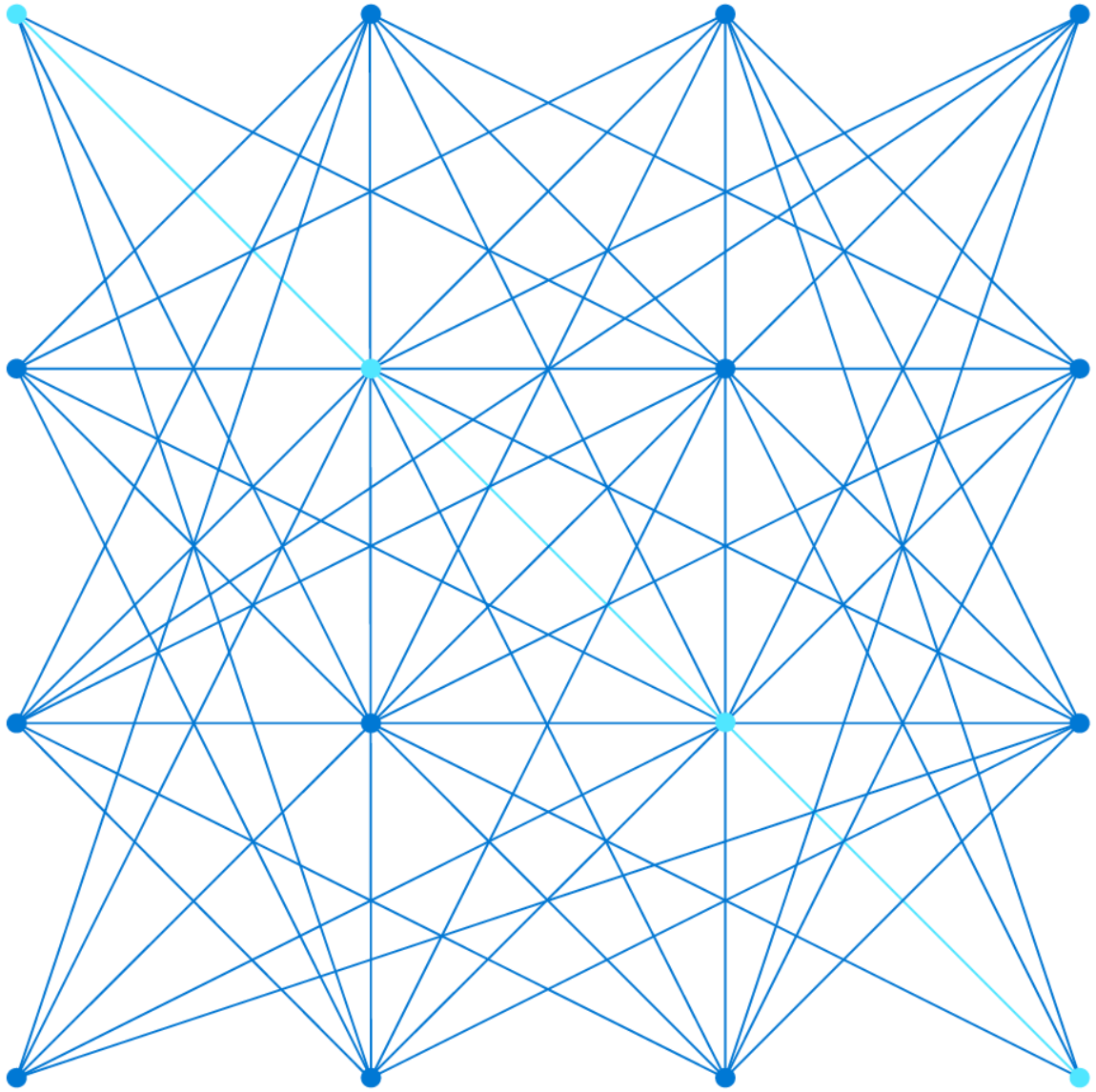
Microsoft Azure

AZ-500

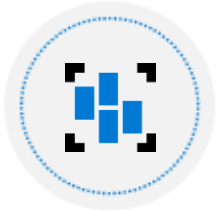
Microsoft Azure Security Technologies



AZ-500 Agenda

Learning Path 1 **Identity and Access**

Learning Path 2 **Implement Platform Protection**



Learning Path 3 **Data and Application Security**

Learning Path 4 **Security Operations**

Learning Path: Data and Application Security

Azure Key Vault

soft KV

hard KV

Storage Security

Database Security

SQL

Module Labs

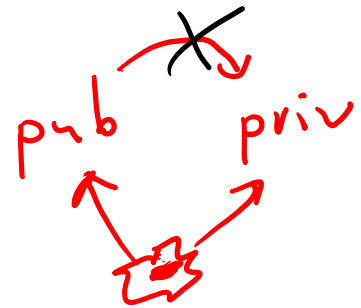
OR

Bring your own key!

Azure Key Vault

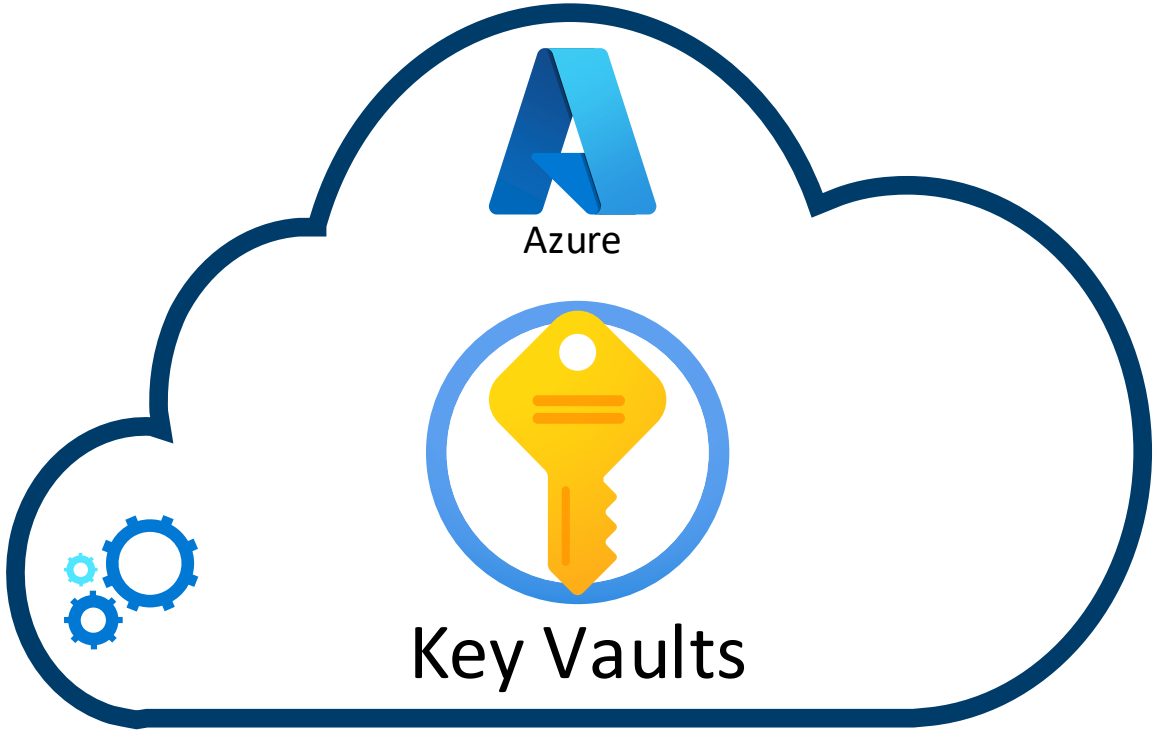
Azure Key Vault

- Azure Key Vault Features
- Key Vault Access
- Key Vault Example
- Key Vault Certificates
- Key Vault Keys
- Customer Managed Keys
- Key Vault Secrets
- Key Rotation



Azure Key Vault Overview

- Increase security and control over keys and passwords
- Use Federal Information Processing Standard (FIPS) 140-2 and Level 3 validated hardware security modules (HSMs)
- Create and import encryption keys in minutes
- Reduce latency with cloud scale and global redundancy
- Applications have no direct access to keys
- Simplify and automate tasks for SSL/TLS certificates



Azure Key Vault is a cloud service for securely storing and accessing secrets.

Azure Key Vault Cryptographic Keys

Resource type	Key protection methods	Data-plane base URL
Vaults	Software-protected **and** HSM-protected (with Premium SKU)	https://{vault-name}.vault.azure.net
Managed HSMs	HSM-protected	https://{hsm-name}.managedhsm.azure.net

Note: Vaults also allow you to store and manage several types of objects like secrets, certificates and storage account keys, in addition to cryptographic keys.

Key Types and Protection Methods

HSM-protected keys

Key type	Vaults (Premium SKU only)	Managed HSMs
EC-HSM: Elliptic Curve key	Supported (P-256, P-384, P-521, P-256K)	Supported (P-256, P-256K, P-384, P-521)
RSA-HSM: RSA key	Supported (2048-bit, 3072-bit, 4096-bit)	Supported (2048-bit, 3072-bit, 4096-bit)
oct-HSM: Symmetric key	Not supported	Supported (128-bit, 192-bit, 256-bit)

Software-protected keys

Key type	Vaults	Managed HSMs
RSA: "Software-protected" RSA key	Supported (2048-bit, 3072-bit, 4096-bit)	Not supported
EC: "Software-protected" Elliptic Curve key	Supported (P-256, P-384, P-521, P-256K)	Not supported

Key Types and Protection Methods (cont'd)

Compliance

Key type and destination	Compliance
Software-protected keys in vaults (Premium & Standard SKUs)	FIPS 140-2 Level 1
HSM-protected keys in vaults (Premium SKU)	FIPS 140-2 Level 2
HSM-protected keys in Managed HSM	FIPS 140-2 Level 3

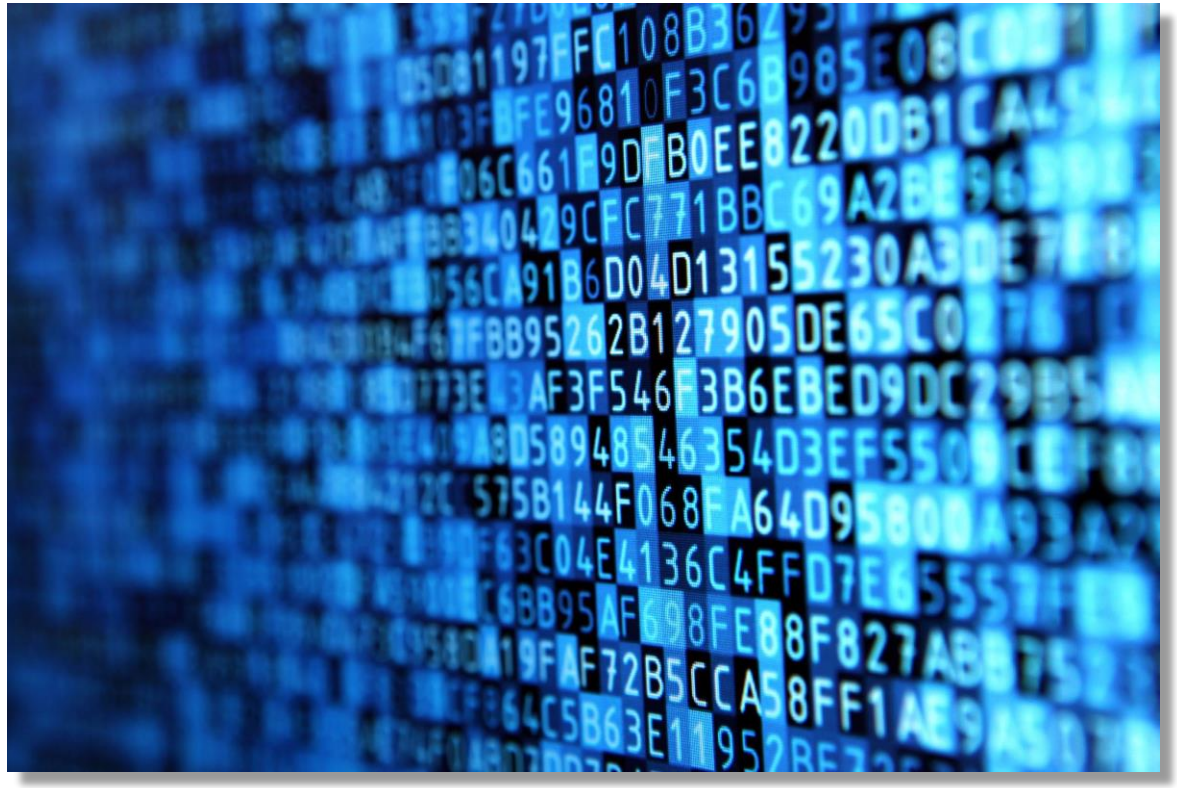
Azure Key Vault Secrets

All secrets in Key Vault are stored encrypted.

Key Vault encrypts secrets at rest with a hierarchy of encryption keys, all keys in that hierarchy are protected by modules that are FIPS 140-2 compliant.

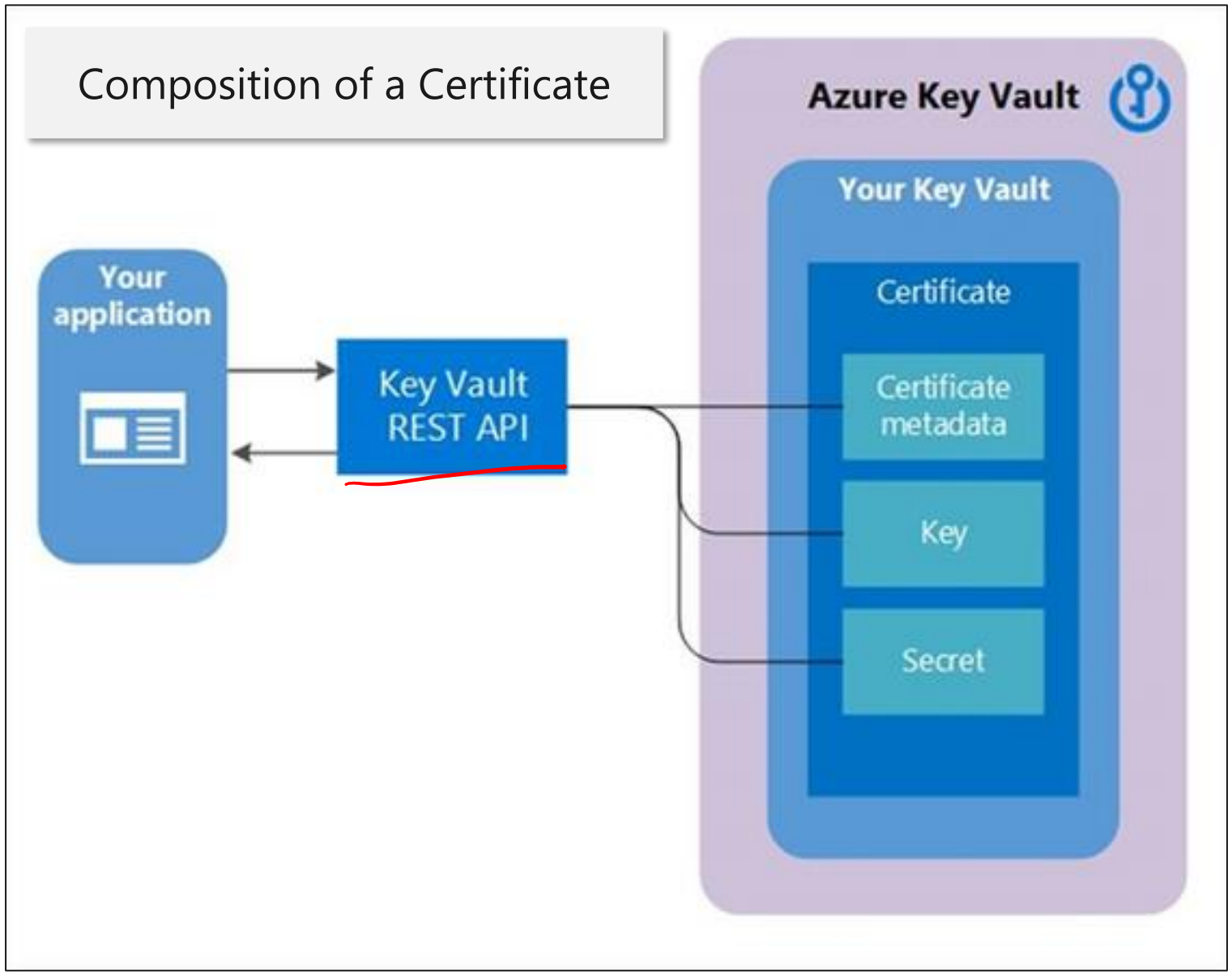
Encryption is transparent and requires no action from the user.

Azure Key Vault service encrypts your secrets when you add them and decrypts them automatically when you read them.



Azure Key Vault accepts the data, encrypts it, stores it, and returns a secret identifier ("id").

Azure Key Vault Certificates



Azure Key Vault Certificates - Exportable or Non-Exportable Key

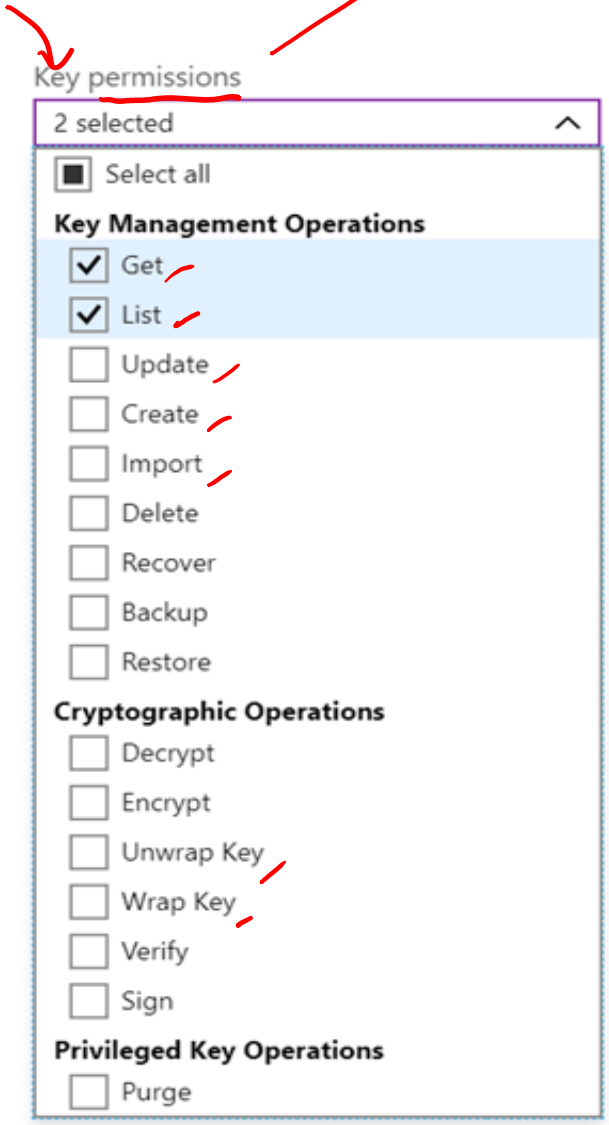
Key type	About	Security
RSA	Software-protected RSA key	FIPS-140-2 Level1
RSA-HSM	HSM-protected RSA key (Premium SKU only)	FIPS 140-2 Level 2 HSM
EC	Software-protected Elliptic Curve key	FIPS 140-2 Level 1
EC-HSM	HSM-protected Elliptic Curve key (Premium SKU only)	FIPS 140-2 Level 2 HSM

Azure Key Vault Keys (cont'd)

Soft (Key vault) and Hard (HSM) keys

Supports operations like create, delete, update, and list

Supports cryptographic operations like sign and verify, key encryption/wrapping, and encrypt and decrypt

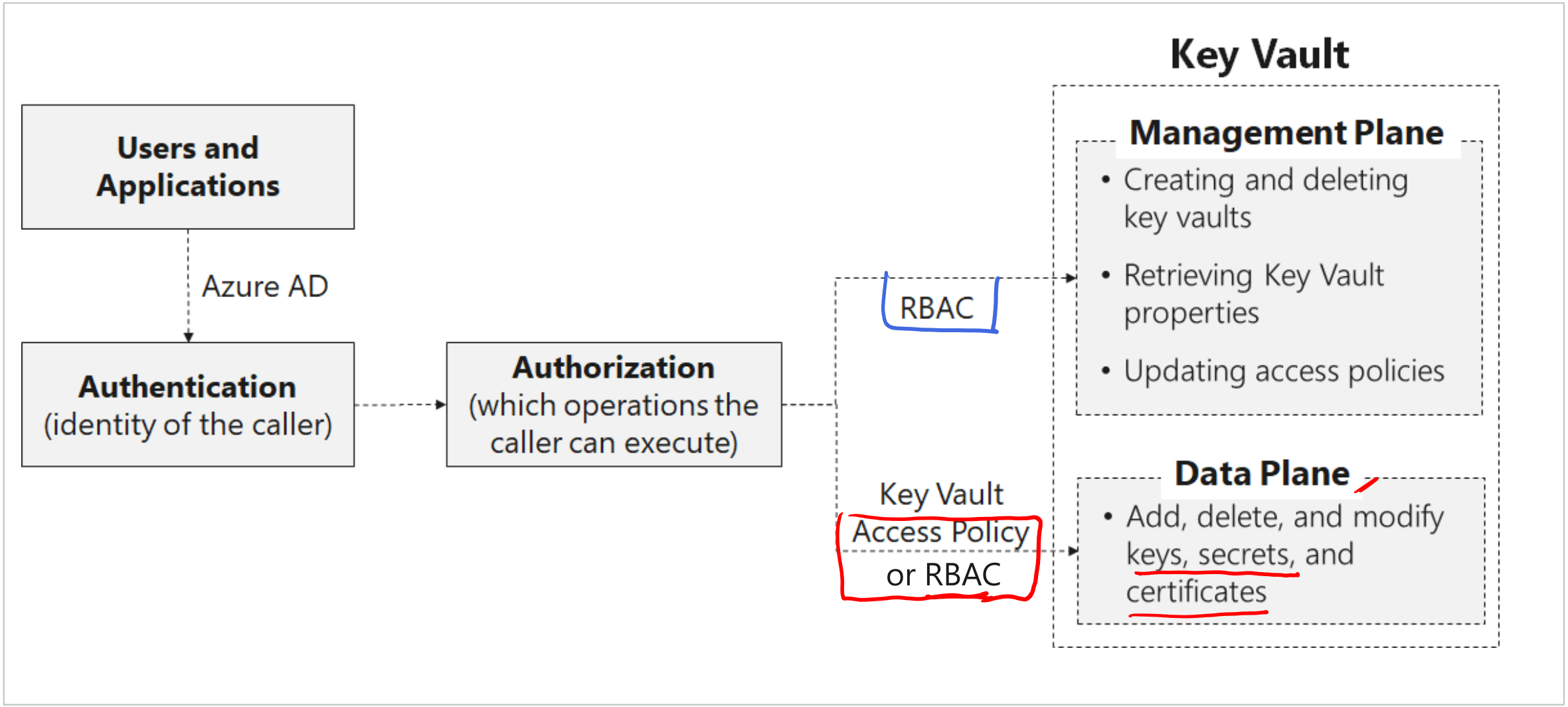


Supports secure transfer of existing keys in Bring Your Own Key (BYOK) scenarios

Premium supports HSM-protected keys

RSA and Elliptic Curve

Key Vault Access



Key Vault Example

SSL certificate for SSL

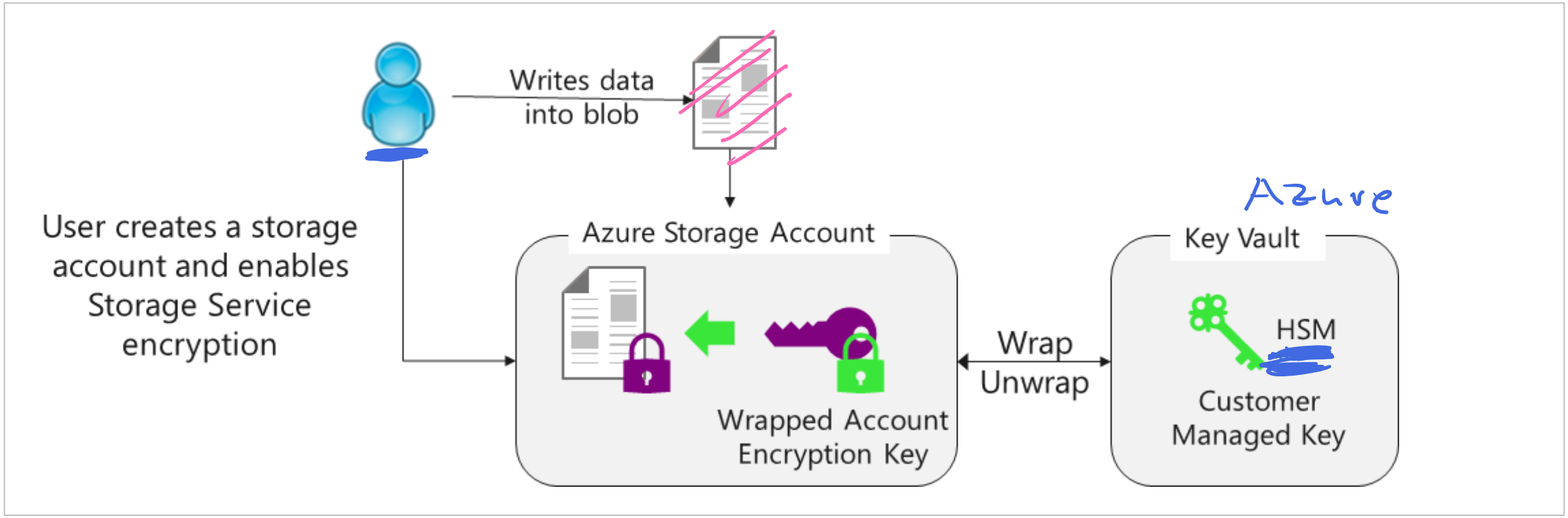
Storage key for access the Storage account

RSA 2,048-bit key for sign in operations

Bootstrap certificate for authentication to Azure AD

Role	Management Plane	Data plane
Security team	Key Vault Contributor	Keys: backup, create, delete, get, import, list, restore Secrets: all operations
Developers and operators	Key Vault deploy permission	None
Auditors	None	Keys: list Secrets: list
Application	None	Keys: sign Secrets: get

Customer Managed Keys



Update keys and secrets without affecting applications

Updates can be manual, programmatic, or automated

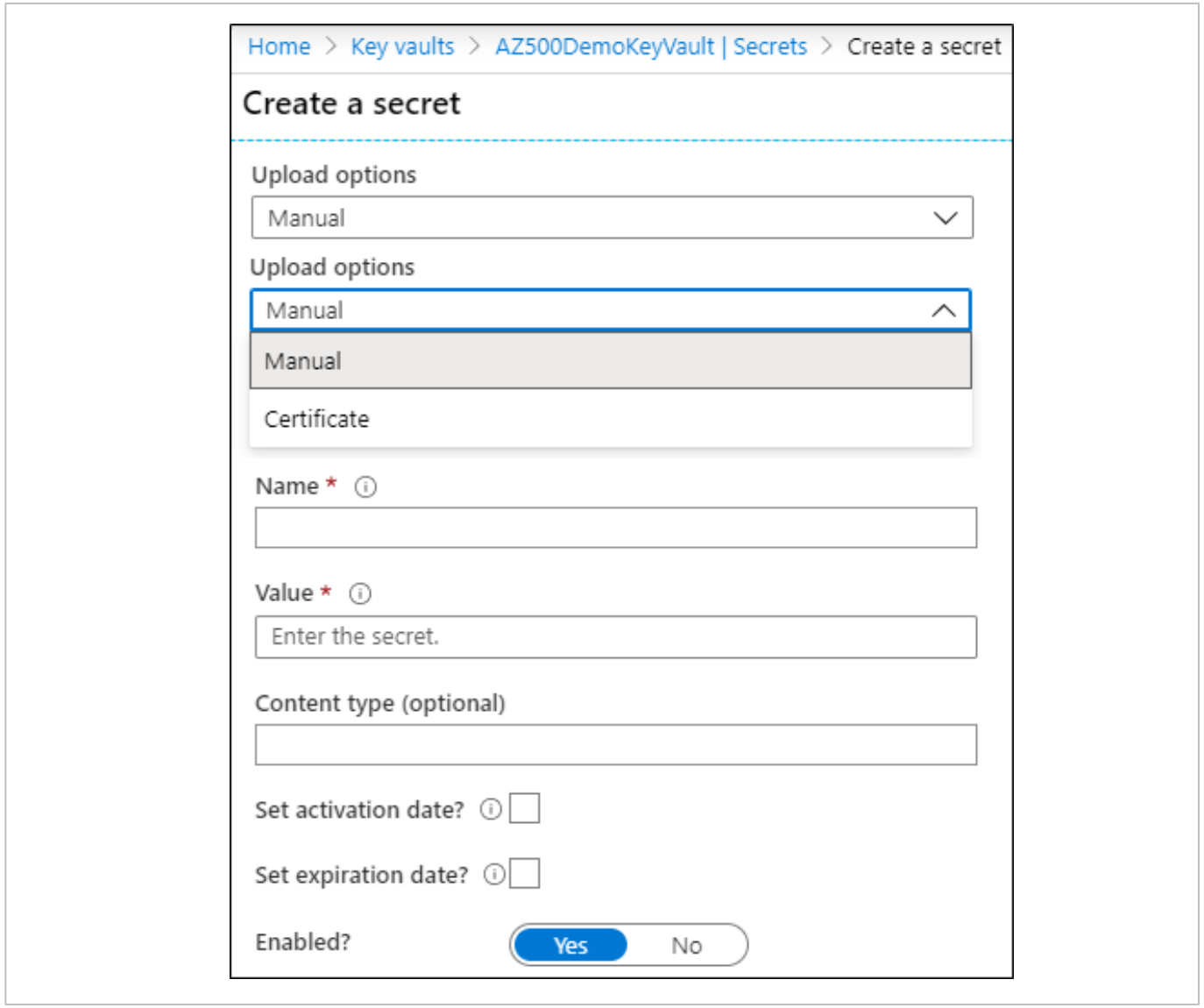
Key Vault Secrets

Name-value pair

Name must be unique in the vault

Value can be any UTF-8 string – max 25 KB in size

Manual or certificate creation

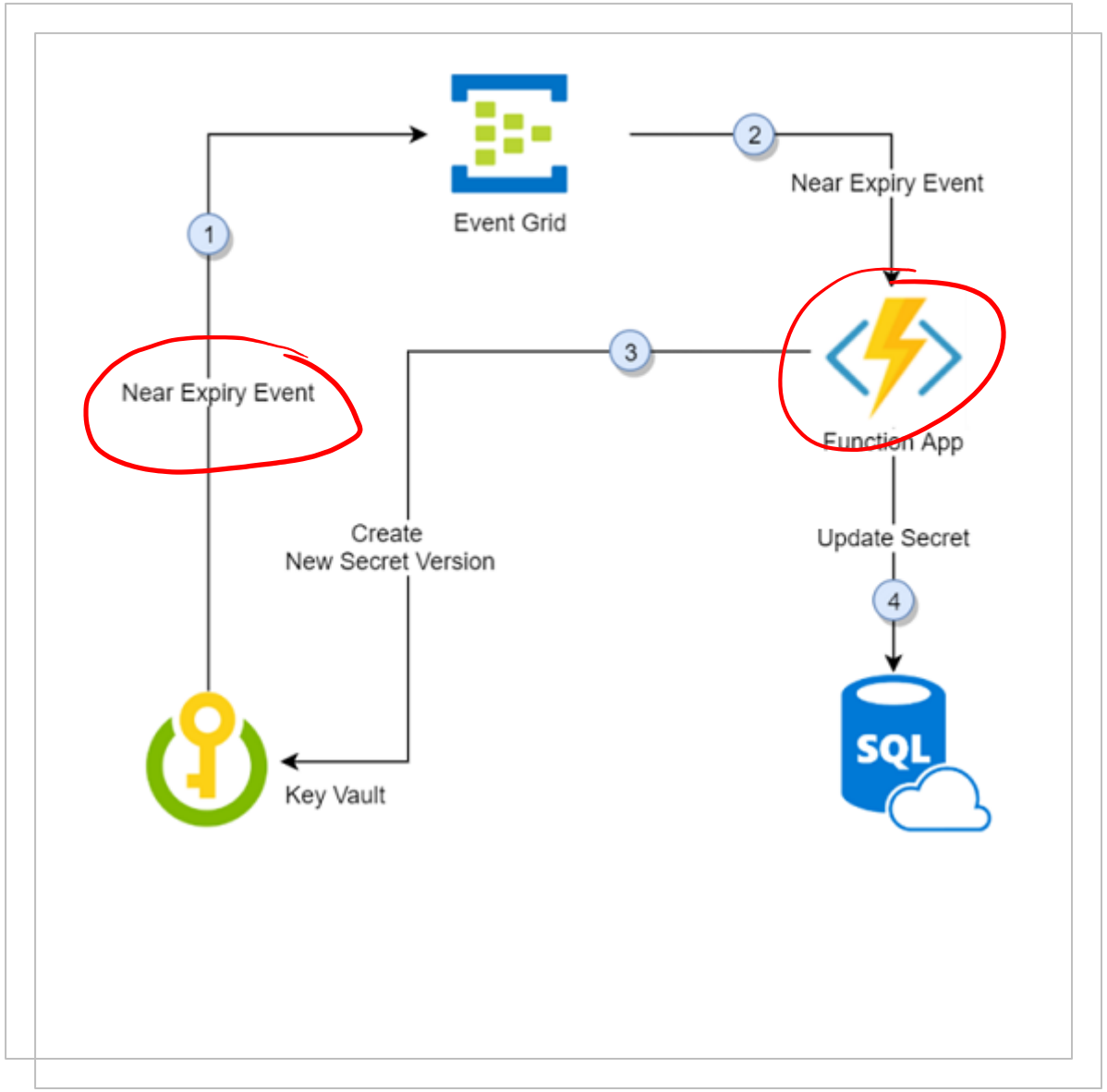


Key and Secret Rotation

Update keys and secrets without affecting your application

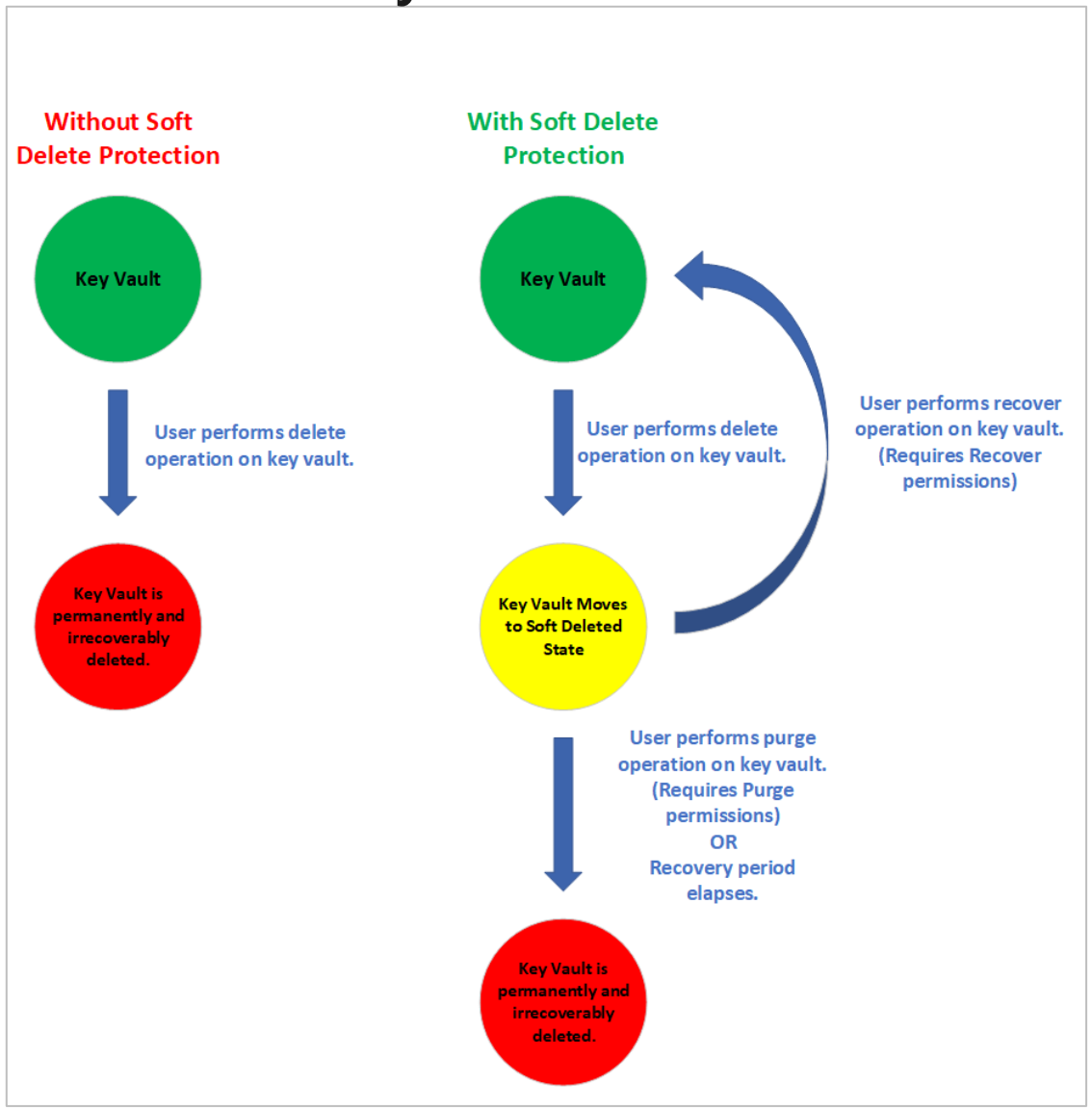
Rotate keys and secrets in several ways:

- As part of a manual process
- Programmatically with the REST API
- With an Azure Automation script

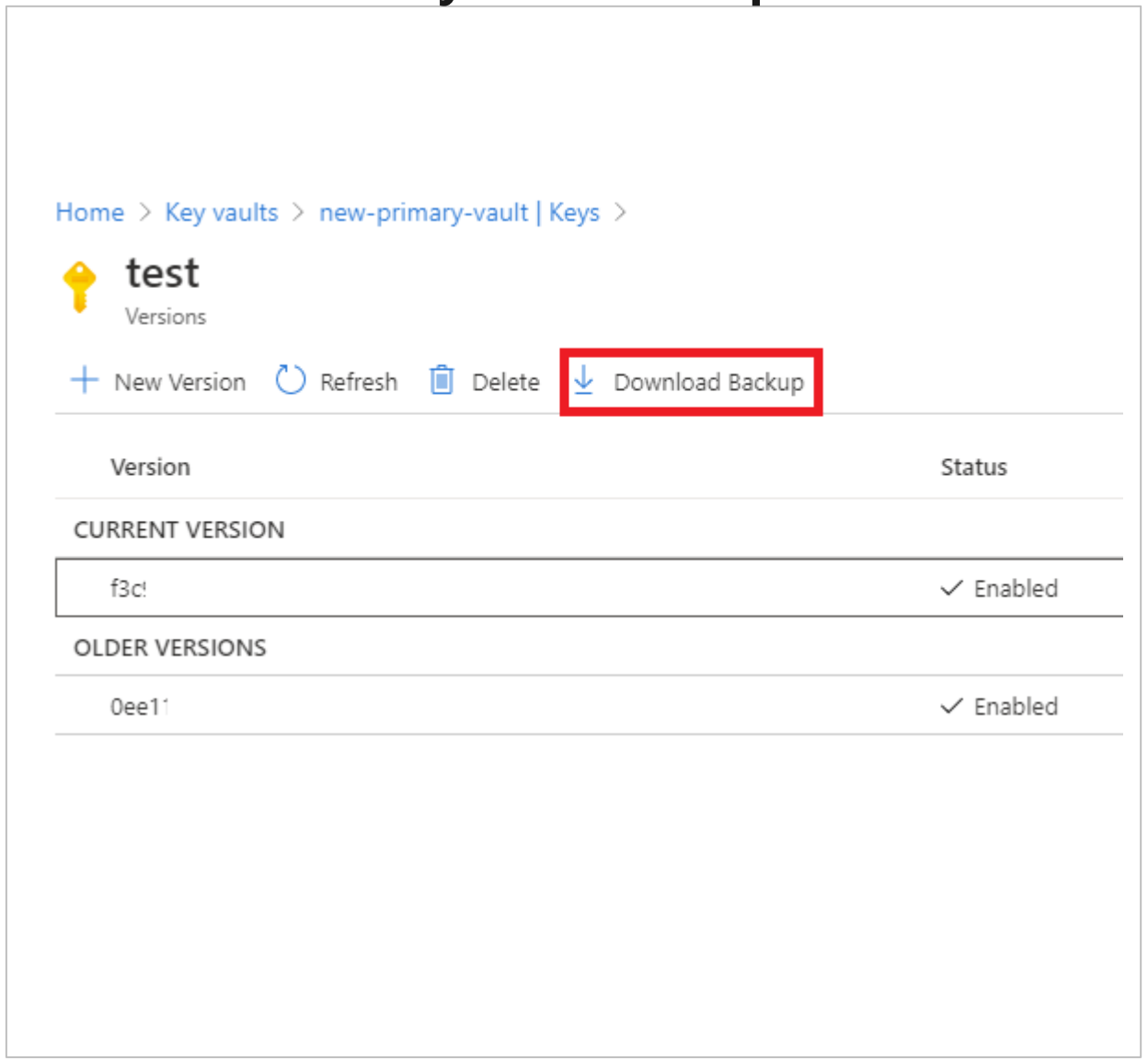


Key Vault Safety and Recovery Features

Key Vault Soft-delete

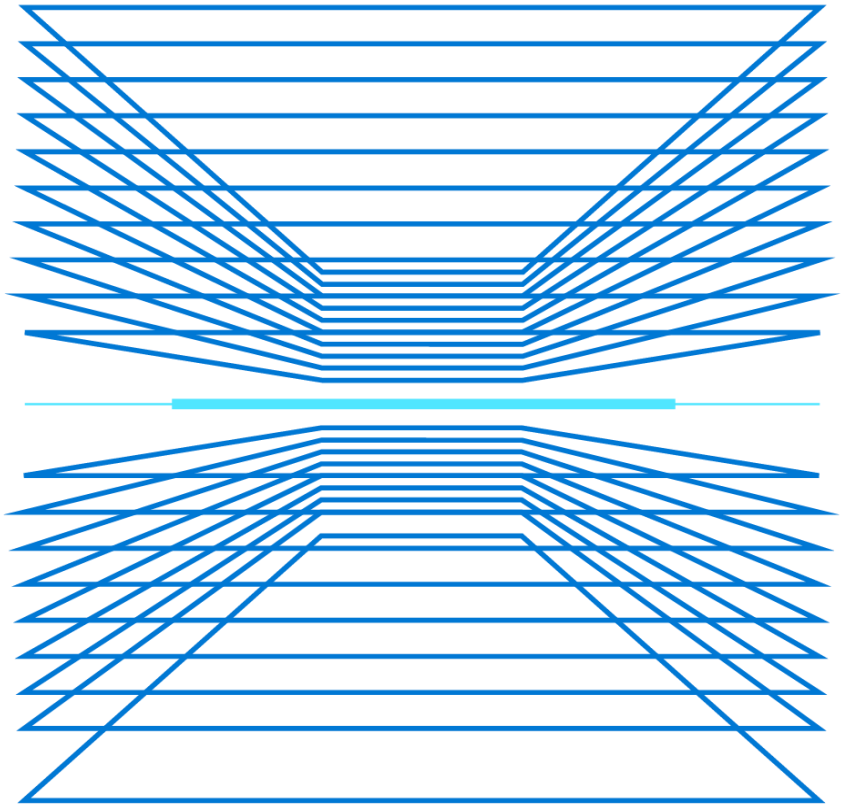


Key Vault Backup



Demonstrations: Azure Key Vault

- Create a Key Vault
- Review Key Vault settings
- Configure access policies



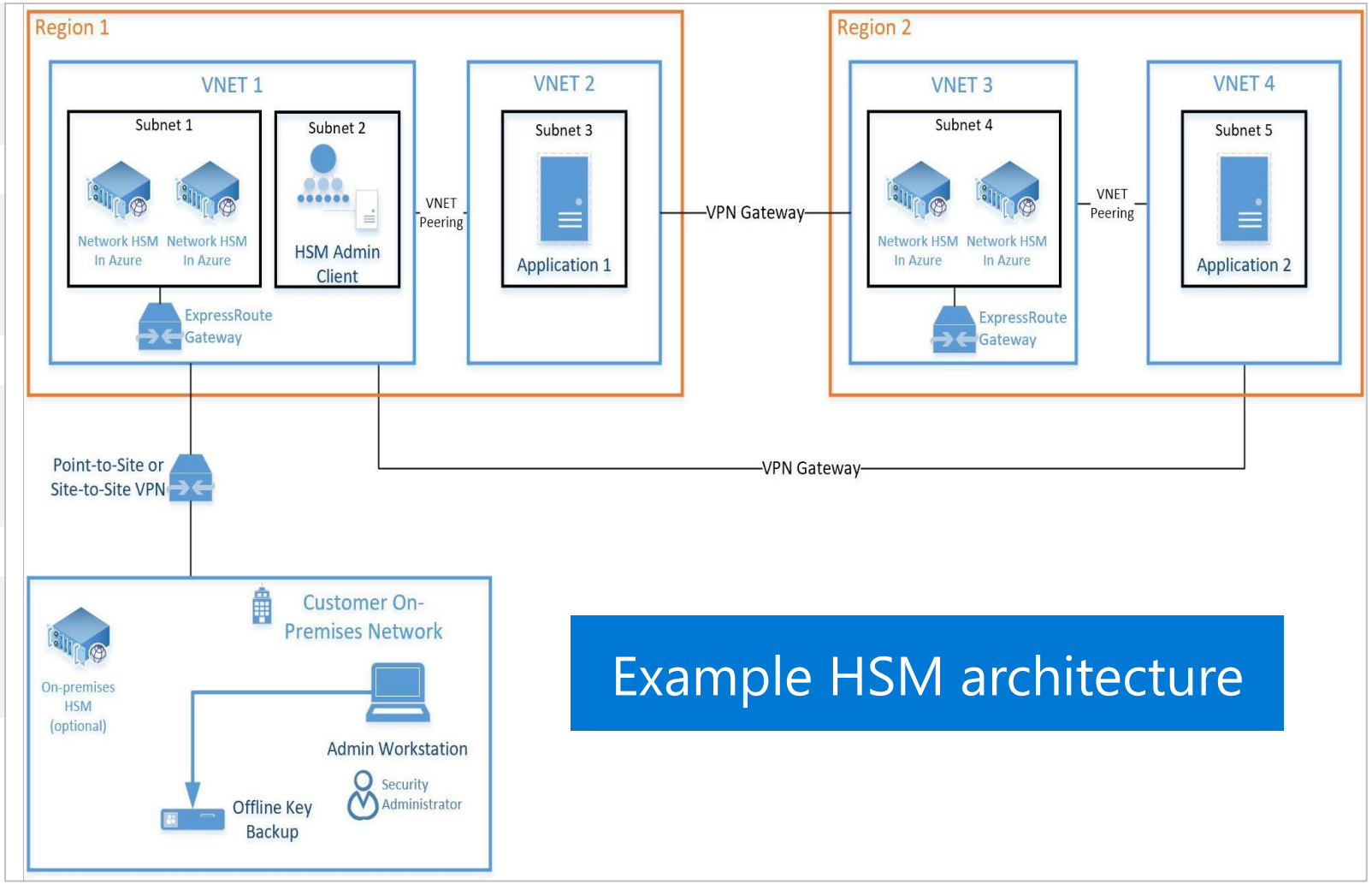
Azure Dedicated HSM (Hardware Security Module)

FIPS 140-2 Level-3 compliant

Dedicated / Single device

Thales Luna 7 HSM model A790

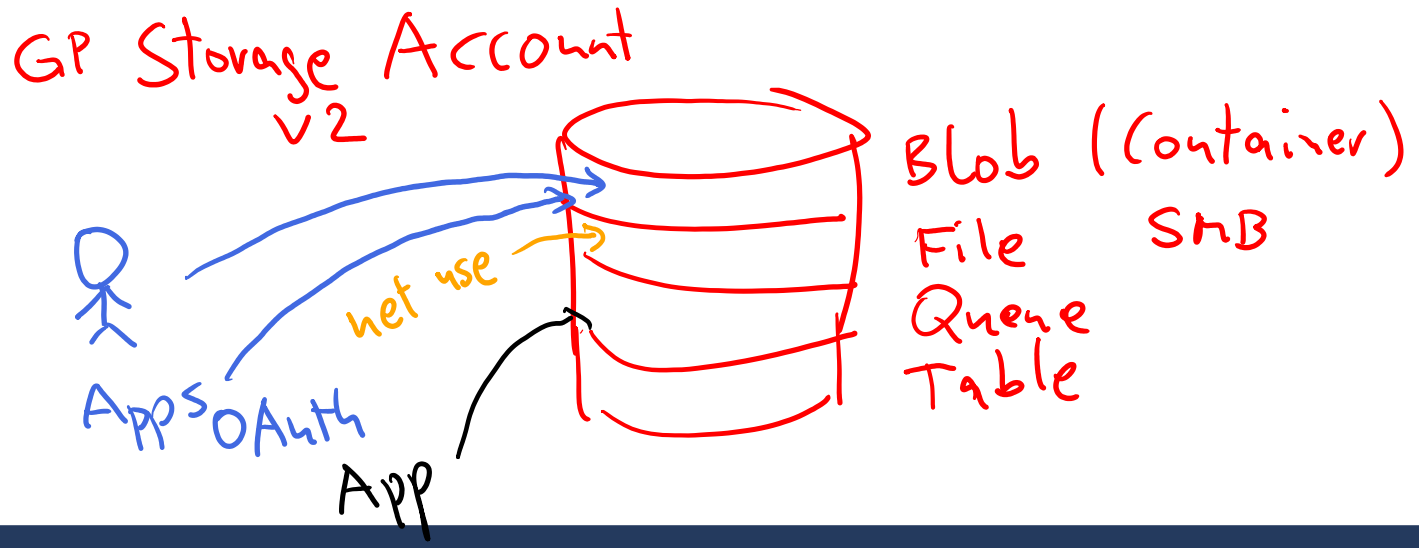
Unique cloud-based offering from Azure



Example HSM architecture

Additional Study – Azure Key Vault

Module Review Questions	Microsoft Learn Modules (docs.microsoft.com/Learn)
	Introduction to securing data at rest on Azure Manage secrets in your server apps with Azure Key Vault (Exercise) Configure and manage secrets in Azure Key Vault (Exercise)

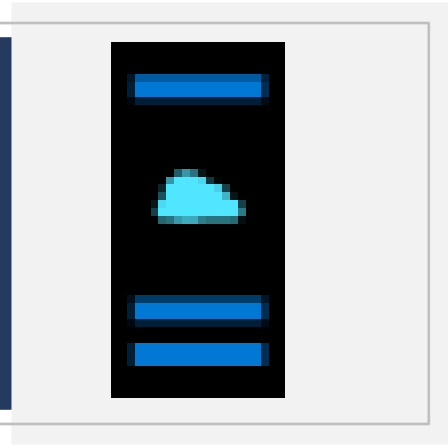


Role RBAC

Connection String
Key

SMB 3

Storage Security



Storage Security

Data Sovereignty

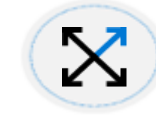
Azure Storage Access

Shared Access Signatures

Azure AD Storage Authentication

Storage Service Encryption

Blob Data Retention Policies

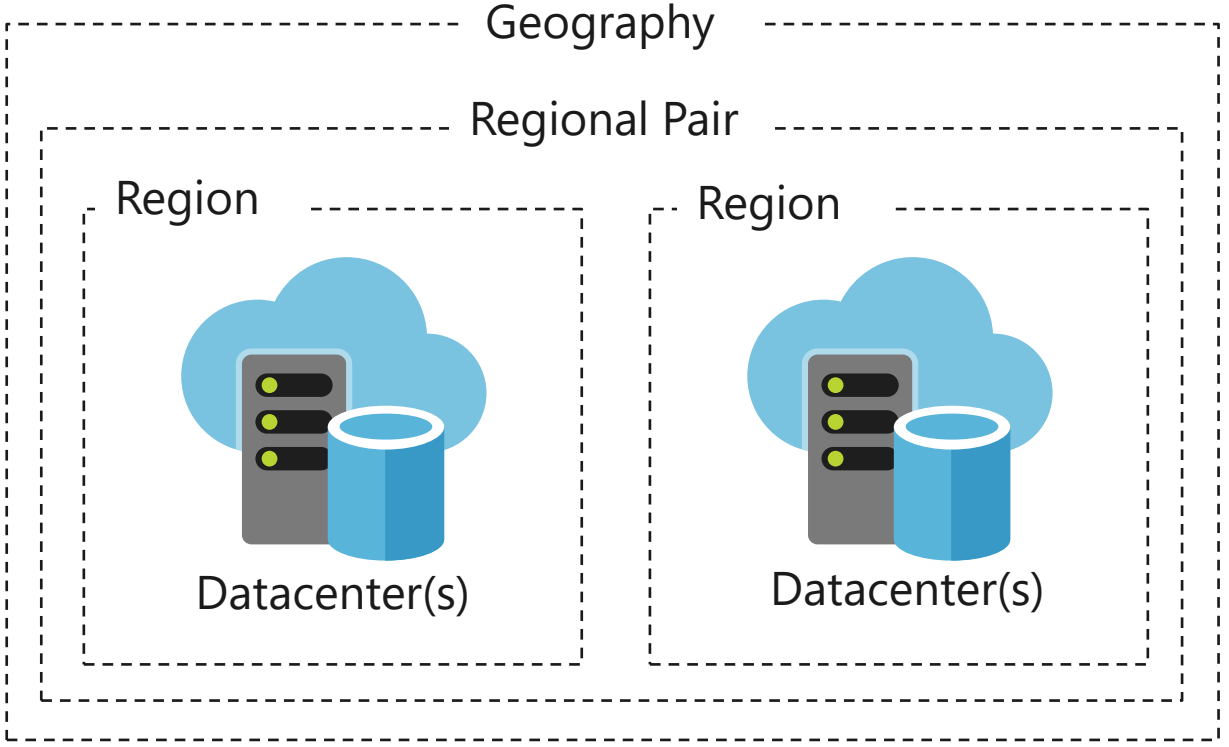


Azure Files Authentication

Secure Transfer Required

Data Sovereignty

- Physical isolation
- Platform-provided replication
- Region recovery order
- Sequential updates
- Data residency



Facilitates compliance
with data location laws

Azure Storage Access

Every storage request must be authorized. There are various authorization methods, including anonymous.

Azure artifact	Shared Key (storage account key)	Shared access signature (SAS)	Azure Active Directory (Azure AD)	On-premises Active Directory Domain Services	Anonymous public read access
Azure Blobs	Supported	Supported	Supported	Not Supported	Supported
Azure Files (SMB)	Supported	Not Supported	Supported, only with AAD Domain Services	Supported, credentials must be synced to Azure AD	Not Supported
Azure Files (REST)	Supported	Supported	Supported	Not Supported	Not Supported
Azure Queues	Supported	Supported	Supported	Not Supported	Not Supported
Azure Tables	Supported	Supported	Supported	Not Supported	Not Supported

Shared Access Signatures

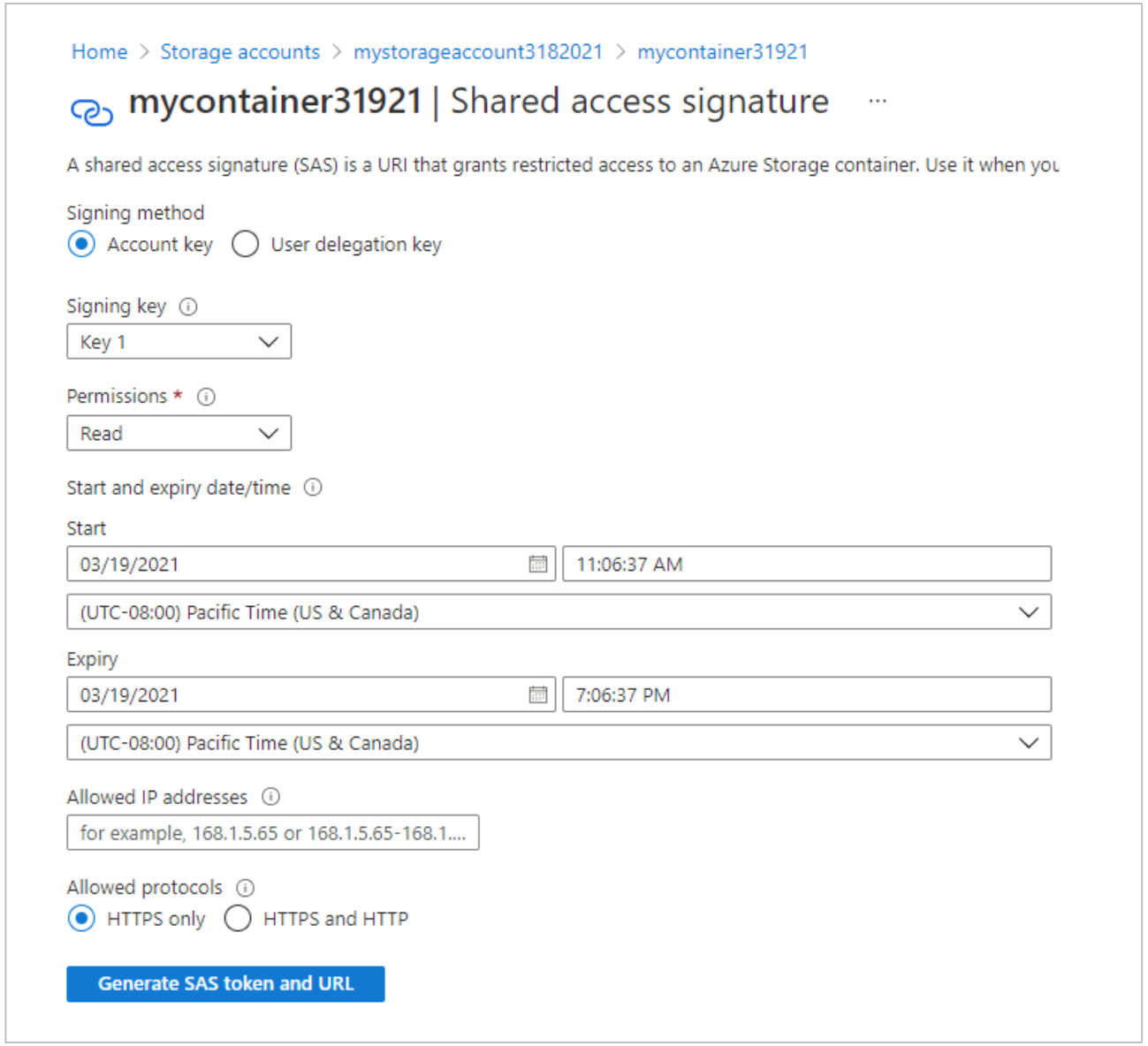
Digitally signed URIs of target storage resources

Grants access to clients without sharing your storage account keys

SAS types:

- Account – multiple storage service
- Service – single storage service
- User delegation – blob only

Configure permissions, start/expiry times, IP addresses, and allowed protocols



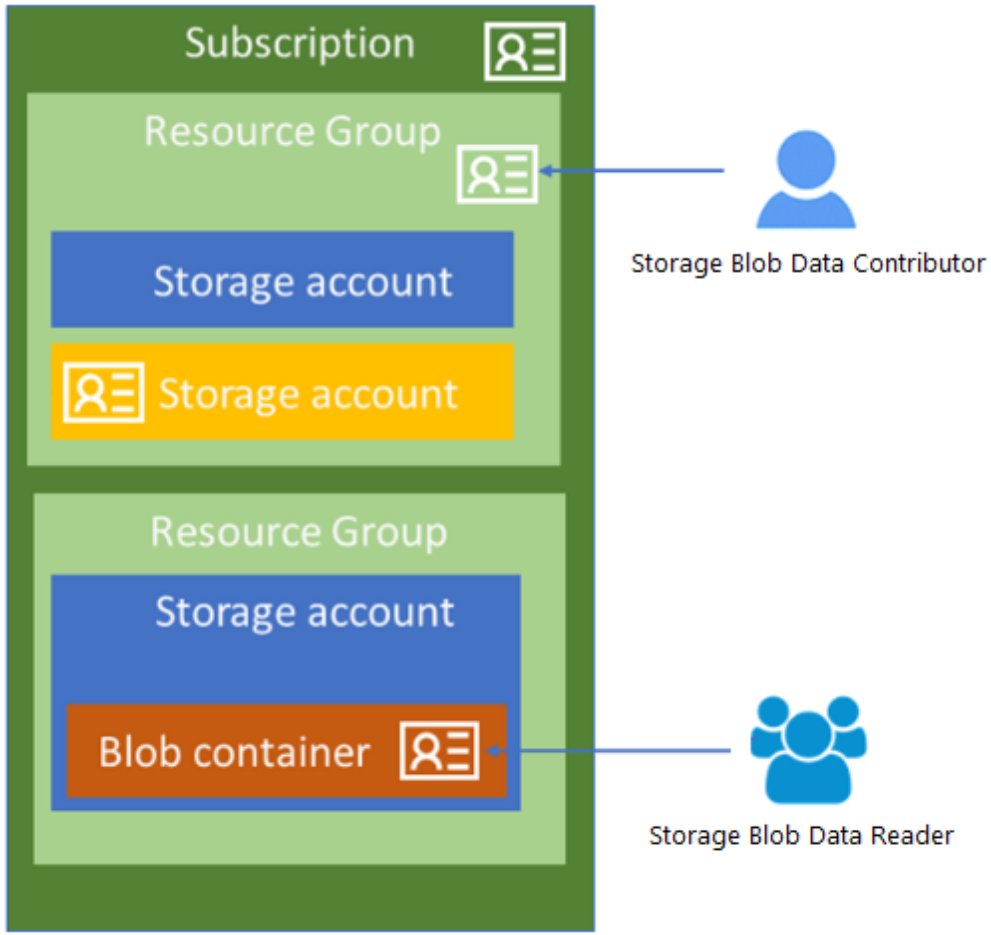
Azure AD Storage Authentication

Available for Blob and Queue storage

Several built-in roles including Data Owner, Data Contributor, and Data Reader

Two-step process: authentication (token returned) and then authorization

Scope from Management Group down to individual blob or queue



Blob Data Retention Policies

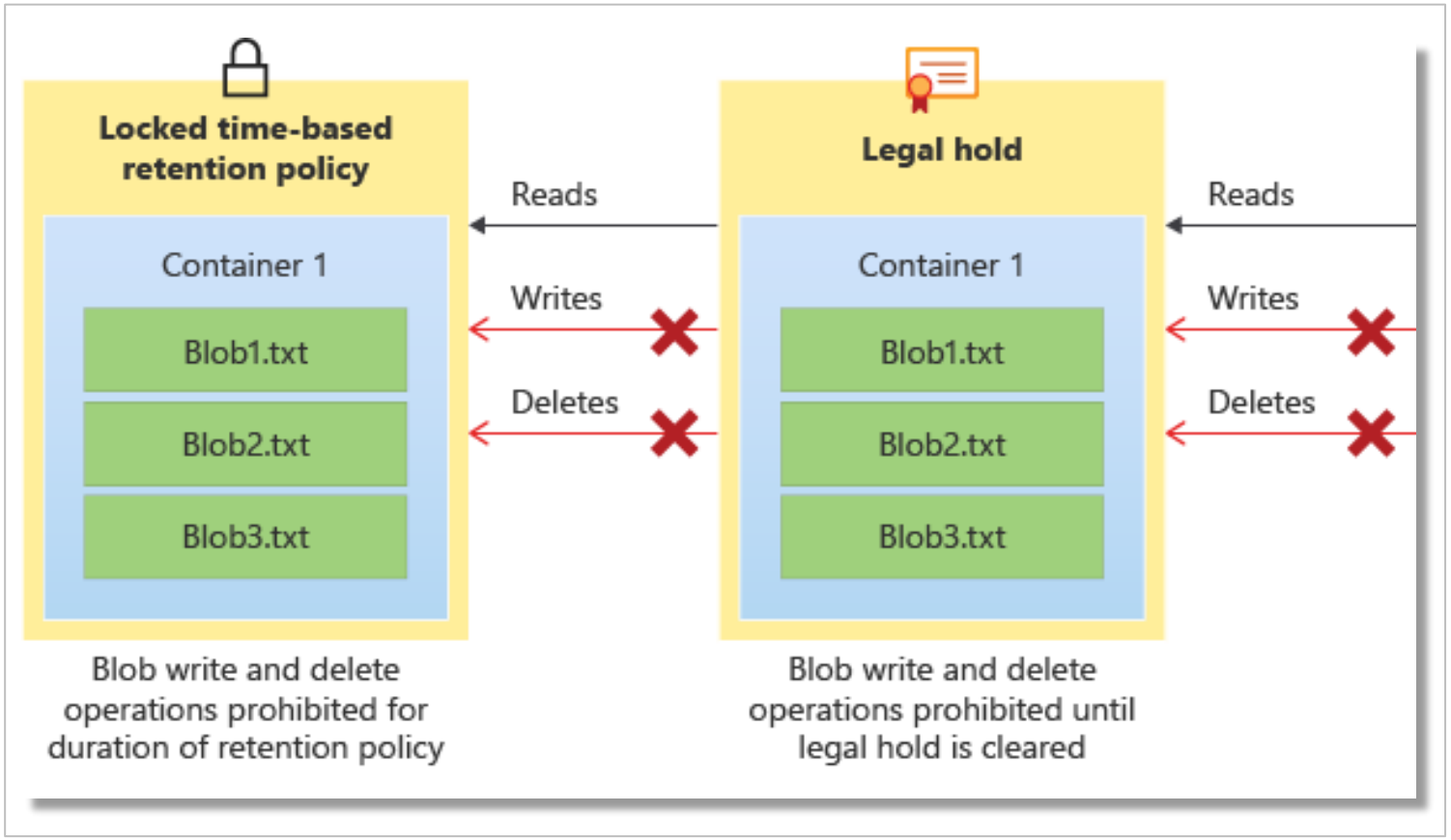
Data recovery and disposal rules

Time-based retention for a specified interval (days)

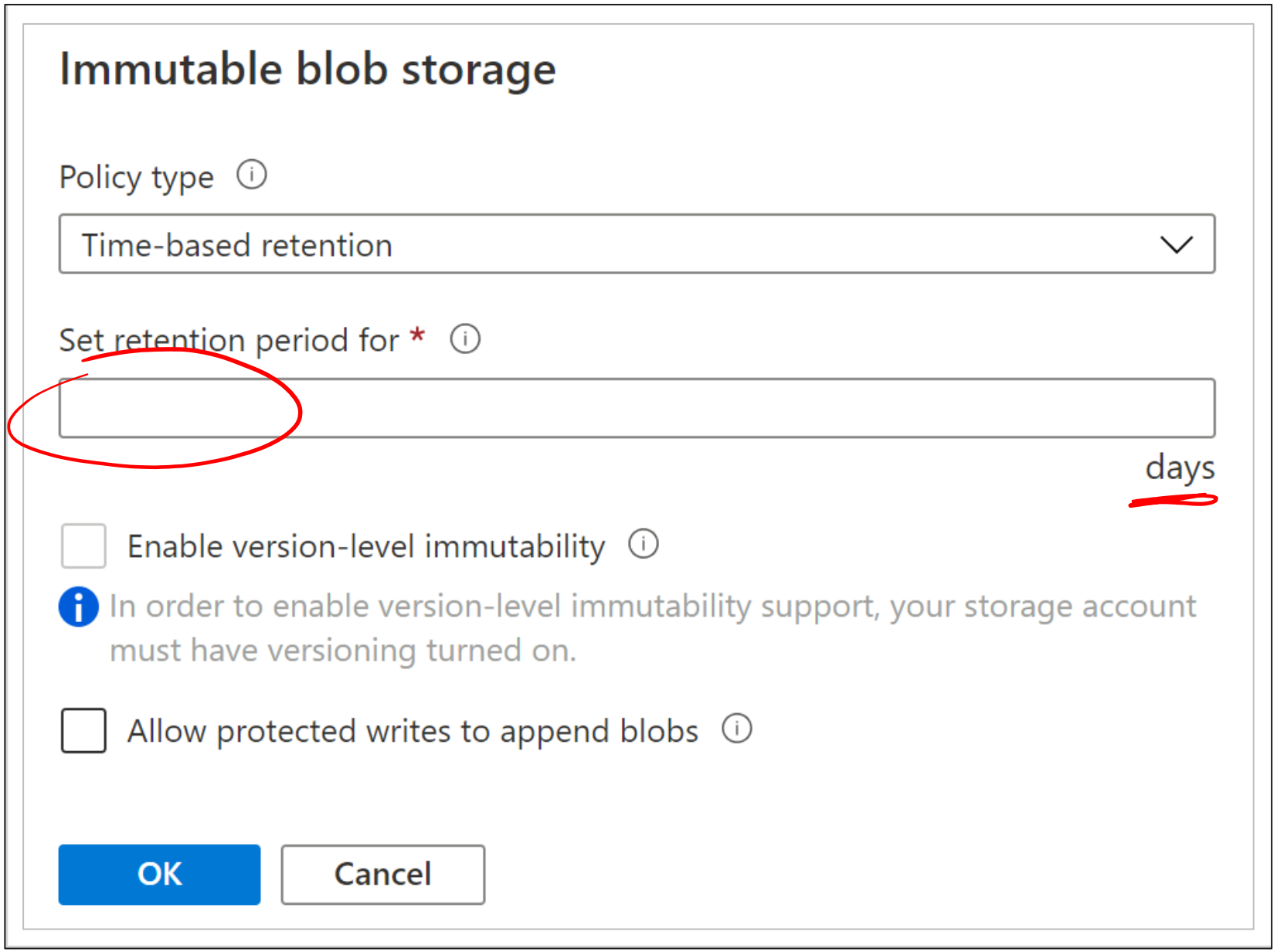
Legal-hold retention based on tags – no editing or deleting of the content

Container policies apply to all existing and new content

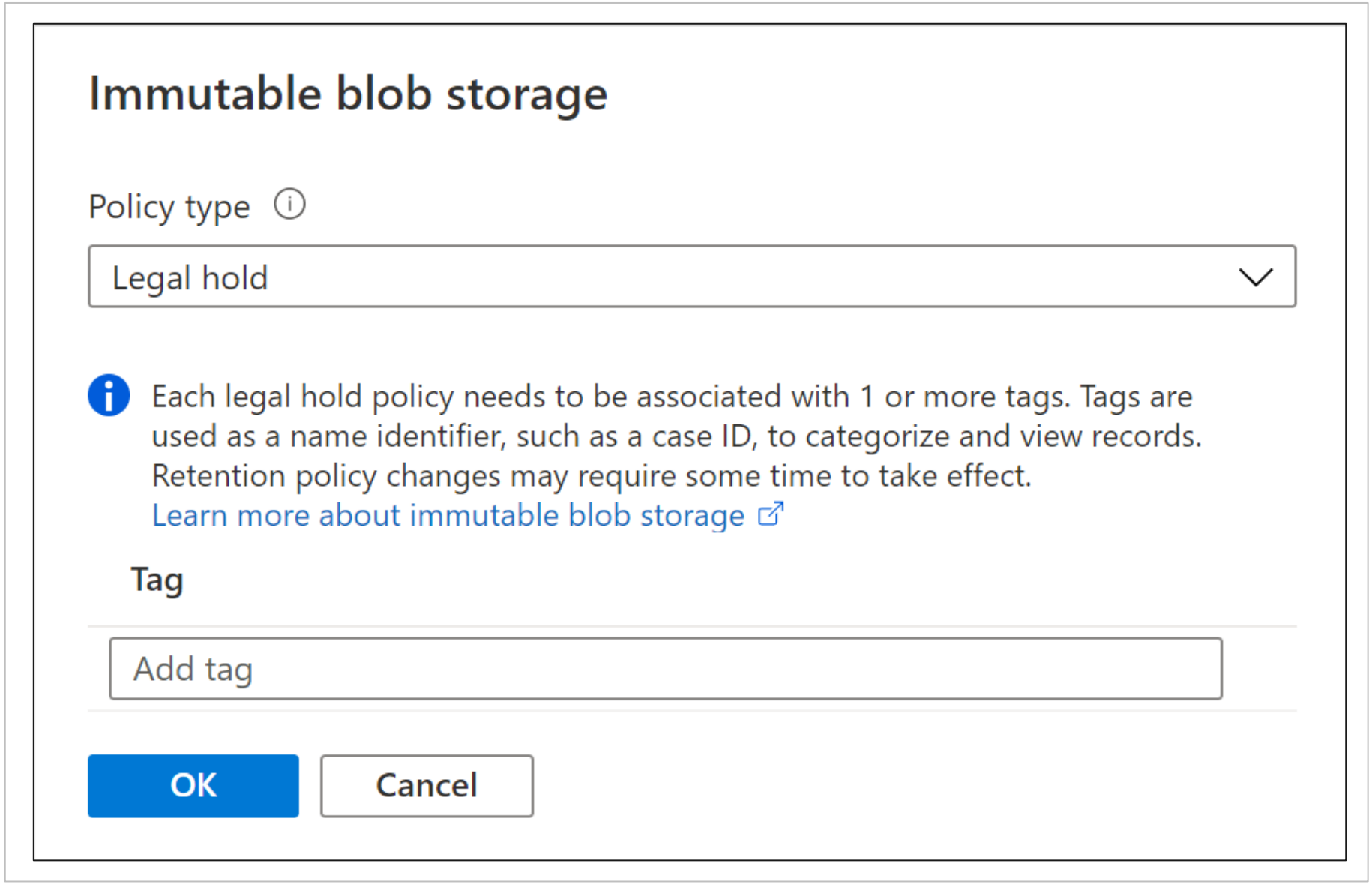
Supports audit logging



Time-based Retention Policies



Legal Hold Policies



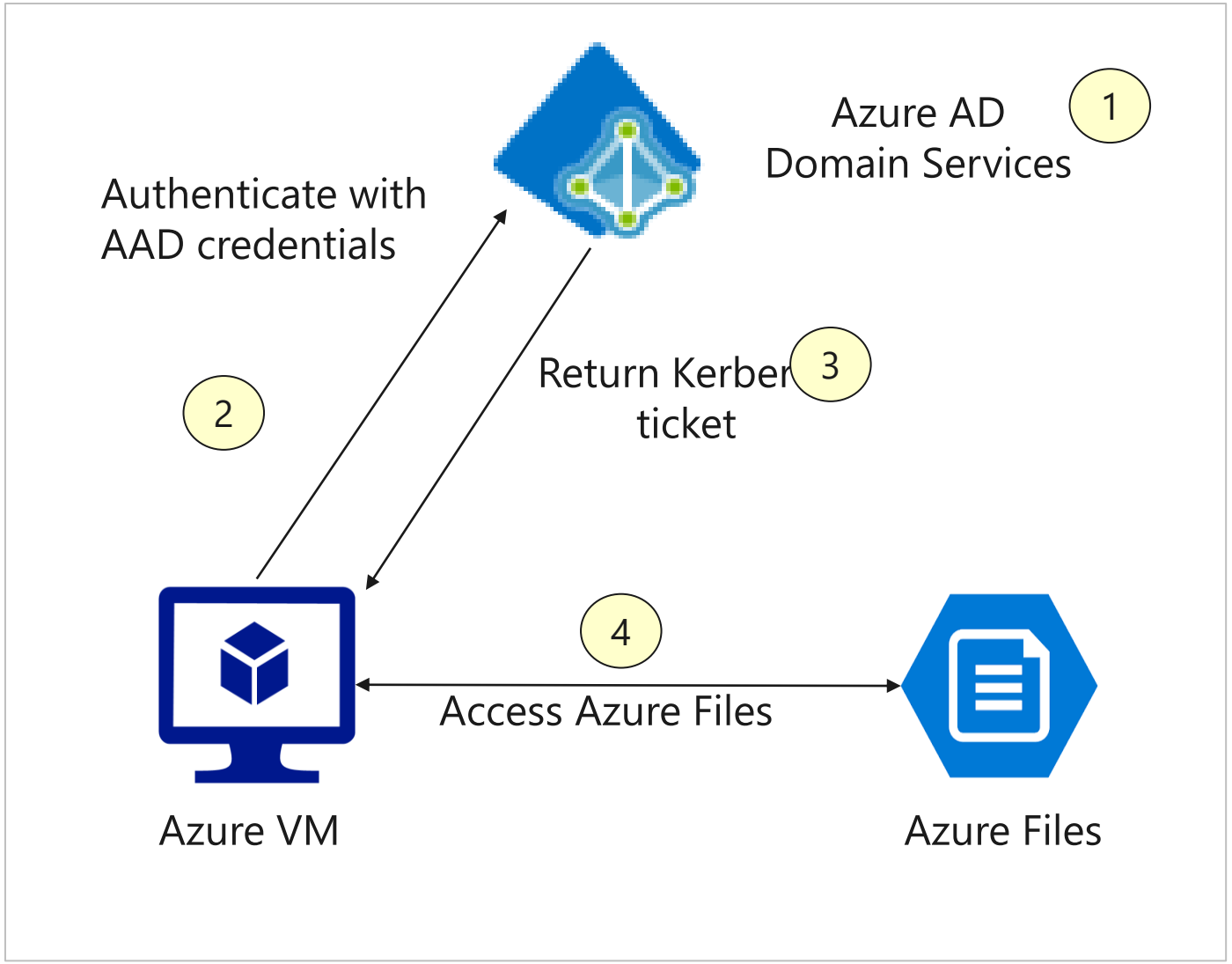
Azure Files Authentication

Enable identity-based authentication

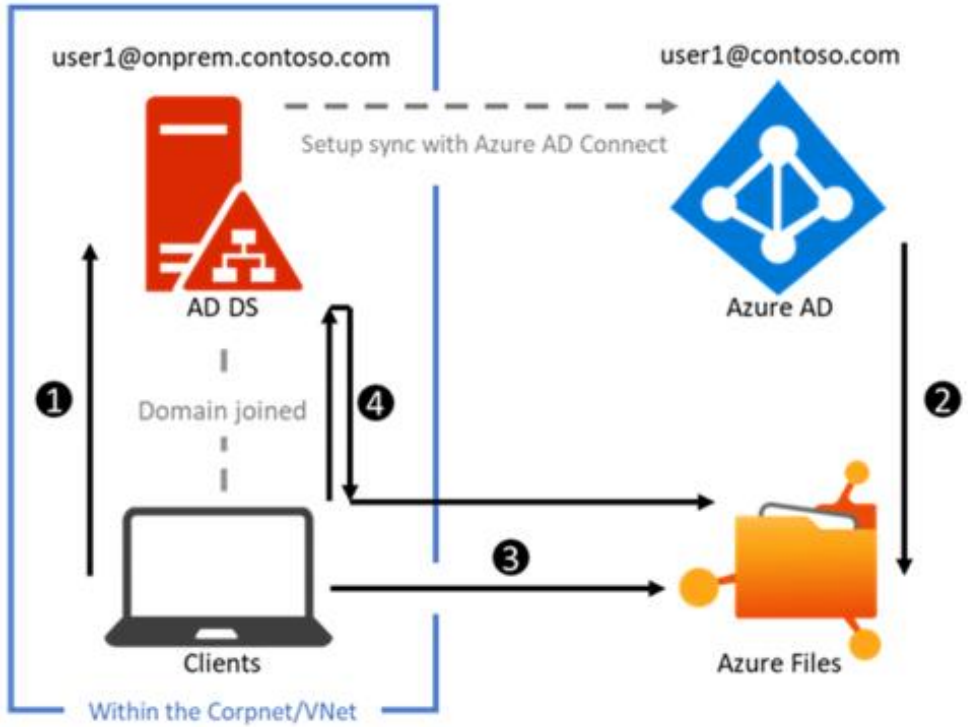
Use Azure AD DS or on-premises AD DS

Use RBAC roles to assign access rights to the file shares

Enforces standard Windows file permissions at both the directory and file level



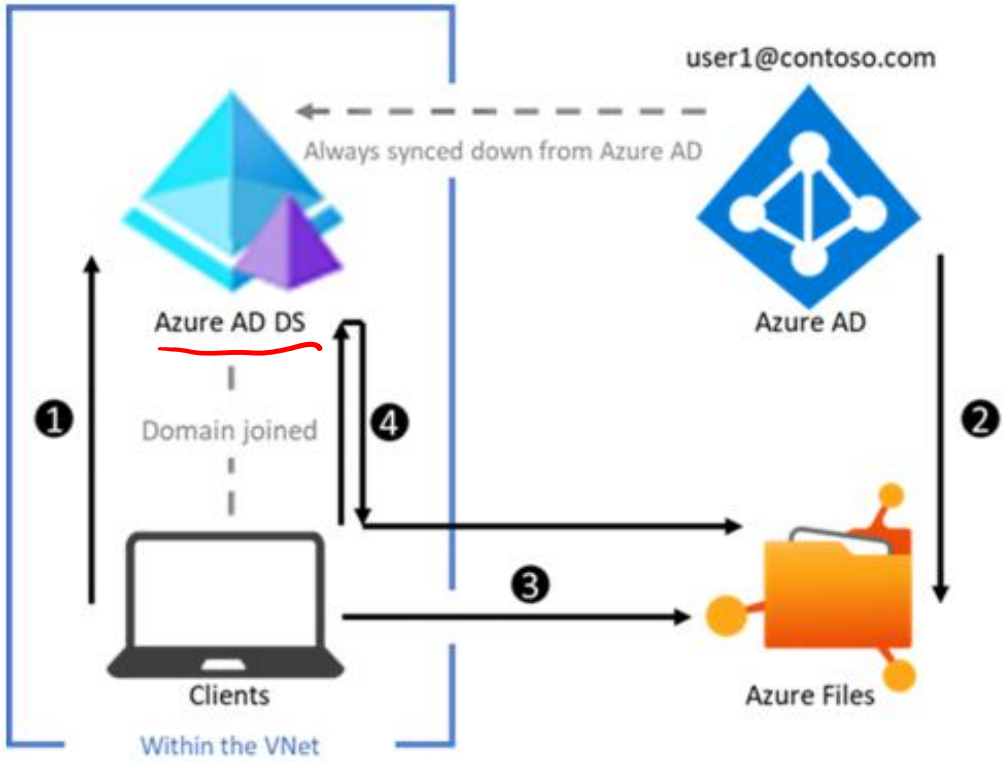
Azure Files Authentication – AD DS



1. Enable Azure Files on-prem AD DS authentication including creating an AD identity to represent the storage account
2. Assign the Azure AD identity that was synced from AD on share level permission to Azure Files (for example: user1@contoso.com)
3. Mount Azure Files with storage account key and configure directory/file level permissions (Windows DACLs) to the AD identity (for example: user1@onprem.contoso.com)
4. Access Azure Files using AD credentials by first authenticating against AD DS and sending the Kerberos token to Azure Files for authorization

On-premises Active Directory Domain Service (AD DS)

Azure Files Authentication – Azure AD DS



1. Enable Azure Files Azure AD DS authentication
2. Assign the Azure AD identity on share level permission to Azure Files (for example: user1@contoso.com)
3. Mount Azure Files with storage account key and configure directory/file level permissions (Windows DACLs) to the Azure AD identity
4. Access Azure Files using Azure AD credentials by first authenticating against Azure AD DS and sending the Kerberos token to Azure Files for authorization

Azure Active Directory Domain Services (Azure AD DS)

Secure Transfer Required

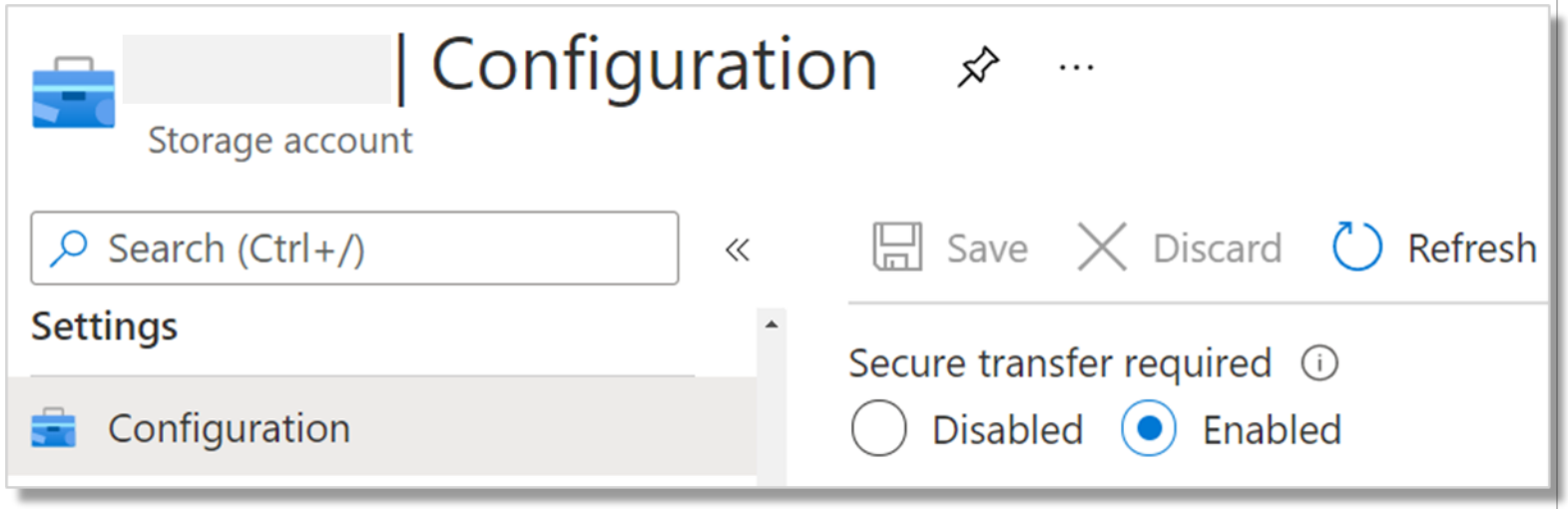
Integrate storage account with a Content Delivery Network (CDN)

Storage account connections must be secure (HTTPs)

HTTPs for custom domain names not supported

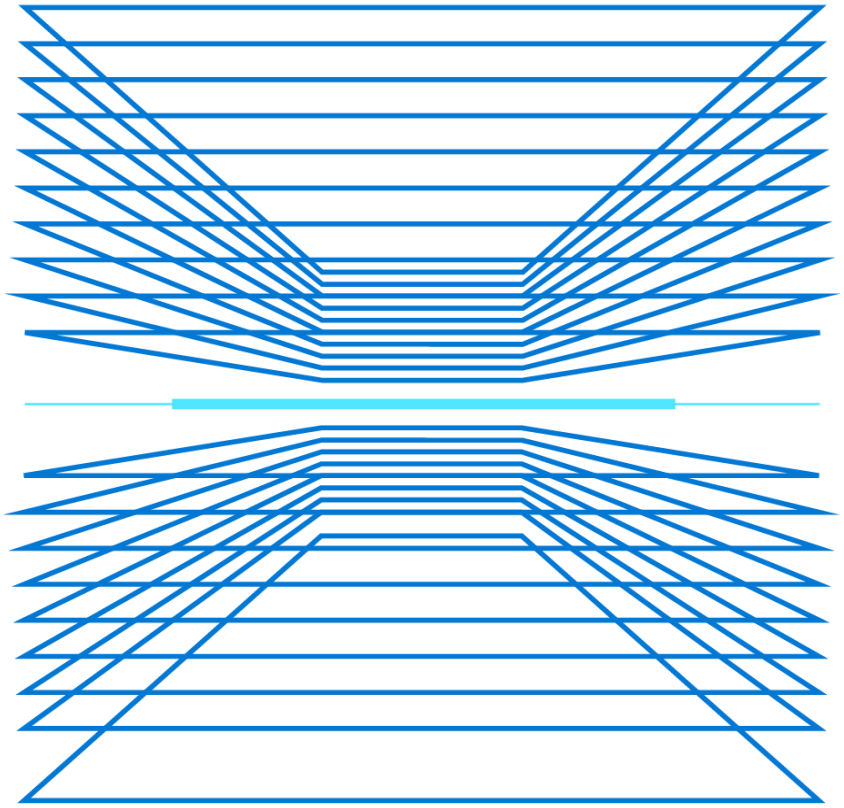
Azure Files connections require encryption (SMB)

Existing Account



Demonstrations: Storage Security

- Generate SAS tokens
- Key rollover
- Storage access policies
- Azure AD user account authentication
- Storage endpoints



Additional Study – Storage Security

Module Review Questions	Microsoft Learn Modules (docs.microsoft.com/Learn)

Core Cloud Services - Azure data storage options

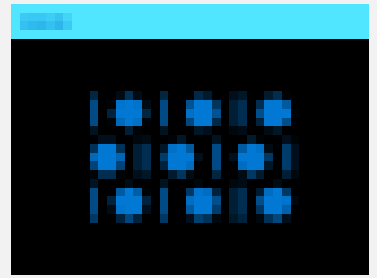
Create an Azure Storage account (Exercise)

Control access to Azure Storage with shared access signatures (Exercise)

Store and share files in your application with Azure Files (Exercise)

Secure your Azure Storage account

Database Security



Database Security


SQL Database Authentication


SQL Database Firewalls


Database Auditing


Data Discovery and Classification


Vulnerability Assessment


Advanced Threat Protection


Dynamic Data Masking


Transparent Data Encryption


Always Encrypted

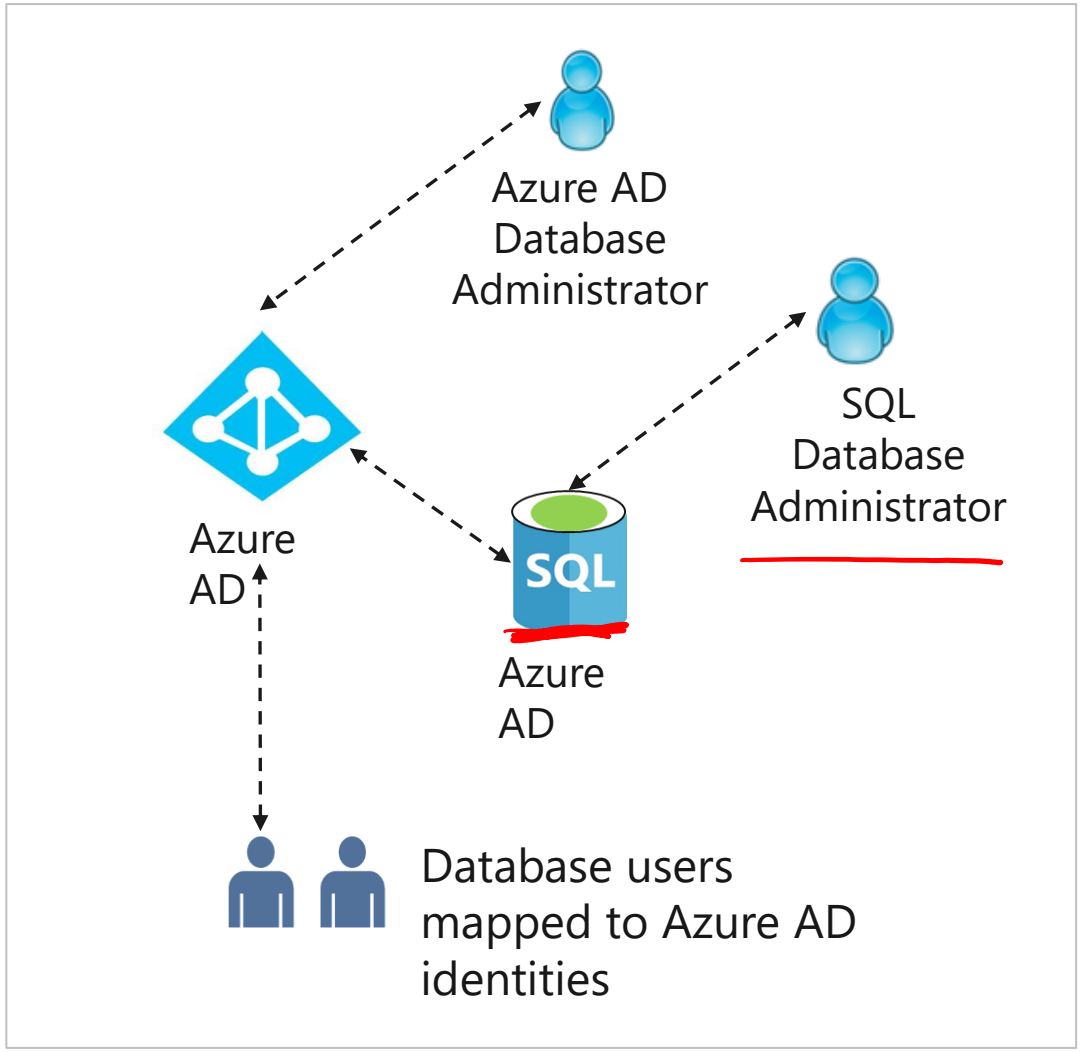
Azure AD Authentication for Azure SQL

An alternative to SQL Server authentication

Helps stop the proliferation of user identities across database servers

Allows password rotation in a single place

Customers can manage database permissions using external (Azure AD) groups



SQL Database Firewalls

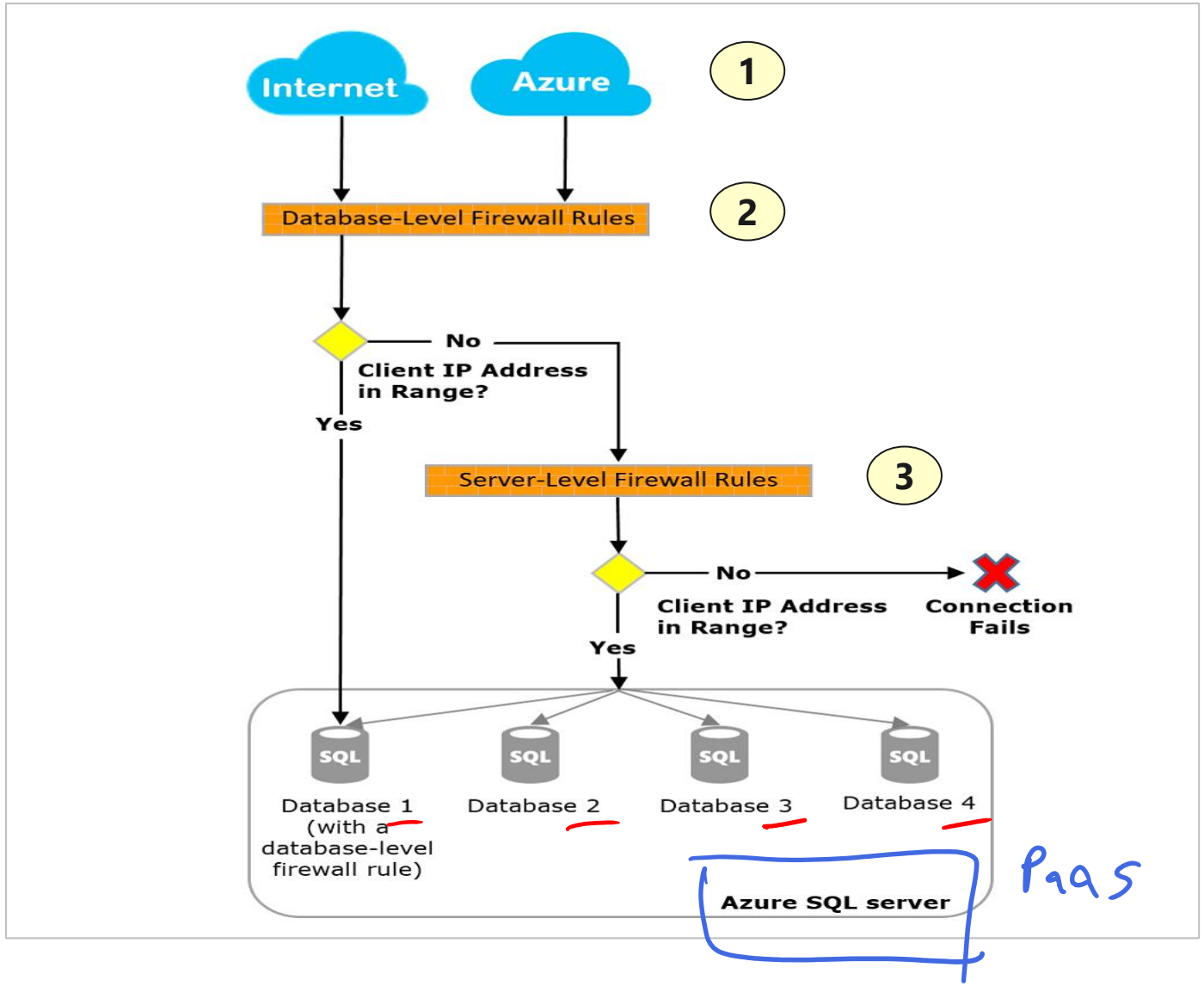
By default, firewall denies all access

Database-level firewall rules add allowed client IP addresses access to specific databases (including Master database).

T-SQL only

Server-level firewall rules enable client and Azure services access to the entire database server.

Portal, T-SQL, or PowerShell



Database Auditing

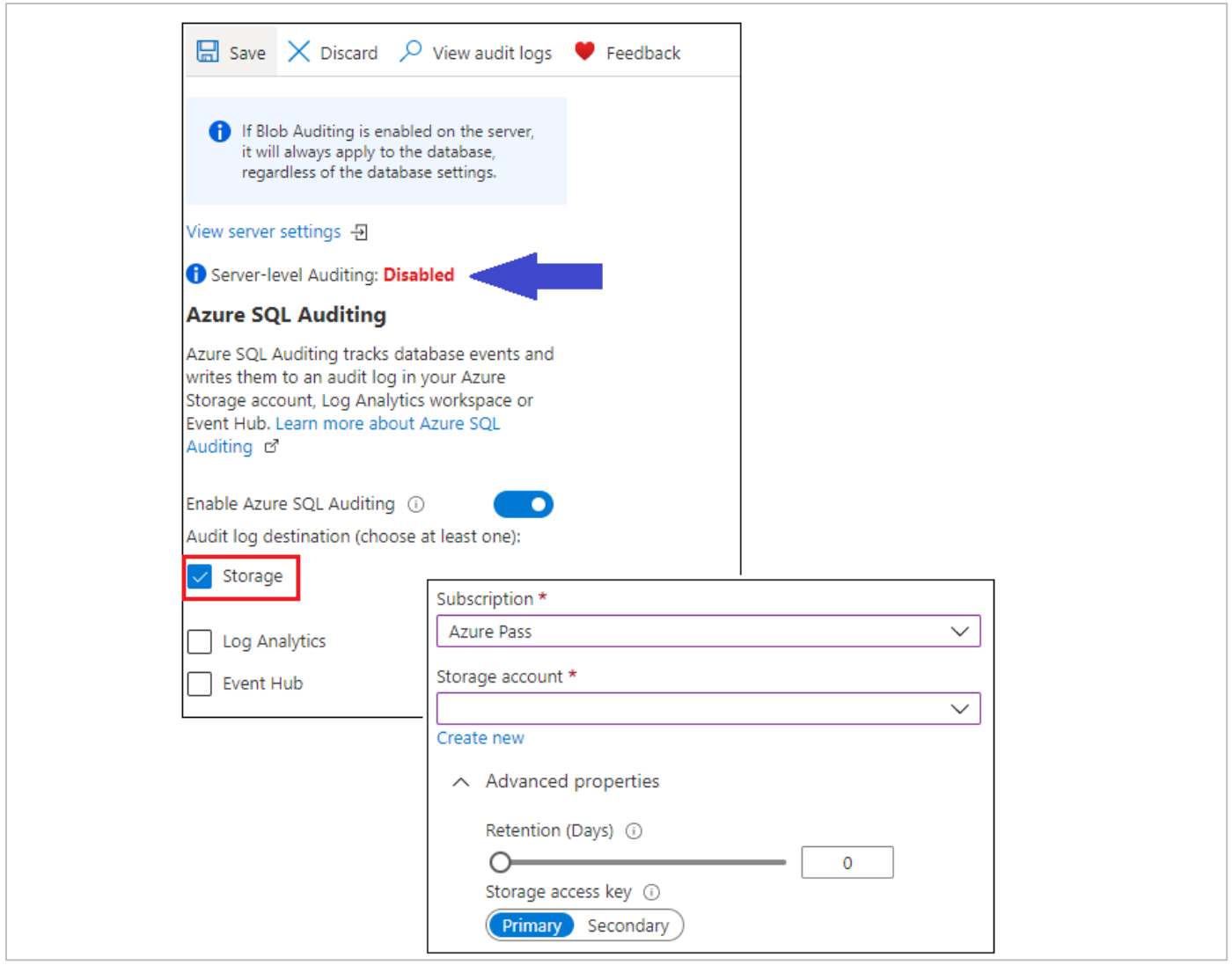
Retain an audit trail of selected events

Report on database activity and analyze results

Configure policies for the server or database level

Configure audit log destination

A new server policy applies to all existing and newly created databases



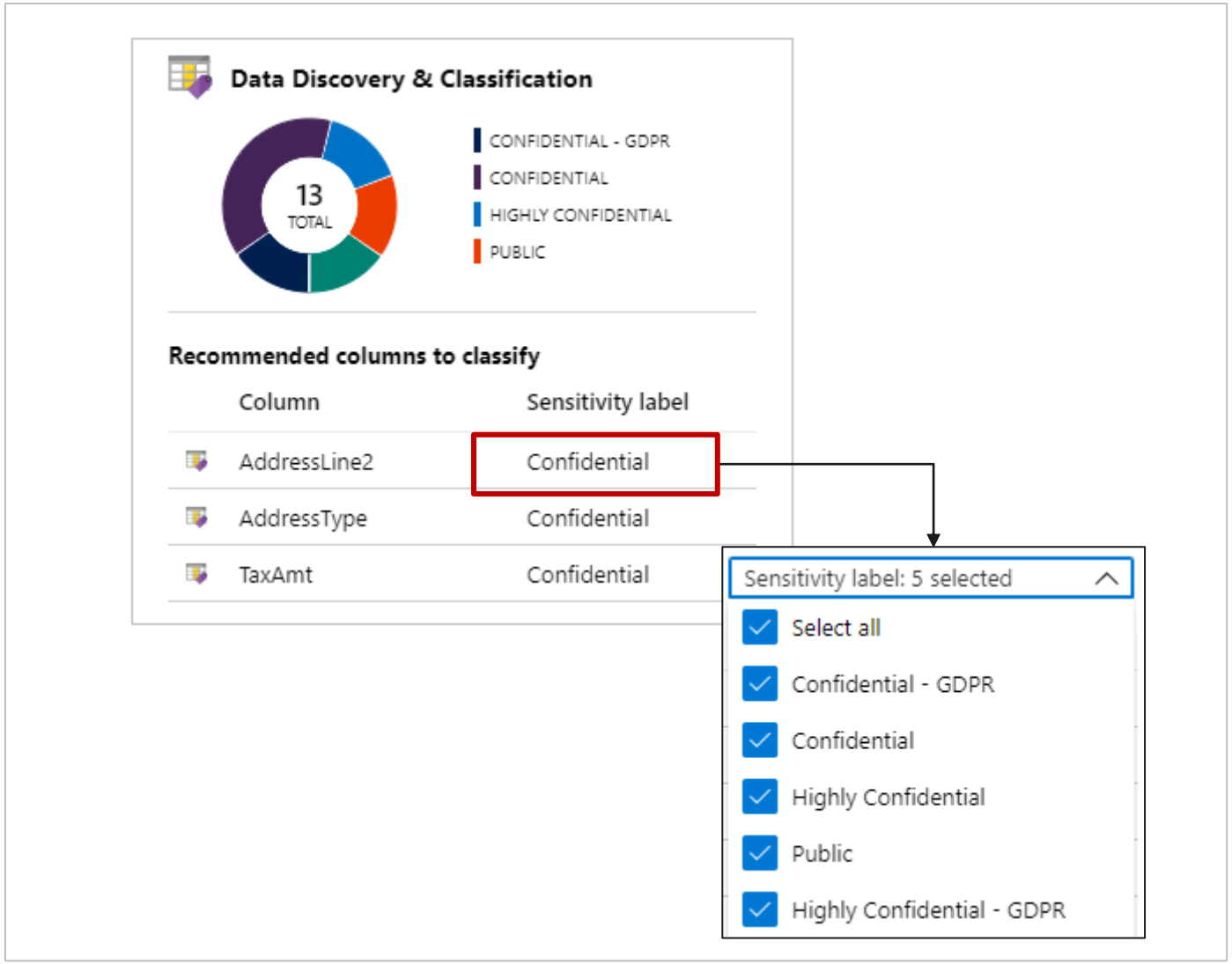
Data Discovery and Classification

Built-in to Azure SQL Database

Scans your database and identifies columns that contain potentially sensitive data

Provides classification recommendations and reports

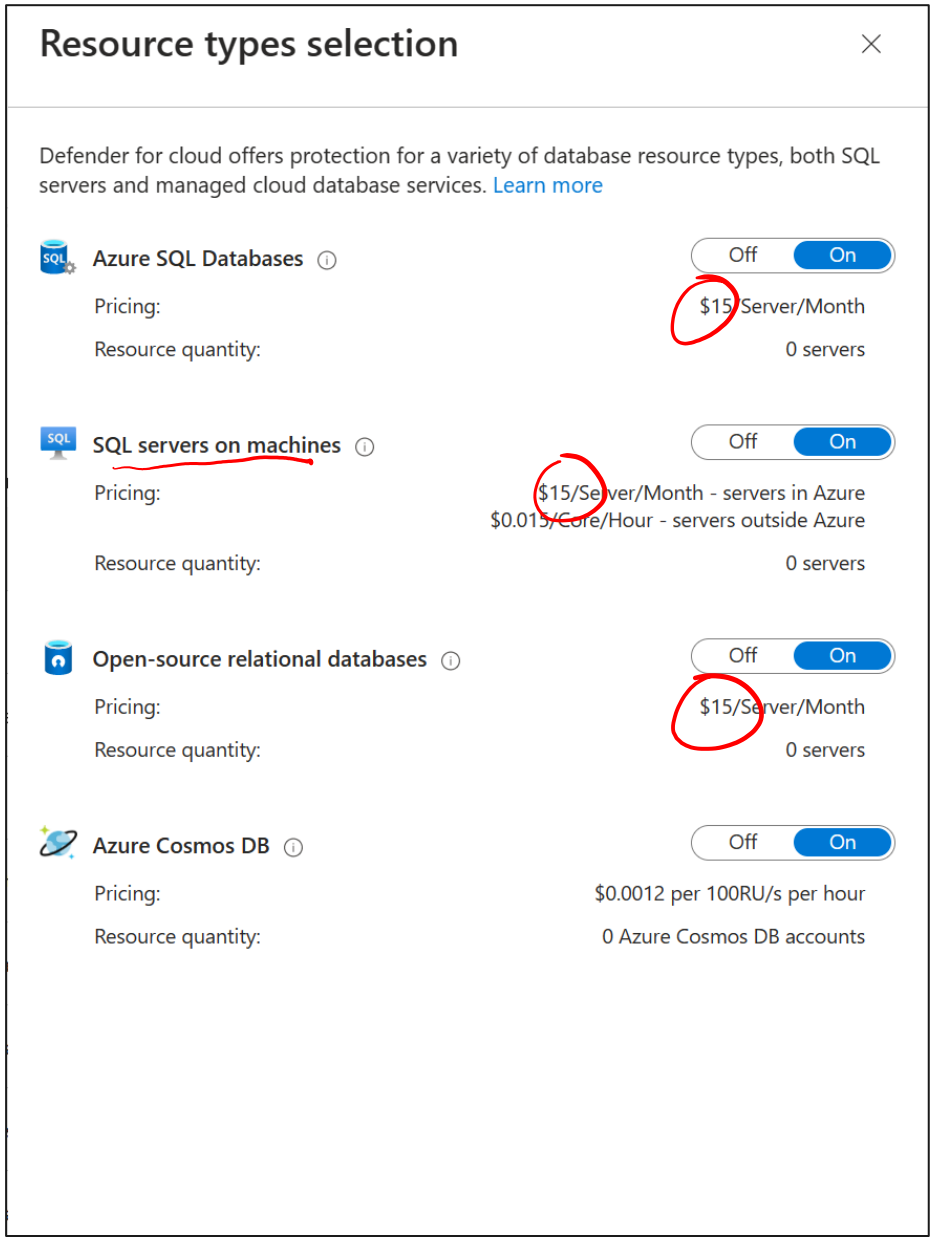
Let's you apply sensitivity-classification labels



Microsoft Defender for SQL

Microsoft Defender for SQL is a Defender plan in Microsoft Defender for Cloud.

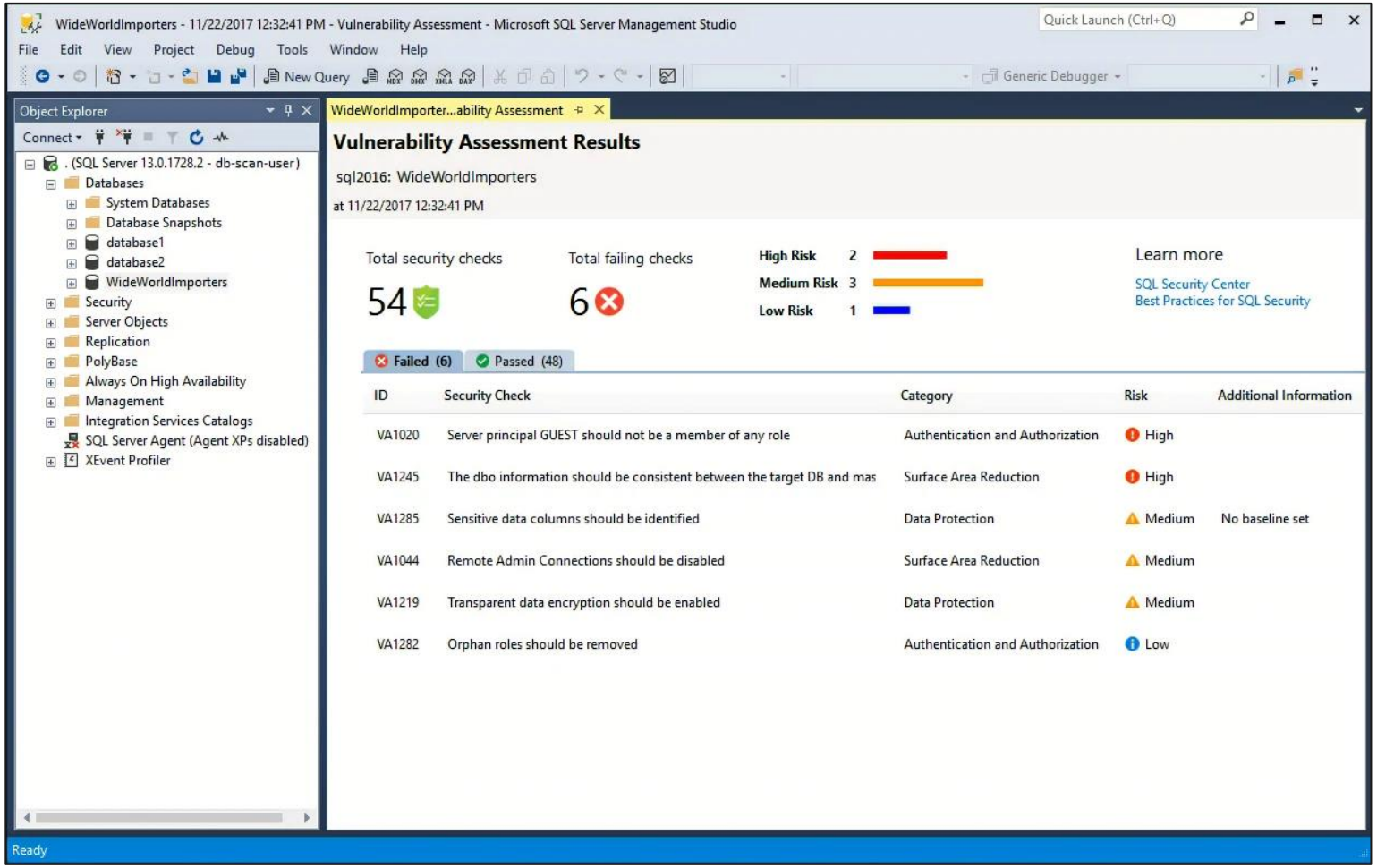
Microsoft Defender for SQL includes functionality for surfacing and mitigating potential database vulnerabilities, and detecting anomalous activities that could indicate a threat to your database.



Vulnerability assessment for SQL Server

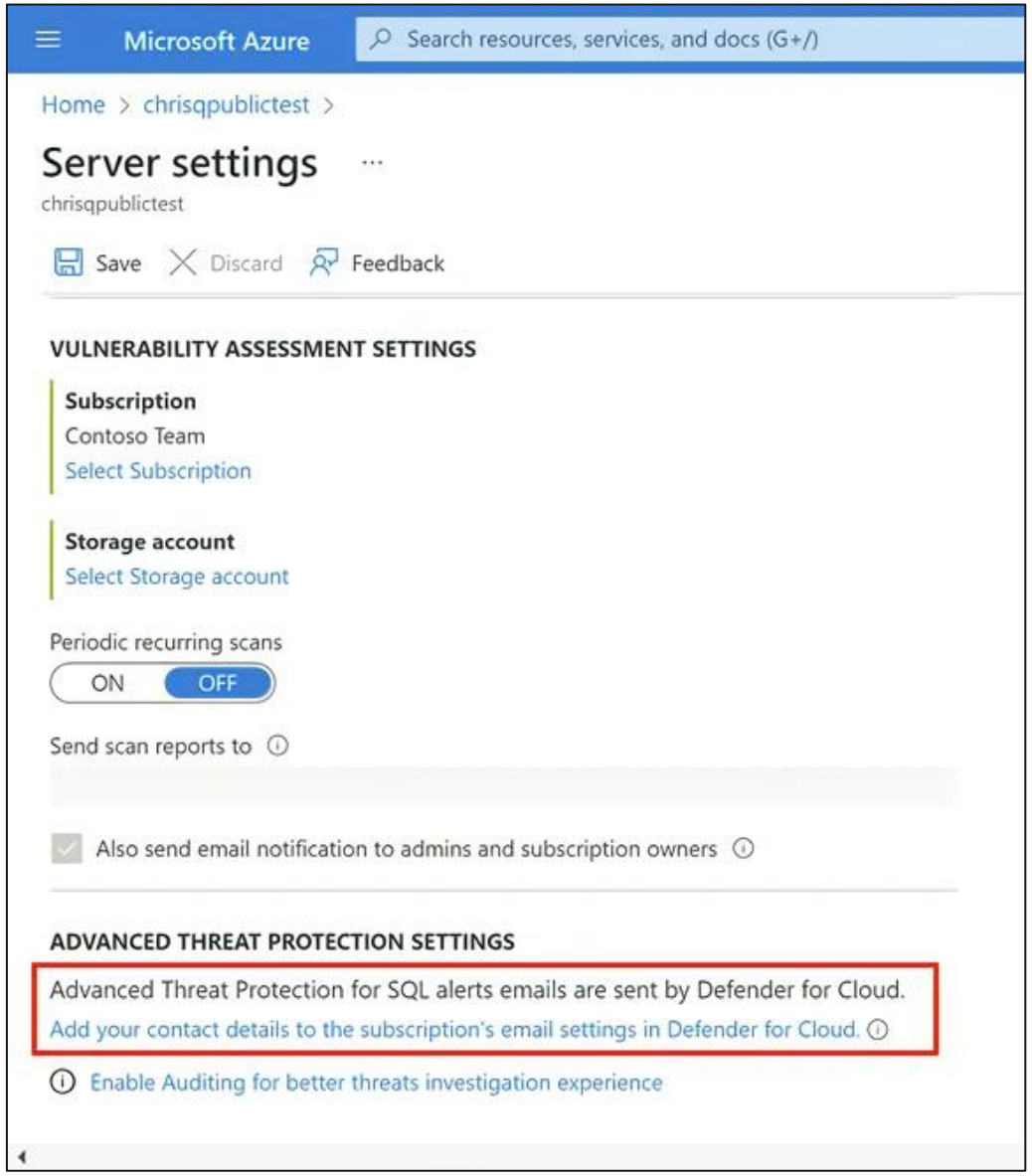
SQL vulnerability assessment (VA) is a service that provides visibility into your security state and includes actionable steps to resolve security issues and enhance your database security.

The VA service runs a scan directly on your database and employs a knowledge base of rules that flag security vulnerabilities and highlight deviations from best practices, such as misconfigurations, excessive permissions, and unprotected sensitive data.



SQL Advanced Threat Protection

Advanced Threat Protection for Azure SQL Database, Azure SQL Managed Instance, Azure Synapse Analytics, SQL Server on Azure Virtual Machines and Azure Arc-enabled SQL Server detects anomalous activities indicating unusual and potentially harmful attempts to access or exploit databases.

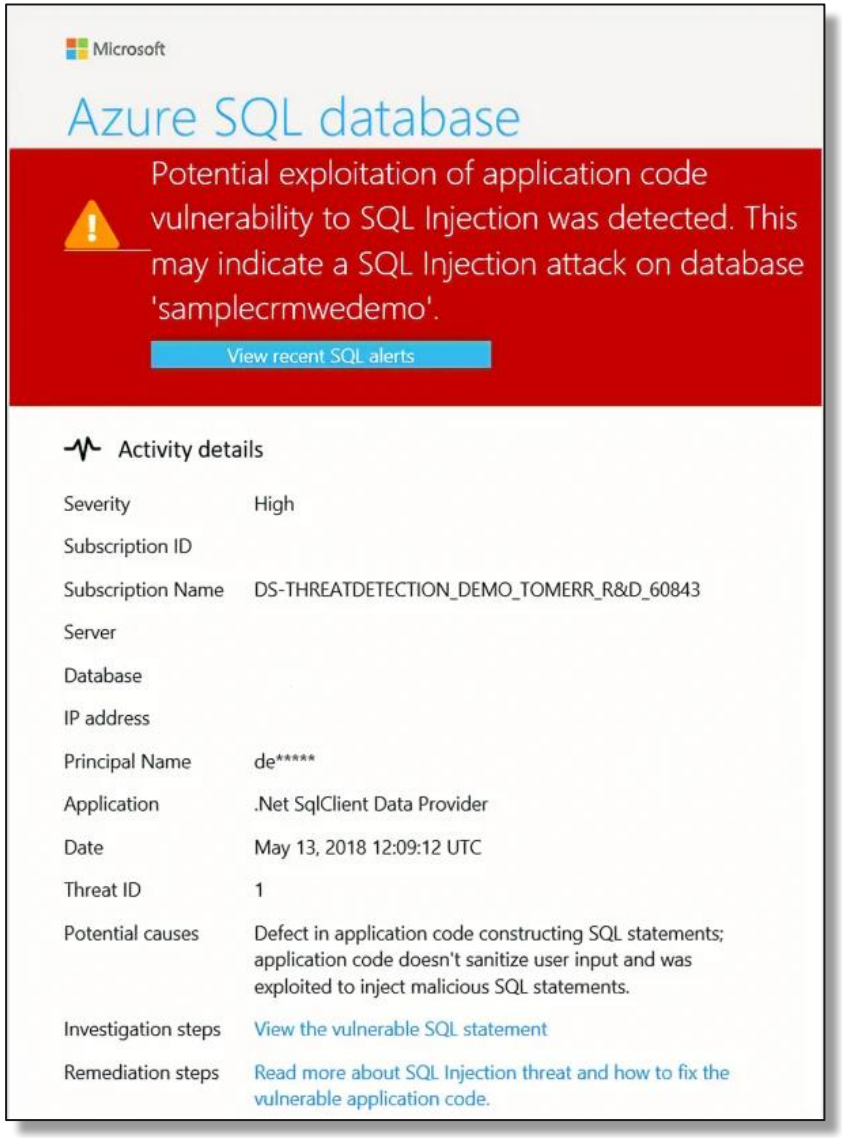


Explore detection of a suspicious event

You receive an email notification upon detection of anomalous database activities.

The email provides information on the suspicious security event including the nature of the anomalous activities, database name, server name, application name, and the event time.

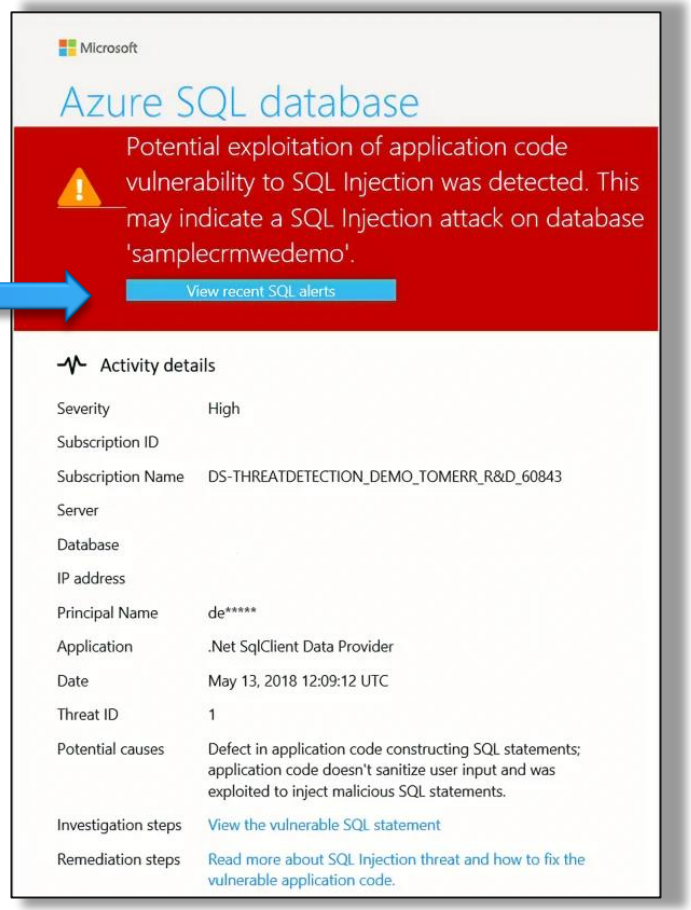
In addition, the email provides information on possible causes and recommended actions to investigate and mitigate the potential threat to the database.



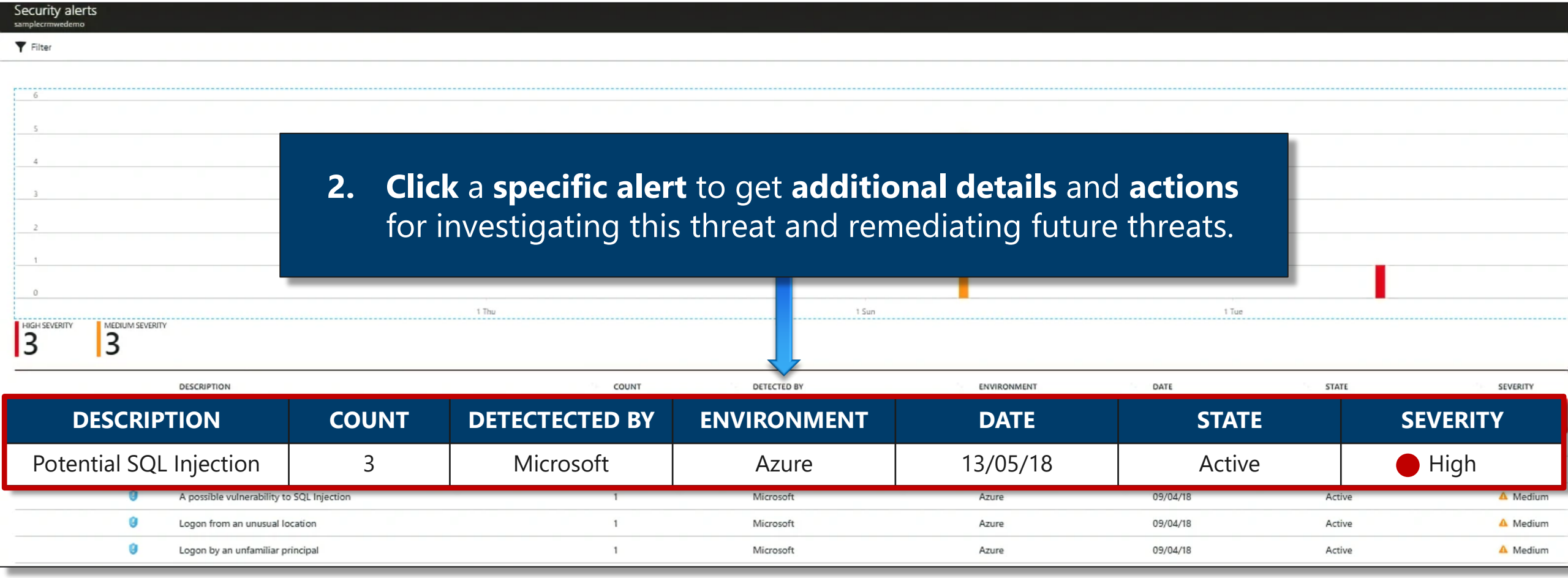
Explore detection of a suspicious event

1. **Click** the **View recent SQL alerts** link in the email to launch the Azure portal and show the Microsoft Defender for Cloud alerts page, which provides an overview of active threats detected on the database.

Example:
View recent SQL alerts



Explore detection of a suspicious event (continued)



2. **Click** a **specific alert** to get **additional details** and **actions** for investigating this threat and remediating future threats.

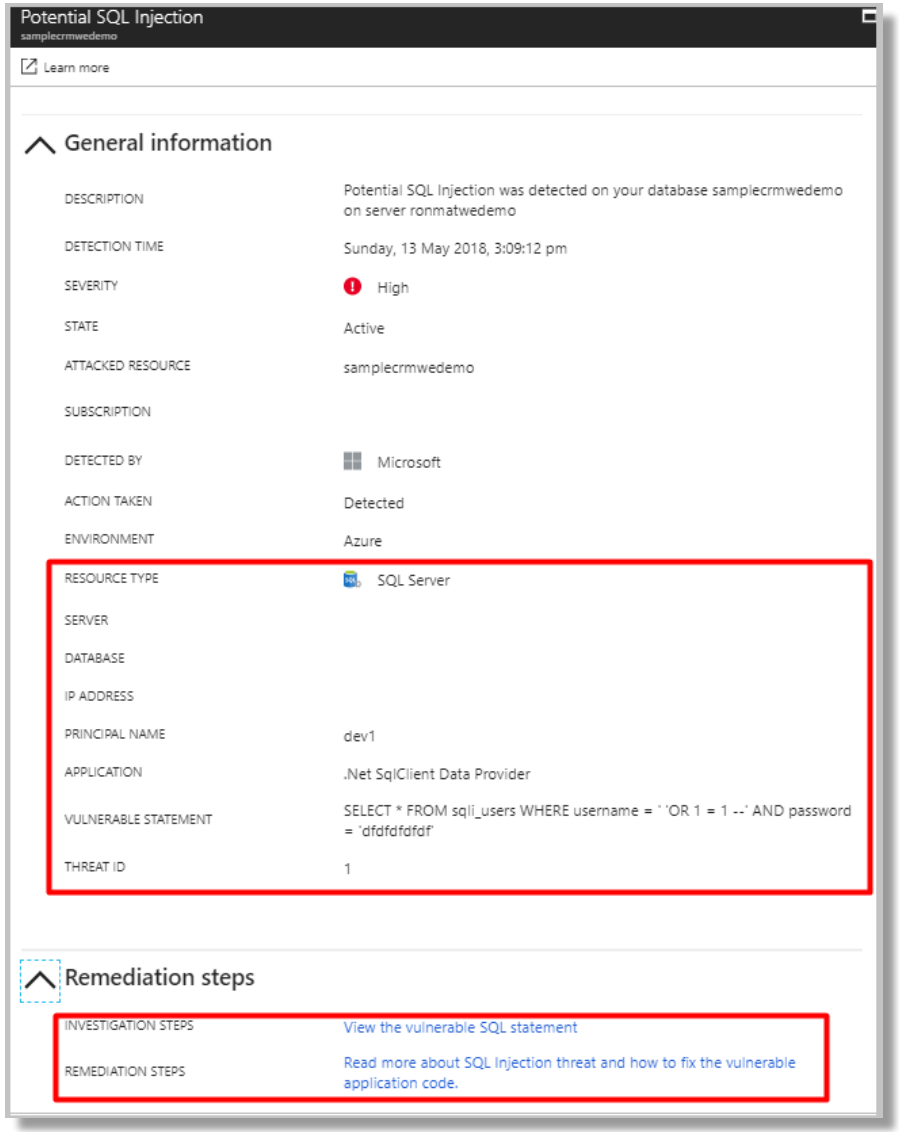
DESCRIPTION	COUNT	DETECTECTED BY	ENVIRONMENT	DATE	STATE	SEVERITY
Potential SQL Injection	3	Microsoft	Azure	13/05/18	Active	High

Explore detection of a suspicious event (continued)

For example, SQL injection is one of the most common Web application security issues on the Internet that is used to attack data-driven applications.

Attackers take advantage of application vulnerabilities to inject malicious SQL statements into application entry fields, breaching or modifying data in the database.

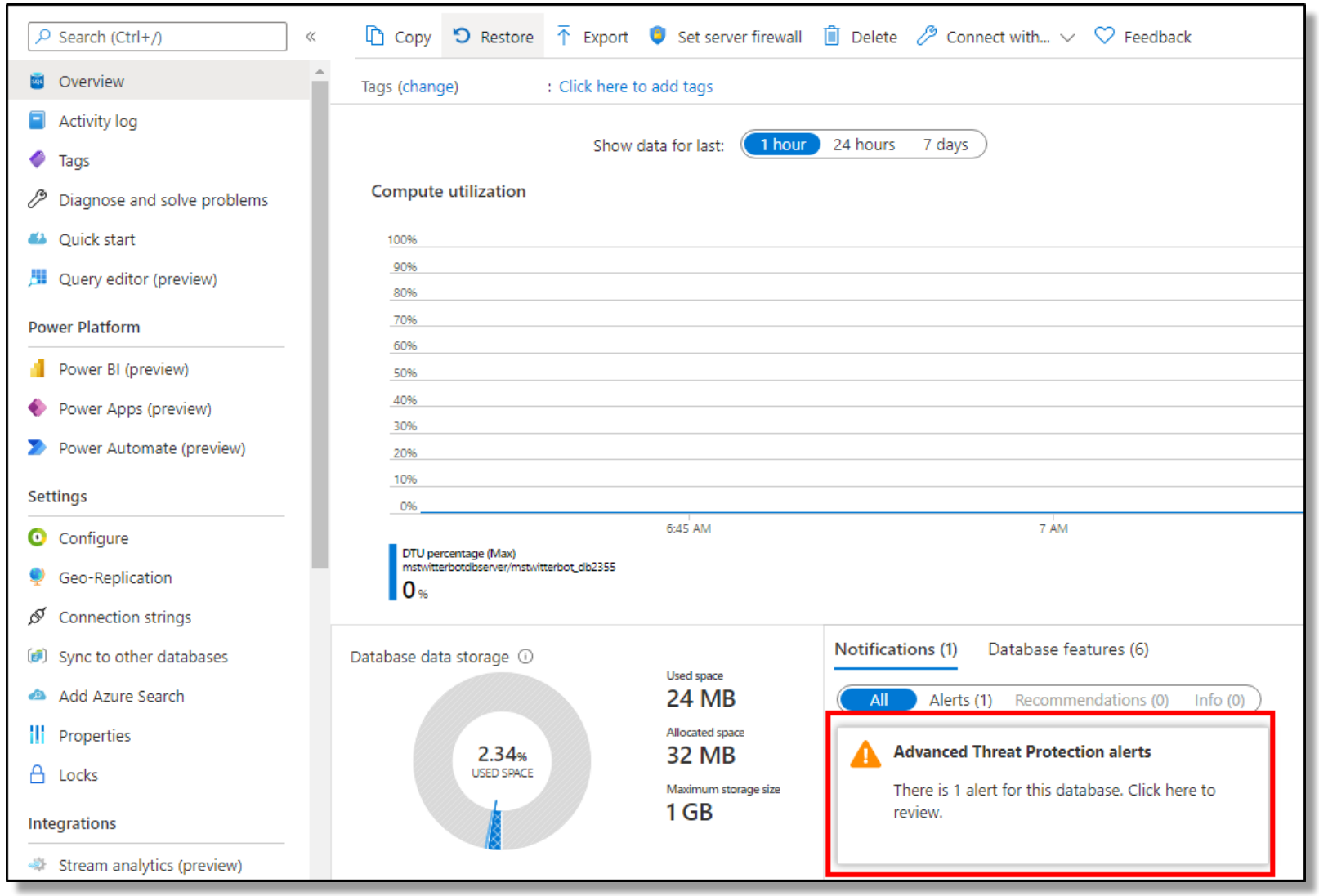
For SQL Injection alerts, the alert's details include the vulnerable SQL statement that was exploited.



Explore detection of a suspicious event -Explore alerts in the Azure portal

Advanced Threat Protection integrates its alerts with Microsoft Defender for Cloud.

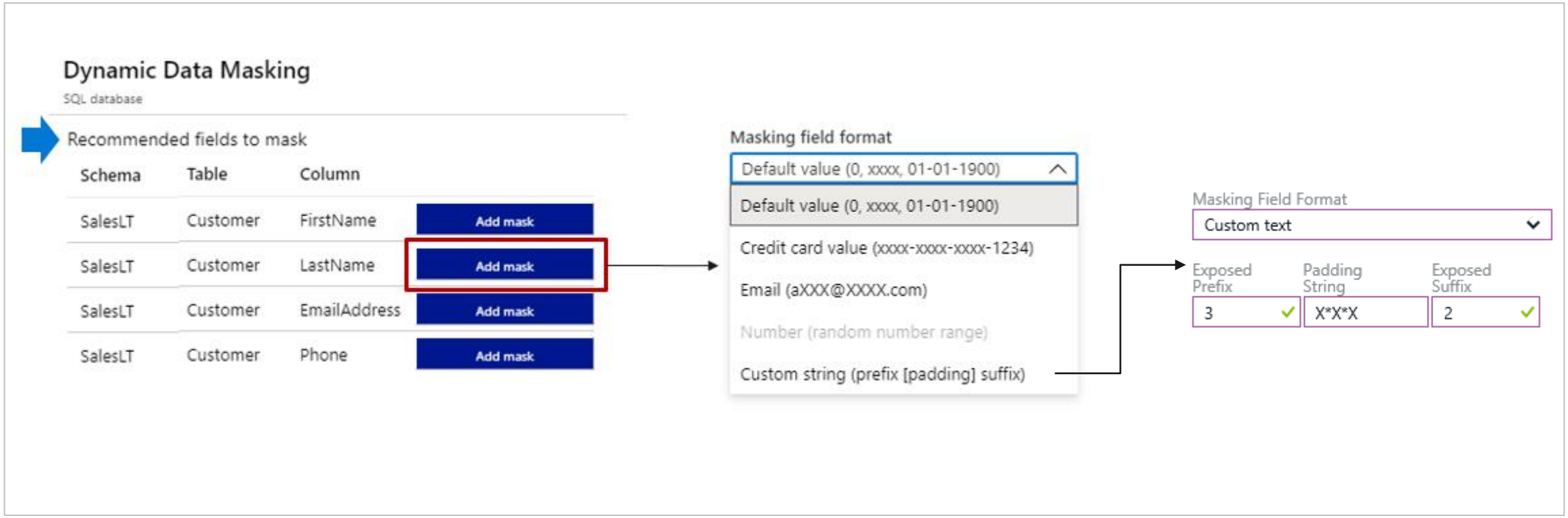
Live SQL Advanced Threat Protection tiles within the database and SQL Microsoft Defender for Cloud blades in the Azure portal track the status of active threats.



SQL vulnerability assessment express and classic configurations

Parameter	Express configuration	Classic configuration
Supported SQL Flavors	• Azure SQL Database (preview) • Azure Synapse Dedicated SQL Pools (formerly SQL Data Warehouse) (preview)	• Azure SQL Database • Azure SQL Managed Instance • Azure Synapse Analytics
Supported Policy Scope	• Subscription • Server	• Subscription • Server • Database
Dependencies	None	Azure storage account
Recurring scan	• Always active • Scan scheduling is internal and not configurable	• Configurable on/off • Scan scheduling is internal and not configurable
Supported Rules	All vulnerability assessment rules for the supported resource type.	All vulnerability assessment rules for the supported resource type.
Baseline Settings	• Batch – several rules in one command • Set by latest scan results. • Single rule	Single rule
Apply baseline	Will take effect without rescanning the database	Will take effect only after rescanning the database
Single rule scan result size	Maximum of 1 MB	Unlimited
Email notifications	Logic Apps	• Internal scheduler • Logic Apps
Scan export	Not supported	Excel format

Dynamic Data Masking



Masks sensitive data for non-privileged users

Administrators are excluded; you can add others

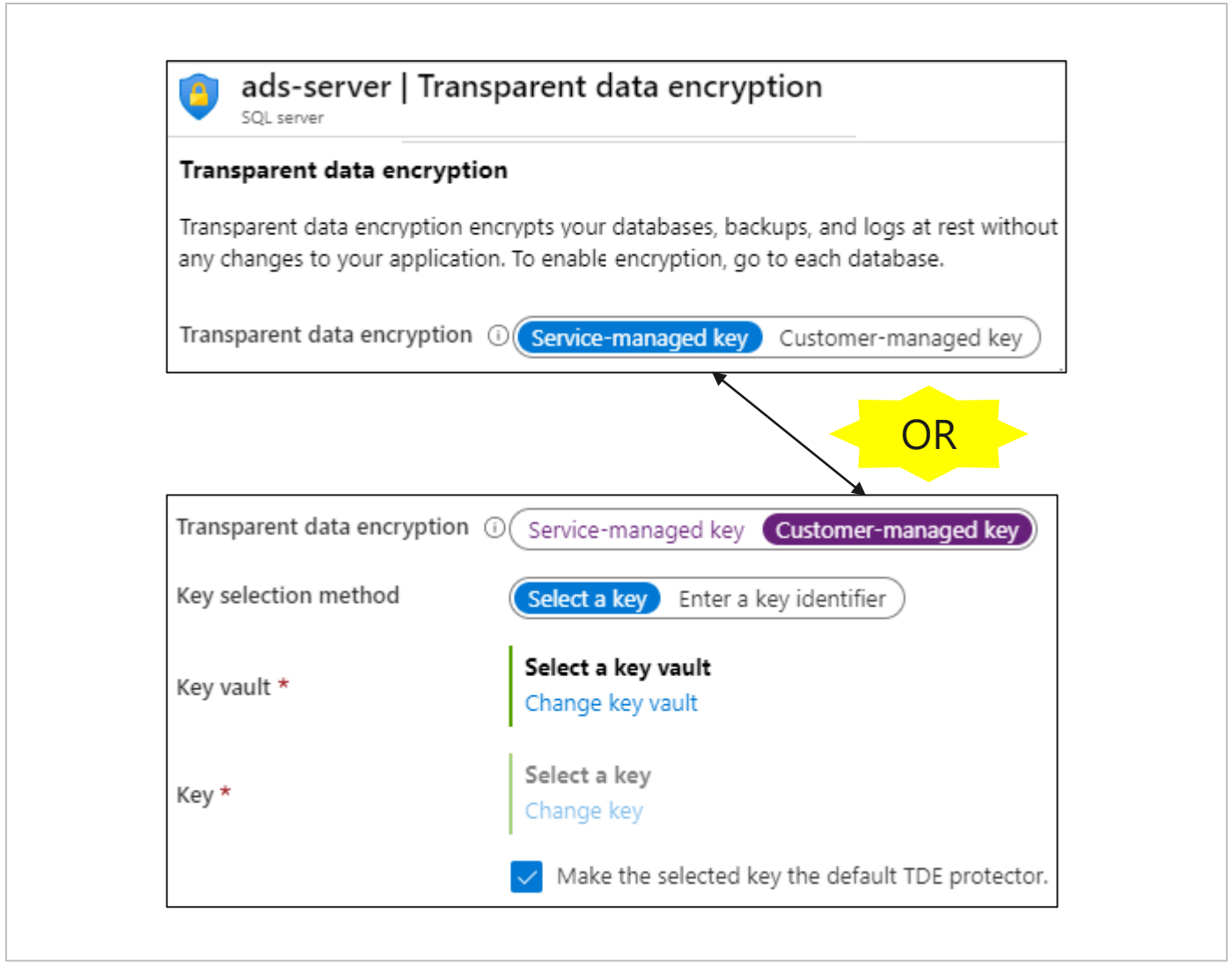
Rules apply the masking logic; several formats are available

Transparent Data Encryption

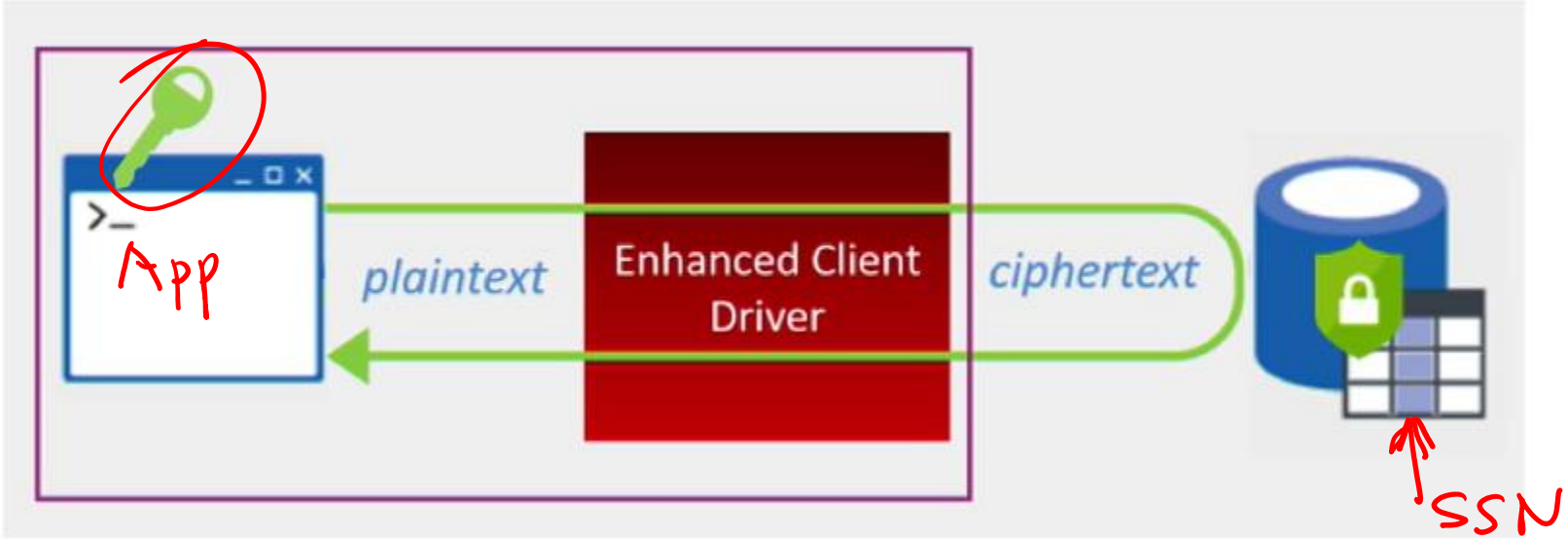
Protects databases, backups, and logs at rest – server level

Real-time page level encryption and decryption - service or customer managed keys

Supports Azure SQL Database (enabled by default), SQL Managed Instance , and Azure Synapse Analytics



Always Encrypted



Protects sensitive data at rest, in transit, and in use

Database data always remains encrypted

Data access is only from client applications and servers

Uses client-side encryption – enhanced client driver

Separates data owners from data managers

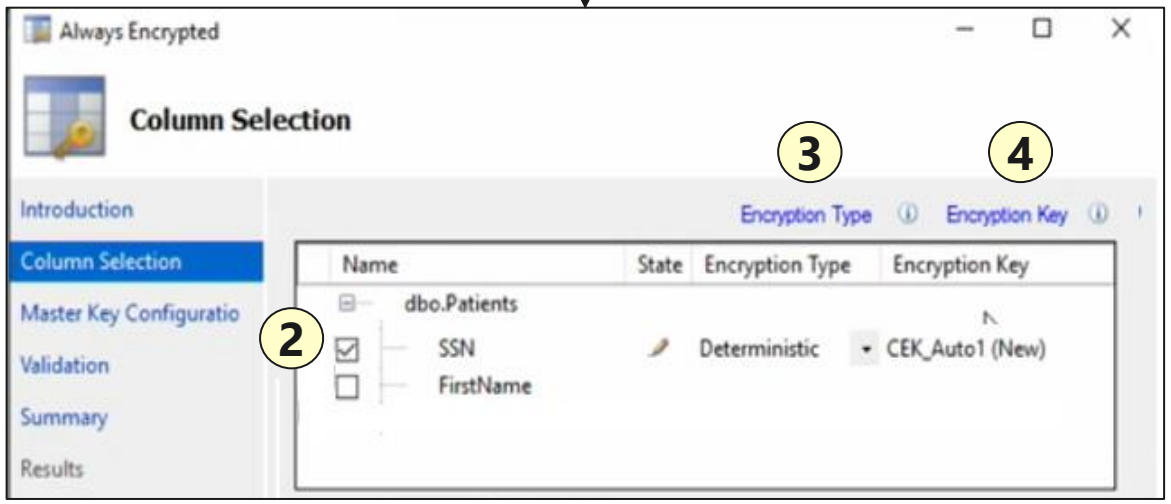
Always Encrypted - Implementation

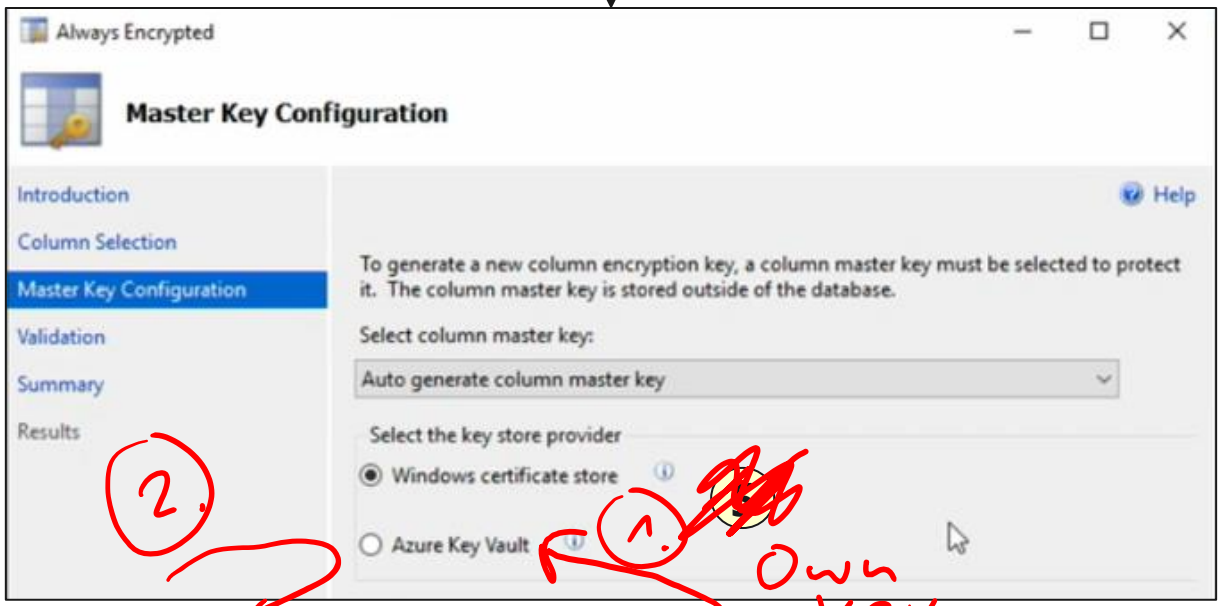
1 SSN	First Name

Always Encrypted Wizard

Column Master Keys encrypt the data

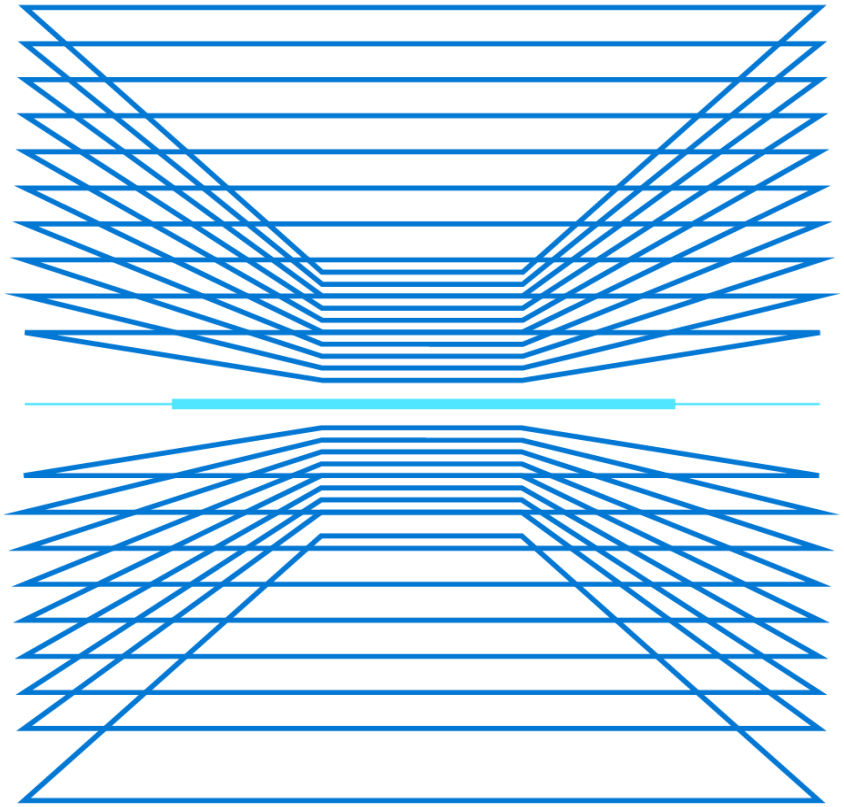
Master Key protects the column master keys





Demonstrations: Database Security

- Advanced Data Security and Auditing
- Diagnostics
- AAD Authentication



Additional Study – Database Security

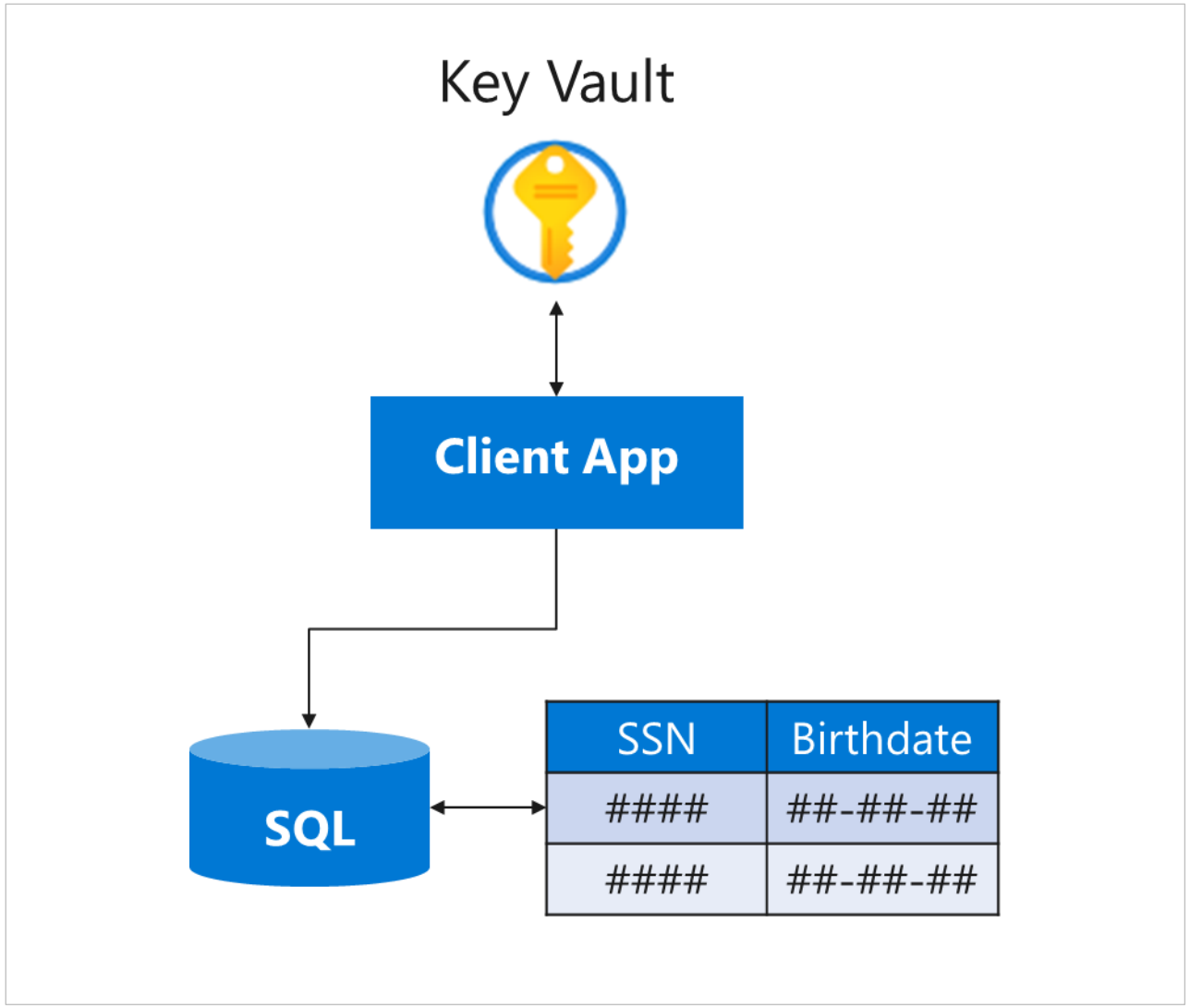
Module Review Questions	Microsoft Learn Modules (docs.microsoft.com/Learn)

- Provision an Azure SQL database to store application data (Exercise)
- Secure your Azure SQL Database (Exercise)
- Configure security policies to manage data (Exercise)
- Migrate your relational data stored in SQL Server to Azure SQL Database (Exercise)

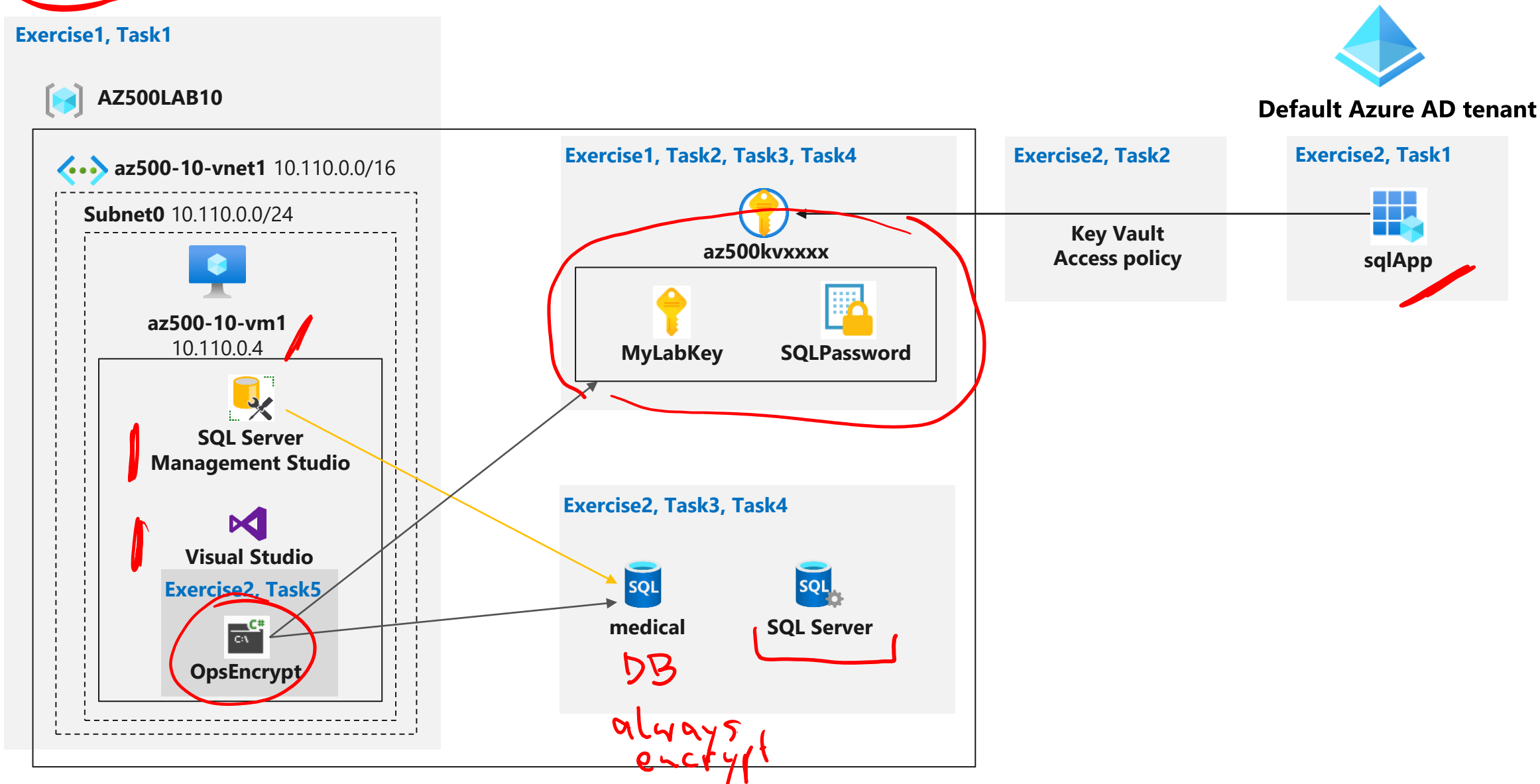
Module Labs

Lab 10 – Key Vault

- Create a Key Vault and configure permissions
- Add a key and a secret to the vault
- Register a client app that uses the key
- Create a SQL database
- Encrypt columns in a table
- Build a console app to test the encryption

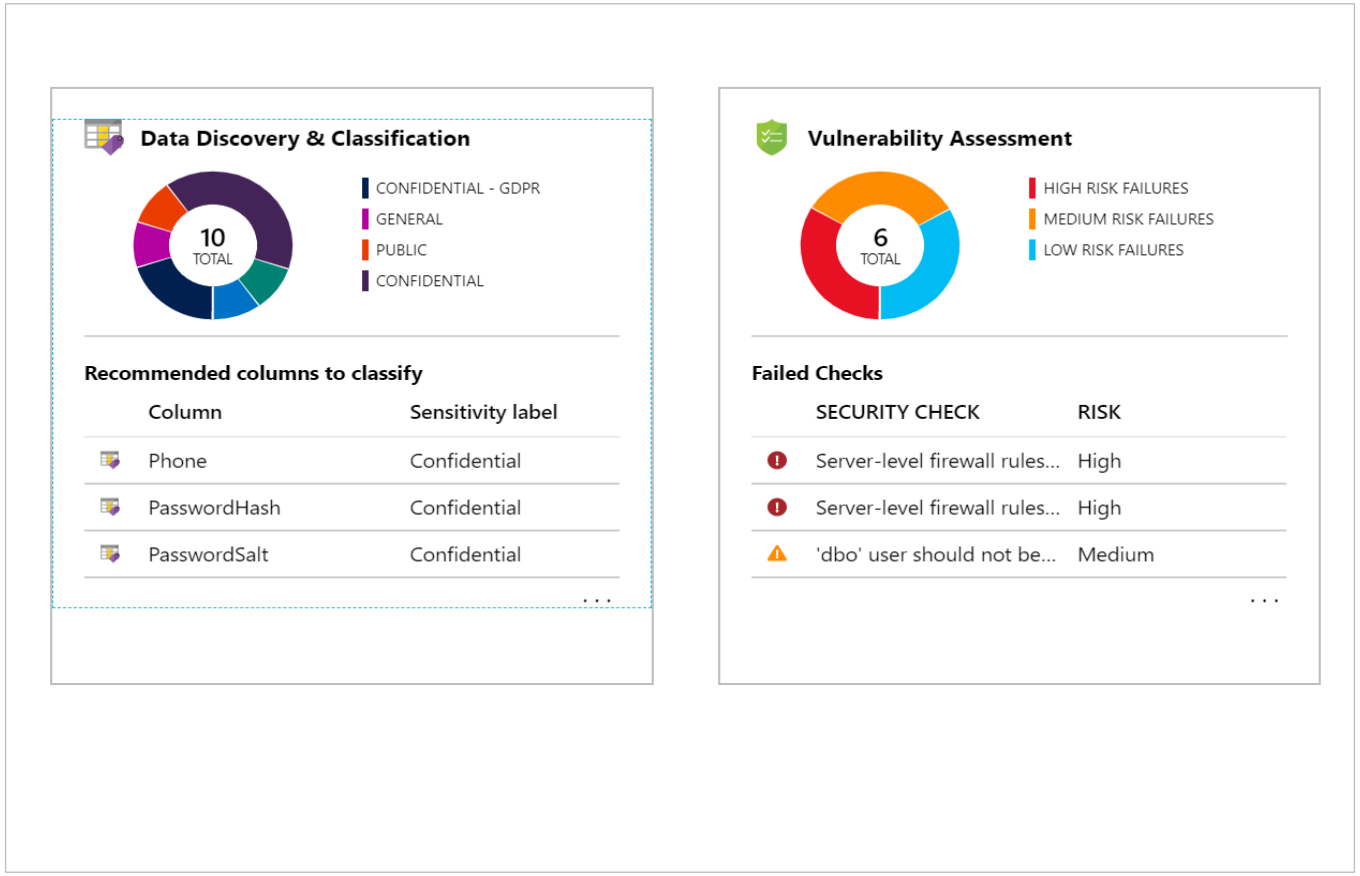


Lab 10 – Key Vault

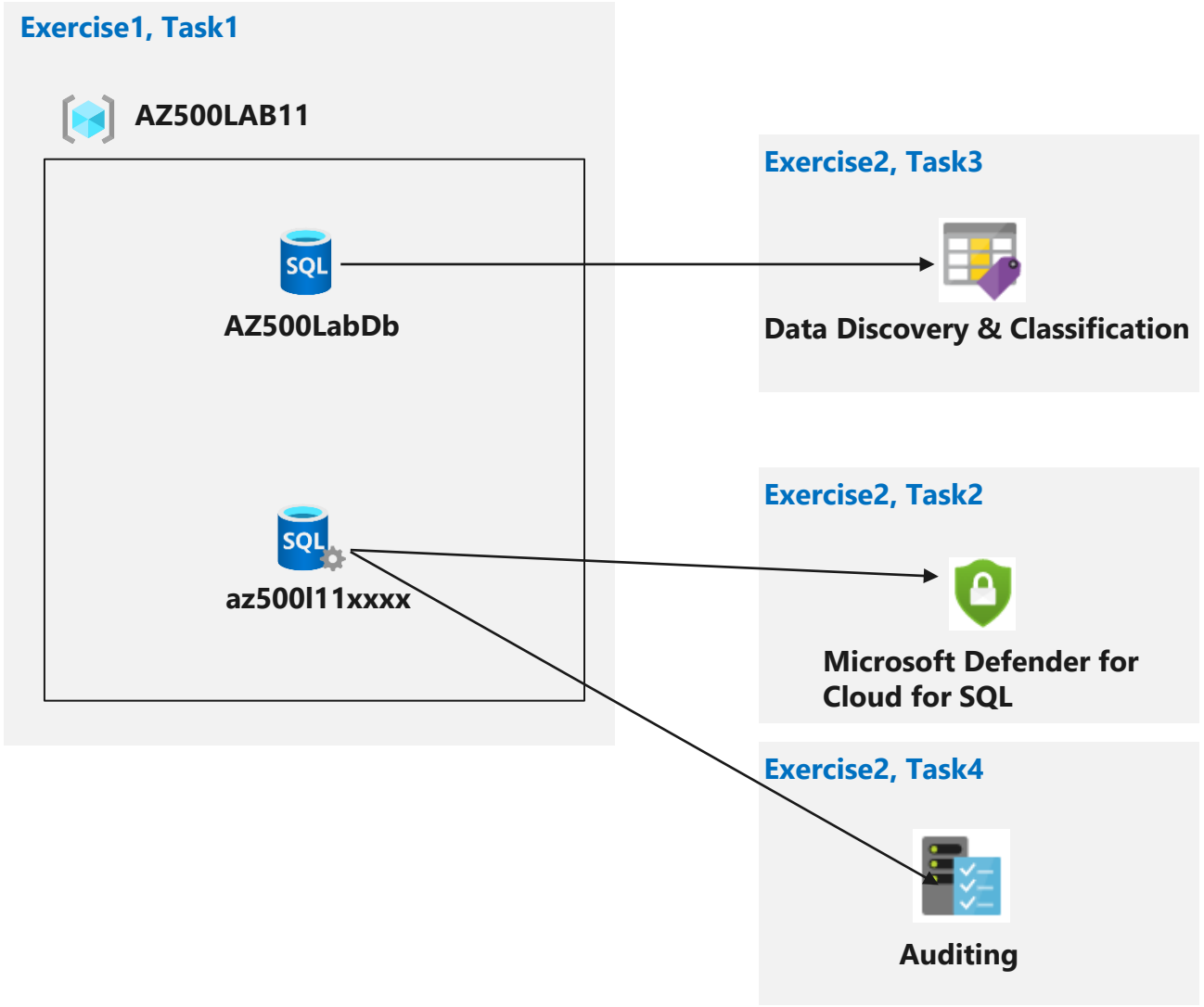


Lab 11 – Securing Azure SQL Database

- Deploy an Azure SQL Database
- Configure Advanced Data Protection
- Configure Data Classification
- Configure Auditing

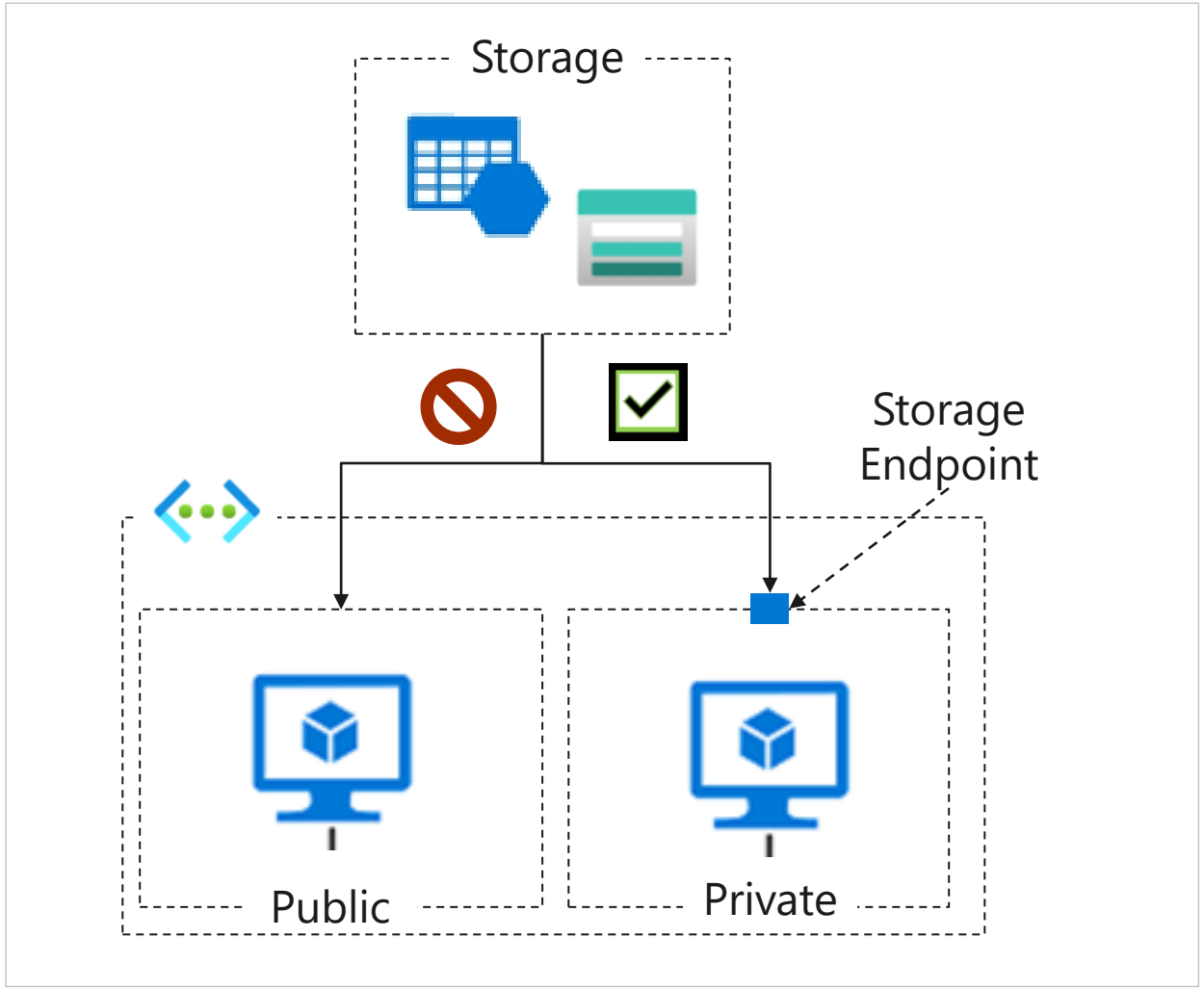


Lab 11 – Securing Azure SQL Database

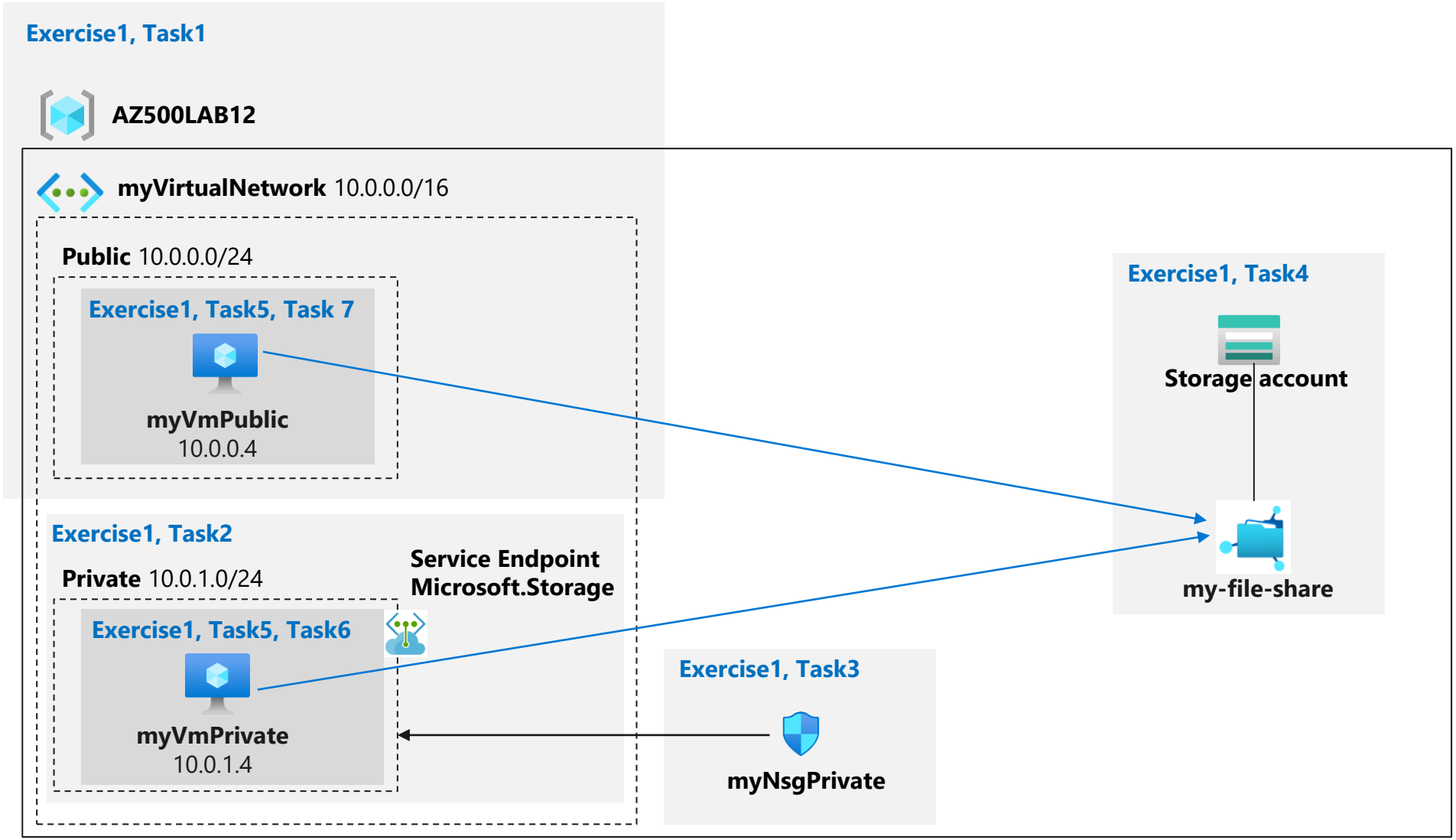


Lab 12 – Service Endpoints and Securing Storage

- Create a virtual network with a Public and Private subnet
- Create a storage endpoint for the Private subnet
- Create a storage account with a file share
- Configure a NSG with rules to allow access to storage and internet
- Confirm storage access from the private subnet
- Confirm storage access is denied from the public subnet



Lab 12 – Service Endpoints and Securing Storage



End of presentation