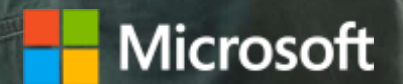


Data Platform Security in Azure

Robin Lester



GDPR with data - common themes

- Key tooling to consider
 - Discovery - Azure Data Catalog
 - SQL encryption technologies
- Right to be forgotten – do I have to delete emails, backups etc?
 - Rights can not overwrite the rights of others
 - As long as processes are in place backup strategy can still stand

Azure Key Vault



Organizations need to safeguard certificates deployed into their VMs.



1



Developers need to safeguard config secrets of their Azure cloud services.

e.g. Storage account key
SQL connection string

2



Organizations need to control encryption keys used by their OWN apps.



3



Organizations need to control encryption keys used by SaaS services.



4

What is Azure Key Vault?

- An Azure resource provider that lets you
 - Store & manage SECRETS (esp app config), and release them at runtime to authorized apps & users.
 - Store & manage KEYS, and perform cryptographic operations on behalf of authorized apps & users.
- Backed by Hardware Security Modules
 - All secrets and keys are protected at rest with key chain terminating in HSMs.
 - Keys marked as 'HSM-protected' are protected even at runtime with HSMs.

Terminology

- Key Vault

- Container for related keys and secrets that are managed together.
- Unit of access control, unit of billing.
- An Azure resource, like a storage account.

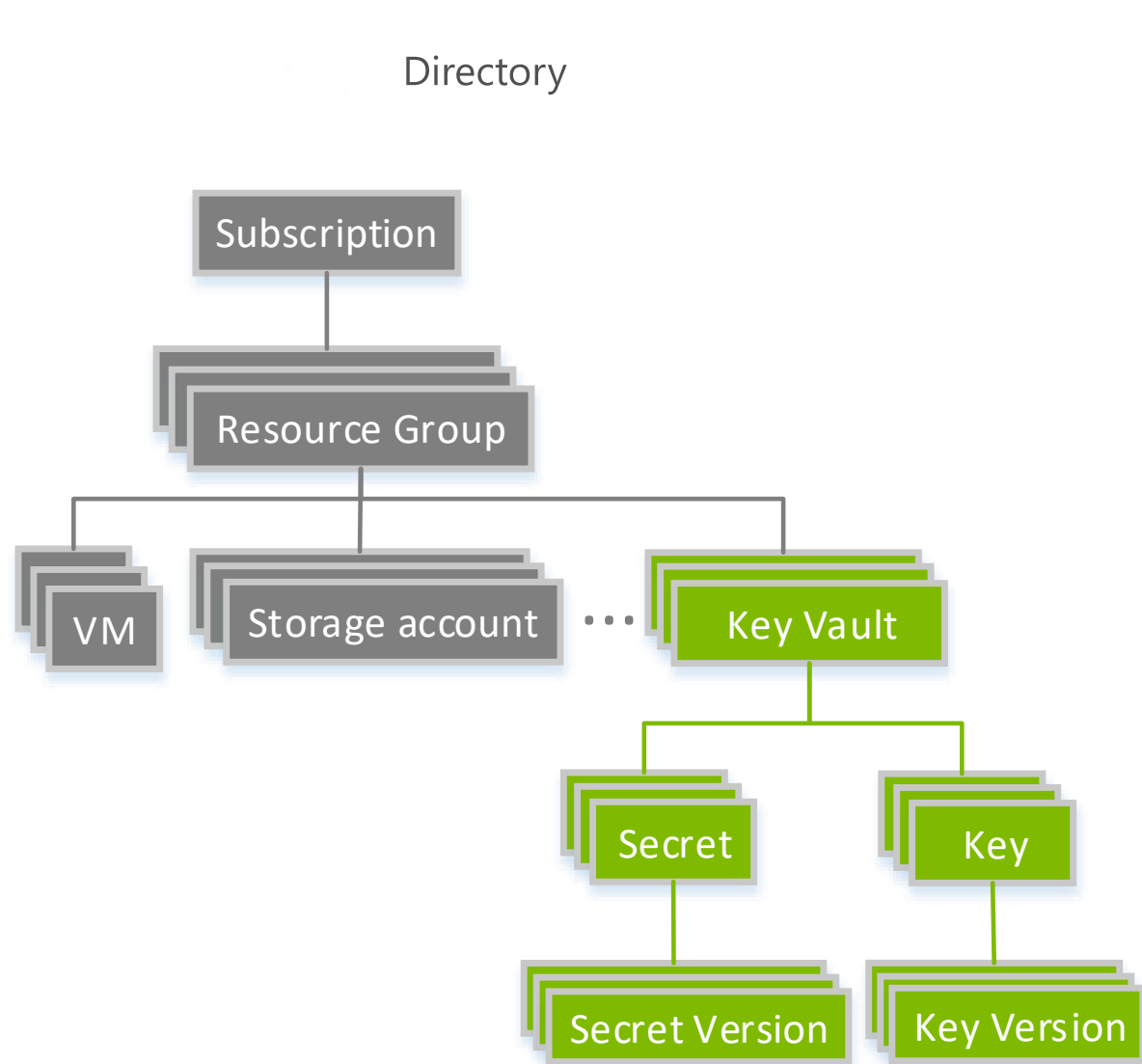
- Secret

- What: Any sequence of bytes under 25KB. E.g. SQL connection string, Storage account key.
- How used: Authorized users/apps write and read back the secret value.

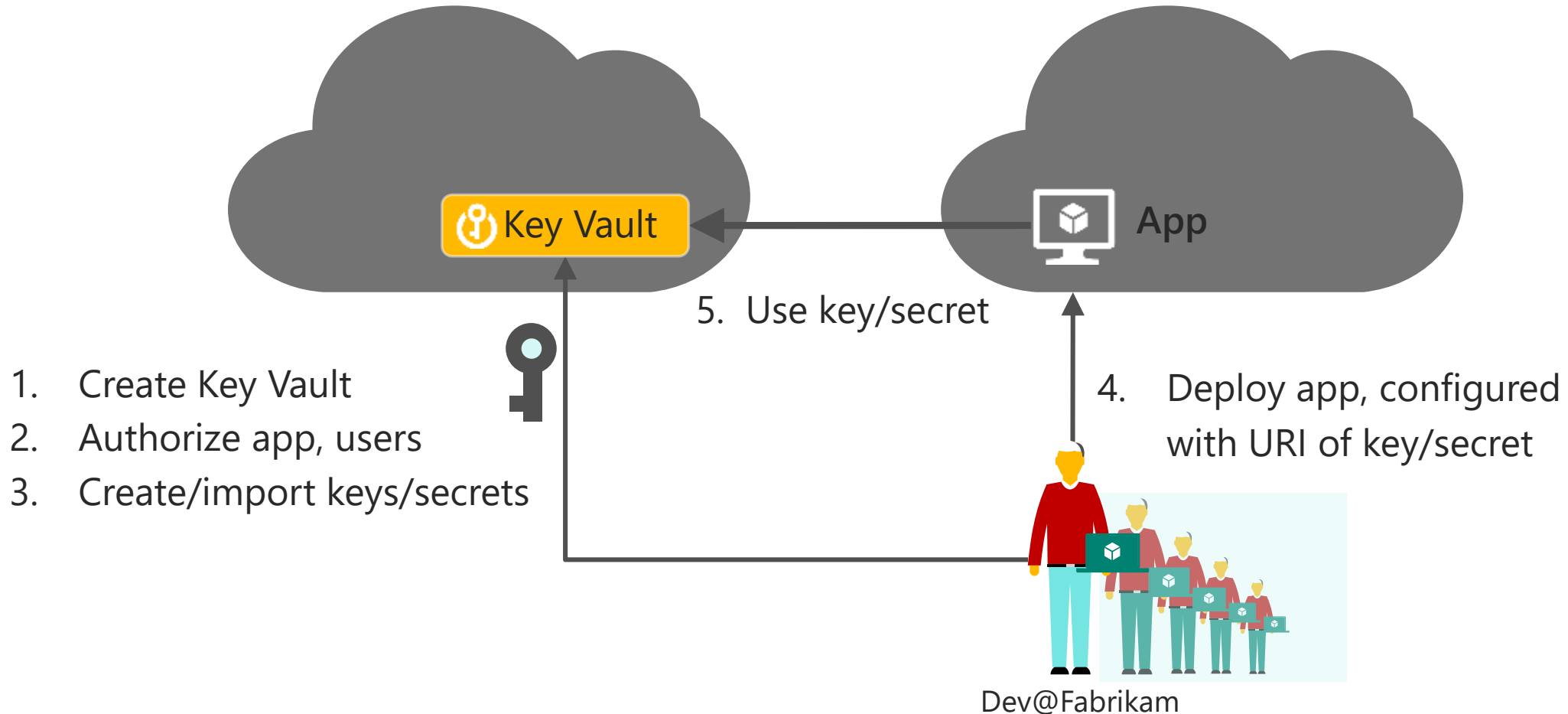
- Key

- What: A cryptographic key. RSA 2048.
- How used: A key cannot be read back. Caller must ask the service to decrypt / sign with the key.

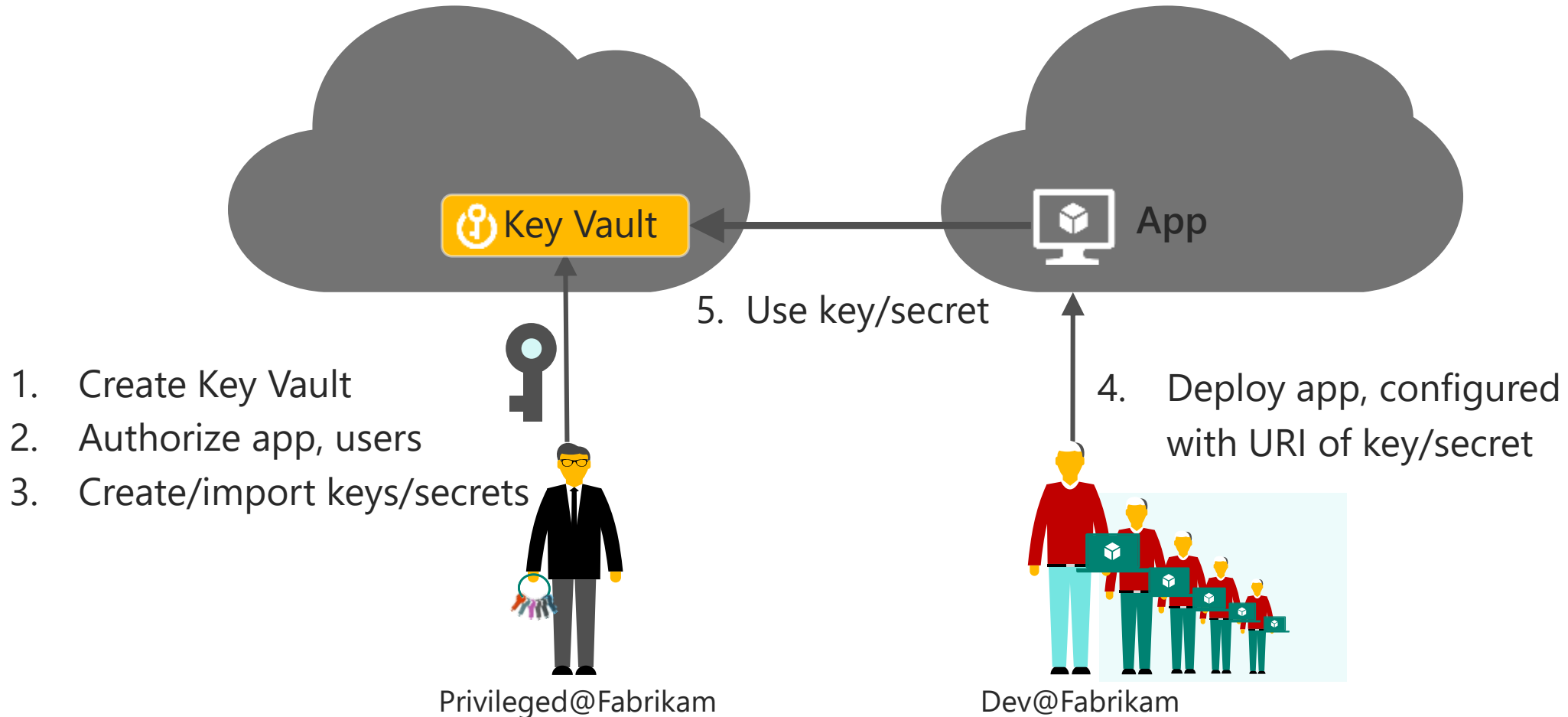
Key Vault within Azure object model



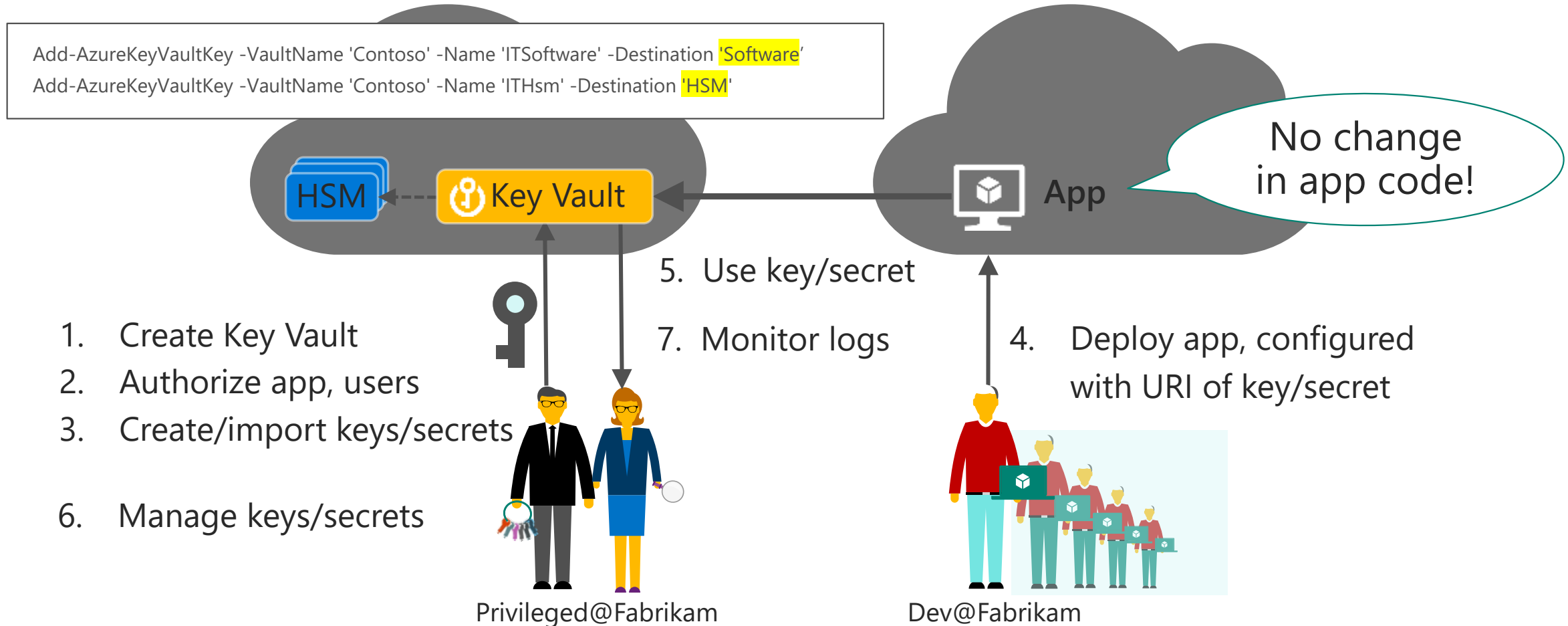
Phase 1: Developer builds/tests application



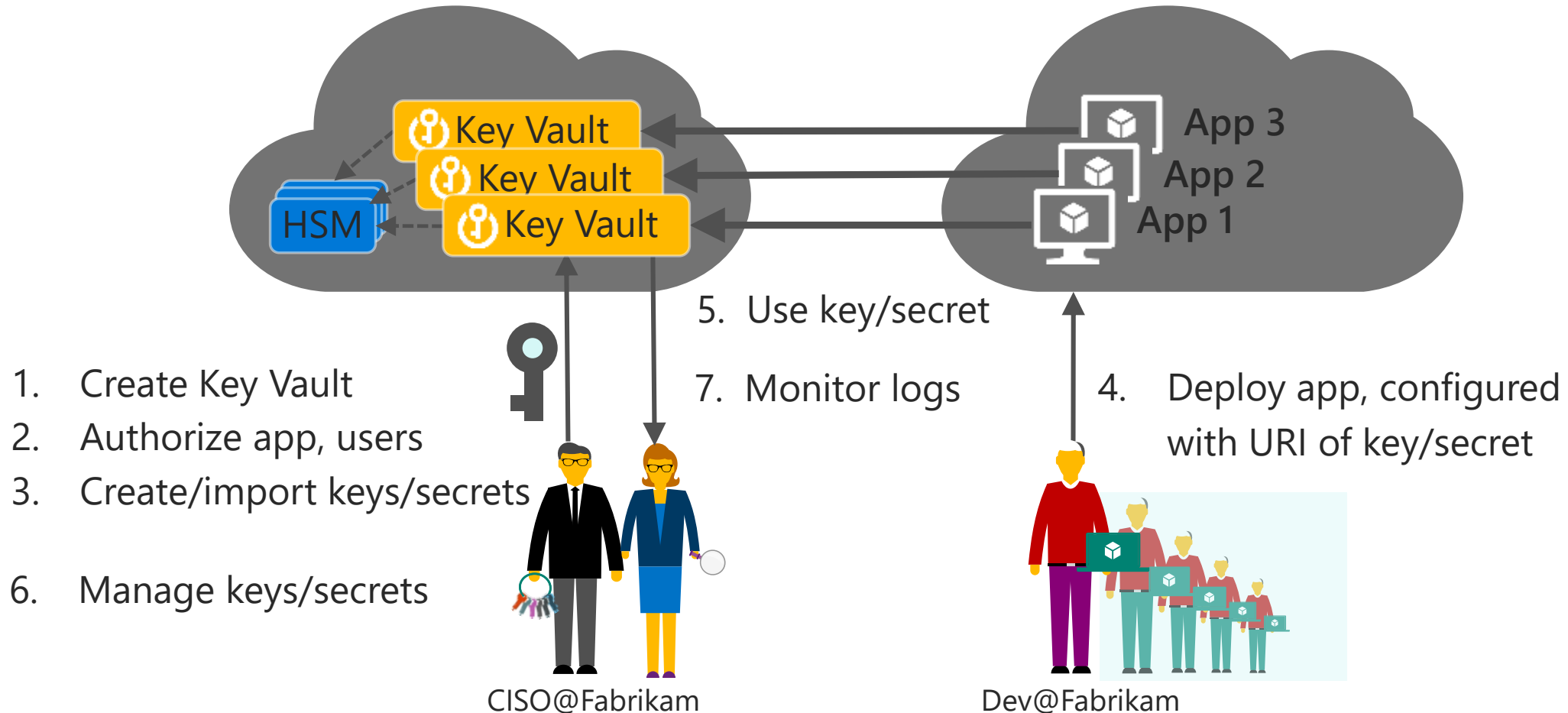
Phase 2: App moves into pilot / pre-prod



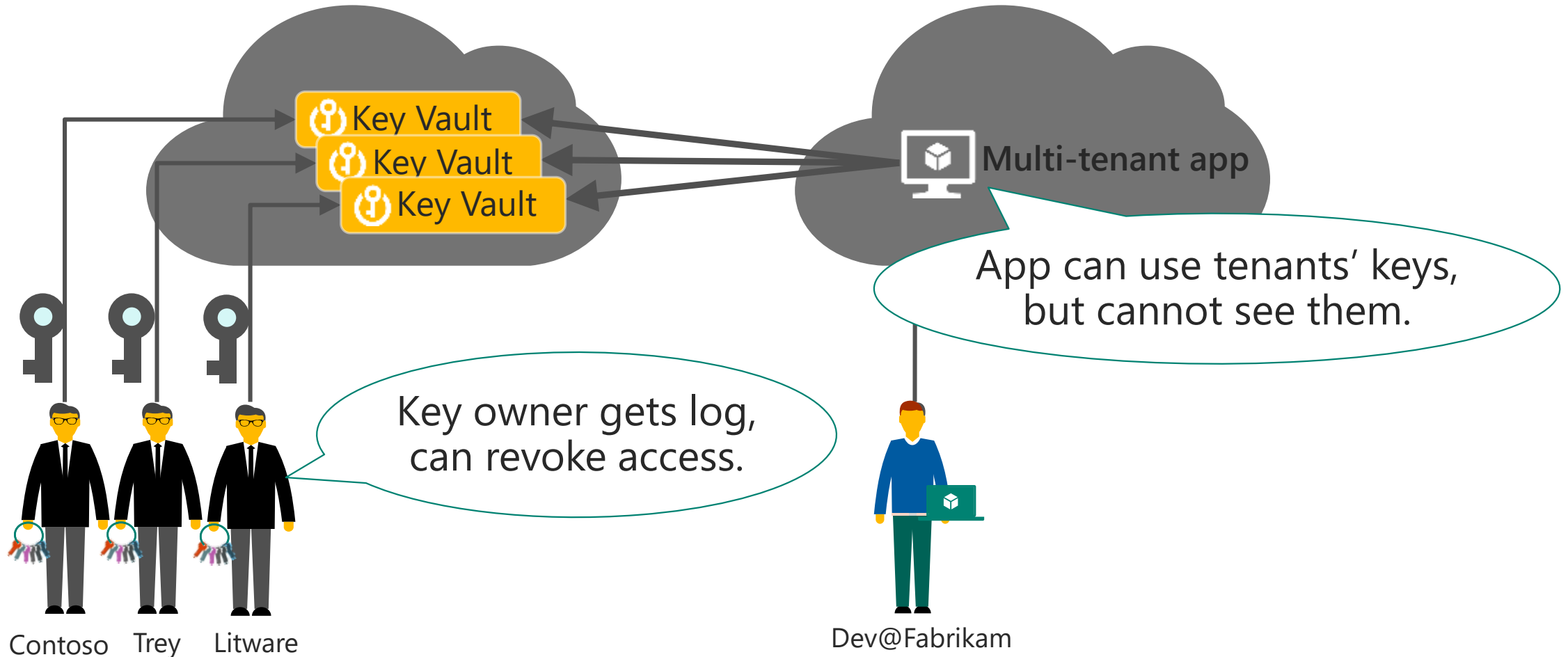
Phase 3: App moves into production



Phase 4: Scale, deploy more apps in minutes



Multi-tenant app offers customer-managed keys



KeyVault Application Setup

- Create a local certificate
- Create an application in Azure Active Directory
 - Using the certificate
- Create a KeyVault
- Allow the application permission to the KeyVault

```
$certificateName = "$applicationName" + "cert"  
$myCertThumbprint = (New-SelfSignedCertificate -Type Custom -Subject
```

```
Set-AzureRmKeyVaultAccessPolicy  
-VaultName $vaultName  
-ObjectId $servicePrincipal.Id  
-PermissionsToKeys all  
-PermissionsToSecrets all  
-PermissionsToCertificate all
```

```
$now = [System.DateTime]::Now  
$oneYearFromNow = $now.AddYears(1)
```

Connecting an app to the Keyvault

- Demo

Admin

- Demo



```
#Set up logging
#Create an new storage account for the logs
$sa = New-AzureRmStorageAccount -ResourceGroupName rgdemovaltra1 -Name keyvaultlogsra1
-
-Type Standard_LRS -Location 'NorthEurope'
#Get the keyvault we want to turn on auditing on
$kv = Get-AzureRmKeyVault -VaultName 'demoVaultra1'
#Turn on logging - retention 30 days
Set-AzureRmDiagnosticSetting -ResourceId $kv.ResourceId -StorageAccountId $sa.Id `
-Enabled $true -Categories AuditEvent -RetentionEnabled $true -RetentionInDays 30
#Test the log by querying the keyvault
Get-AzureKeyVaultSecret -VaultName 'demoVaultra1' -Name "ConnectionString"
```

Log Analytics

Diagnostics settings

Save

Discard

Delete

Name

service

☒ Archive to a storage account

Storage account

keyvaultlogsral

>

☐ Stream to an event hub

☒ Send to Log Analytics

Log Analytics

Configure

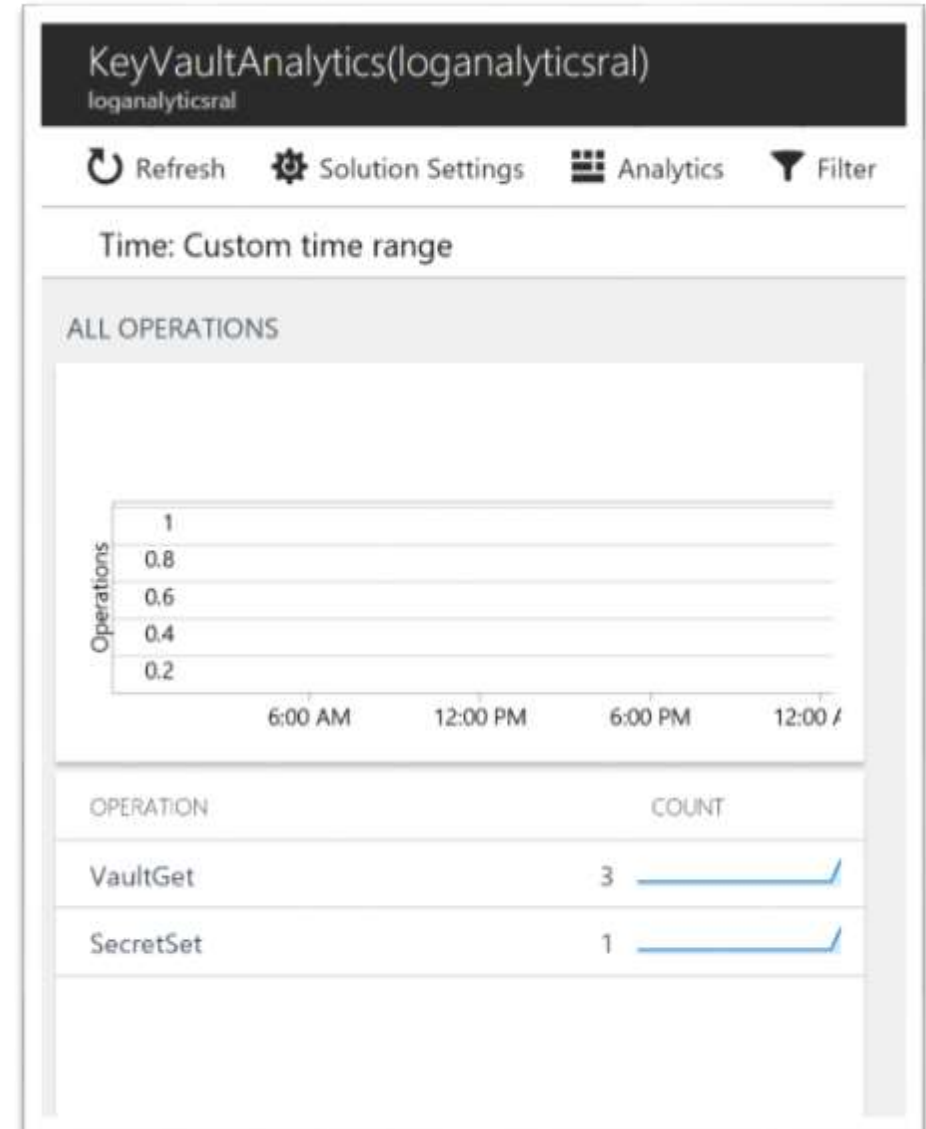
>

LOG

☒ AuditEvent




Retention (days) ?

30

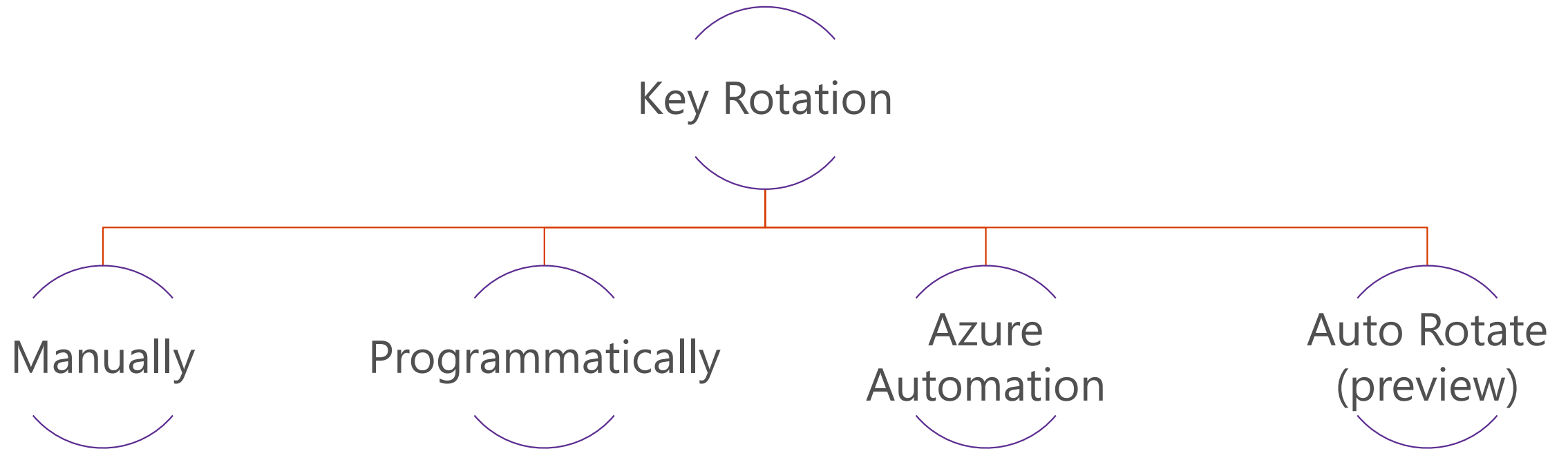


Key Vault Versioning

- Demo
- Encrypt
 - Should always be the latest version
- Decrypt
 - Should be the version that was used to encrypt the version of the data

ConnectionString Versions			
<div> New Version  Refresh  Delete</div>			
VERSION	STATUS	ACTIVATION DATE	EXPIRATION DATE
CURRENT VERSION			
d9d65b7003c44...	✓ Enabled		
OLDER VERSIONS			
458bad54069f43...	✓ Enabled		
c694a5bb972e4b...	✓ Enabled		

Key Vault



Storage

Blob Storage

- Account keys 512-bit strings
- Primary and secondary keys for key rotation
- Manual Key Vault rotation
 - App is using key 1
 - Regenerate key 2
 - Swap app to use key 2
 - Regenerate key 1
- Or use key vault for key rotation

Blob Storage

- Shared Access Signatures (SAS)
 - Give the client just the permissions they need for a limited amount of time
 - Can revoke without affecting anyone else
 - Requests can be restricted to an IP address and can be restricted to https
- Secure Transfer Required
 - Enforced https connections

Deployment model ⓘ

Resource manager Classic

Account kind ⓘ

General purpose ▼

Performance ⓘ

Standard Premium

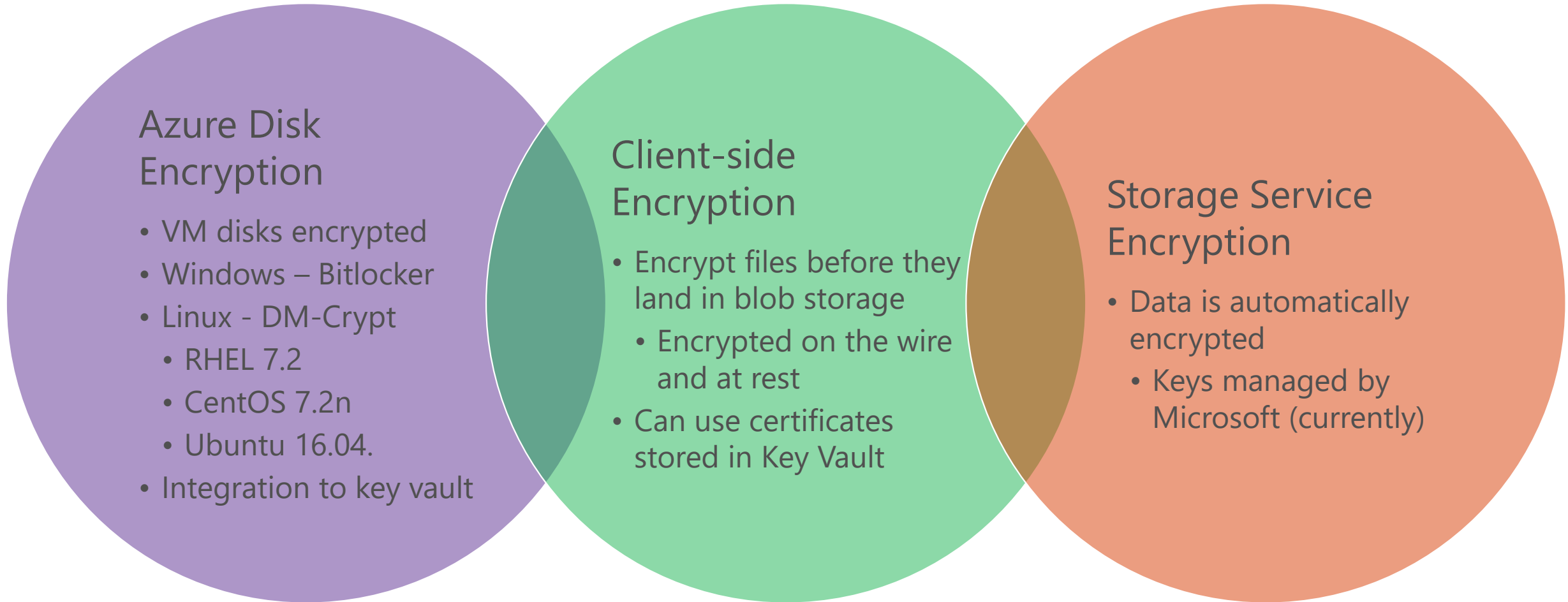
Replication ⓘ

Locally-redundant storage (LRS) ▼

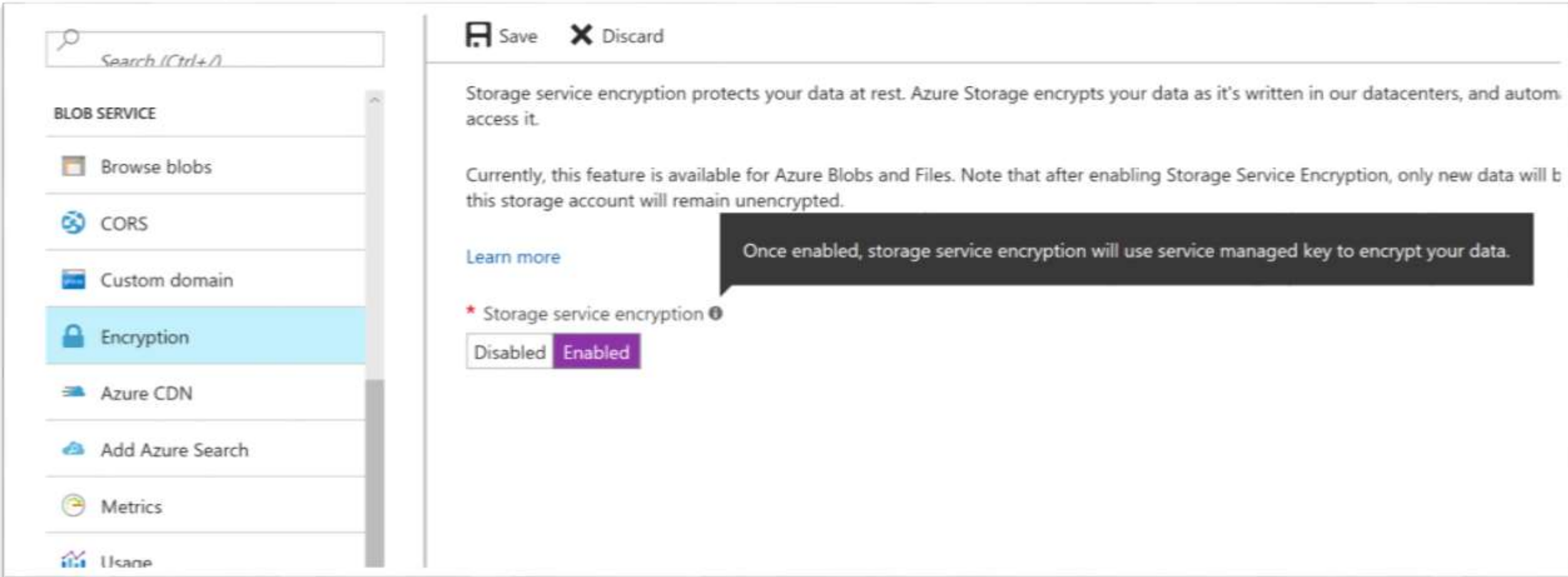
★ Secure transfer required ⓘ

Disabled Enabled

Blob Storage Encryption Options



Azure Storage Service Encryption for Data at Rest



The screenshot shows the Azure Storage Service Encryption settings page. On the left is a navigation pane with a search bar and a list of services: BLOB SERVICE, Browse blobs, CORS, Custom domain, Encryption (highlighted), Azure CDN, Add Azure Search, Metrics, and Uptime. The main content area has a 'Save' button and a 'Discard' button. It contains a paragraph explaining that storage service encryption protects data at rest and is available for Azure Blobs and Files. Below this is a 'Learn more' link and a toggle switch for 'Storage service encryption' which is currently set to 'Enabled'. A dark callout box states: 'Once enabled, storage service encryption will use service managed key to encrypt your data.'

Search (Ctrl+I)

BLOB SERVICE

- Browse blobs
- CORS
- Custom domain
- Encryption**
- Azure CDN
- Add Azure Search
- Metrics
- Uptime

Save Discard

Storage service encryption protects your data at rest. Azure Storage encrypts your data as it's written in our datacenters, and automatically access it.

Currently, this feature is available for Azure Blobs and Files. Note that after enabling Storage Service Encryption, only new data will be encrypted. Existing data in this storage account will remain unencrypted.

[Learn more](#)

★ Storage service encryption ⓘ

Disabled **Enabled**

Once enabled, storage service encryption will use service managed key to encrypt your data.

Blob Virtual Network Service Endpoints

The screenshot displays the Azure portal interface for configuring Blob Virtual Network Service Endpoints. The left sidebar contains a search bar and a list of navigation items: 'Firewalls and virtual networks...', 'Metrics (preview)', 'Properties', 'Locks', 'Automation script', and a section titled 'BLOB SERVICE' which includes 'Browse blobs', 'CORS', 'Custom domain', 'Encryption', 'Azure CDN', 'Add Azure Search', and 'Metrics'. The main content area has a top bar with 'Save' and 'Discard' buttons. Below this, the 'Allow access from' section shows 'Selected networks' as the chosen option. The 'Virtual networks' section provides links to 'Add existing virtual network' and 'Add new virtual network'. A table with headers 'VIRTUAL NETW...', 'SUBNET', 'ADDRESS RAN...', 'ENDPOINT ST...', 'RESOURCE GR...', and 'SUBSCRIPTION' is present, but it is empty with the message 'No network selected.' below it. The 'Firewall' section includes a link to 'Learn more' and an 'ADDRESS RANGE' section with a text input field containing the placeholder 'IP address or CIDR'. The 'Exceptions' section at the bottom has three checkboxes: 'Allow trusted Microsoft services to access this storage account' (checked), 'Allow read access to storage logging from any network' (unchecked), and 'Allow read access to storage metrics from any network' (unchecked).

Search (Ctrl+/)

Save Discard

Allow access from

☐ All networks ☒ Selected networks

Configure network security for your storage accounts. [Learn more.](#)

Virtual networks

Secure your storage account with virtual networks. [+ Add existing virtual network](#)
[+ Add new virtual network](#)

VIRTUAL NETW...	SUBNET	ADDRESS RAN...	ENDPOINT ST...	RESOURCE GR...	SUBSCRIPTION
No network selected.					

Firewall

Add IP ranges to allow access from the internet or your on-premises networks. [Learn more.](#)

ADDRESS RANGE

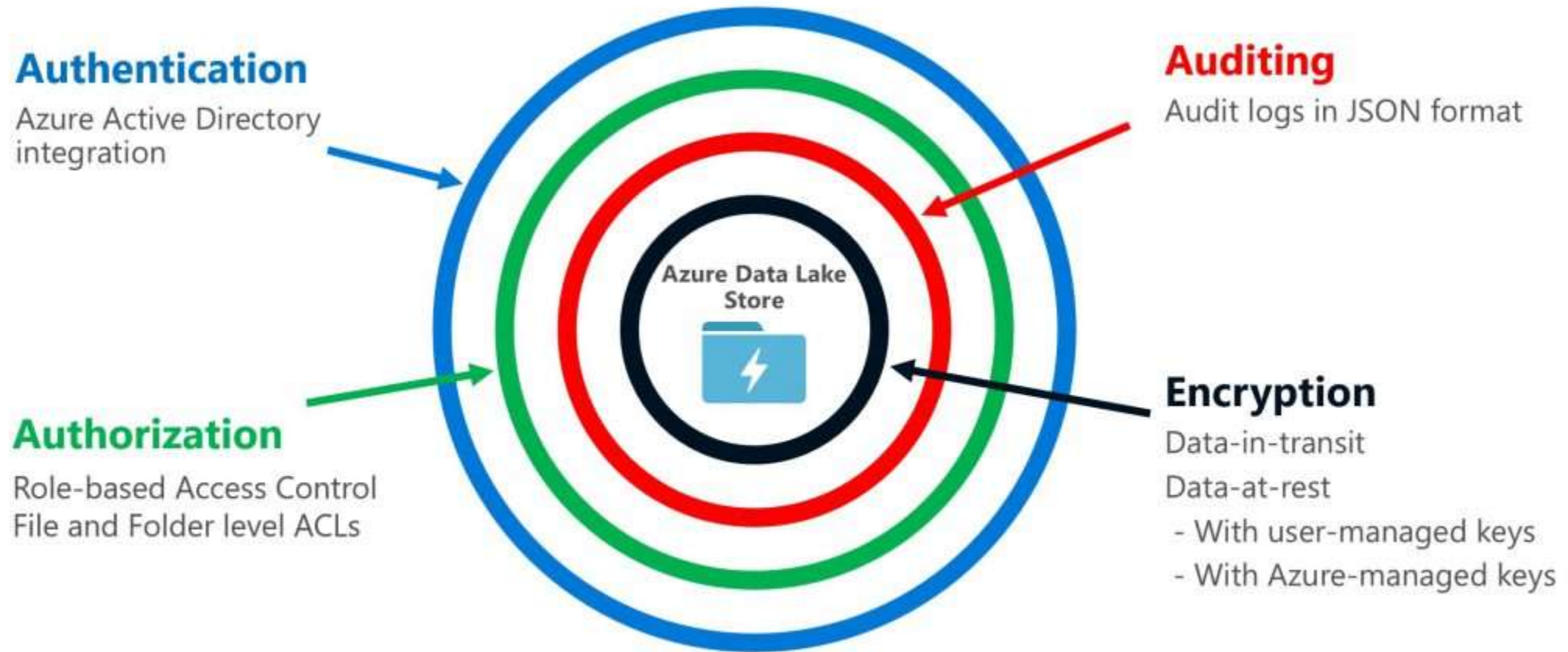
Exceptions

☒ Allow trusted Microsoft services to access this storage account ⓘ




☐ Allow read access to storage logging from any network

☐ Allow read access to storage metrics from any network


Data lake Store - Always encrypted, role-based security, ACLs and Auditing



Data Lake Store Firewall

 Save  Discard  Add Client IP

Enable Firewall ON OFF



"Allow Azure Services" must be turned on to allow Azure services and applications to connect to this Data Lake Store account. If this option is not turned on, analytics services such as Data Lake Analytics jobs or HDInsight clusters using this account will fail due to access issues. This option is also required for other services such as Data Factory, Data Warehouse, etc to connect to this account.

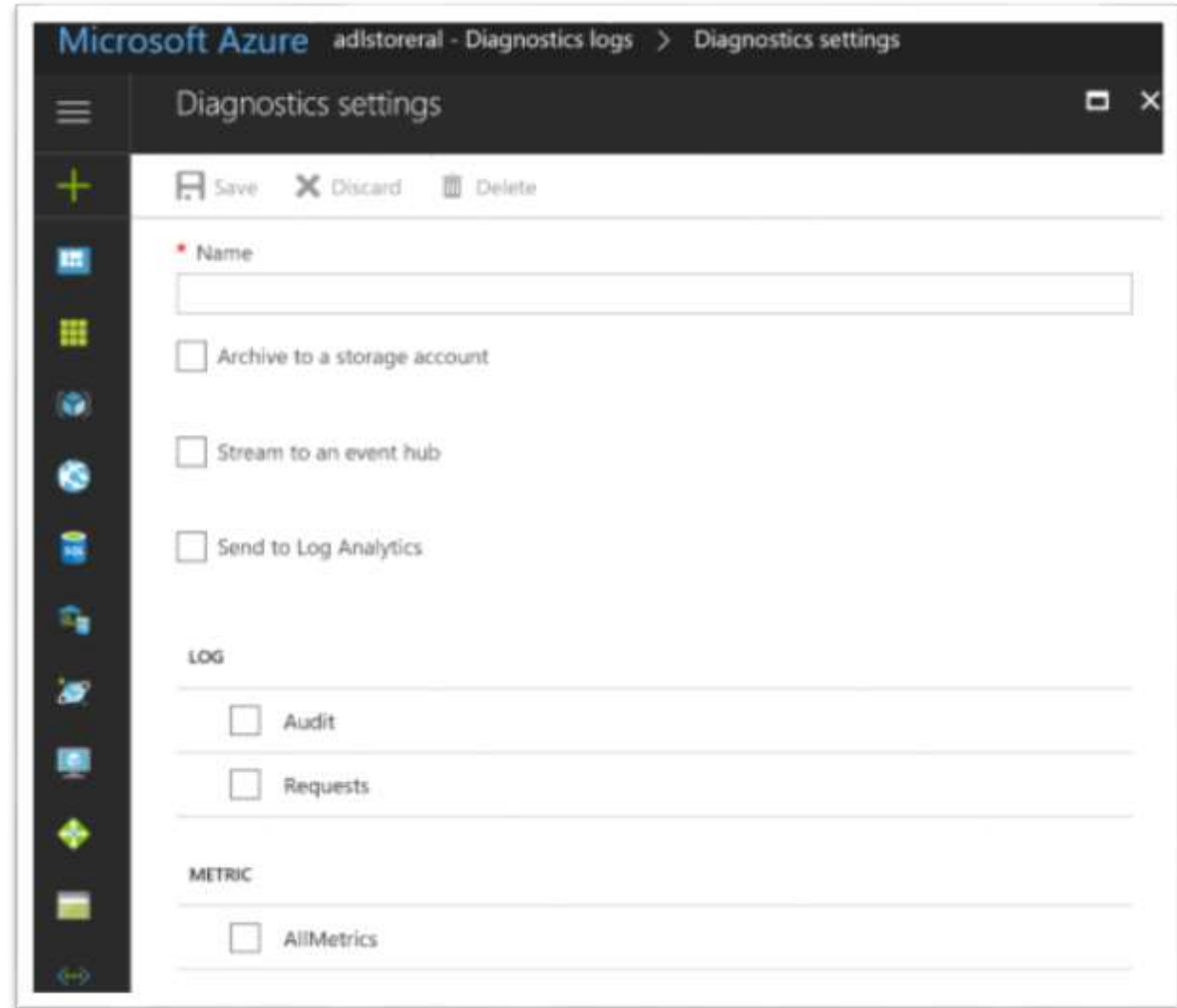
Allow access to Azure services ON OFF

Client IP Address [151.230.53.215](#)

RULE NAME	START IP	END IP
No entries.		
<input type="text"/>	<input type="text"/>	<input type="text"/> ...

Data lake Store

- Enabling Auditing



Microsoft Azure adlstoreal - Diagnostics logs > Diagnostics settings

Diagnostics settings

Save Discard Delete

* Name

☐ Archive to a storage account

☐ Stream to an event hub

☐ Send to Log Analytics

LOG

☐ Audit

☐ Requests

METRIC

☐ AllMetrics

Data lake Store

- Azure AD Integrations

Access
Books (Folder)

+ Add

Save

Discard

Advanced

Your Permissions

rolester@microsoft.com's effective permissions on this folder are: Read,Write,Execute.

i

You have superuser privileges on this account.

Owners	Read	Write	Execute
<div><div></div><div>Robin Lester</div><div>Robin.Lester@microsoft.com</div></div>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
<div><div></div><div>Robin Lester</div><div>Robin.Lester@microsoft.com</div></div>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>

Assigned Permissions

spark101s

☒

☒

☒

Everyone Else

Users not covered above will be limited by these permissions

☐

☐

☐

Assign Permissions

Select User or Group

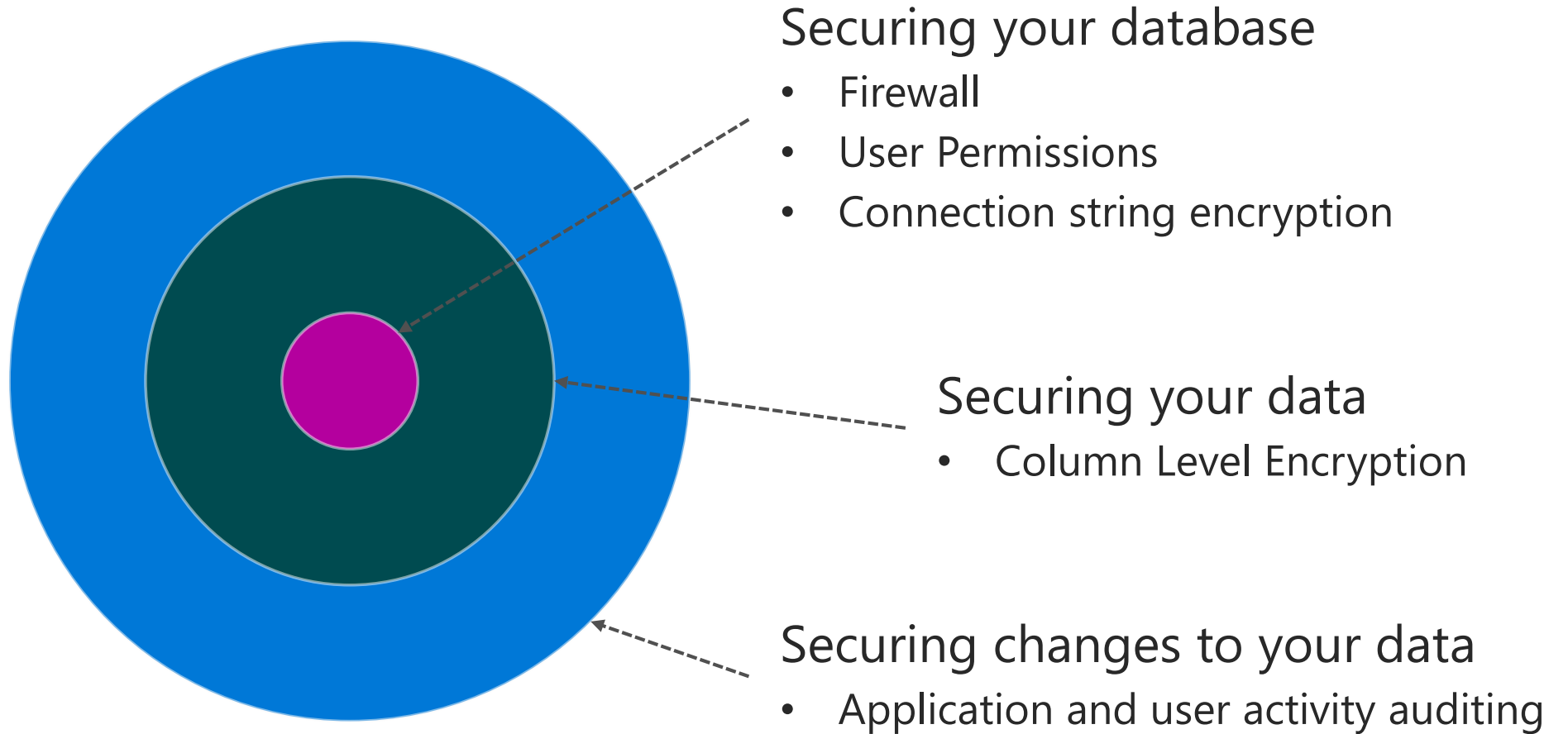
Configure required settings

Select Permissions

Configure required settings

Azure SQL Database

Layered Approach to Security



SQL Security Landscape



Application Access

Dynamic Data Masking

Limit exposure of sensitive data by masking it to non-privileged users

Row-level Security

Keep multi-tenant databases secure from unauthorized access by other users who share the same tables

Database Access

SQL Authentication

SQL built-in identity management and server authentication (aka SQL logins)

SQL Permissions

SQL agent roles that enable management of permissions, e.g. for data selection and modification

SQL Firewall

Prevention of access to the SQL server unless the IP address of the SQL client is specified

Azure Active Direct. Authentication

Azure central identity management, which combats proliferation of identities

Proactive Monitoring

Auditing

Track database activity and log directly to your Azure storage account

SQL Threat Detection

Receive alerts on anomalous database activity in the form of common database threats

Data Encryption

Encryption in flight

Encrypt data that is transmitted across the network, protecting against snooping & man-in-the-middle attacks

Encryption-at-rest (TDE)

Server-side encryption of the database content on physical storage, protecting against offline media attacks

Always Encrypted

Client-side encryption of sensitive data using keys that are never revealed to the database system

Cloud-only

Transparent Data Encryption

Protect sensitive data stored in a SQL database from unauthorized access

Encrypted at rest, in flight, and while in use

SQL Server does not have the keys (nor does it need the keys)

Keep application changes to a minimum

Encryption/decryption of data done transparently in TCE-enabled client driver

Support for equality operations (include joins) on encrypted data

Azure manages encryption keys



TDE

Settings
sqlrep

MONITORING

Alert rules

Database size

Events

FEATURES

Geo-Replication

Index advisor (preview)

Query Performance Insight (preview)

SECURITY

Auditing & Threat detection


Dynamic data masking

Transparent data encryption

Transparent data encryption

Save

Discard



Transparent Data Encryption protects your data and helps meet compliance requirements by encrypting your database, associated backups, and transaction log files at rest without requiring changes to your application.


[Learn more about transparent data encryption.](#)

Data encryption

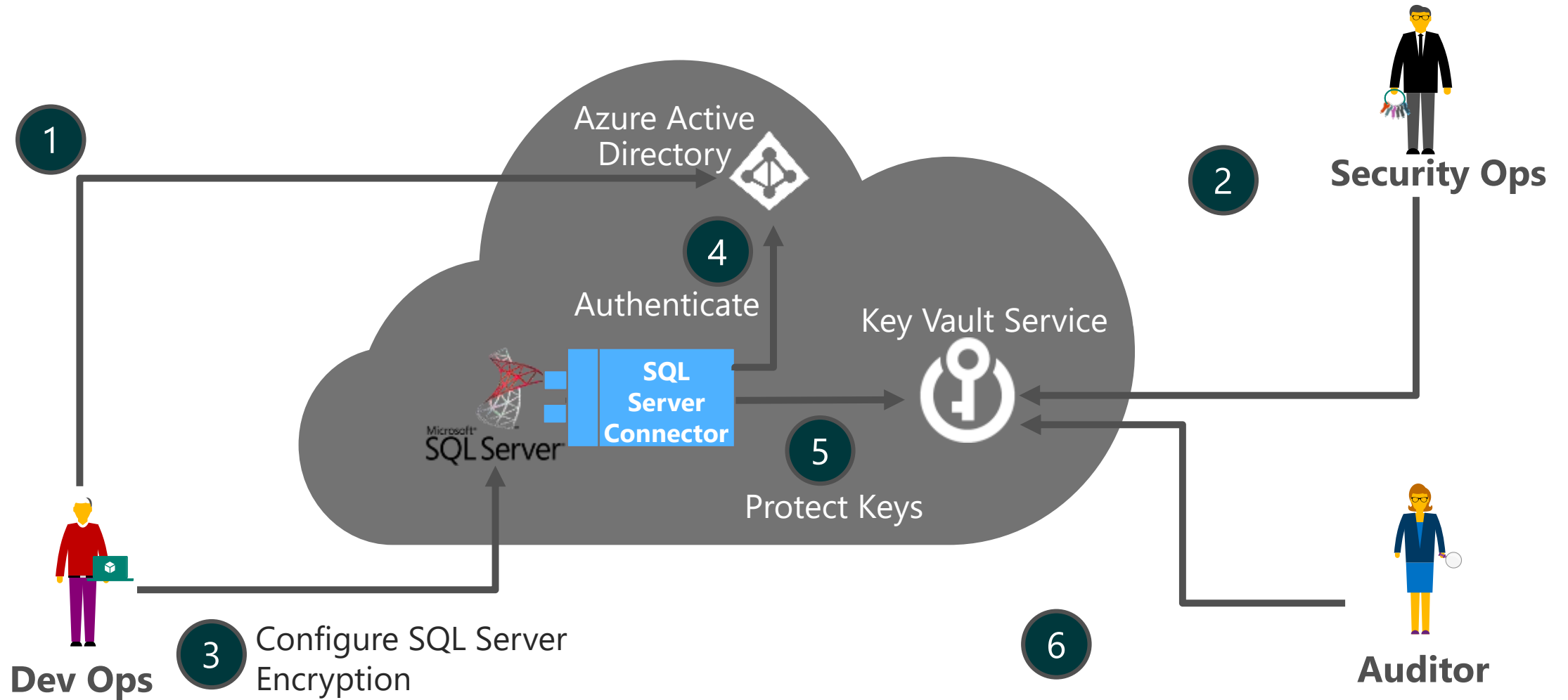
ON

OFF

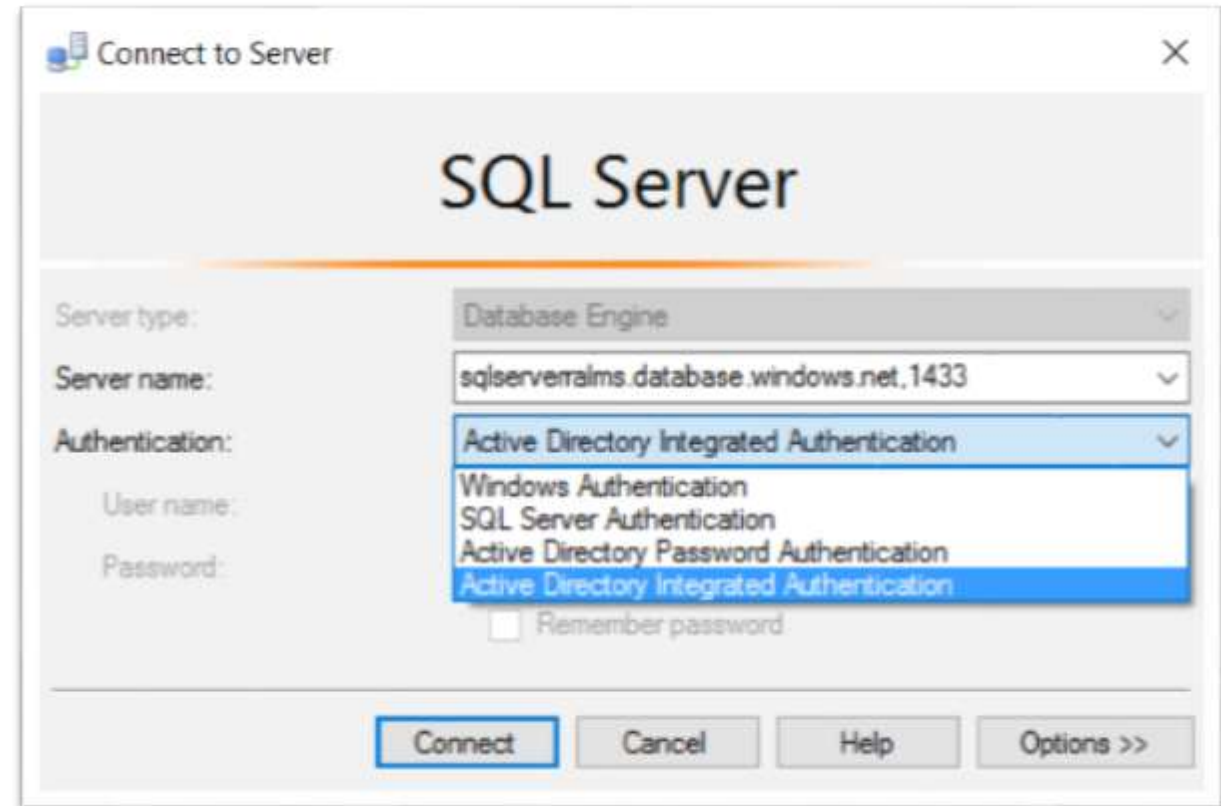
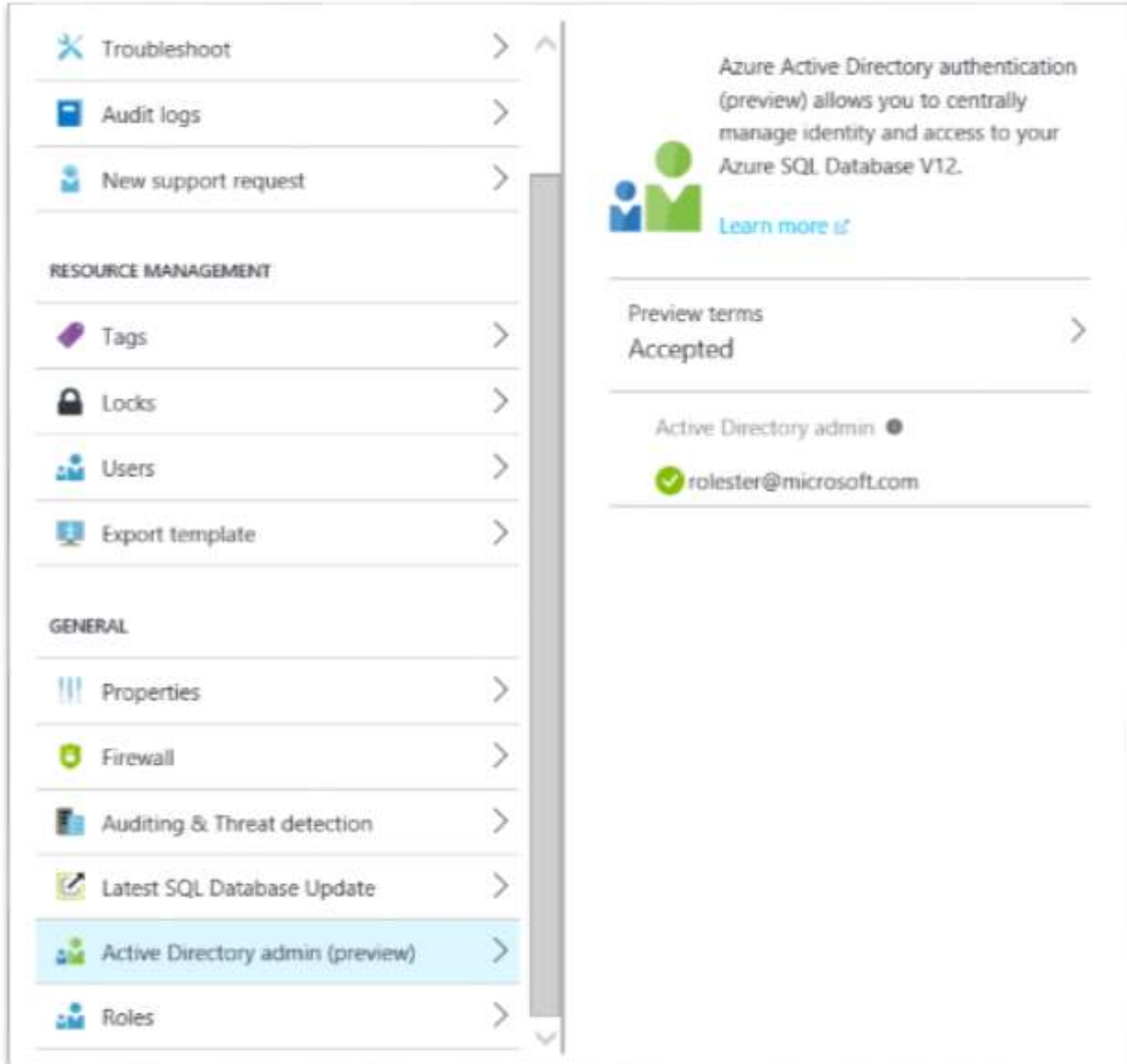
Encryption status

 Encryption in progress...

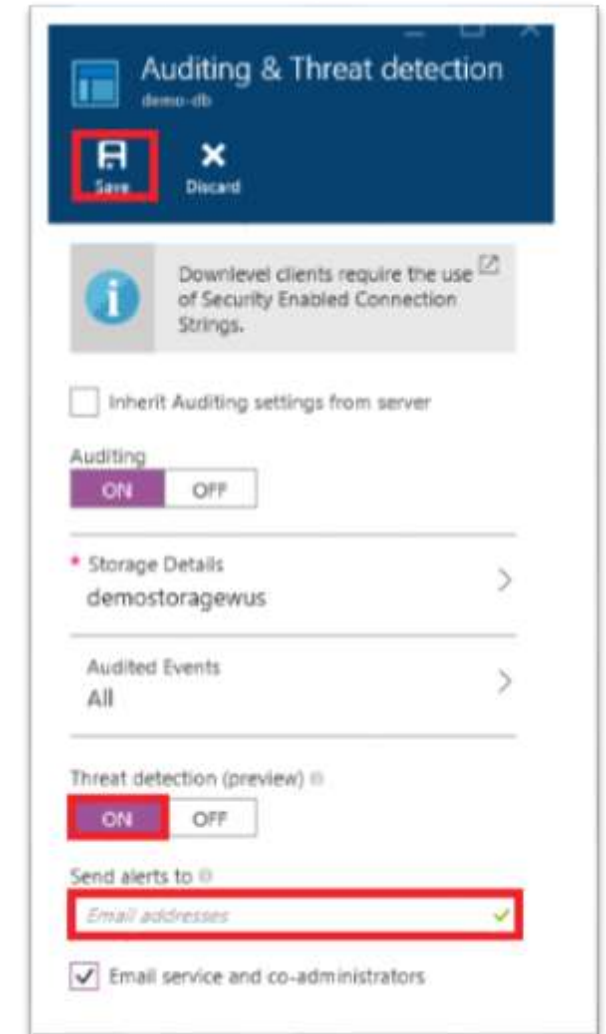
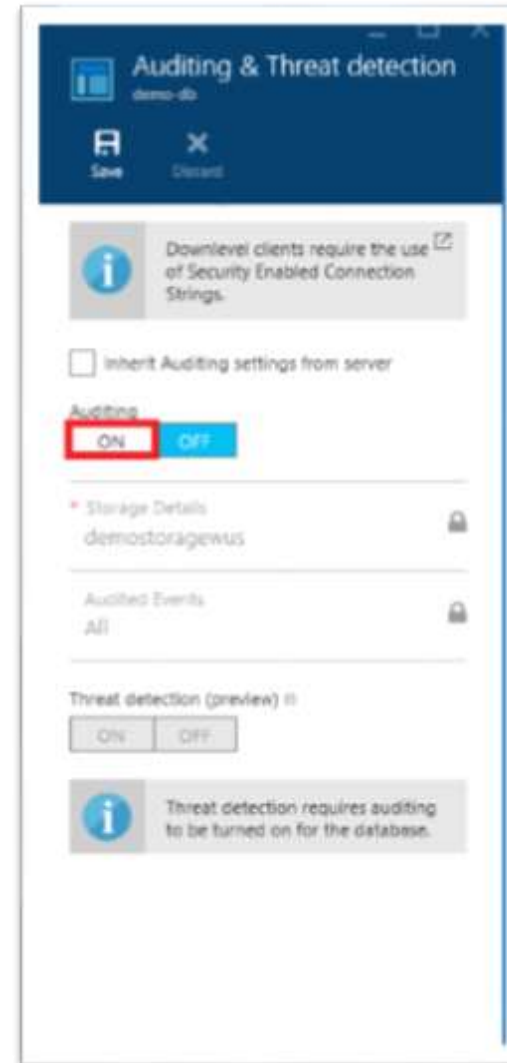
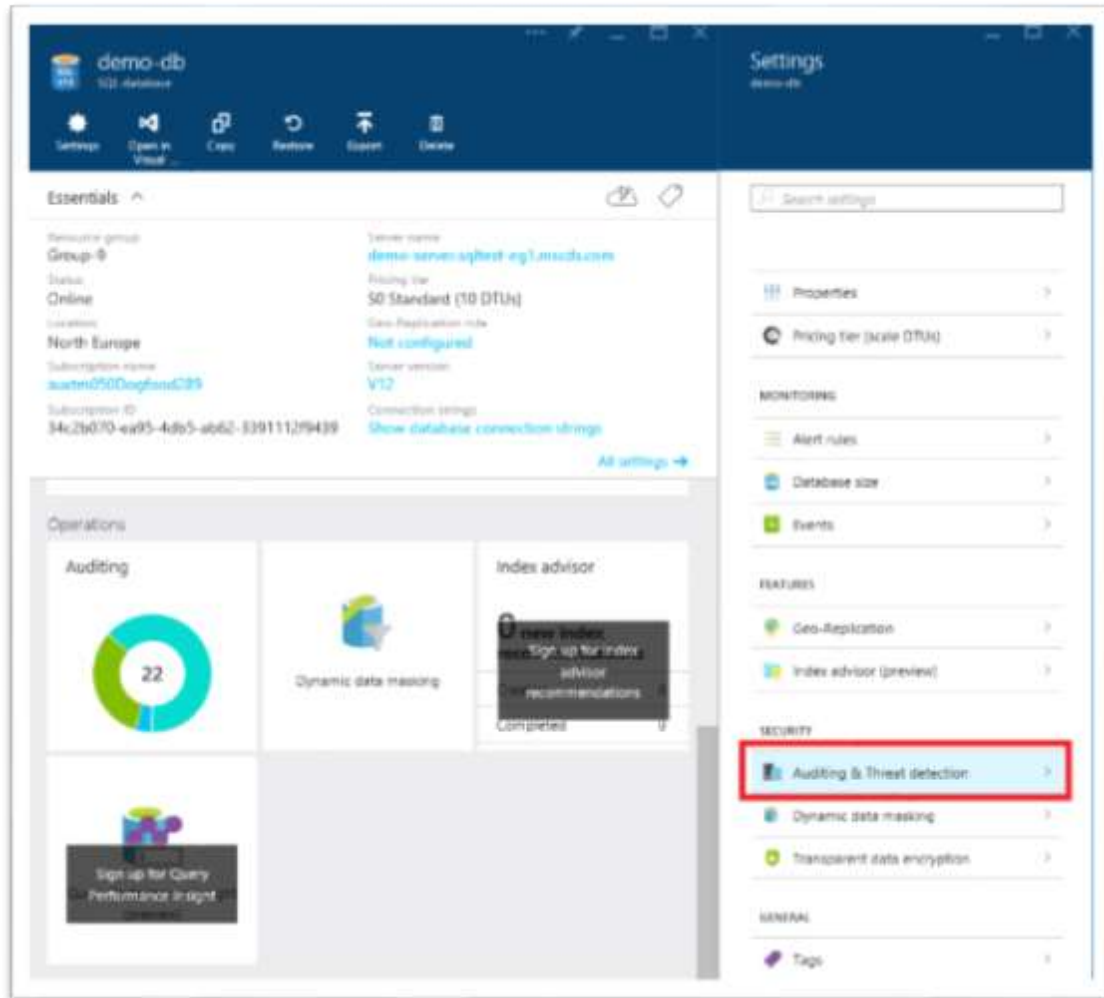
Enable TDE with customer-managed keys



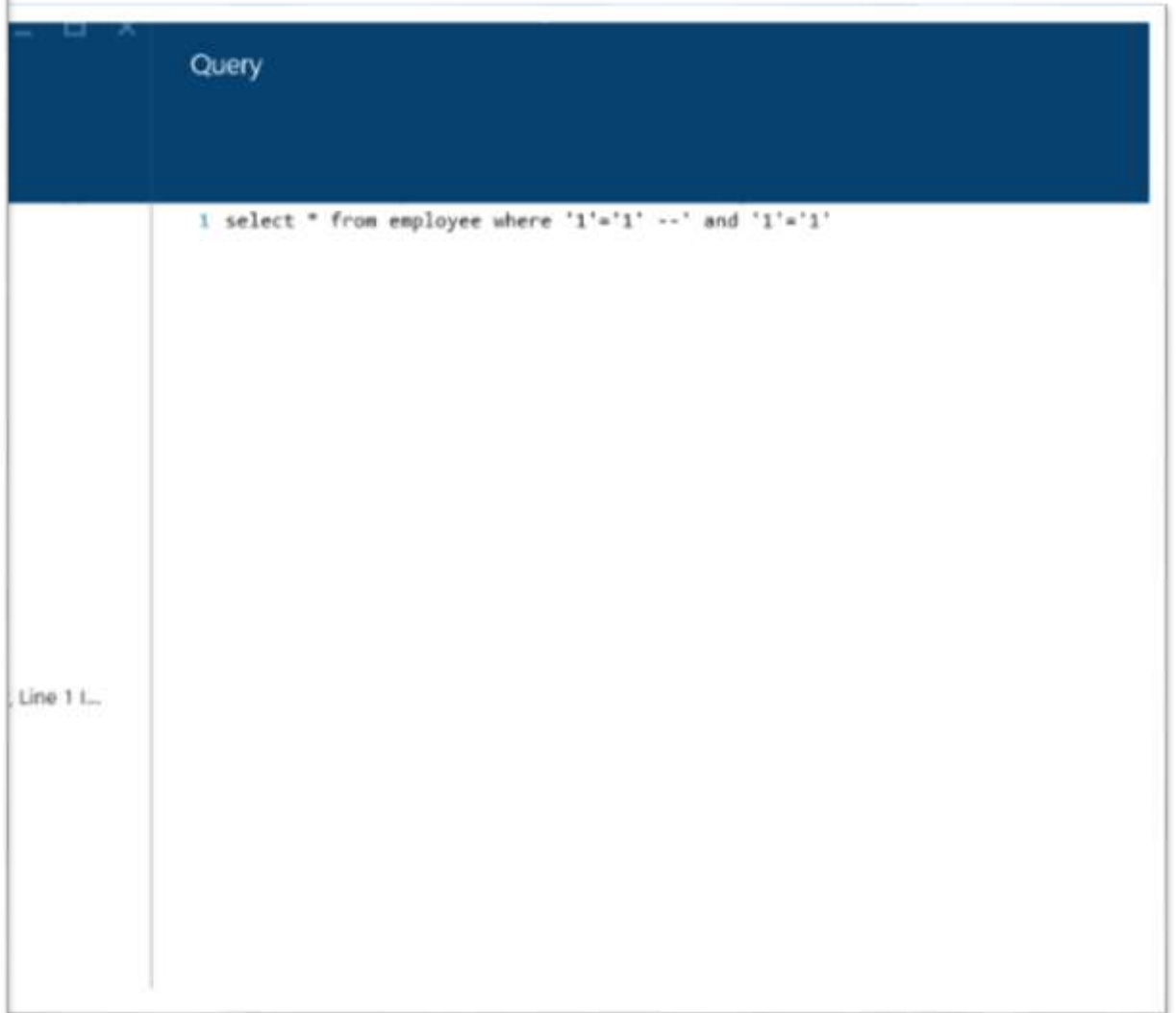
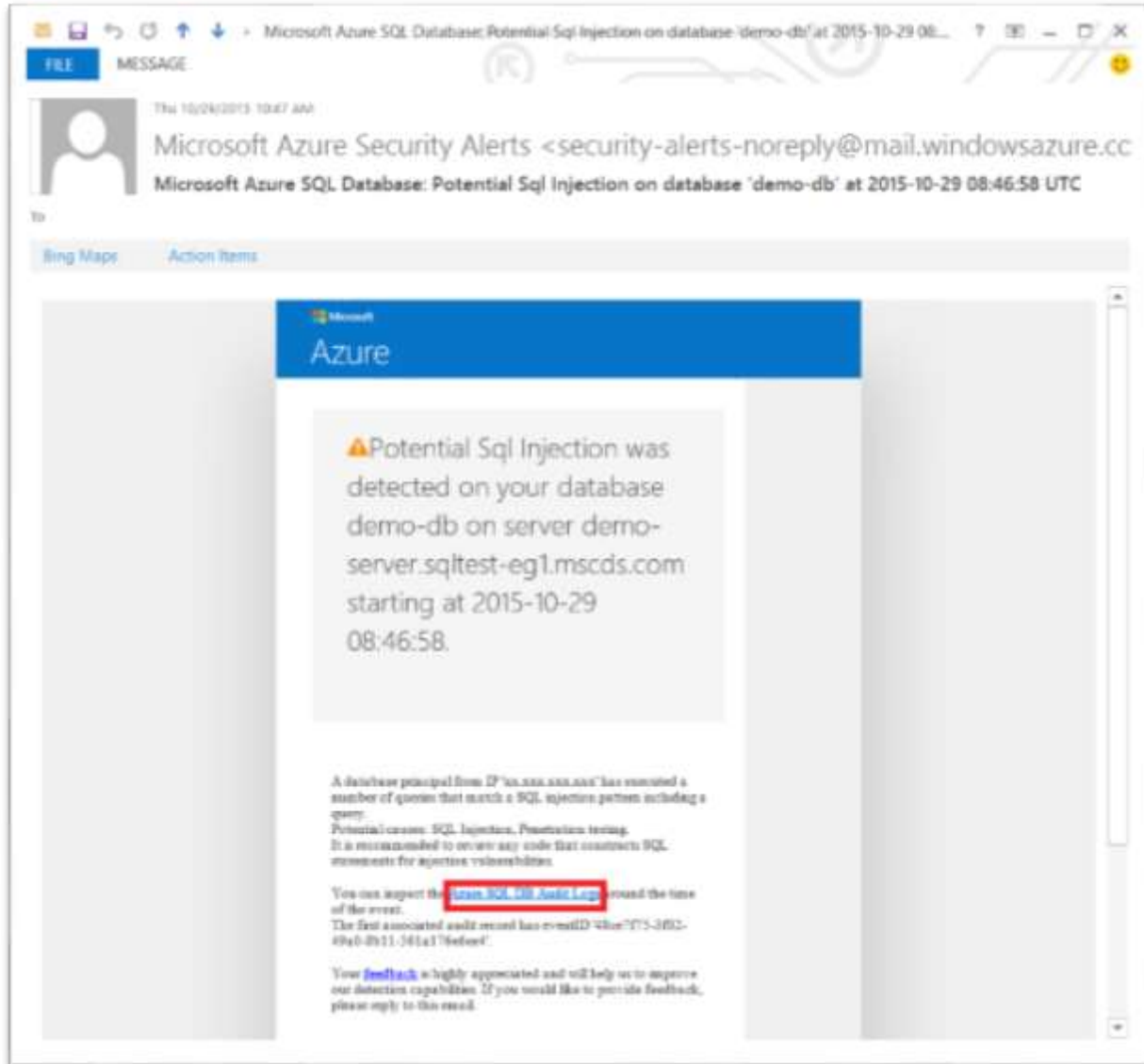
Azure Active Directory Integration



Threat Detection



Threat Detection



Auditing

Gain insight into database events and streamline compliance-related tasks

Configurable to track and log database activity

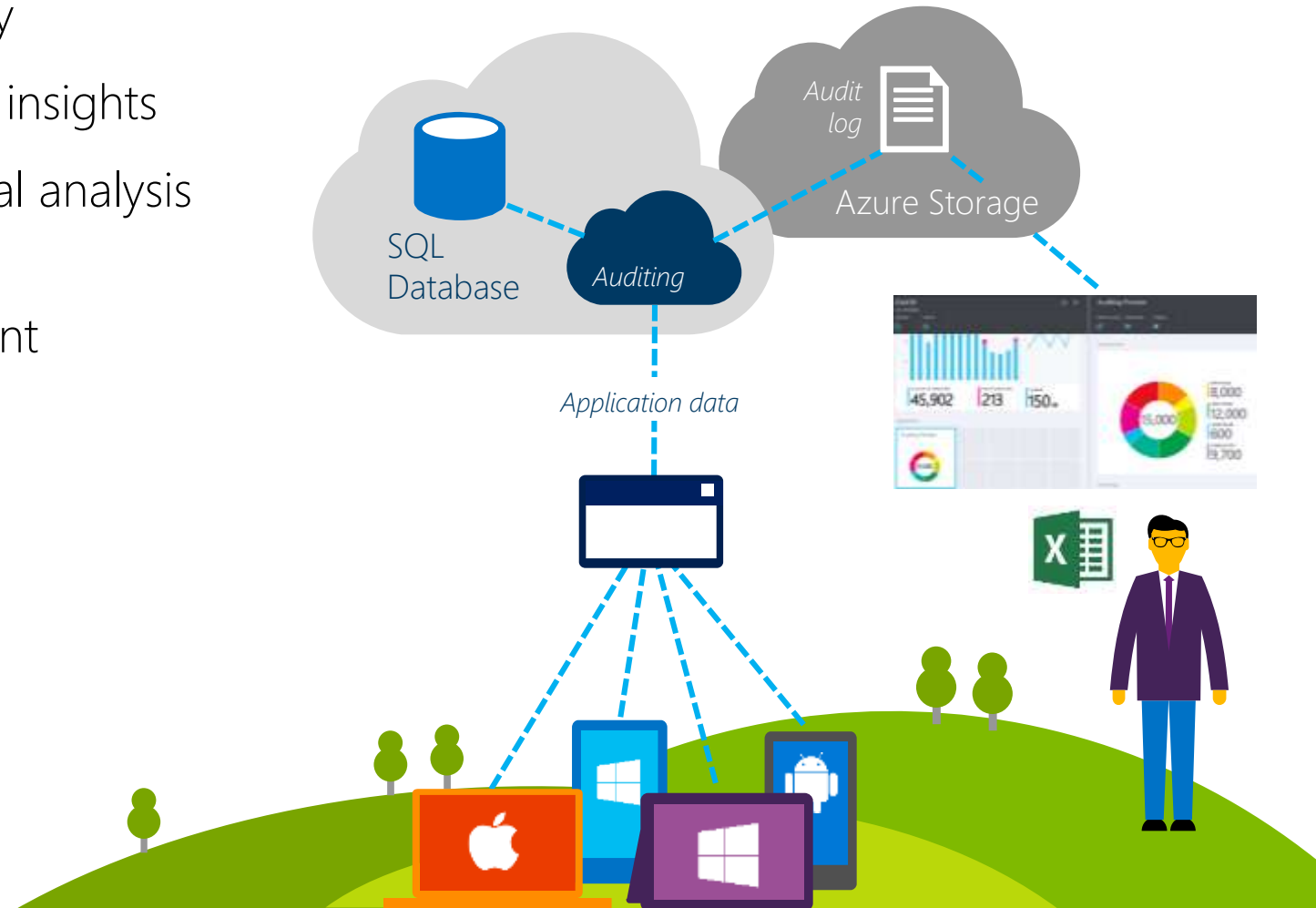
Dashboard views in the portal for at-a-glance insights

Pre-defined Power View reports for deep visual analysis on Audit log data

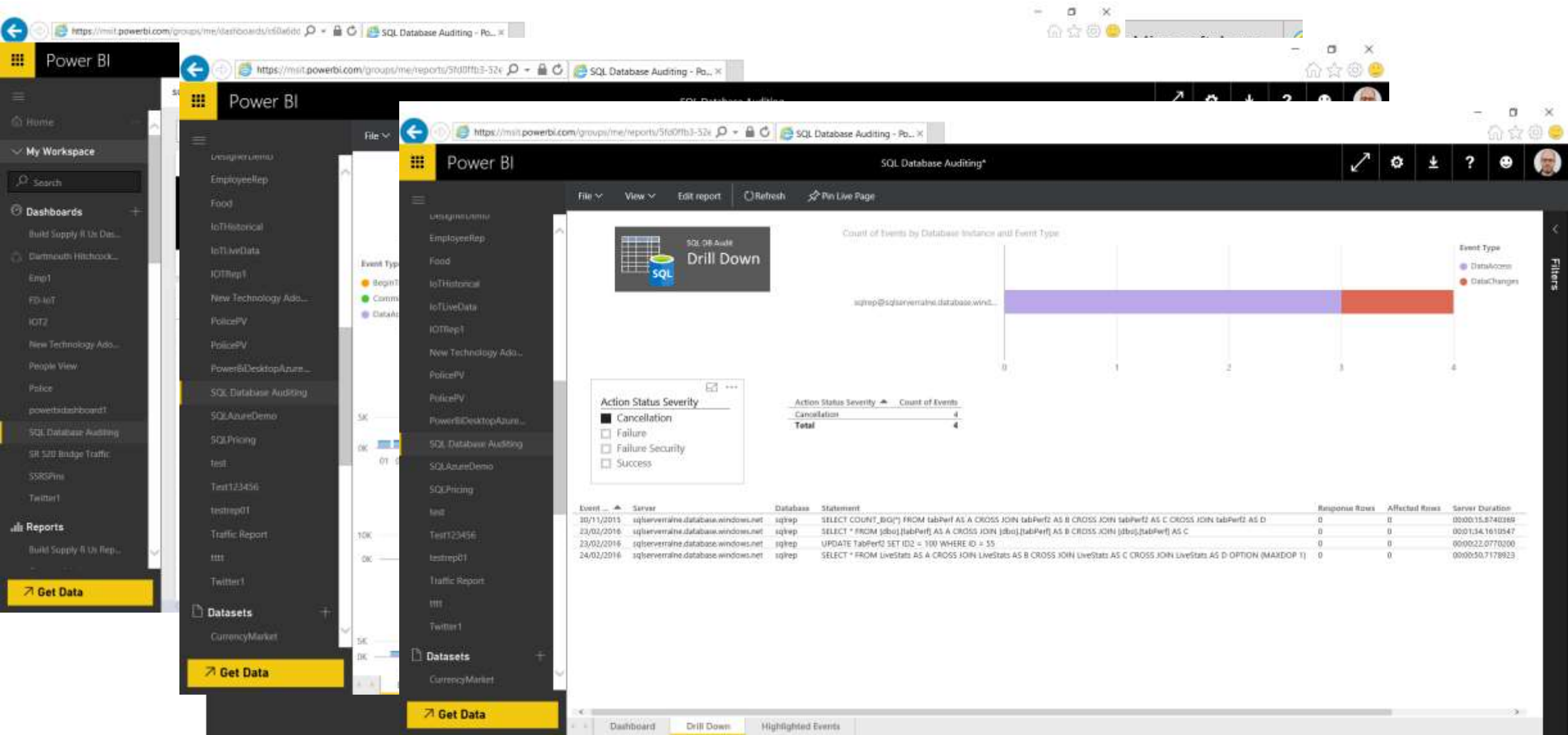
Audit logs reside in your Azure Storage account

Available in Basic, Standard, and Premium

Access via the new Azure preview portal

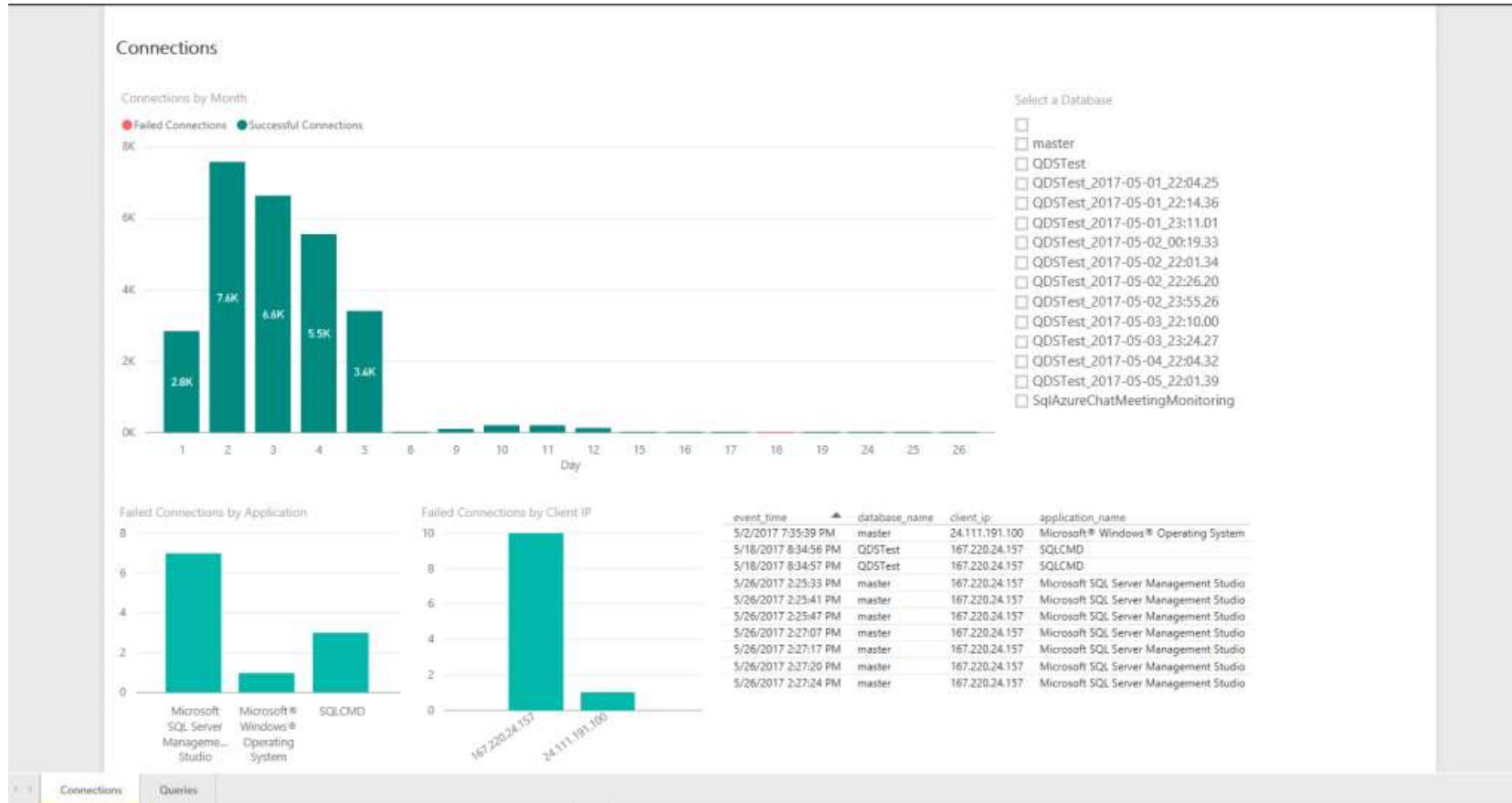


Viewing Audit Logs (only table storage – Deprecated this month)



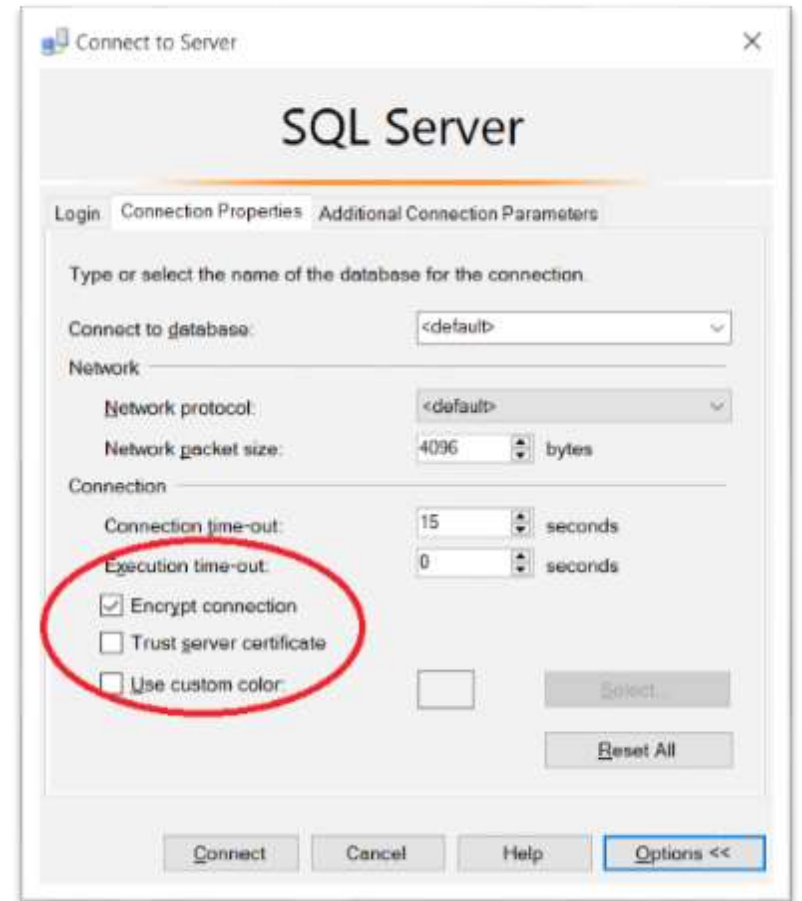
Audit Logs on blob storage

<https://blogs.msdn.microsoft.com/azuresqlsupport/2017/05/26/sql-azure-blob-auditing-basic-power-bi-dashboard/>

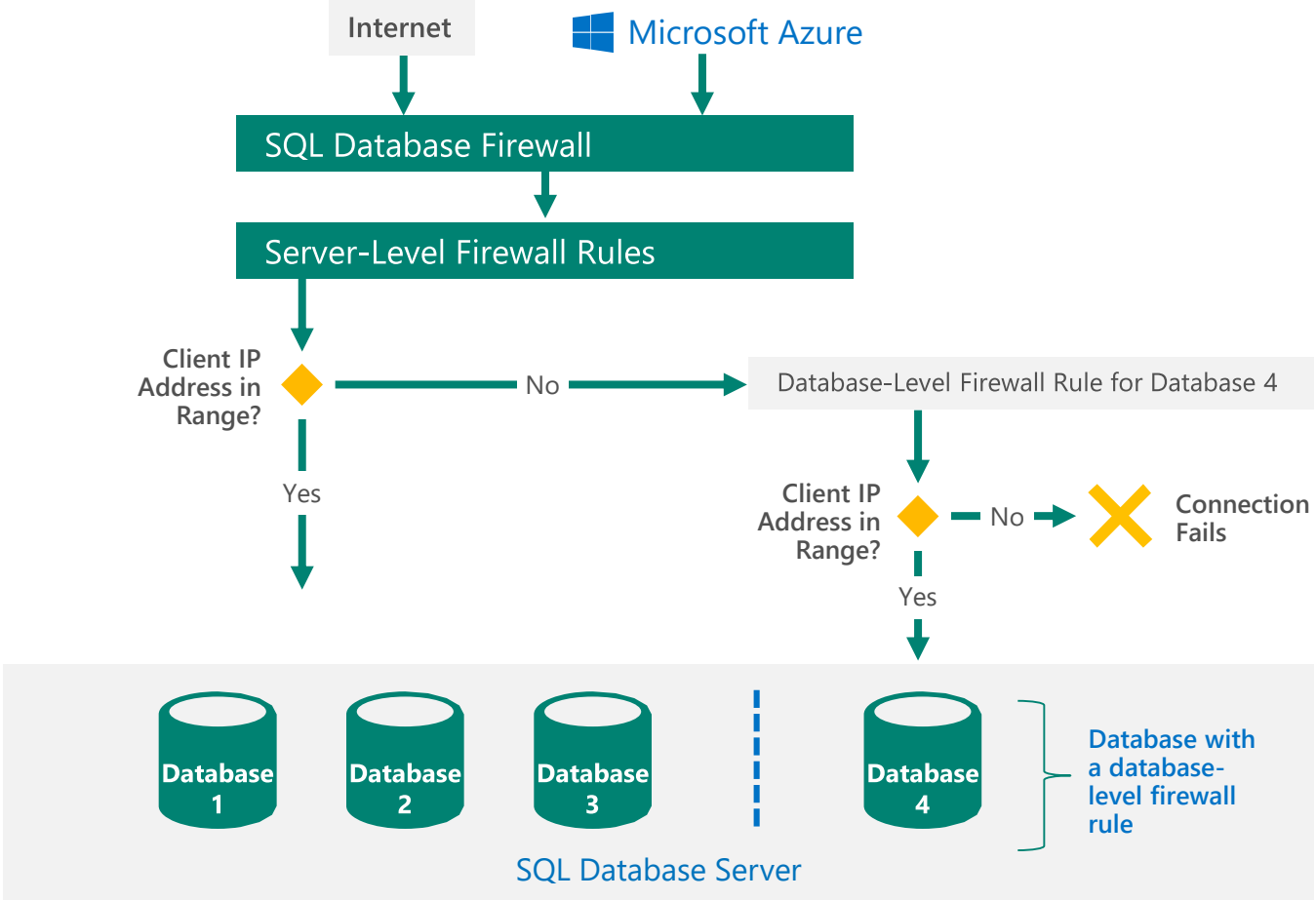


SQL Network Connections

- Azure DB Firewall
- Site to Site VPN
- Express route
- Connection is always encrypted
- Valid certificate protects against man-in-the-middle attacks (only if connection set to not trust server certificate)



SQL Database Firewalls



Windows Azure Platform

Firewall configuration using portals

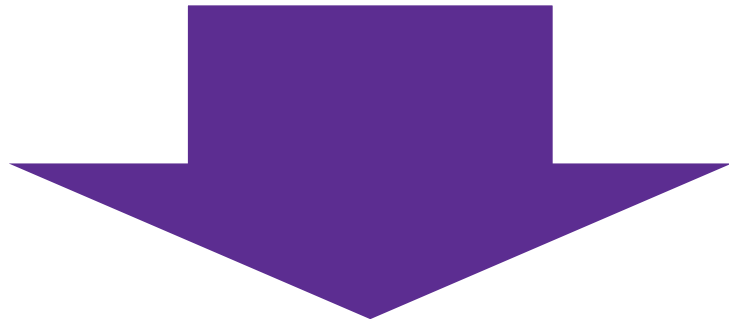
The first screenshot shows the 'AVAILABLE' section of the Azure portal for a resource group 'gb9b7uwyrl'. It lists an 'SQL SERVER' resource 'gb9b7uwyrl' with a status of 'SQL SERVER'. Below this, there are buttons for 'Reset Password' and 'Import database'. A 'Summary' section shows a tree view with 'Default-SQL-WestUS' and 'gb9b7uwyrl SQL server'. The 'gb9b7uwyrl SQL server' is highlighted, and a 'SETTINGS' button is visible. The second screenshot shows the 'Settings' page for the 'GB9B7UWYRL' resource group. It has a search bar and two main sections: 'Properties' and 'Firewall'. The 'Firewall' section is highlighted. The third screenshot shows the 'Firewall Settings' page. It has a toggle for 'Allow access to Azure services' set to 'ON'. Below this is a table with columns 'RULE NAME', 'START IP', and 'END IP'. The table contains three rows of rules.

RULE NAME	START IP	END IP
ClientIPAddress_2014-12-05...	131.107.160.14	131.107.160.14
ClientIPAddress_2015-02-02...	50.200.196.194	50.200.196.194
ClientIPAddress_2015-58-29...	67.170.61.126	67.170.61.126

- By default, Azure blocks all external connections to port 1433.

Azure SQL Database – Connecting to other services

Allow access to Azure services



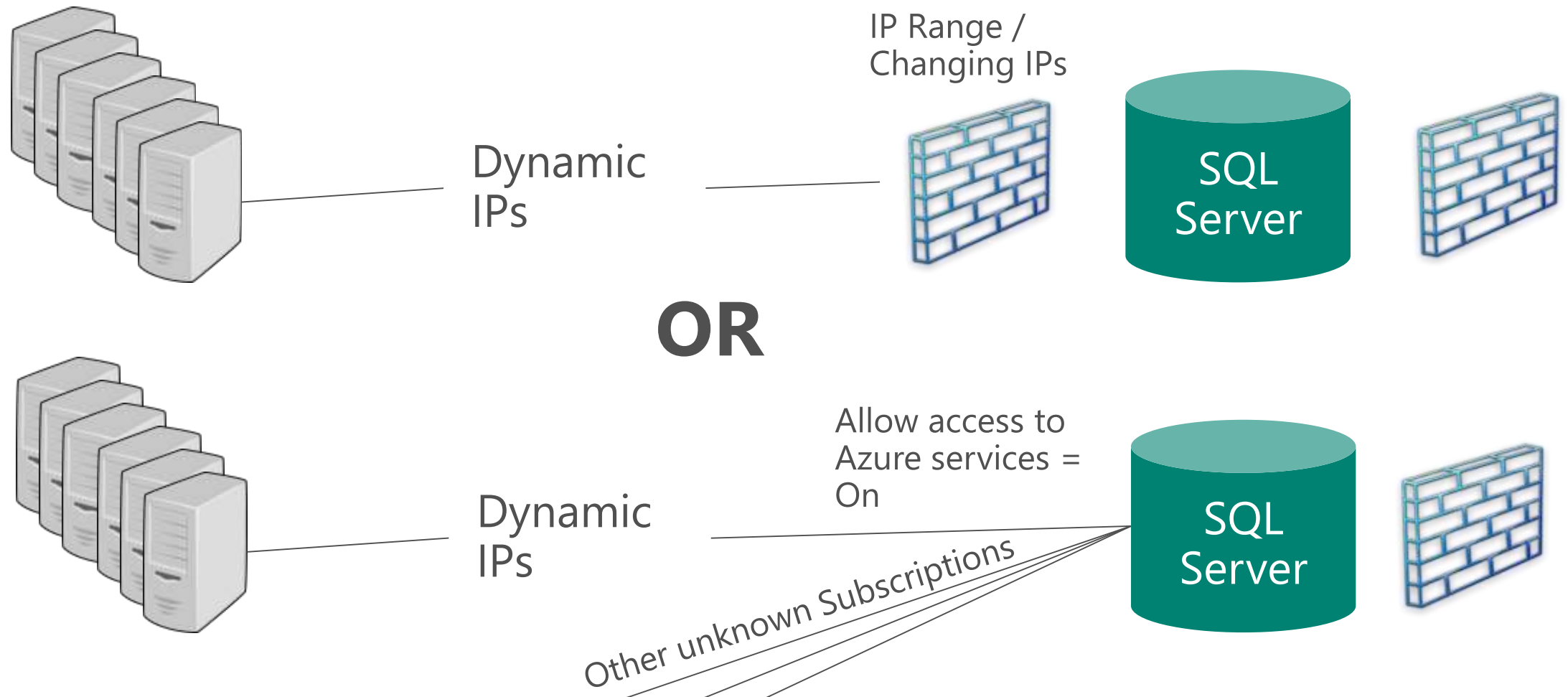
On = **All** Azure IPs
and **All** Subnets

Off = **No** Azure IPs
and **No** Subnets

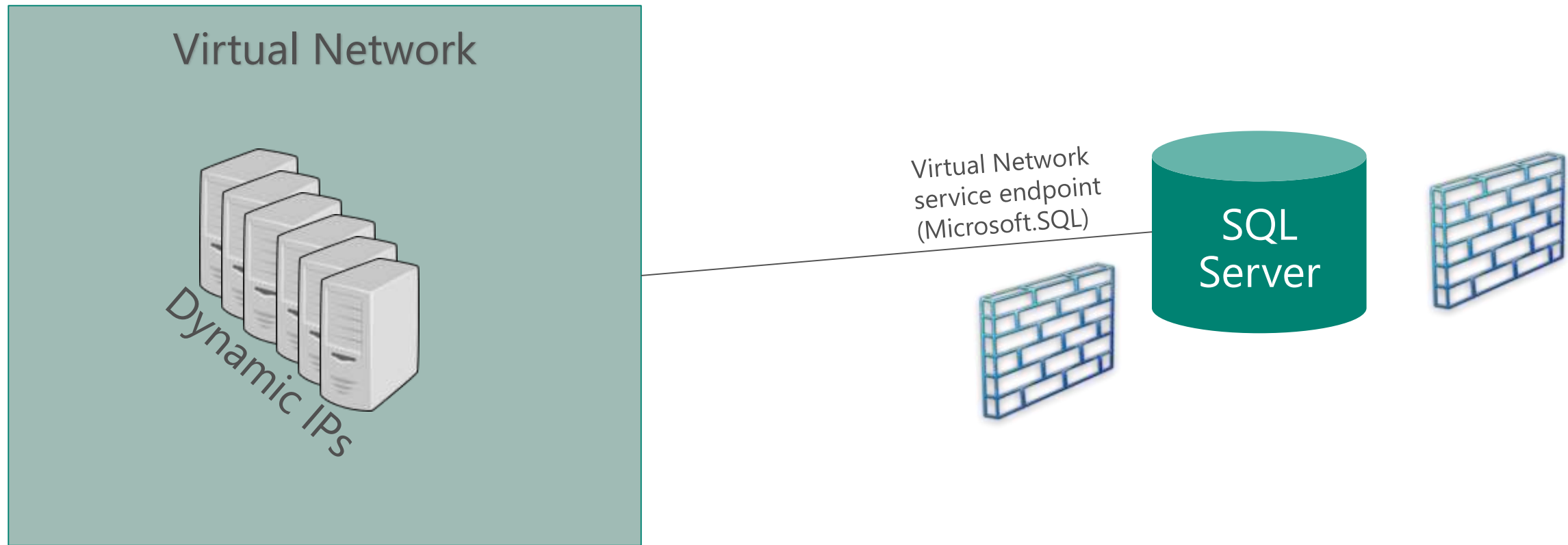


SQL Database Networking

- VMs in Azure generally have dynamic IPs (Static are expensive at scale and management requirement)



SQL Database Virtual Network service endpoints



SQL Database Virtual Network service endpoints

- Considerations

- Server level only
- Azure Resource Manager only
- Site to site VPN and Express route need to have their IPs explicitly stated in the firewall

Row-level security

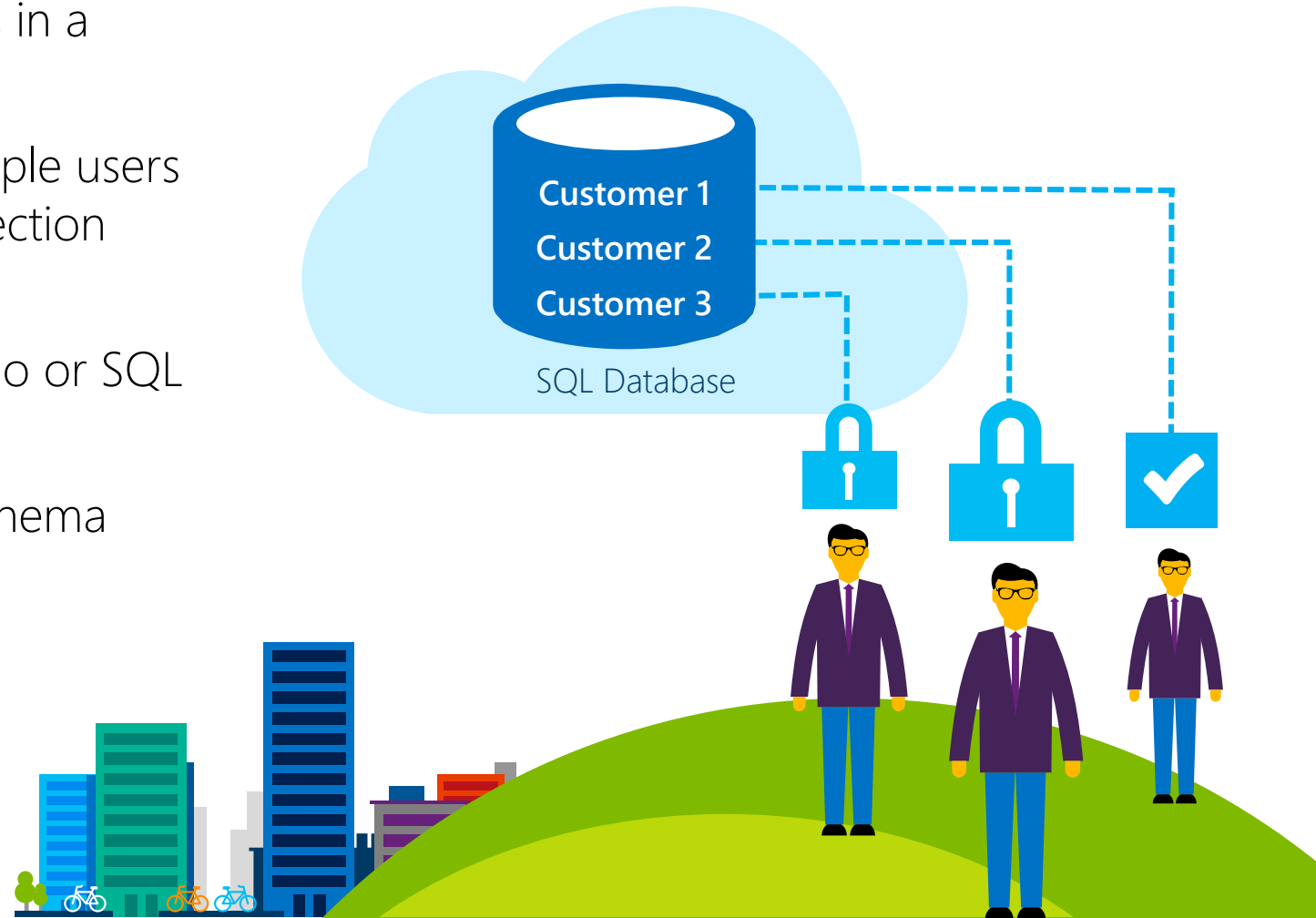
Protect data privacy by ensuring the right access across rows

Fine-grained access control over specific rows in a database table

Help prevent unauthorized access when multiple users share the same tables, or to implement connection filtering in multitenant applications

Administer via SQL Server Management Studio or SQL Server Data Tools

Enforcement logic inside the database and schema bound to the table.



Row Level Security

- Demo

Common RLS Use Cases...

- Traditional RLS workloads

- Custom business logic to determine which rows each user can SELECT, INSERT, UPDATE, DELETE based on their role, department, security level, etc.
- Target sectors: Finance, insurance, healthcare, oil/gas, Federal, etc.

- Multi-tenant databases

- Ensuring tenants can only access their own rows of data in a shared database, with enforcement logic in the database rather than in the app tier
- E.g. multi-tenant shards with elastic database tools on Azure SQL Database

- Reporting, analytics, data warehousing

- Different users access same database through various reporting tools, and work with different subsets of data based on their identity/role

Dynamic Data Masking

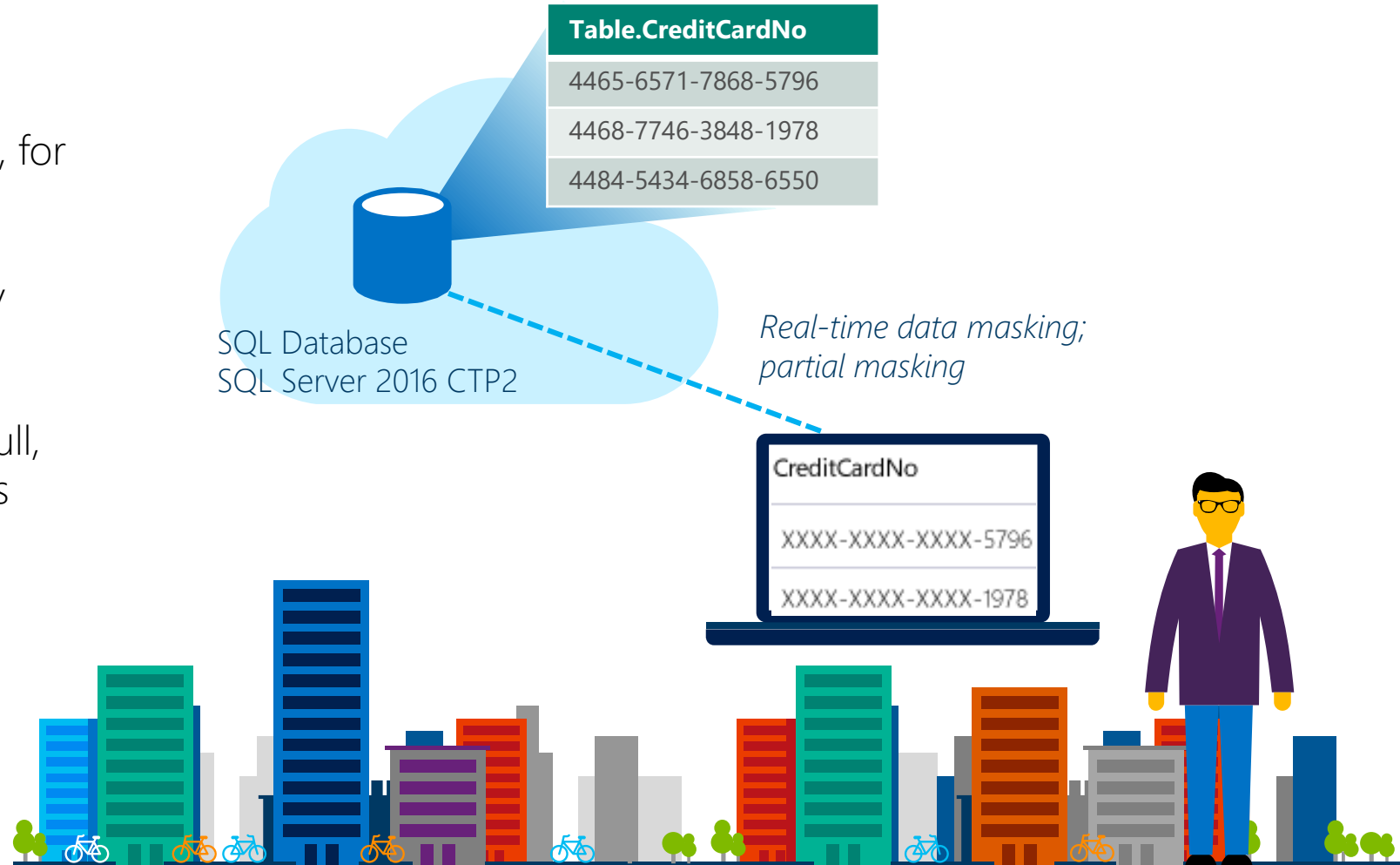
Prevent the abuse of sensitive data by hiding it from users

Configuration made easy in the new Azure portal

Policy-driven at the table and column level, for a defined set of users

Data masking applied in real-time to query results based on policy

Multiple masking functions available (e.g. full, partial) for various sensitive data categories (e.g. Credit Card Numbers, SSN, etc.)



Dynamic Data Masking

- Demo

 Search (Ctrl+/)

 Overview

 Activity log

 Tags

 Diagnose and solve problems

SETTINGS

 Quick start

 Pricing tier (scale DTUs)

 Geo-Replication

 Auditing & Threat Detection

 Vulnerability Assessment (Pre...)

 Dynamic Data Masking

 Transparent data encryption

 Connection strings

 Sync to other databases

 Properties

 Save  Discard  Add mask  Feedback

Masking rules

MASK NAME

dbo_SalesData_CCNumber1

dbo_SalesData_Email

dbo_SalesData_Pin

MASK FUNCTION

Custom string (prefix [padding] suffix)

Email (aXXX@XXXX.com)

Default value (0, xxxx, 01-01-1900)

SQL users excluded from masking (administrators are always excluded) ⓘ

Manager;



Recommended fields to mask

SCHEMA

dbo

dbo

dbo

dbo

SalesLT

TABLE

Patients

Patients

Patients

Patients

Address

COLUMN

SSN

FirstName

LastName

StreetAddress

AddressID

ADD MASK

ADD MASK

ADD MASK

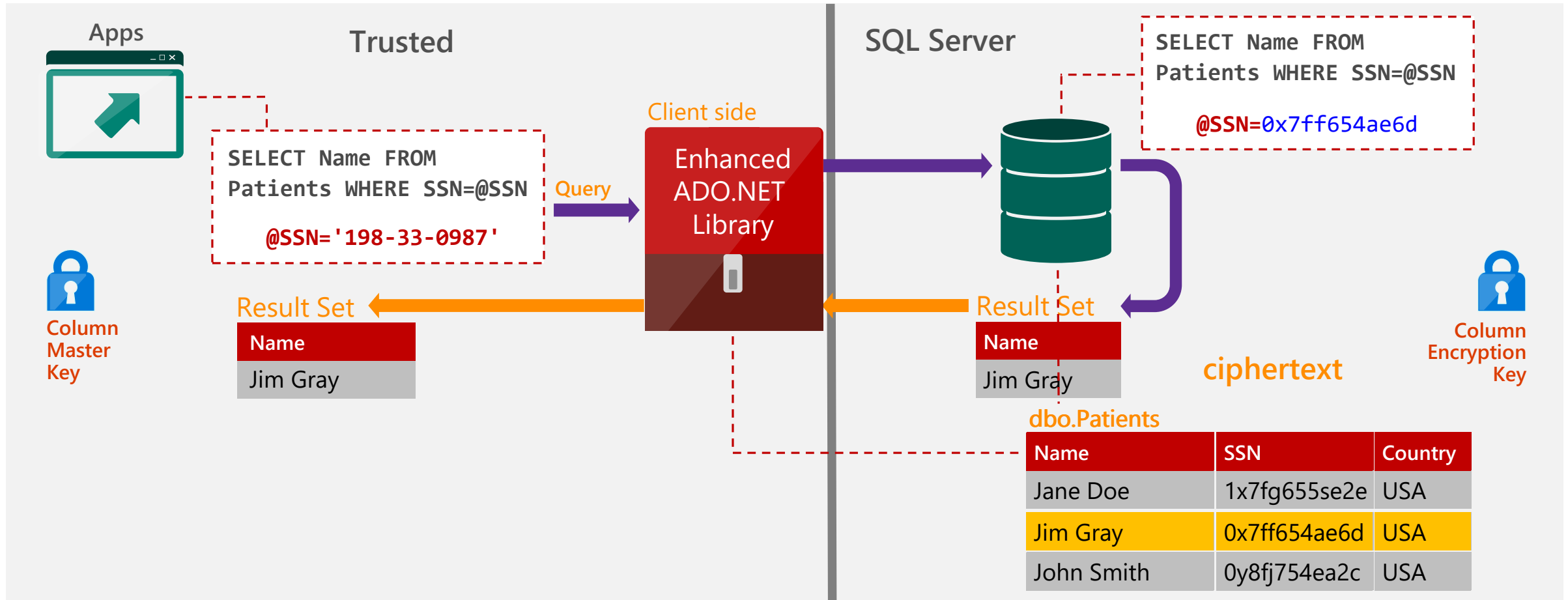
ADD MASK

ADD MASK

[Load more](#)

Always Encrypted

Help protect data at rest and in motion, on-premises & cloud



Types of Encryption for Always Encrypted

- Randomized encryption

- Encrypt('123-45-6789') = 0x17cfd50a
- Repeat: Encrypt('123-45-6789') = 0x9b1fcf32
- Allows for transparent retrieval of encrypted data but NO operations
- More secure

- Deterministic encryption

- Encrypt('123-45-6789') = 0x85a55d3f
- Repeat: Encrypt('123-45-6789') = 0x85a55d3f
- Allows for transparent retrieval of encrypted data AND equality comparison
 - E.g. in WHERE clauses and joins, distinct, group by

Two types of encryption available

Randomized encryption uses a method that encrypts data in a less predictable manner

Deterministic encryption uses a method which always generates the same encrypted value for any given plain text value (for equality excretions)

Security

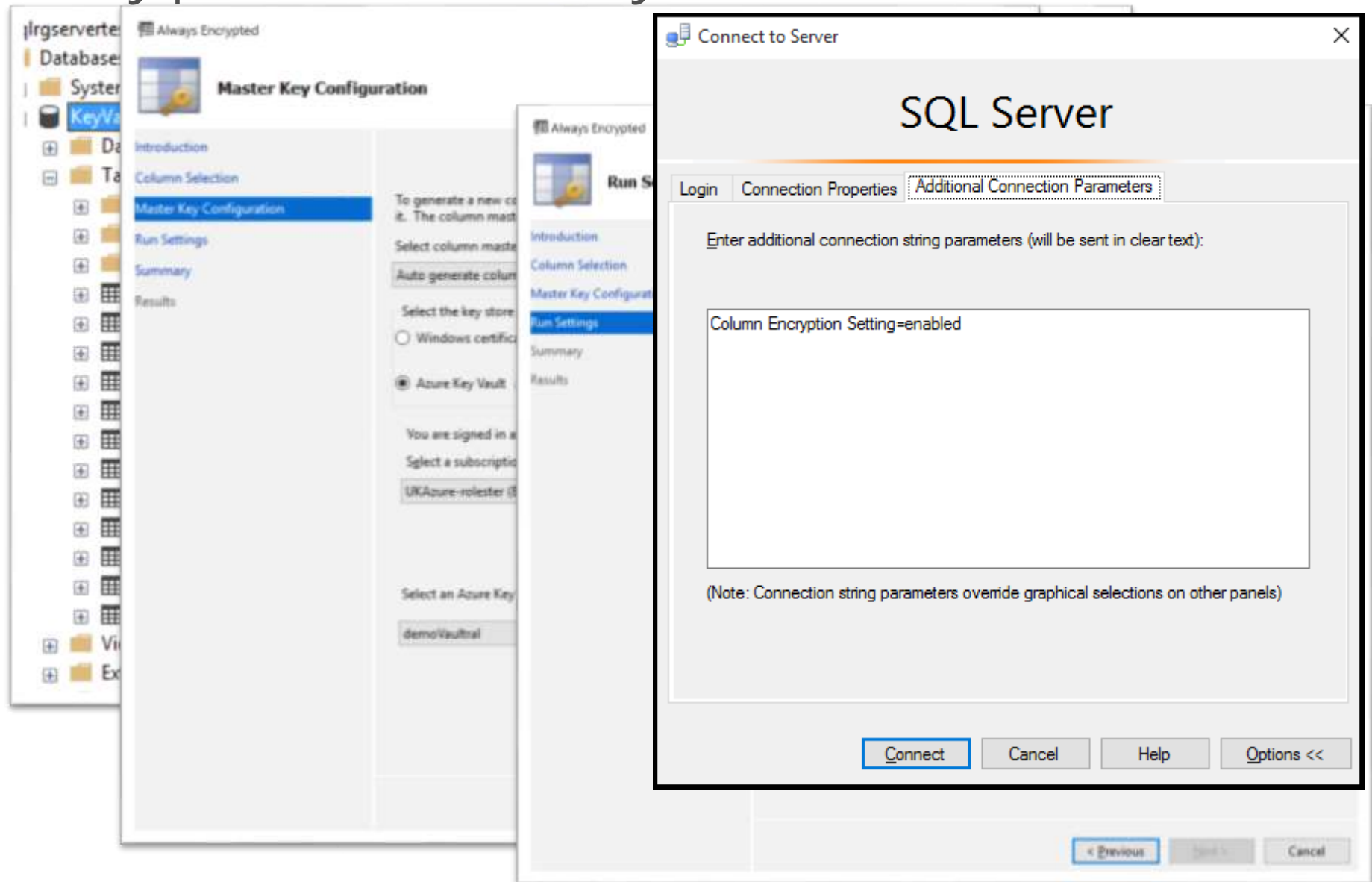
- Deterministic and Randomized just as secure
- Except
 - With deterministic if you know there are a fixed number of records of a certain type in a table you can identify those records by the number of occurrences.
 - EG: if it were know that there were three people that were admins

Name	Security Level
Jane	0x85a55d3f
Jim	0x17cfd50a
Joe	0x9b1fcf32
Julia	0x85a55d3f
Jill	0x85a55d3f
Jerry	0x7a2bda11

- EG: How many different types of a category are there

Always Encrypted with Key Vault

- Demo



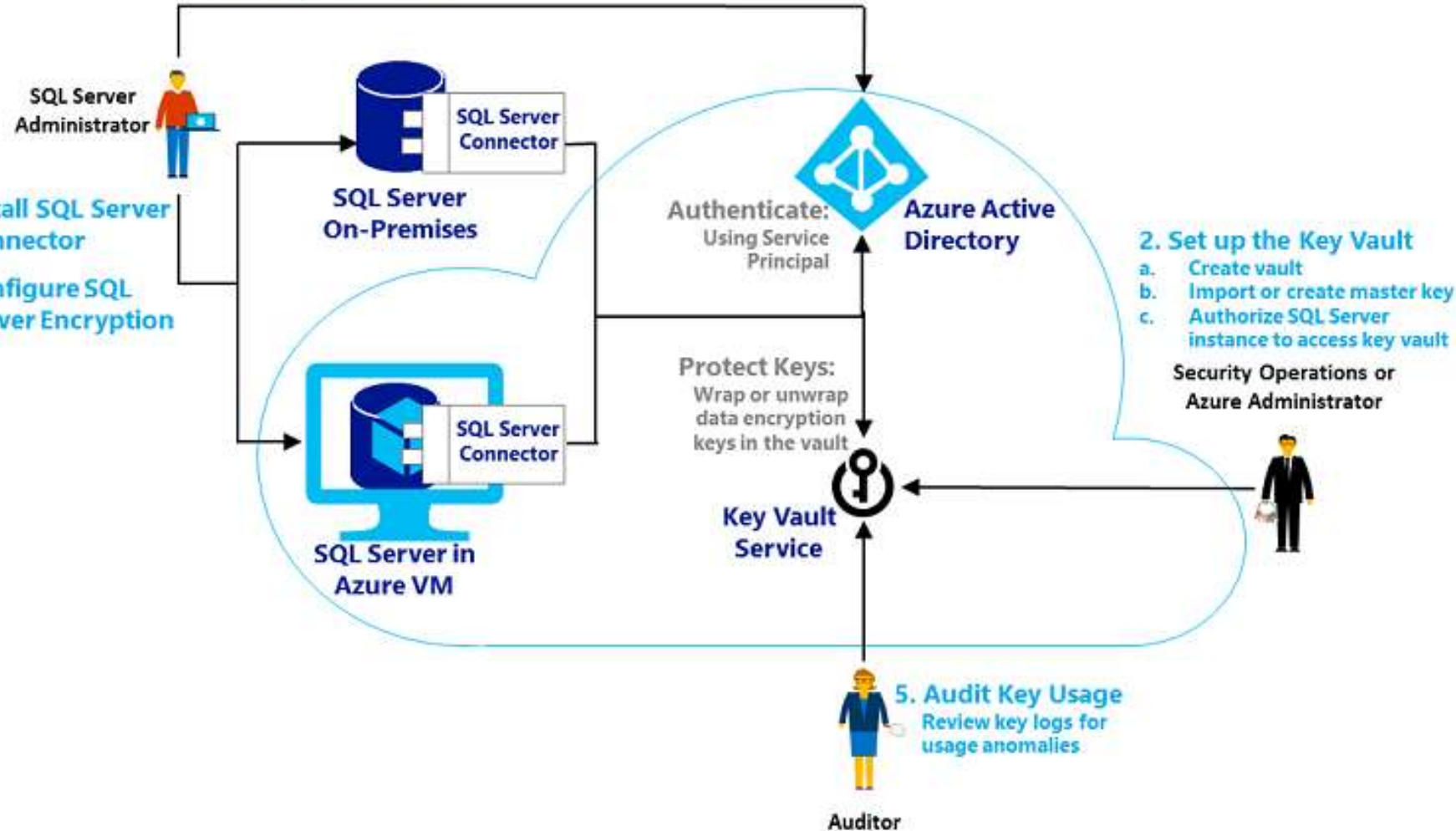
Overview of Encryption Technologies

Feature Capability	Always Encrypted	Transparent Data Encryption	Cell-level Encryption	App-Controlled Encryption
Level of protection	End-to-end	At-rest	At-rest	End-to-end
Can server see sensitive data?	No	Yes	Yes	No
T-SQL operations on encrypted data	Equality comparison	All (after decryption)	All (after decryption)	Possible with the appropriate encryption algo
App development cost to use feature	Low	Very low	High	Very High
Encryption granularity	Column	Database	Cell	Cell

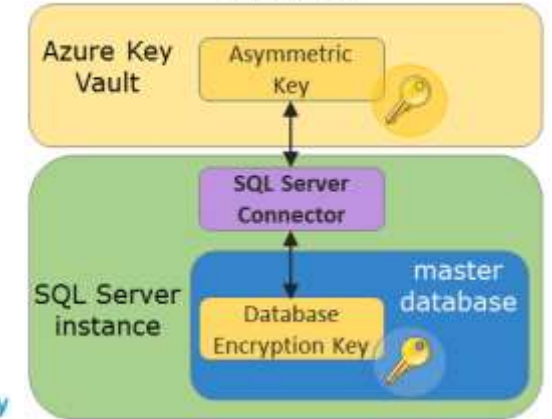
1. Register SQL Server Application

Register service principal (identity) for SQL Server instance in Azure Active Directory

- 3. Install SQL Server Connector
- 4. Configure SQL Server Encryption



Encryption Key Hierarchy (with AKV)





Microsoft