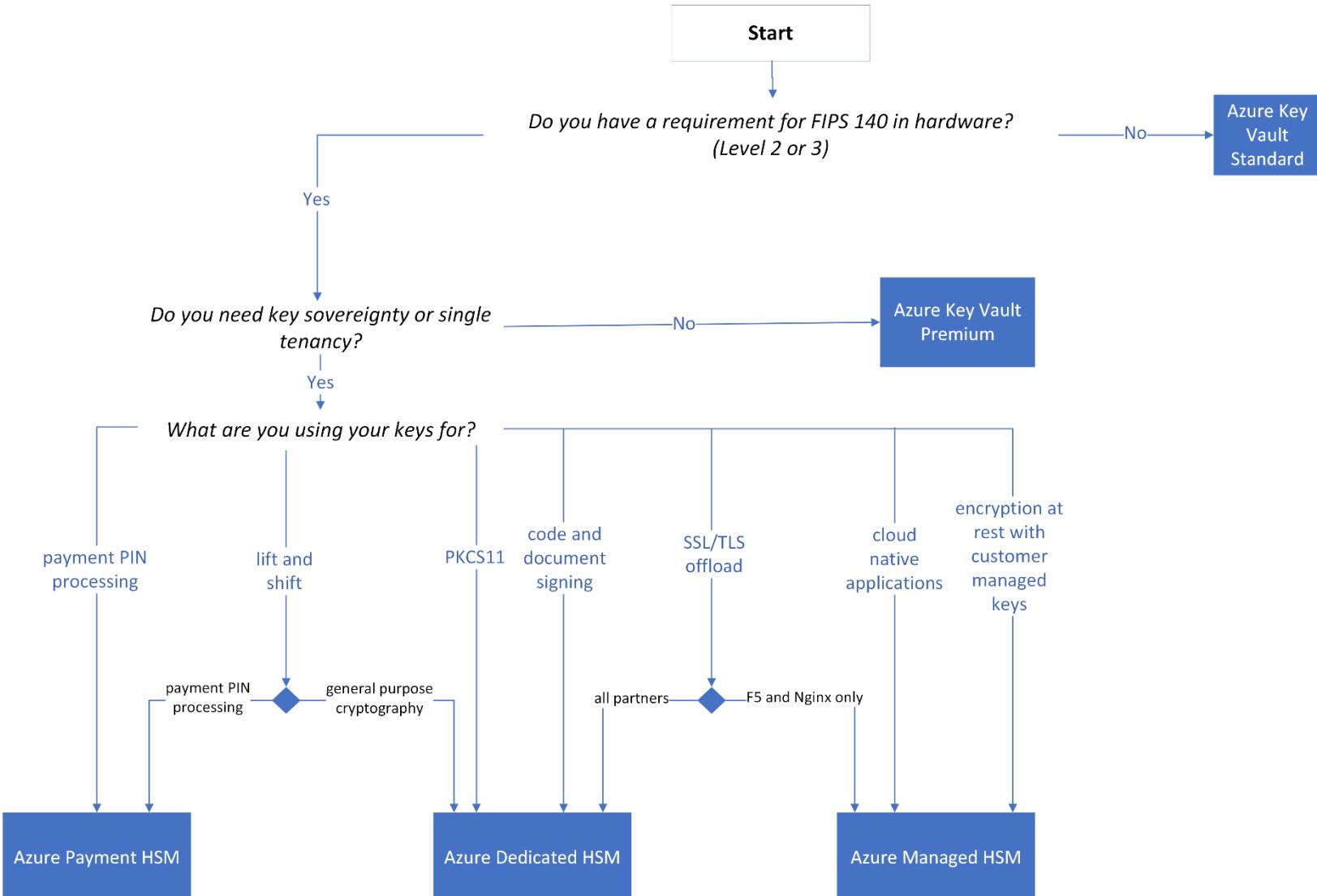
Transparent data encryption (TDE)

- Azure SQL Managed Instance, Azure SQL DB, SQL Server on IaaS, and SQL Server on-premises all support Transparent Data Encryption (TDE) to protect data at rest (data, transaction log, and backup files).
- When enabling TDE at the database level, there is a protector key which will be stored in **Azure Key Vault** or **Managed HSM** that is used to encrypt the database level encryption key (DEK).
- For PaaS, encryption at rest is available by using
 - Service Managed Key
 - Customer Managed Key
 - Support for Azure Key Vault Managed HSM (Hardware Security Module)

Azure SQL PaaS vs Azure SQL IaaS TDE

- Azure SQL PaaS fully supports auto-key rotation
- SQL Server requires the customer to perform the key rotation pieces that are contained within SQL (credential etc.) to complete the key rotation
- SQL Server (IaaS) requires installation of the latest version of the EKM connector
- SQL Server has a slight difference in the credential creation syntax between AKV and managed HSM
- Managed HSM requires including the full path to the managed HSM whereas AKV requires only the name of the vault

Choosing Managed HSM Over Azure Key Vault

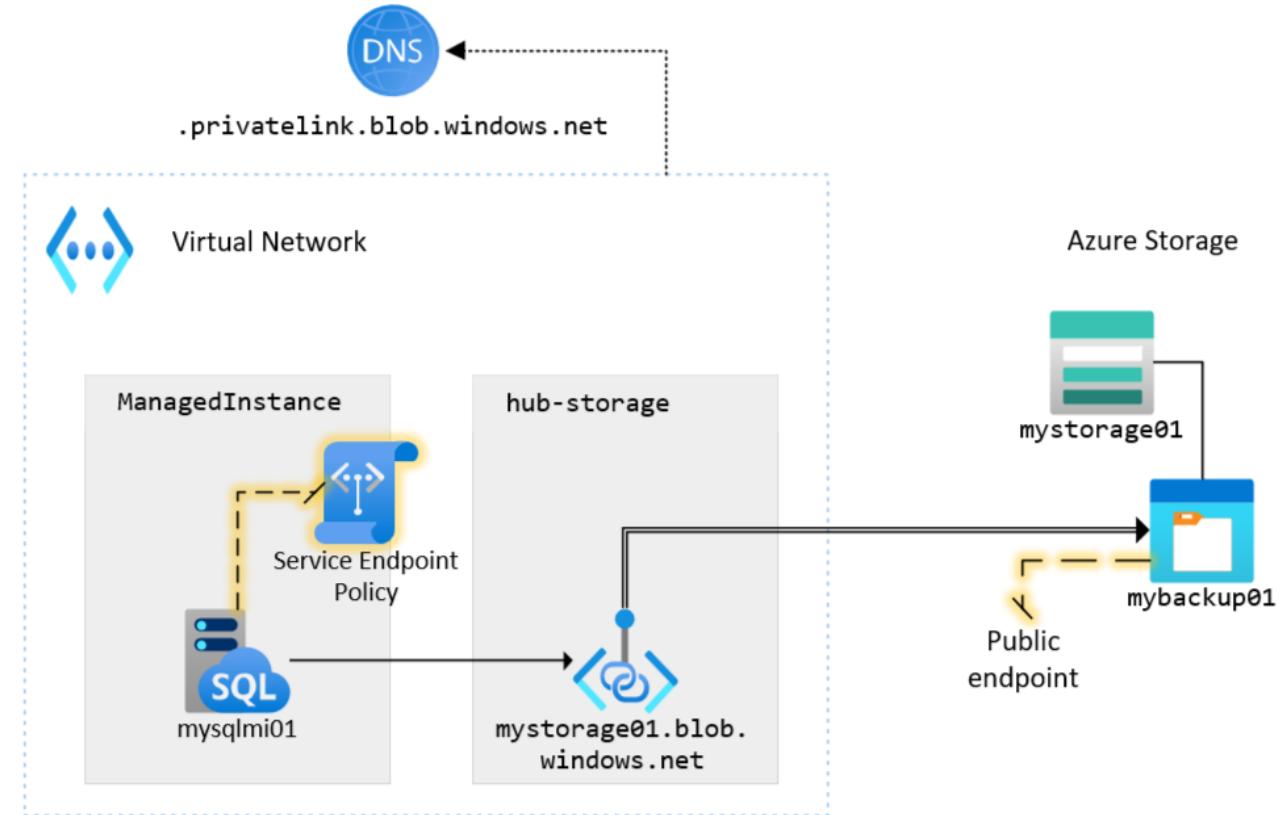


Securing backups

for Azure SQL DBA

Steps for secure customer backups on Azure SQL MI

- Use Managed Identity to authorize your Azure SQL Managed Instance to write to the blob storage.
- Set up a private endpoint to establish connectivity from Azure SQL Managed Instance to blob storage.
- Close off public access on the blob storage account.
- Apply a service endpoint policy on the Azure SQL Managed Instance's subnet to prevent data exfiltration.
- Consider encrypting backup for ensuring additional level of protection



Microsoft Purview

For Azure SQL DBAs



Discover and govern Azure SQL in Microsoft Purview

When you're scanning Azure SQL Database, Microsoft Purview supports extracting technical metadata from these sources:

- Server
- Database
- Schemas
- Tables, including columns
- Views, including columns (with lineage extraction enabled, as part of scanning)
- Stored procedures (with lineage extraction enabled)
- Stored procedure runs (with lineage extraction enabled)

Azure SQL Database

Metadata Extraction	Full Scan	Incremental Scan	Scoped Scan	Classification	Labeling	Access Policy	Lineage	Data Sharing	Live view
Yes	Yes	Yes	Yes	Yes	Yes	Yes (preview)	Yes (preview)	No	Yes

Azure SQL Managed Instance

Metadata Extraction	Full Scan	Incremental Scan	Scoped Scan	Classification	Labeling	Access Policy	Lineage	Data Sharing	Live view
Yes	Yes	Yes	Yes	Yes	Yes	Yes	Limited**	No	No

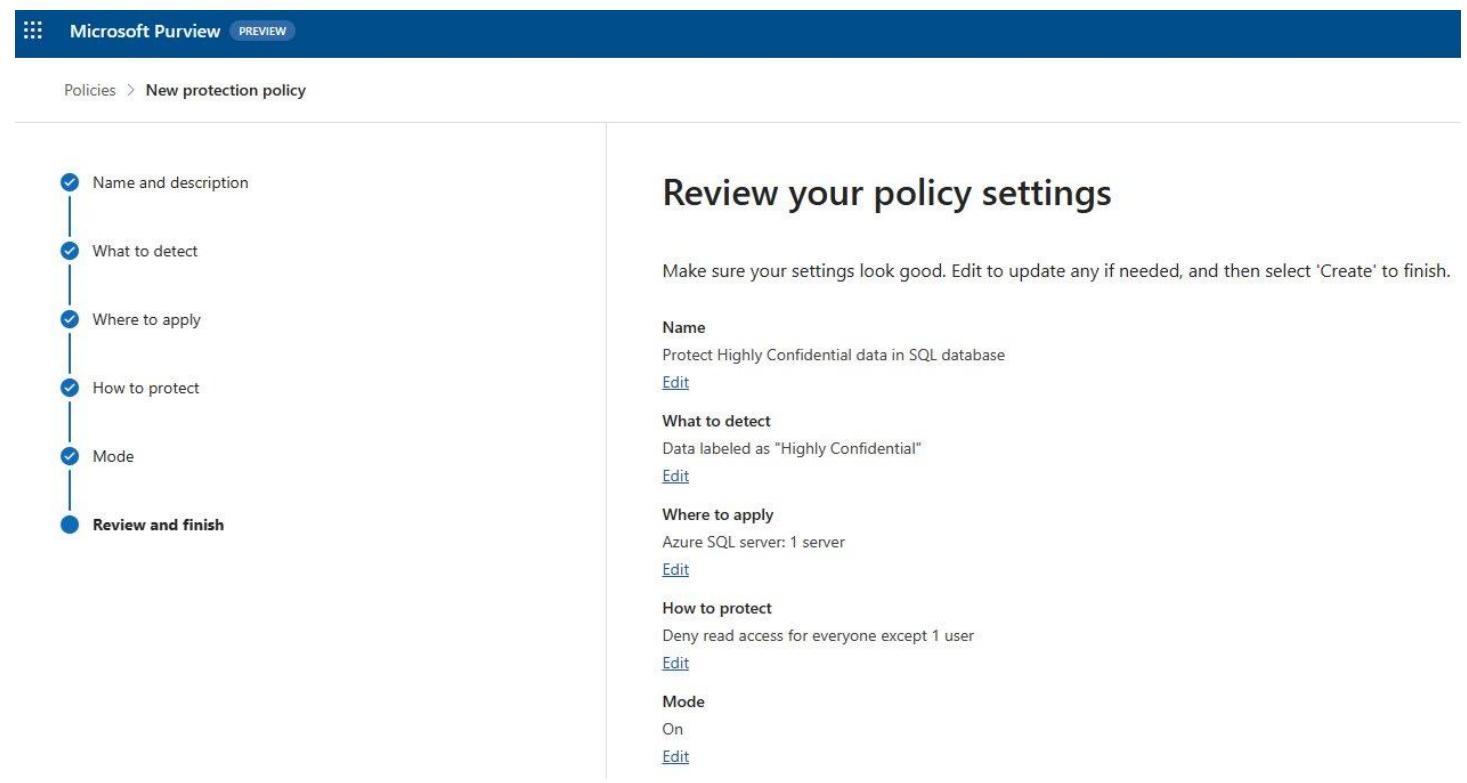
Label-based access control using Purview policies (preview)

Provision protection policies in Purview to restrict access to sensitive data in Azure SQL

Enterprise admins can authorize data access for a particular sensitivity label to specific users/groups

Access control is automatically imposed whenever sensitive information is accessed by users

Getting started with the preview:
<https://aka.ms/sql-purview-protection-preview-docs>



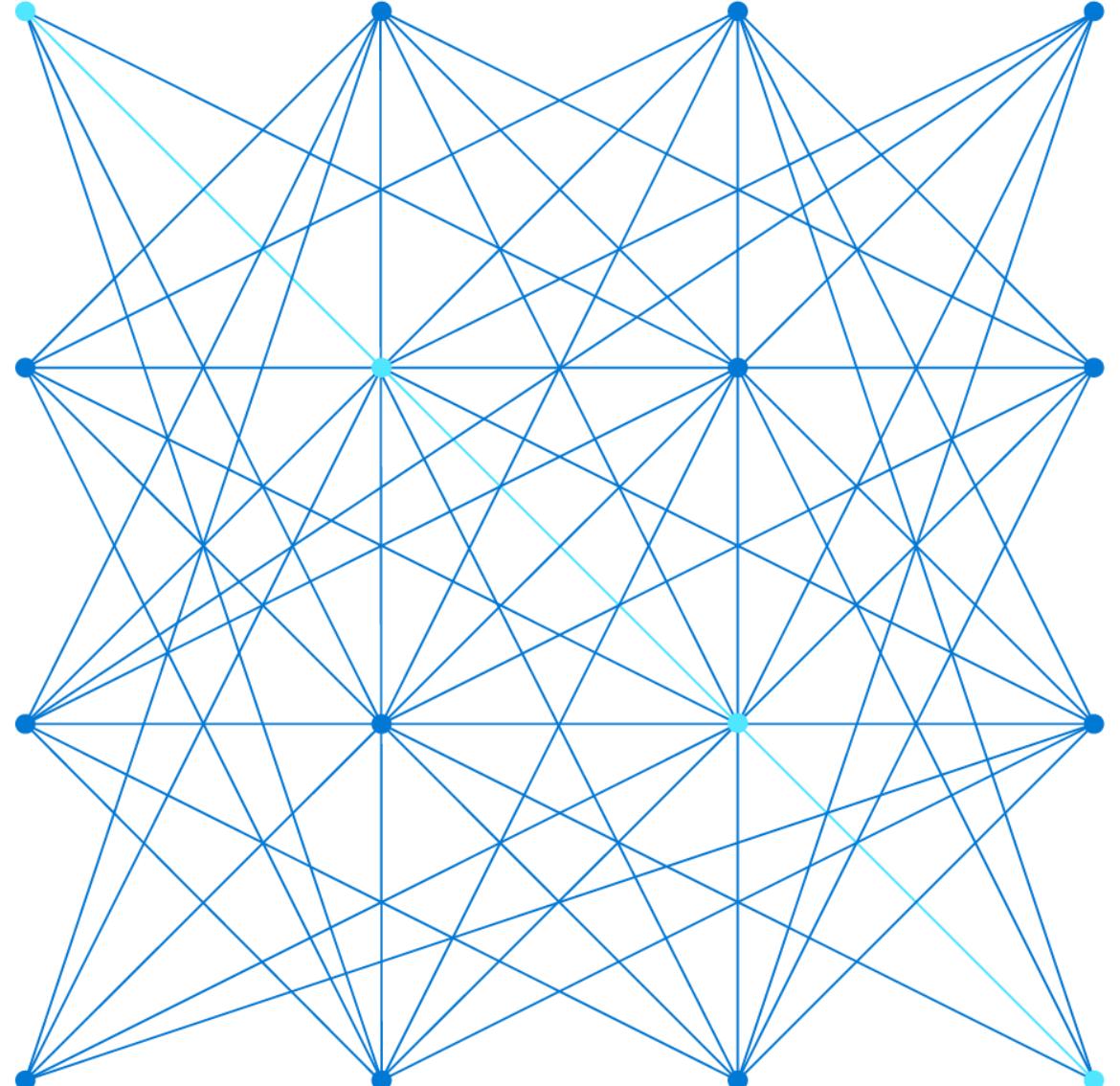
The screenshot shows the Microsoft Purview 'New protection policy' wizard. The top navigation bar includes 'Microsoft Purview PREVIEW'. Below it, the breadcrumb trail reads 'Policies > New protection policy'. On the left, a vertical checklist shows five steps: 'Name and description' (checked), 'What to detect' (checked), 'Where to apply' (checked), 'How to protect' (checked), and 'Mode' (unchecked). The current step, 'Review and finish', is highlighted with a blue dot. To the right, the 'Review your policy settings' section displays the configuration details:

- Name:** Protect Highly Confidential data in SQL database
[Edit](#)
- What to detect:** Data labeled as "Highly Confidential"
[Edit](#)
- Where to apply:** Azure SQL server: 1 server
[Edit](#)
- How to protect:** Deny read access for everyone except 1 user
[Edit](#)
- Mode:** On
[Edit](#)

Below this, a note says: 'Make sure your settings look good. Edit to update any if needed, and then select 'Create' to finish.'

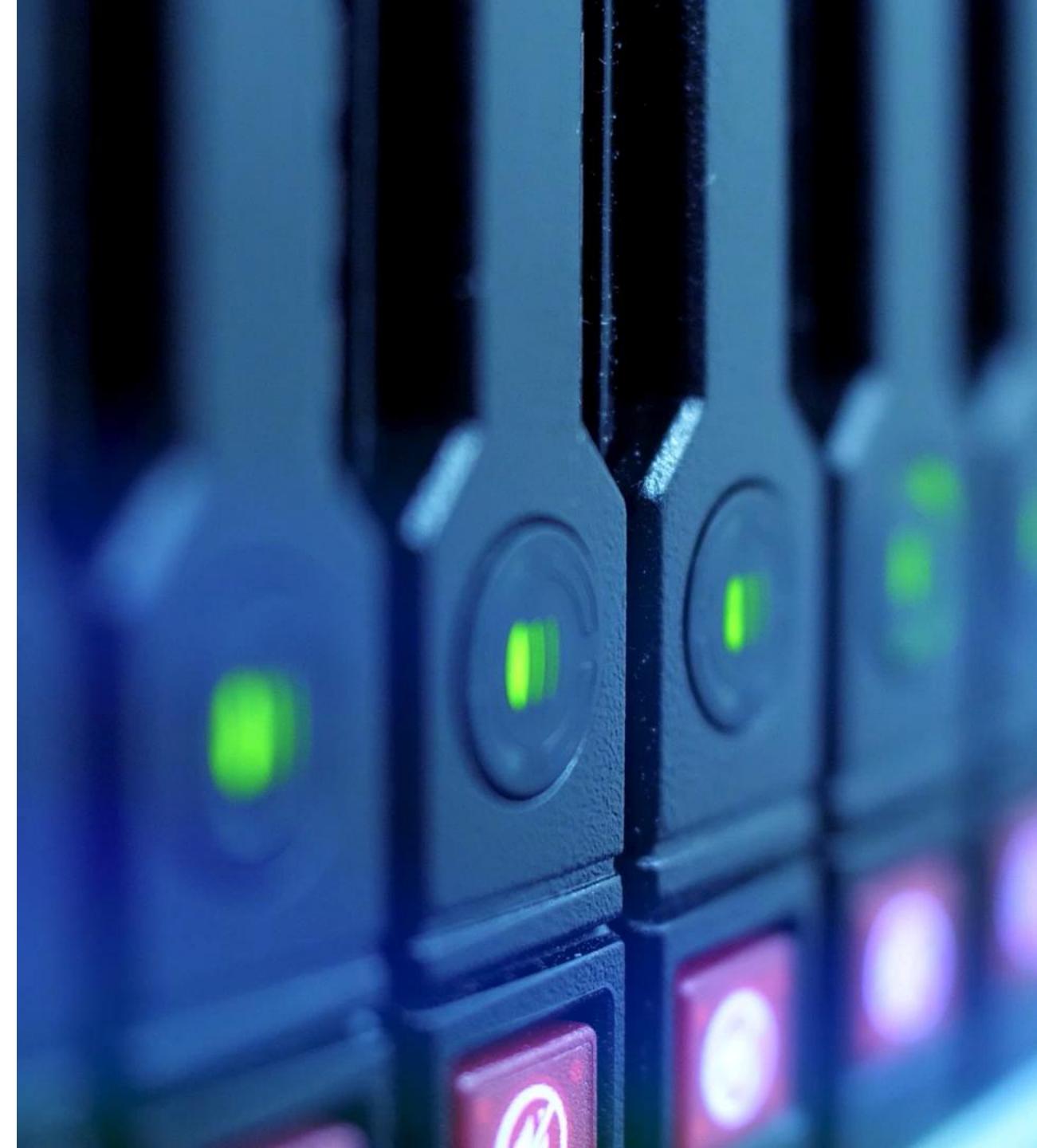
Discovering Threats

For Azure SQL DBAs



Do not rest too much your watchful eye:

- Be observant, do not limit your focus just on usual SQL Server sources of information – go beyond just SQL Server DMVs, Extended Events, Error Logs, DBCCs, etc
- Use good monitoring software with alerting
- Consider acquiring SIEM (Security information and event management)
- Follow the Well Architected Framework principles.
- Take advantage of the Azure recommendations (Policy, Advisor, etc)





For more details on observability, attend session “**Becoming an Azure SQL DBA – Performance Monitoring, Tuning and Alerting**” on Thu, 7th of Nov 2024 at 11:30 AM – 12:30 PM in Rooms 345-346

Azure SQL platform observability sources

- Azure Service Health
- Resource Health
- Activity Log
- Azure Monitor
- Diagnostic Settings (Logs)
- Azure SQL Audit
- Azure Advisor
- Microsoft Entra reports

Value proposition of SQL Auditing

Gain insight into database events and streamline compliance-related tasks

Helps you to understand database activity and gain insight into discrepancies and anomalies that could indicate business concerns or suspected security violations.



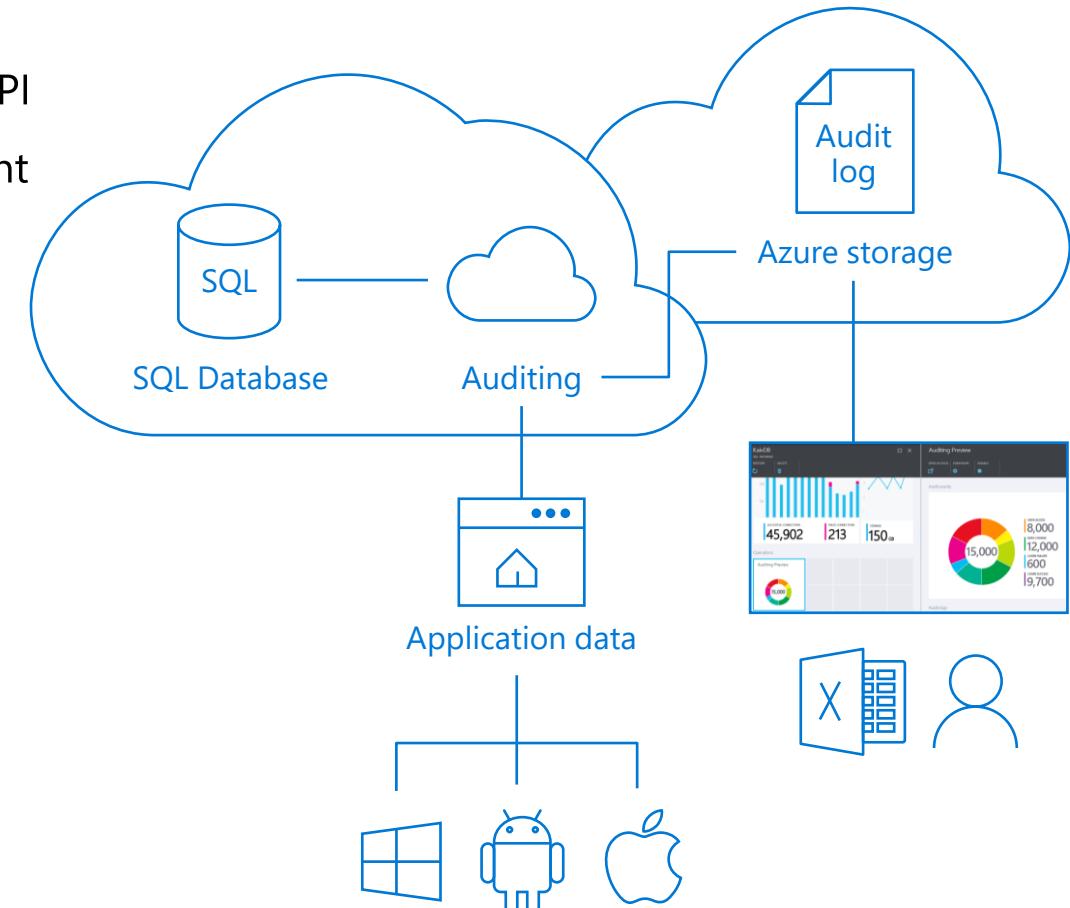
Azure SQL Database & Azure SQL MI Auditing

Gain insight into database events and streamline compliance-related tasks

- ✓ Configurable audit policy via the Azure portal and standard API
- ✓ Audit logs reside in your Azure Storage account, or can be sent directly to Log Analytics or Event Hub
- ✓ Azure portal viewer and SSMS for analysis of audit log
- ✓ Compatible with SQL Server box auditing, including high granularity in defining audit policy

Benefits:

- Transparency into workforce activities.
- Anomaly detection.
- Trend visualization.
- Data loss prevention.



Microsoft Defender for Databases

for Azure SQL DBA

Value proposition of Microsoft Defender for SQL



Discover and mitigate potential database vulnerabilities



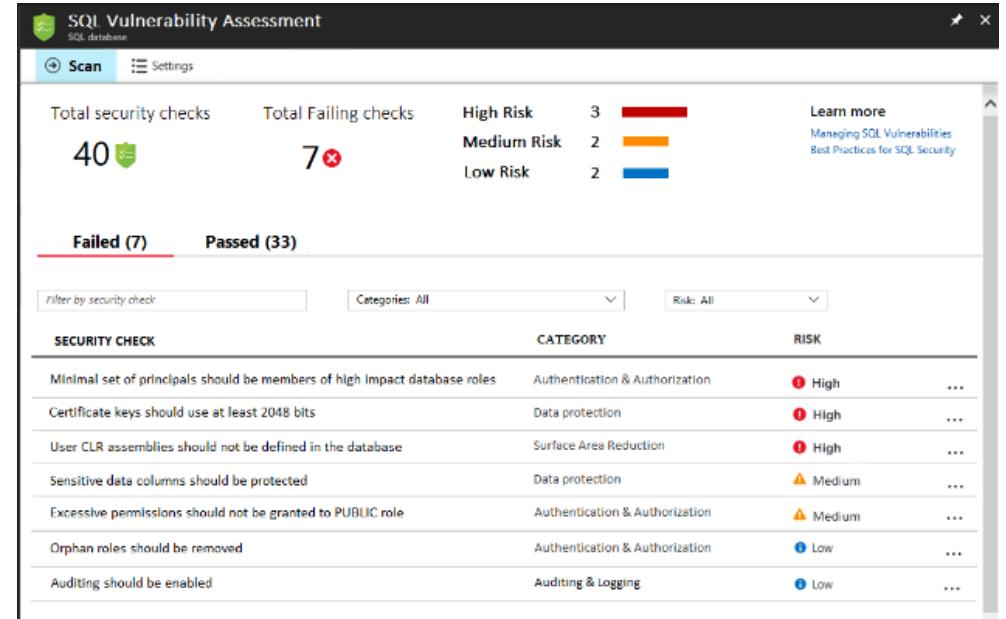
Advanced threat protection



Alerts you to anomalous activities that might be an indication of a threat to your databases.

Vulnerability Assessment

- Get visibility
 - Discover sensitive data and potential security holes
- Remediate
 - Actionable remediation and security hardening steps
- Customize
 - Baseline policy tuned to your environment, allowing you to focus on deviations
- Report
 - Pass internal or external audits to facilitate compliance



Azure SQL Database



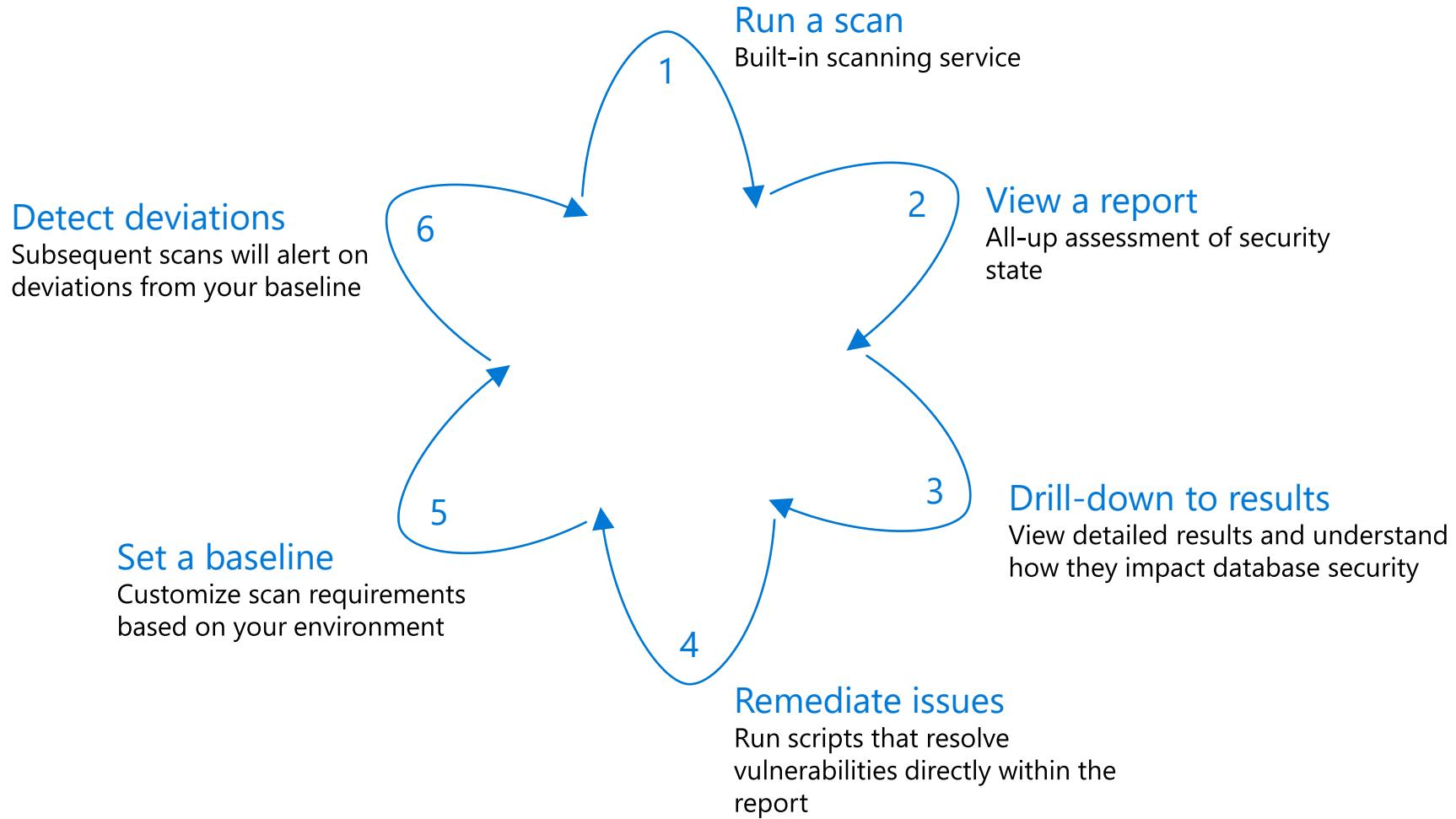
Vulnerability Assessment

Identifies, tracks, and resolves SQL security vulnerabilities



Developer/DBA

Using Vulnerability Assessment



SQL Advanced Threat Protection

- Receive an alert
 - Suspicious database activities
 - Potential vulnerabilities
 - SQL injection attacks
 - Anomalous database access and queries patterns
- Details of suspicious activity
 - Recommend action on how to investigate and mitigate the threat
- Recommended to enable auditing

Azure SQL database

Potential exploitation of application code vulnerability to SQL Injection was detected. This may indicate a SQL Injection attack on database 'samplecrmwedemo'.

View recent SQL alerts

Activity details

Severity: High

Subscription ID:

Subscription Name: DS-THREATDETECTION_DEMO_TOMERR_R&D_60843

Server:

Database: Security alerts

IP address: Filter Security Center

Principal Name:

Application:

Date:

Threat ID:

Potential ca

Investigation:

Remediation:

DESCRIPTION

Potential SQL Injection

Potential SQL Brute Force attempt

Attempted logon by a potentially harmful application

A possible vulnerability to SQL Injection

Logon from an unusual location

Logon by an unfamiliar principal

General information

DESCRIPTION: Potential SQL Injection was detected on your database samplecrmwedemo on server ronmatwedemo

DETECTION TIME: Sunday, 13 May 2018, 3:09:12 pm

SEVERITY: High

STATE: Active

ATTACKED RESOURCE: samplecrmwedemo

SUBSCRIPTION: Microsoft

DETECTED BY: Microsoft

ACTION TAKEN: Detected

ENVIRONMENT: Azure

RESOURCE TYPE: SQL Server

SERVER: dev1

DATABASE:

IP ADDRESS:

PRINCIPAL NAME: .Net SqlClient Data Provider

APPLICATION:

VULNERABLE STATEMENT: SELECT * FROM sqli_users WHERE username = ''OR 1 = 1--' AND password = 'dfdfdfafaf'

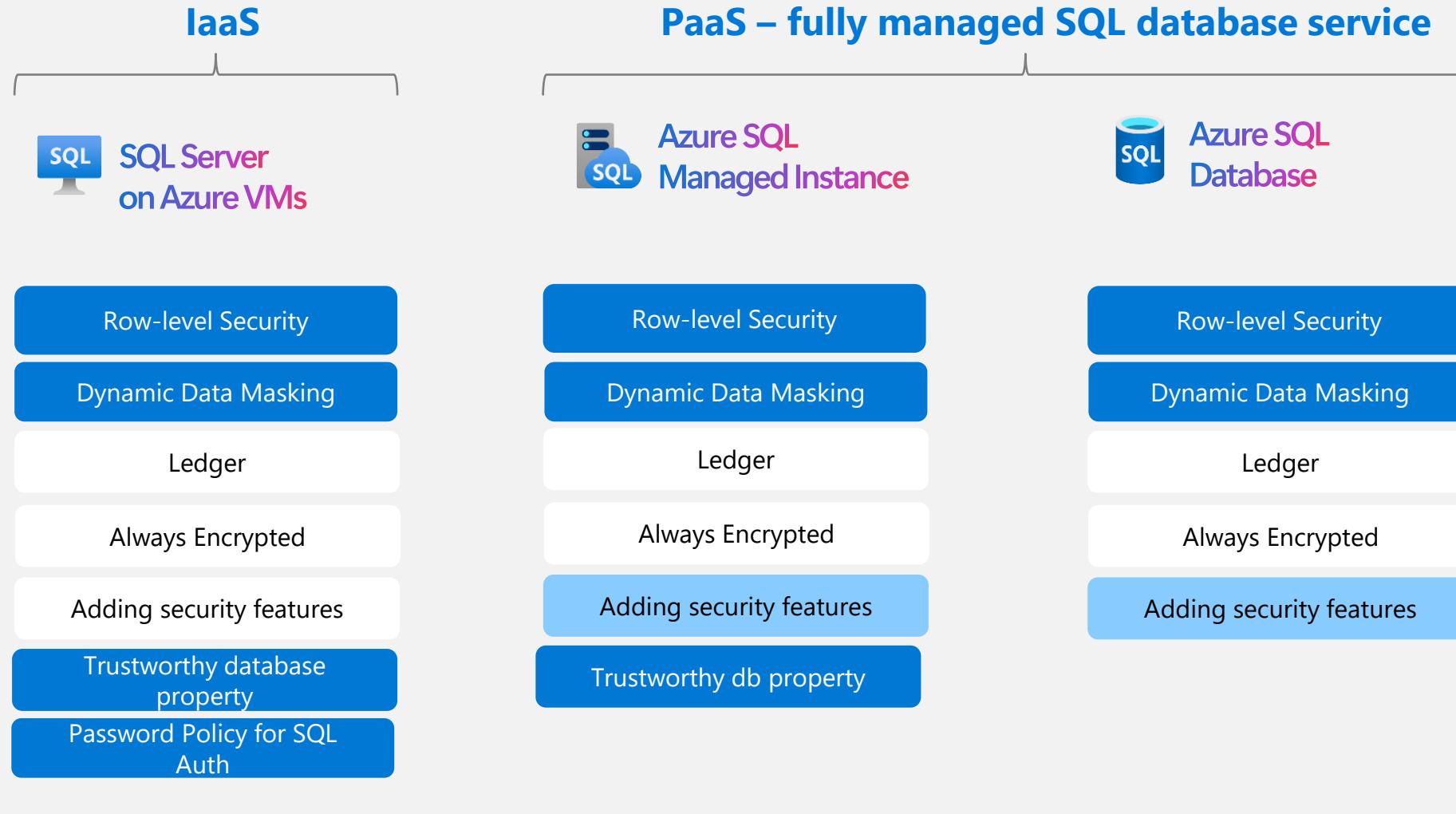
THREAT ID: 1

Remediation steps

INVESTIGATION STEPS: View the vulnerable SQL statement

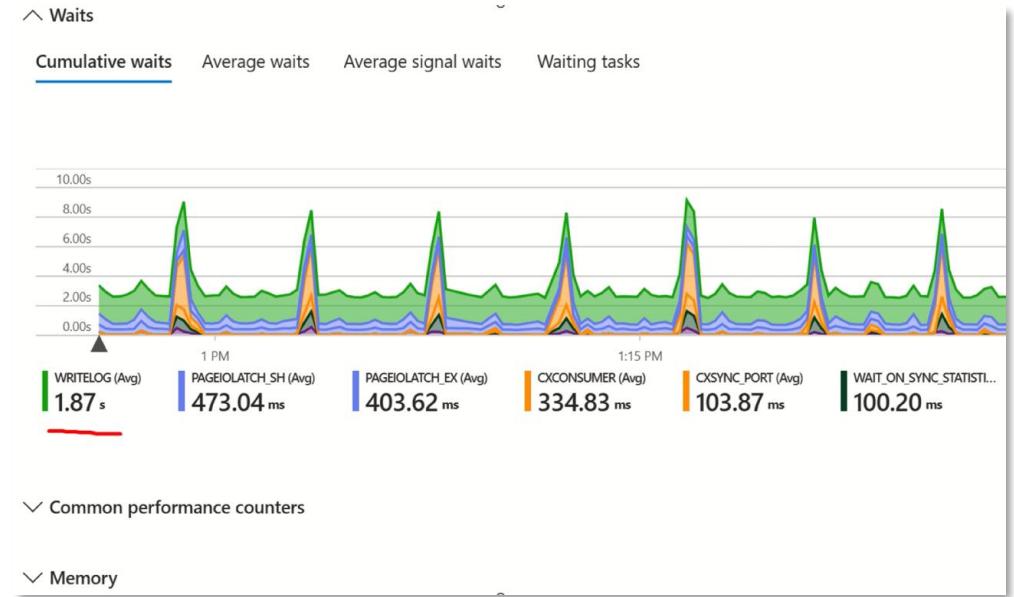
REMEDIATION STEPS: Read more about SQL Injection threat and how to fix the vulnerable application code.

Other Security technologies



Database Watcher (Preview)

- New tool to help you manage SQL resources in Azure
- Built-in native Azure monitoring solution for SQL resources



The screenshot shows the 'Active sessions' section of the Azure Database Watcher dashboard. It lists various sessions with details such as Request duration, Session ID, Status, Command, Input buffer, Blocked by, Blocker, Index suggestions, CPU usage, Logical reads, DOP, Wait type, and Wait time. One session is highlighted in yellow: 14.12:52:05.171, Session ID 105, suspended, SELECT, (@source nvarchar(256))SELECT The table also includes a 'Selected session details' section with 'Input buffer text' and 'Statement text' fields.

Request duration	Session ID	Status	Command	Input buffer	Blocked by	Blocker	Index suggestions	CPU	Logical reads	DOP	Wait type	Wait time
14.12:52:05.171	105	suspended	SELECT	(@source nvarchar(256))SELECT ...				0us	0	1	XE_LIVE_TARGET_TV	0.00:03:37.817
14.12:52:04.985	109	suspended	SELECT	(@source nvarchar(256))SELECT ...				0us	0	1	XE_LIVE_TARGET_TV	0.00:05:49.61
0.00:00:00.011	139	idle	SELECT	(@P1 int,@P2 int,@P3 int,@P4 in...				90.909us	11.636	1		
0.00:00:00.010	145	idle	COMMIT TRANSACTION	(@P1 int,@P2 int,@P3 datatype2...				400us	25.9	1		
0.00:00:00.007	132	idle	DELETE	(@P1 int,@P2 int,@P3 int,@P4 in...				428.571us	35.143	1		
0.00:00:00.006	138	suspended	COMMIT TRANSACTION	(@P1 int,@P2 int,@P3 int,@P4 in...				166.667us	27.667	1	HADR_SYNC_COMMIT	0.00:00:00.002
0.00:00:00.004	135	suspended	COMMIT TRANSACTION	(@P1 int,@P2 int,@P3 datatype2...				0ms	11	1	HADR_SYNC_COMMIT	0.00:00:00.003
0.00:00:00.004	143	suspended	COMMIT TRANSACTION	(@P1 int,@P2 int,@P3 int,@P4 in...				500us	66	1	HADR_SYNC_COMMIT	
0.00:00:00.003	144	running	UPDATE	(@P1 int,@P2 int,@P3 int,@P4 in...				1ms	81.333	1		

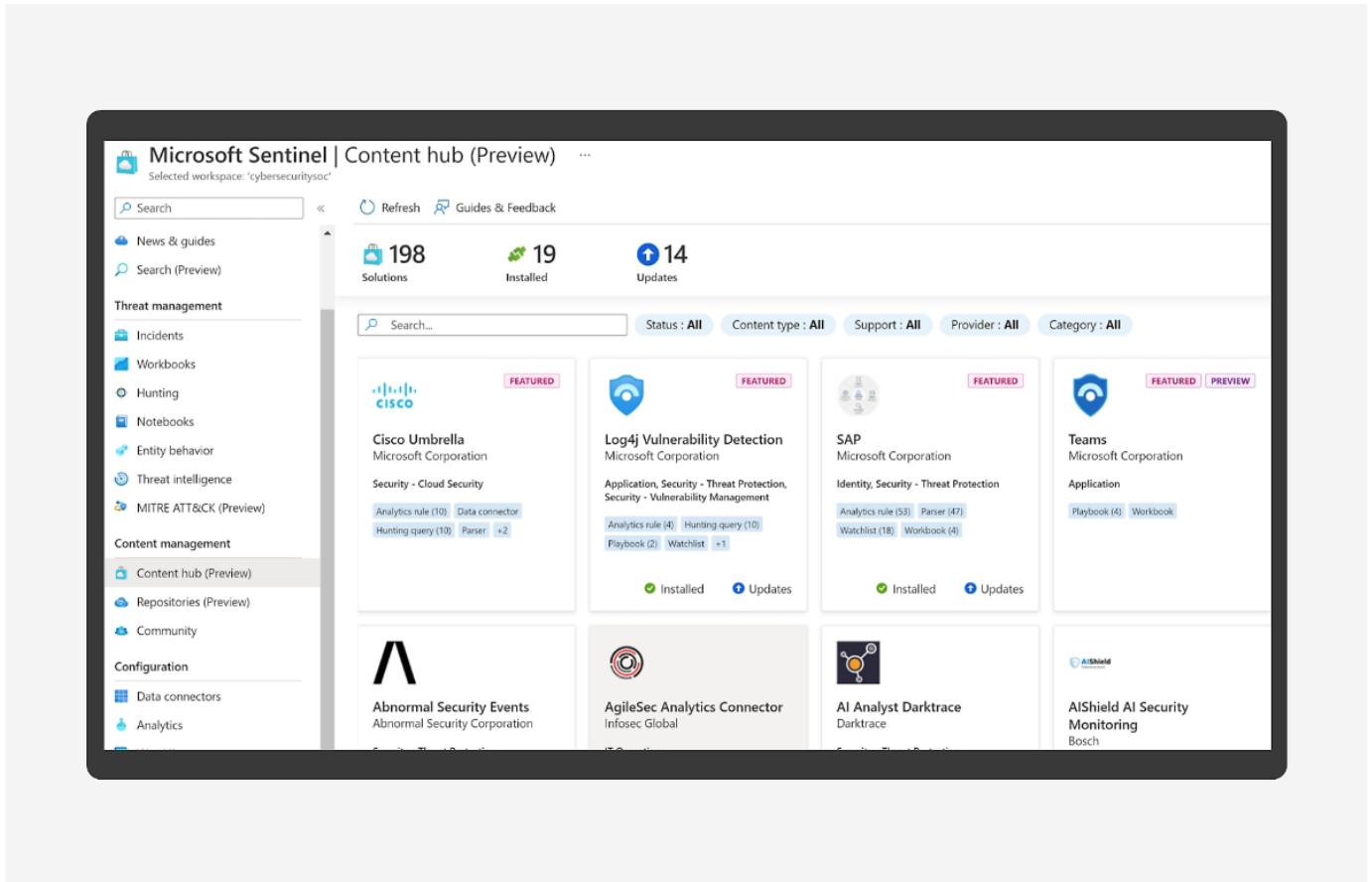
Microsoft Sentinel

Collect data at cloud scale

Stay ahead of cyberthreats

Streamline investigation with incident insights

Accelerate response and save time by automating common tasks

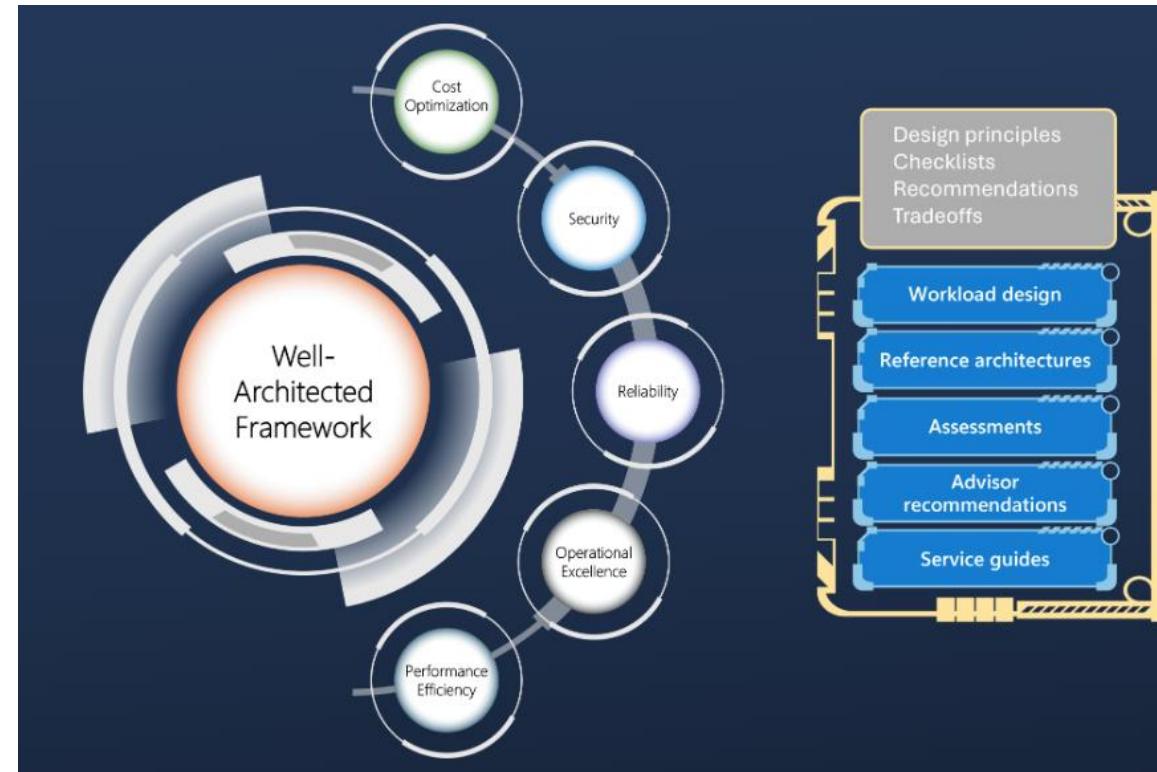


Well Architected Framework

The Azure Well-Architected Framework is a set of quality-driven tenets, architectural decision points, and review tools intended to help solution architects build a technical foundation for their workloads.

The Azure Well-Architected Framework is a design framework that can improve the quality of a workload by helping it to:

- **Be resilient, available, and recoverable.**
- **Be as secure as you need it to be.**
- **Deliver a sufficient return on investment.**
- **Support responsible development and operations.**
- **Accomplish its purpose within acceptable timeframes.**



Azure Advisor



Advisor is a digital cloud assistant that helps you follow best practices to optimize your Azure deployments. It analyzes your resource configuration and usage telemetry and then recommends solutions that can help you improve the cost effectiveness, performance, reliability, and security of your Azure resources.

•**Reliability:** To ensure and improve the continuity of your business-critical applications.

•**Security:** To detect threats and vulnerabilities that might lead to security breaches.

•**Performance:** To improve the speed of your applications.

•**Cost:** To optimize and reduce your overall Azure spending

•**Operational excellence:** To help you achieve process and workflow efficiency, resource manageability, and deployment best practices.

Reliability

Total recommendations: 5

Recommendations by impact: 2 High impact, 2 Medium impact, 1 Low impact

Impacted resources: 56

Impact ↑	Description	Potential benefits	Impacted resources	Last updated
High	Use Availability zones for better resiliency and availability	Usage of zonal VMs protect your apps from zonal outage in any other...	5 Virtual machines	3/6/2024, 11:00 AM
High	Create an Azure Service Health alert	Stay informed about issues and advisories across 4 areas (Service...	1 Subscription	3/6/2024, 04:25 PM
Medium	Enable Cross Region Restore for your recovery Services Vault	As one of the restore options, Cross Region Restore (CRR) allows you t...	37 Recovery Services va...	3/6/2024, 06:14 PM
Medium	Use NAT gateway for outbound connectivity	Prevent outbound connection failures with NAT gateway	8 Virtual networks	3/6/2024, 04:38 PM
Low	Use Service Bus premium tier for improved resilience	Service Bus premium tier offers better resiliency with CPU and...	5 Service bus namespaces	3/6/2024, 06:34 PM

Showing 1 - 5 of 5 results.

Are these recommendations helpful?

Overview

Subscription equals 27 of 38 selected | Recommendation Status equals Active | Resource Group equals All | Type equals All | Add filter

Category	Score	Recommendations	Impacted resources
Cost	100%	3 Recommendations	0 High impact, 3 Medium impact, 0 Low impact
Security	54%	5 Recommendations	2 High impact, 3 Medium impact, 0 Low impact
Reliability	92%	51 Impacted resources	0 High impact, 2 Medium impact, 1 Low impact
Operational excellence	78%	40 Impacted resources	0 High impact, 2 Medium impact, 1 Low impact

Tips & tricks

- You can customize Advisor to process recommendations for resources that matter to you the most.
- Explore workbooks in Advisor gallery to get additional optimization insights.
- Add firewall rules for MySQL Flexible Server

Get started in Advisor

Advisor provides Microsoft best practices to help you improve your workloads, identify cost saving opportunities or explore best practices.

Get started

In Advisor help!

Requirements for Azure SQL DBAs in the security space:

- Be up-to-date with the latest in Azure frameworks and services
- Ensuring solution's compliance
- Having network control proficiency is a must for securing your data
- Proactively monitor and react on the potential threats

We give you the tools

But it is YOU who need to

- Select the destination
- Make a good plan
- Prepare the alternatives
- Ensure that every piece of the solution is communicating well and is secure



Additional Resources



Azure free online courses

<https://learn.microsoft.com/training/browse/>



COURSE

Microsoft Azure Fundamentals

Course AZ-900T00-A: Microsoft Azure Fundamentals

Describe features and tools for managing and deploying Azure resources

22 min • Module • 6 Units

Describe monitoring tools in Azure

13 min • Module • 6 Units

Feedback

Describe Azure identity, access, and security

43 min • Module • 11 Units

Feedback

Describe Azure compute and networking services

1 hr 8 min • Module • 14 Units

Feedback

Microsoft Azure AI Fundamentals: AI Overview

3 hr 7 min • Learning Path • 3 Modules

Describe cloud service types

12 min • Module • 6 Units

Feedback

Describe the core architectural components of Azure

48 min • Module • 9 Units

Feedback

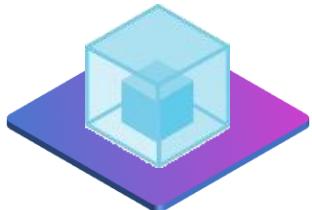
Experience Azure SQL for free

Azure SQL Managed Instance



aka.ms/freesqlMI

What's included



- **1 instance** per Azure subscription
- **4 or 8 vCores** of GP compute
- **750 vCore hours** per month
- **64 GB data** storage
- **64 GB backup** storage

Use it for 12 months



- Use this free offer to support your migration proof of concepts for **12 months**.

You're in control



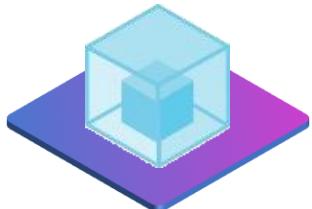
- Optimize your monthly available vCore hours by **stopping** and **starting** the instance when necessary.

Azure SQL Database



aka.ms/SQLfreeoffer

What's included



- **1 Azure SQL Database** per Azure subscription
- **100,000 vCore seconds** per month.
- **32 GB data** storage
- **32 GB backup** storage

No time limits



- Apply this free offer for the **life** of your **subscription**.

Need more? No problem.



- Stick with the default **auto-pause** option or continue usage for additional charges.

Your feedback is important
to us



Evaluate this session at:

www.PASSDataCommunitySummit.com/evaluation

Thank you

Please Free! free to reach out to us.



Niko Neugebauer

nneugebauer@microsoft.com



Dani Ljepava

daniel@microsoft.com



Erin Stellato

erinstellato@microsoft.com



Pam Lahoud

pamela@microsoft.com

Other Azure services that are important and relevant for Azure SQL DBAs

Microsoft Entra Id



Azure Blob Storage



Azure Key Vault



Azure Key Vault HSM



Azure Key Vault and Managed HSM



Azure Key Vault (AKV)

- Azure Key Vault is one of several key management solutions in Azure, and helps solve the following problems:
- **Secrets Management** - Azure Key Vault can be used to Securely store and tightly control access to tokens, passwords, certificates, API keys, and other secrets
- **Key Management** - Azure Key Vault can be used as a Key Management solution. Azure Key Vault makes it easy to create and control the encryption keys used to encrypt your data.
- **Certificate Management** - Azure Key Vault lets you easily provision, manage, and deploy public and private Transport Layer Security/Secure Sockets Layer (TLS/SSL) certificates for use with Azure and your internal connected resources.

AKV Managed HSM

Azure Key Vault Managed HSM (**Hardware Security Module**) is a fully managed, highly available, single-tenant, standards-compliant cloud service that enables you to safeguard cryptographic keys for your cloud applications, using **FIPS 140-2 Level 3 validated HSMs**. It is one of several key management solutions in Azure.

Generate (or import using BYOK) keys and use them to encrypt your data at rest in Azure services such as Azure Storage, Azure SQL, etc.

Supports cross region replication of key material without service failover.