



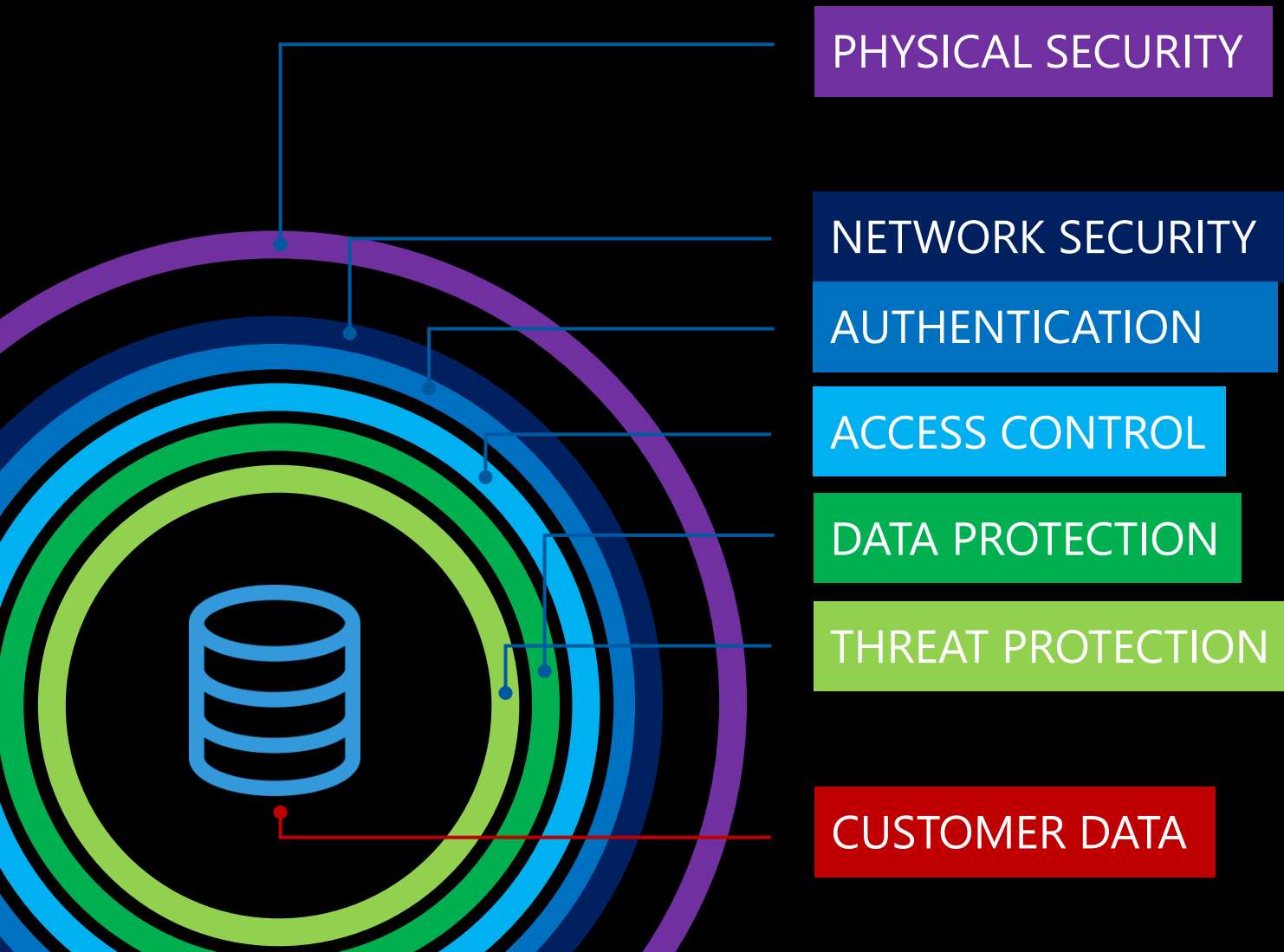
Securing your modern analytical platform



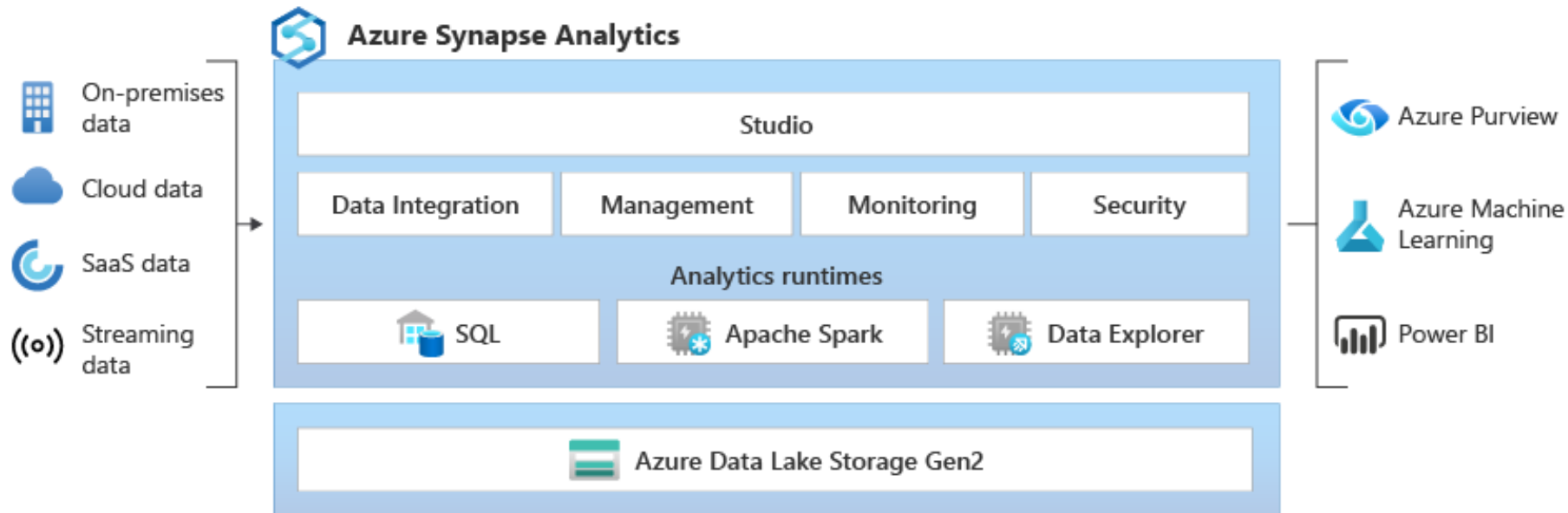
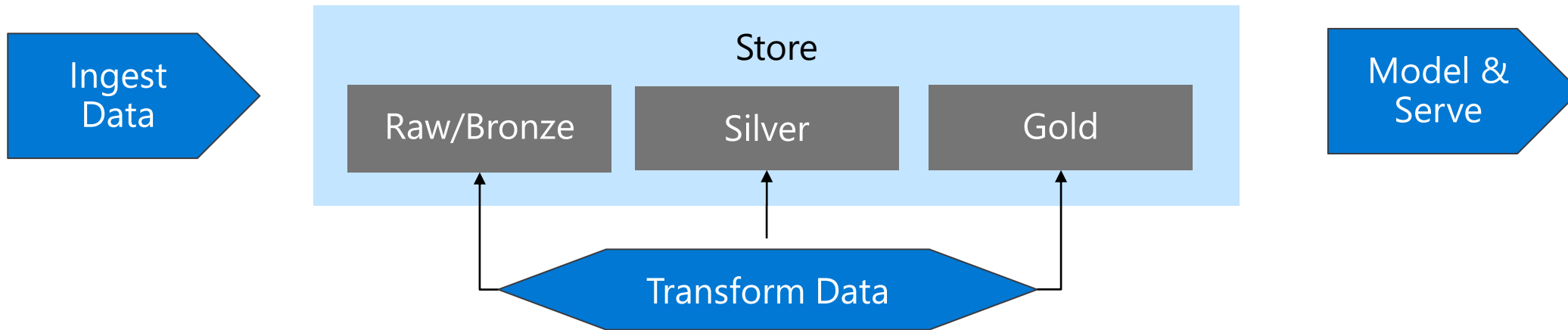
Vengatesh Parasuraman

Senior Program Manager, Microsoft

How **secure** is your data in Cloud ?



Modern Analytical Platform – with Azure Synapse Analytics





Azure **Synapse** Analytics

Network Security

Synapse Workspace



Dedicated SQL Pools



Serverless SQL Pools



Apache Spark Pools



Pipelines and Data Flows



Logical *Securable* Boundary



IP Firewall Rules



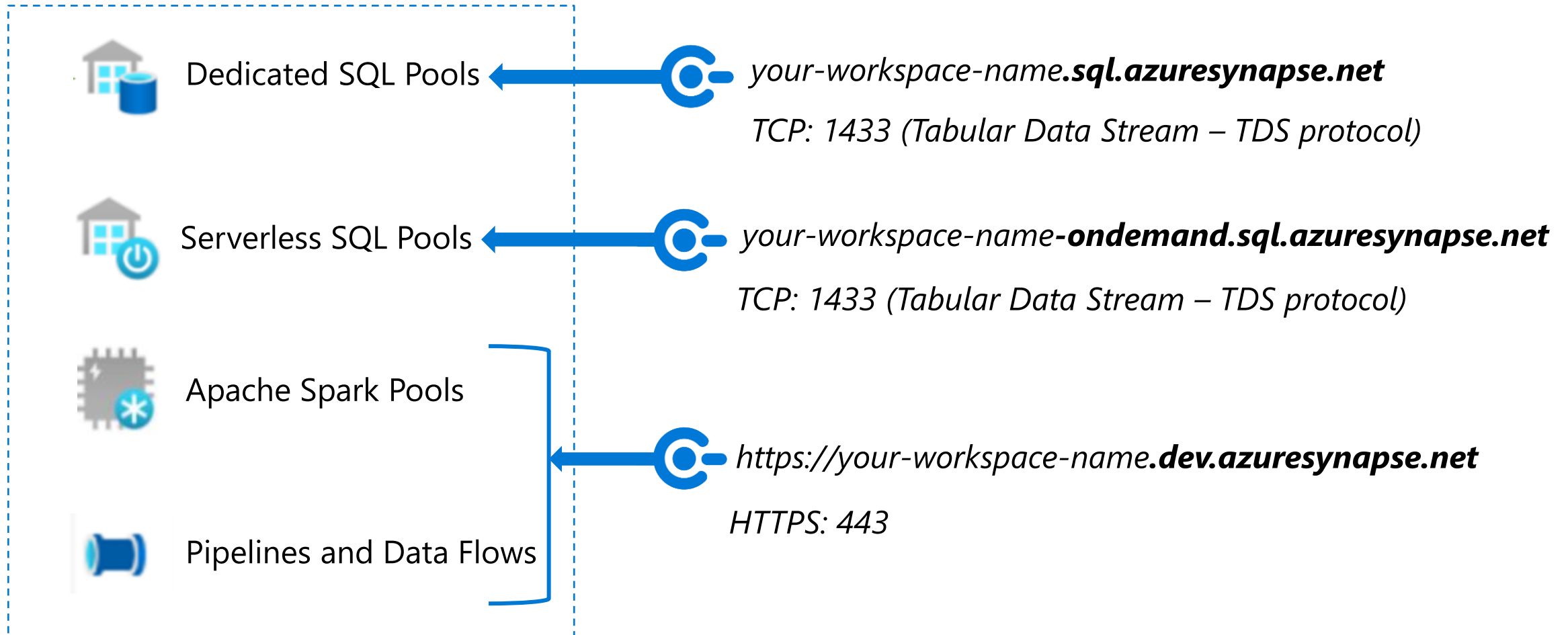
Disabling Public Access



Data Exfiltration Protection

Workspace Endpoints

- Endpoint – Point of incoming connection to access a service from a client



Synapse Studio

- Synapse Studio is a *secure* web front end development environment for Azure Synapse Analytics
- Caters to various personas
- Primarily used for performing various data plane and management operations:
 - Connecting to dedicated SQL pools, serverless SQL pools, and running SQL scripts
 - Developing and running notebooks on Apache Spark pools
 - Developing and running pipelines
 - Monitoring dedicated SQL pools, serverless SQL pools, Apache Spark pools, and pipeline jobs
 - Managing Synapse RBAC permissions of the workspace items
- Synapse Studio *securely* connects to all three workspace endpoints behind the scenes

Public Endpoints & IP Firewall Rules

Public access *enabled*:

« Save Discard Refresh

Overview

Activity log

Access control (IAM)

Tags

Diagnose and solve problems

Settings

SQL Active Directory admin

Properties

Locks

Analytics pools

SQL pools

Apache Spark pools

Data Explorer pools (preview)

Security

Encryption

Networking

Identity

Public network access

Choose whether to permit public network access to your workspace. You can modify the firewall rules after you enable this setting. [Learn more](#)

Public network access to workspace endpoints

☒ Enabled ☐ Disabled

Firewall rules

You can bypass the firewall rules from your trusted Azure services and resources to the Azure Synapse workspace. [Learn more](#)

☐ Allow Azure services and resources to access this workspace

Client IP address

+ Add client IP

Rule name	Start IP	End IP	
allowAll	0.0.0.0	255.255.255.255	...
<input type="text"/>	<input type="text"/>	<input type="text"/>	

Public access *disabled*:

« Save Discard Refresh

Overview

Activity log

Access control (IAM)

Tags

Diagnose and solve problems

Settings

SQL Active Directory admin

Properties

Locks

Analytics pools

SQL pools

Apache Spark pools

Data Explorer pools (preview)

Security

Encryption

Networking

Identity

Public network access

Choose whether to permit public network access to your workspace. You can modify the firewall rules after you enable this setting. [Learn more](#)

Public network access to workspace endpoints

☐ Enabled ☒ Disabled

Disabling this setting will require you to use private endpoints to connect to your workspace. [Create a private endpoint](#)

Firewall rules

Your rules have been saved and will be applied if you enable Public network access again.

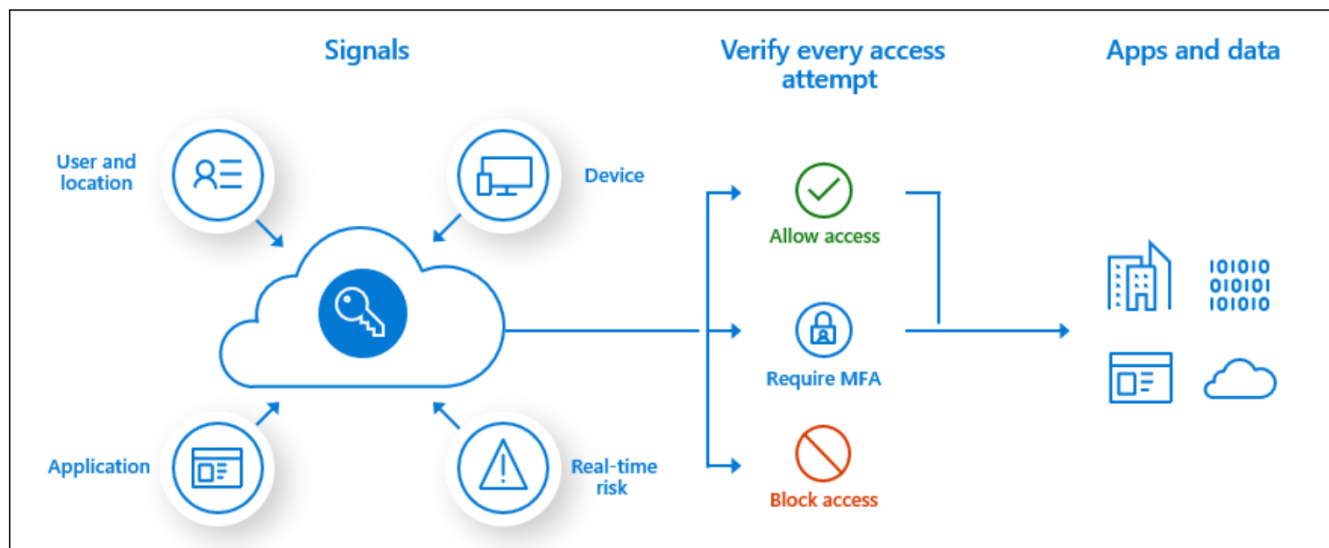
You can bypass the firewall rules from your trusted Azure services and resources to the Azure Synapse workspace. [Learn more](#)

☐ Allow Azure services and resources to access this workspace

+ Add client IP

Rule name	Start IP	End IP	
allowAll	0.0.0.0	255.255.255.255	...
<input type="text"/>	<input type="text"/>	<input type="text"/>	

AAD Conditional Access



1. Sign into the Azure portal using an account with *global administrator permissions*, select **Azure Active Directory**, choose **Security** from the menu.

2. Select **Conditional Access**, then choose **+ New Policy**, and provide a name for the policy.

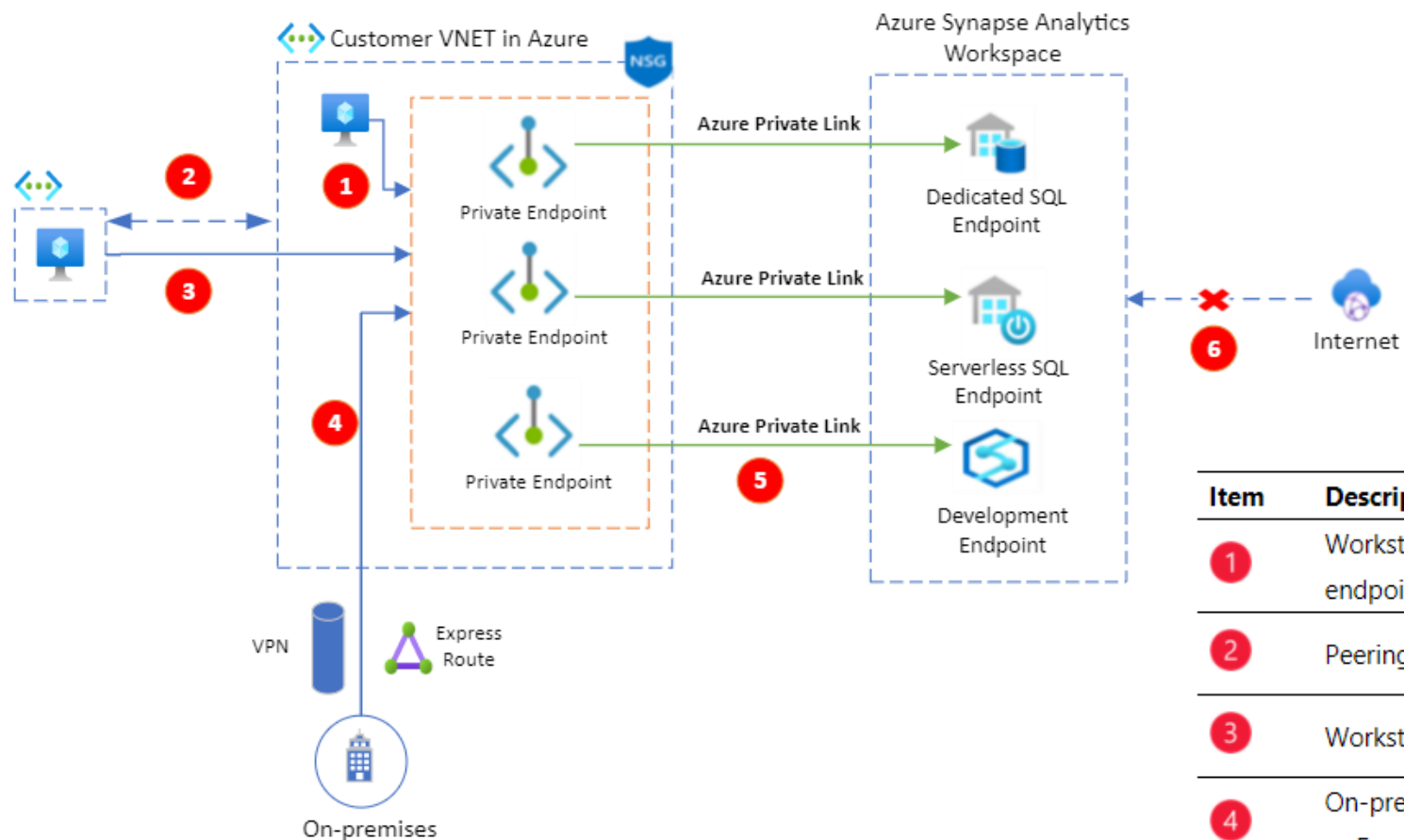
3. Under **Assignments**, select **Users and groups**, check the **Select users and groups** option, and then select an Azure AD user or group for Conditional access. Click **Select**, and then click **Done**.

4. Select **Cloud apps**, click **Select apps**. Select **Microsoft Azure Synapse Gateway**. Then click **Select** and **Done**.

5. Under **Access Controls**, select **Grant** and then check the policy you want to apply, and select **Done**.

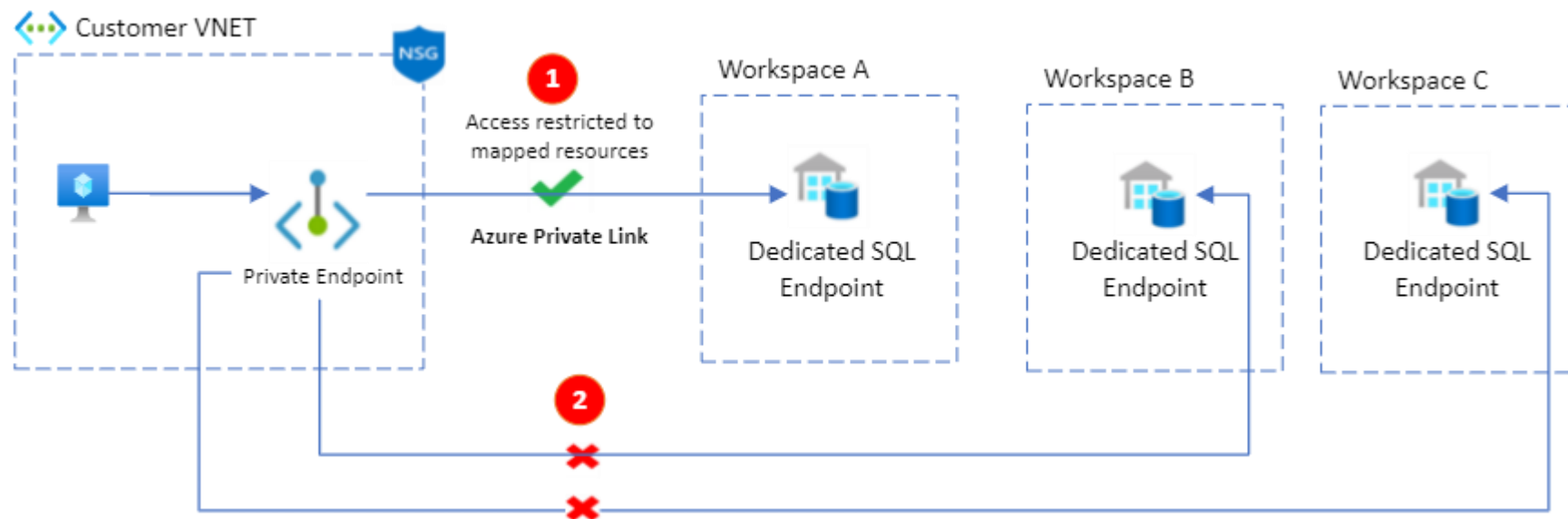
6. Set the **Enable policy** toggle to **On**, then select **Create**.

Private Endpoints



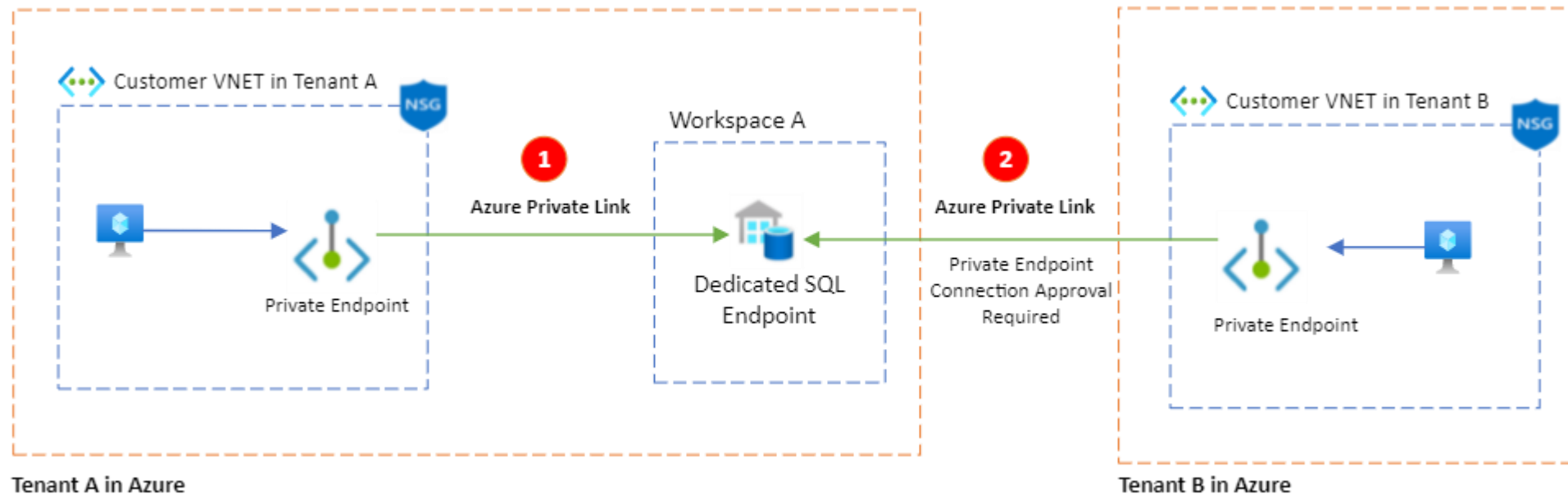
Item	Description
1	Workstations from within the customer VNet access the Synapse private endpoints.
2	Peering between customer VNet and another VNet.
3	Workstation from peered VNet access the Synapse private endpoints.
4	On-premises network access the Synapse Analytics private endpoints through VPN or ExpressRoute.
5	Workspace endpoints mapped into customer's VNet through private endpoints using Azure Private Link service.
6	Public access disabled on Synapse workspace.

Private Endpoints



Item	Description
1	Private endpoint in customer VNet mapped to a single dedicated SQL pool endpoint in Workspace A.
2	Other SQL pool endpoints in other workspaces B and C aren't accessible through this private endpoint, minimizing the exposure.

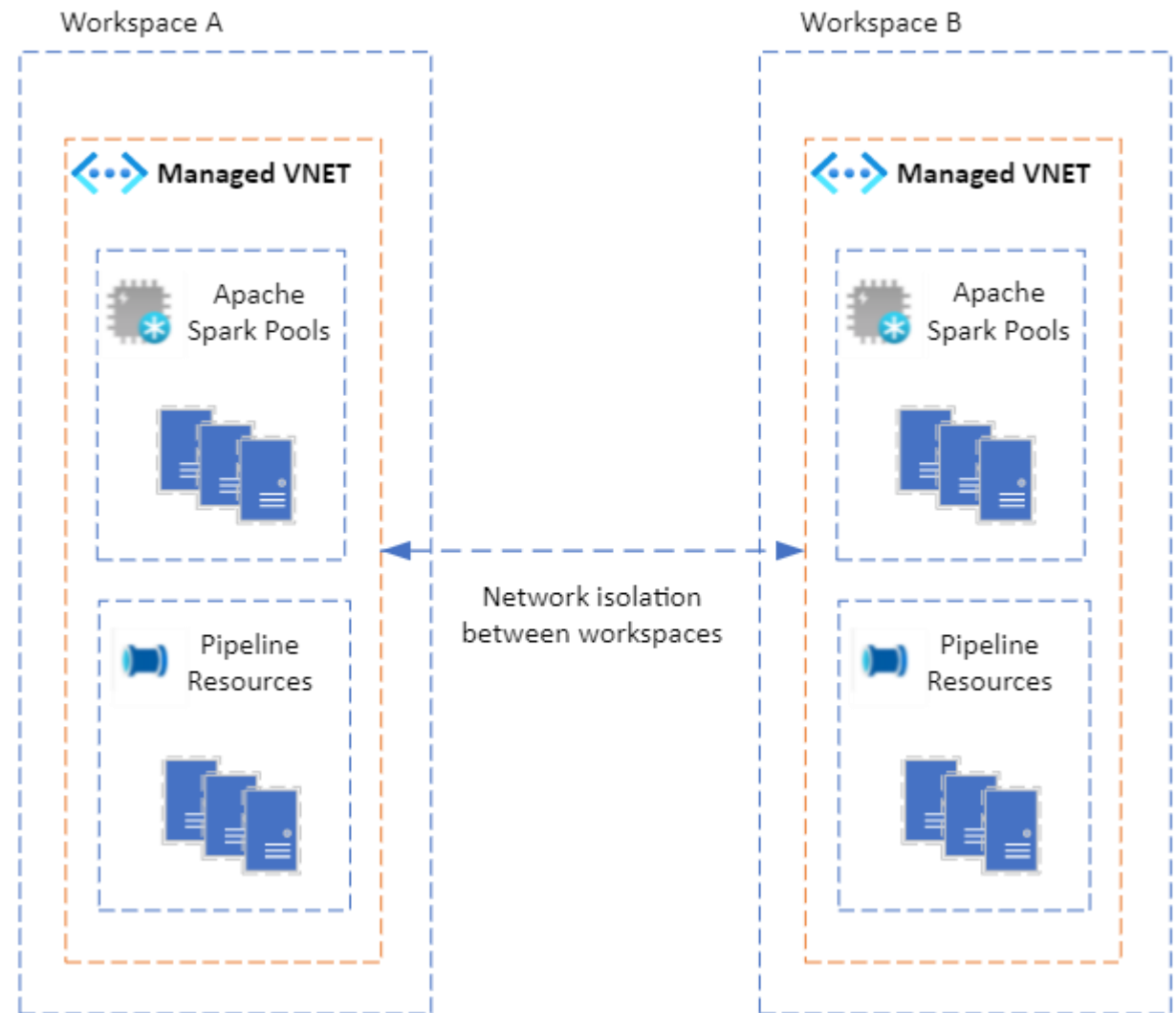
Private Endpoints



Item	Description
1	Dedicated SQL pool in Workspace A in Tenant A accessed by a private endpoint in Customer VNet in Tenant A.
2	Same dedicated SQL pool in Workspace A in Tenant A accessed by a private endpoint in Customer VNet in Tenant B through connection approval workflow.

Managed VNet

- Fully managed network isolation between Synapse workspaces
- Eliminates VNet Injection complexities
- User level network isolation for Spark clusters within the same workspace
- Not applicable to dedicated SQL pools and serverless SQL pools



Advanced Spark Security

New Apache Spark pool ...

* Basics * Additional settings Tags Review + create

Create a Synapse Analytics Apache Spark pool with your preferred configurations. Complete the Basics tab then go to Review + create to provision with smart defaults, or visit each tab to customize.

Apache Spark pool details

Name your Apache Spark pool and choose its initial settings.

Apache Spark pool name *

Isolated compute ⓘ ☐ Enabled ☒ Disabled

Node size family

Node size *

Autoscale * ⓘ ☒ Enabled ☐ Disabled

Number of nodes *

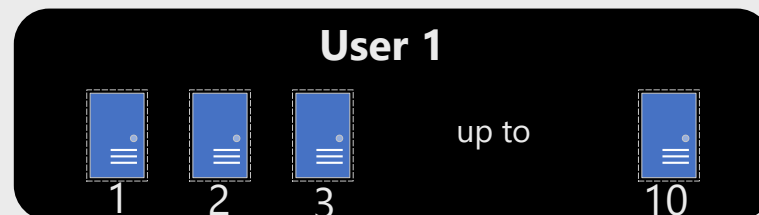
Dynamically allocate executors ⓘ ☐ Enabled ☒ Disabled

Estimated price ⓘ **Est. cost per hour**
3.30 to 11.00 USD
[View pricing details](#)

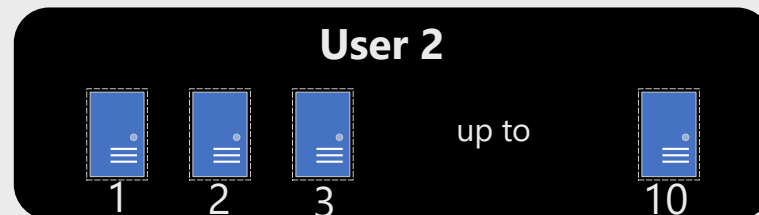


Managed VNet

Subnet 1

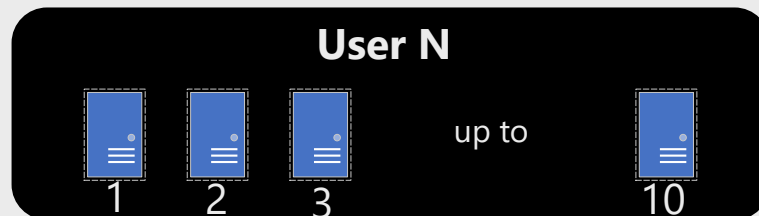


Subnet 2



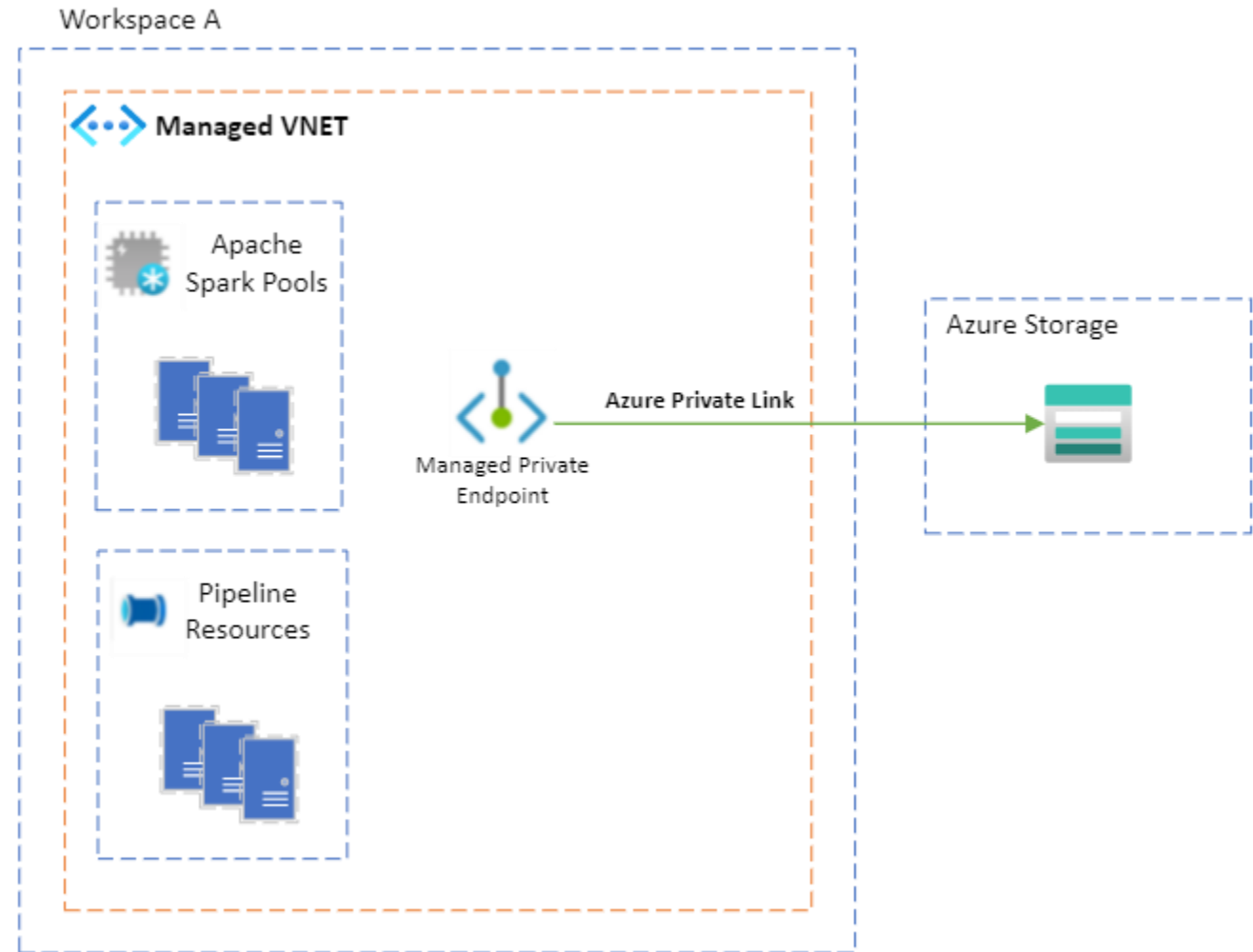
• • • • • • • • • •

Subnet N



Managed private endpoint connection

- Connect to Azure PaaS services securely and seamlessly
- Example – Connect to Azure Storage privately with Azure IR, without having to use self-hosted IR
- Not applicable to dedicated SQL pools and serverless SQL pools




Azure Storage Firewall Exceptions

Public network access

☐ Enabled from all networks

☒ Enabled from selected virtual networks and IP addresses

☐ Disabled

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

Virtual networks


+ Add existing virtual network

+ Add new virtual network

Virtual Network	Subnet	Address range
No network selected.		

Firewall

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

☐ Add your client IP address ('174.95.179.115') 

Address range


IP address or CIDR

Resource instances

Specify resource instances that will have access to your storage account based on their system-assigned managed identity.

Resource type	Instance name
<div>Microsoft.Synapse/workspaces</div>	<div>veng-synapse-ws-001</div>
<div>Select a resource type</div>	<div>Select one or more instances</div>

Exceptions


☒ Allow Azure services on the trusted services list to access this storage account. 

☐ Allow read access to storage logging from any network

☐ Allow read access to storage metrics from any network


Network Routing

Determine how you would like to route your traffic as it travels from its source to an Azure endpoint. Microsoft routing is recommended for most customers.

Routing preference * 

☒ Microsoft network routing

☐ Internet routing

Publish route-specific endpoints 

☐ Microsoft network routing


☐ Internet routing

Public network access

☐ Enabled from all networks


☐ Enabled from selected virtual networks and IP addresses

☒ Disabled

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


Network Routing

Determine how you would like to route your traffic as it travels from its source

Routing preference * 

☒ Microsoft network routing

☐ Internet routing

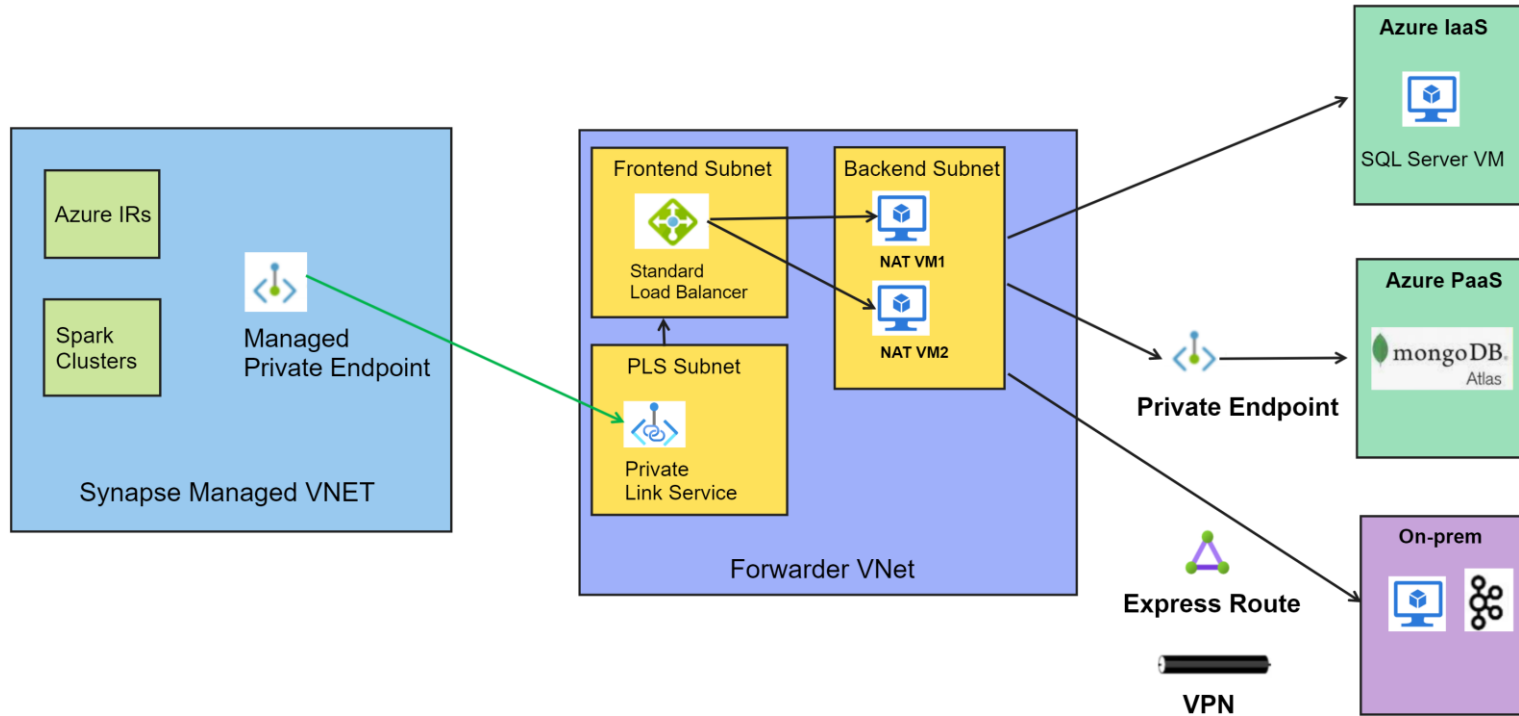
Publish route-specific endpoints 

☐ Microsoft network routing

☐ Internet routing

Trusted Services

MPE with Private Link Service

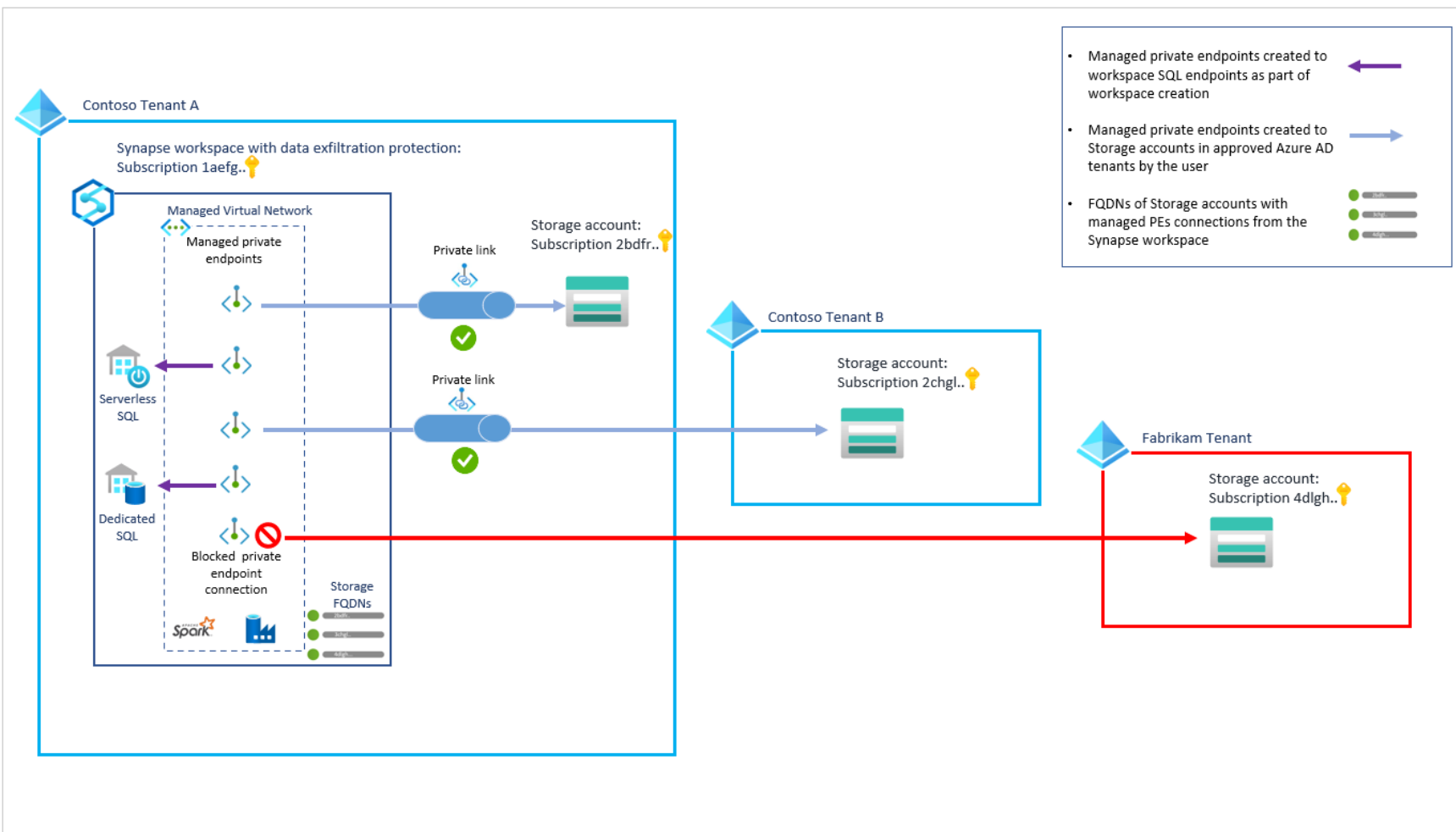


Samples:

[Access on-premises SQL Server from Managed VNet](#)

[Connect Synapse Spark to On-Prem Apache Kafka](#)

Data exfiltration protection



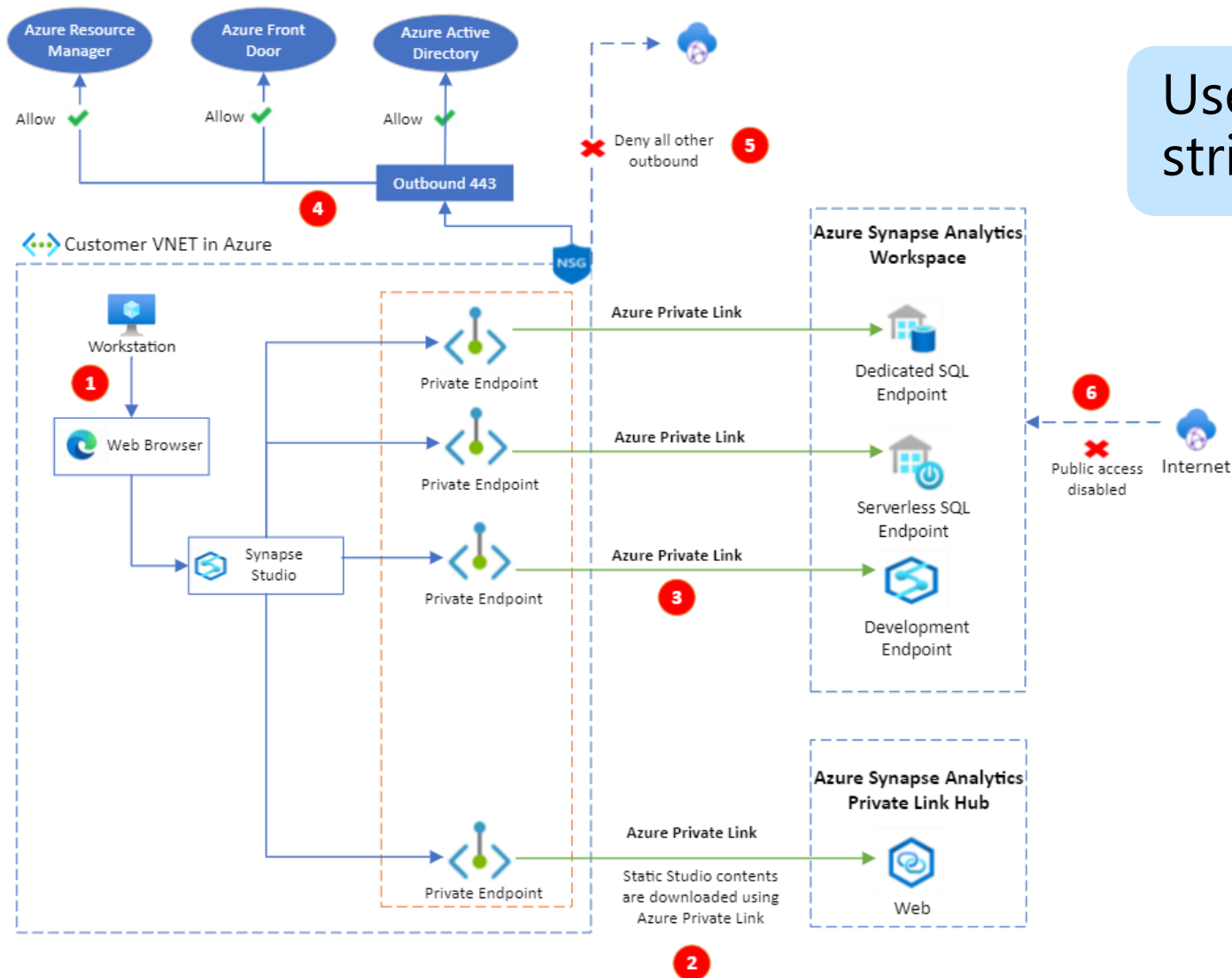
Note:

- SHIR – Not controlled by DEP
- PLS Forwarding – Not controlled by DEP
- SQL Pools can read from any storage, but only CETAS is protected by DEP
- Spark and Pipelines cannot read/write from unapproved tenants

Best Practices:

- Use DEP enabled and not-enabled zones with different workspaces
- Use only for PROD or Pre-PROD scenarios, don't use for DEV/TEST

Private Link Hub for Synapse Studio



Use only for networks with strict internet outbound restrictions !!!

Item	Description
1	Workstation in a restricted customer VNet accessing the Synapse Studio using a web browser.
2	Private endpoint created for private link hubs resource to download the static studio contents using Azure Private Link.
3	Private endpoints created for Synapse workspace endpoints to access the workspace resources securely using Azure Private Links.
4	Network security group rules in the restricted customer VNet allows outbound traffic over port 443 to a limited set of Azure services, such as Azure Resource Manager, Azure Front Door and Azure Active Directory.
5	Network security group rules in the restricted customer VNet denies all other outbound traffic from the VNet.
6	Public access disabled on Synapse workspace.

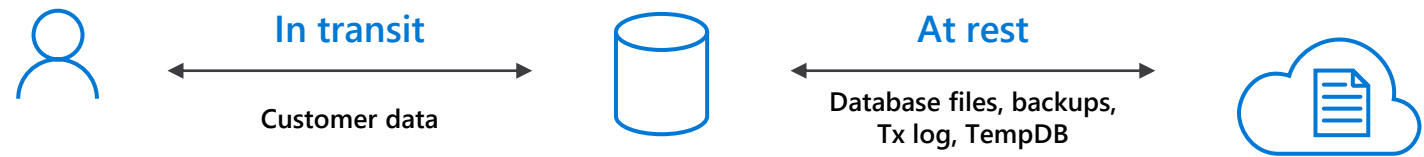


Azure Synapse Analytics

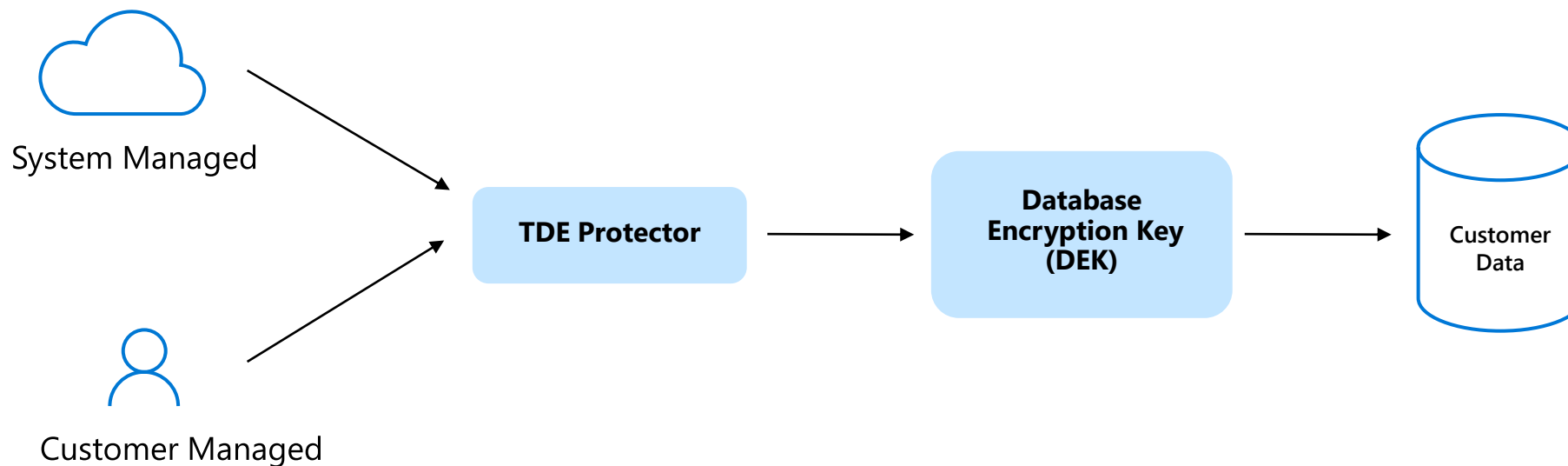
Data Protection

Types of data encryption

Data Encryption	Encryption Technology	Customer Value
In transit	Transport Layer Security (TLS) from the client to the server TLS 1.2	Protects data between client and server against snooping and man-in-the-middle attacks
At rest	Transparent Data Encryption (TDE) for Azure Synapse Analytics	Protects data on the disk User or Service Managed key management is handled by Azure, which makes it easier to obtain compliance



TDE Explained



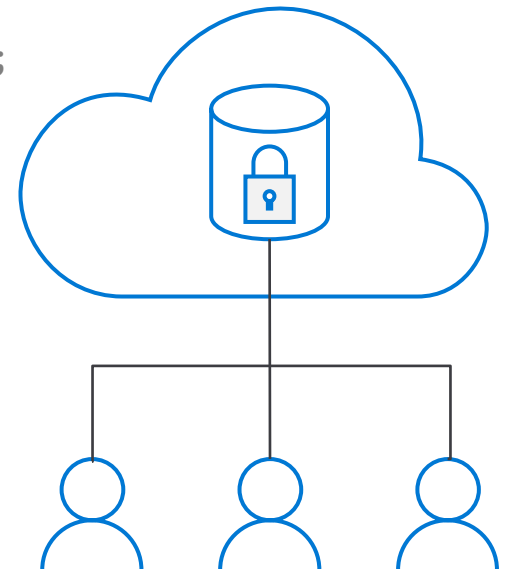
- TDE performs real-time I/O encryption and decryption of the data at the page level.
- Each page is decrypted when it's read into memory and then encrypted before being written to disk.
- TDE encrypts the storage of an entire database by using a symmetric key called the Database Encryption Key (DEK).
- On database startup, the encrypted DEK is decrypted and then used for decryption and re-encryption of the database files in the SQL Server database engine process.
- DEK is protected by the TDE protector.
- TDE protector is either a service-managed certificate (SMK) or an asymmetric key stored in [Azure Key Vault](#) (CMK/BYOK).

System Managed TDE

Overview

- In Azure, the default setting for TDE is that the DEK is protected by a built-in server certificate.
- The built-in server certificate is unique for each server and the encryption algorithm used is AES 256.
- If two databases are connected to the same server, they also share the same built-in certificate.
- Microsoft automatically rotates these certificates in compliance with the internal security policy and the root key is protected by a Microsoft internal secret store.
- Customers can verify compliance with internal security policies in independent third-party audit reports available on the [Microsoft Trust Center](#).
- Microsoft also seamlessly moves and manages the keys as needed for geo-replication and restores.

```
USE master;
GO
CREATE MASTER KEY [ ENCRYPTION BY PASSWORD = '<UseStrongPasswordHere>' ];
go
CREATE CERTIFICATE MyServerCert WITH SUBJECT = 'My DEK Certificate';
go
USE MyDatabase;
GO
CREATE DATABASE ENCRYPTION KEY
WITH ALGORITHM = AES_128
ENCRYPTION BY SERVER CERTIFICATE MyServerCert;
GO
ALTER DATABASE MyDatabase
SET ENCRYPTION ON;
GO
```

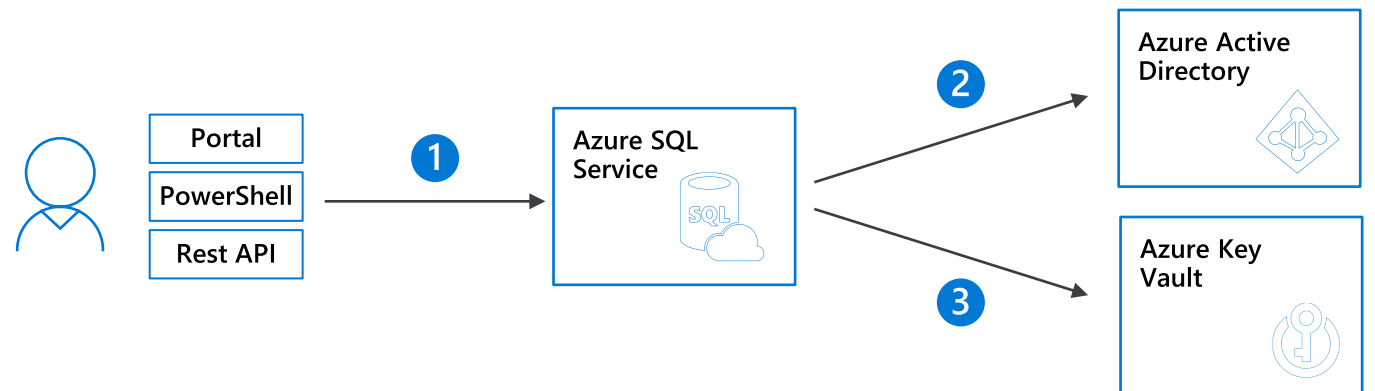


Customer Managed TDE

Key Vault

Benefits with User Managed Keys

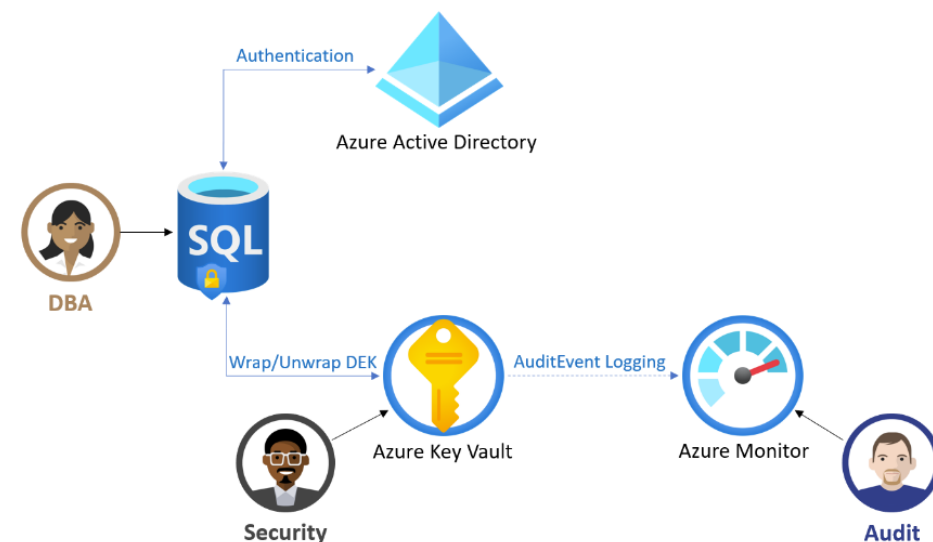
- Full and granular control over usage and management of the TDE protector;
- Transparency of the TDE protector usage;
- Ability to implement separation of duties in the management of keys and data within the organization;
- Key Vault administrator can revoke key access permissions to make encrypted database inaccessible;
- Central management of keys in AKV;
- Greater trust from your end customers, since AKV is designed such that Microsoft can't see nor extract encryption keys;



1 The Key Vault admin grants vault access to the SQL Database server using its unique Azure Active Directory (AD) identity

2 The server uses its Azure AD identity to authenticate with Azure AD for access to your Key Vault

3 The server sends get, wrap key, and unwrap key request to the asymmetric key in key Vault for database encryption key protection.



Row-level security

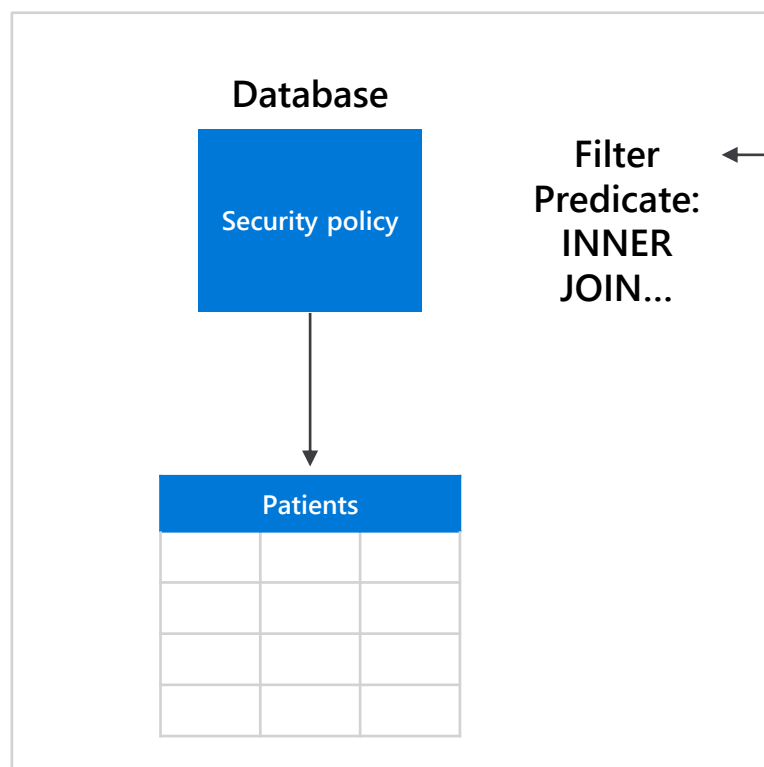
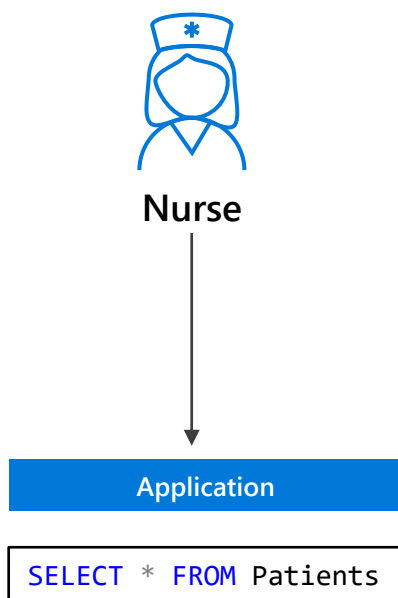
Three steps:

1. Policy manager creates filter predicate and security policy in T-SQL, binding the predicate to the patients table.
2. App user (e.g., nurse) selects from Patients table.
3. Security policy transparently rewrites query to apply filter predicate.

Refer to [best practices](#)



Policy manager



```
CREATE FUNCTION dbo.fn_securitypredicate(@wing int)
RETURNS TABLE WITH SCHEMABINDING AS
return SELECT 1 as [fn_securitypredicate_result] FROM
  StaffDuties d INNER JOIN Employees e
  ON (d.EmpId = e.EmpId)
  WHERE e.UserID = SUSER_SID() AND @wing = d.Wing;

CREATE SECURITY POLICY dbo.SecPol
ADD FILTER PREDICATE dbo.fn_securitypredicate(Wing) ON Patients
WITH (STATE = ON)
```

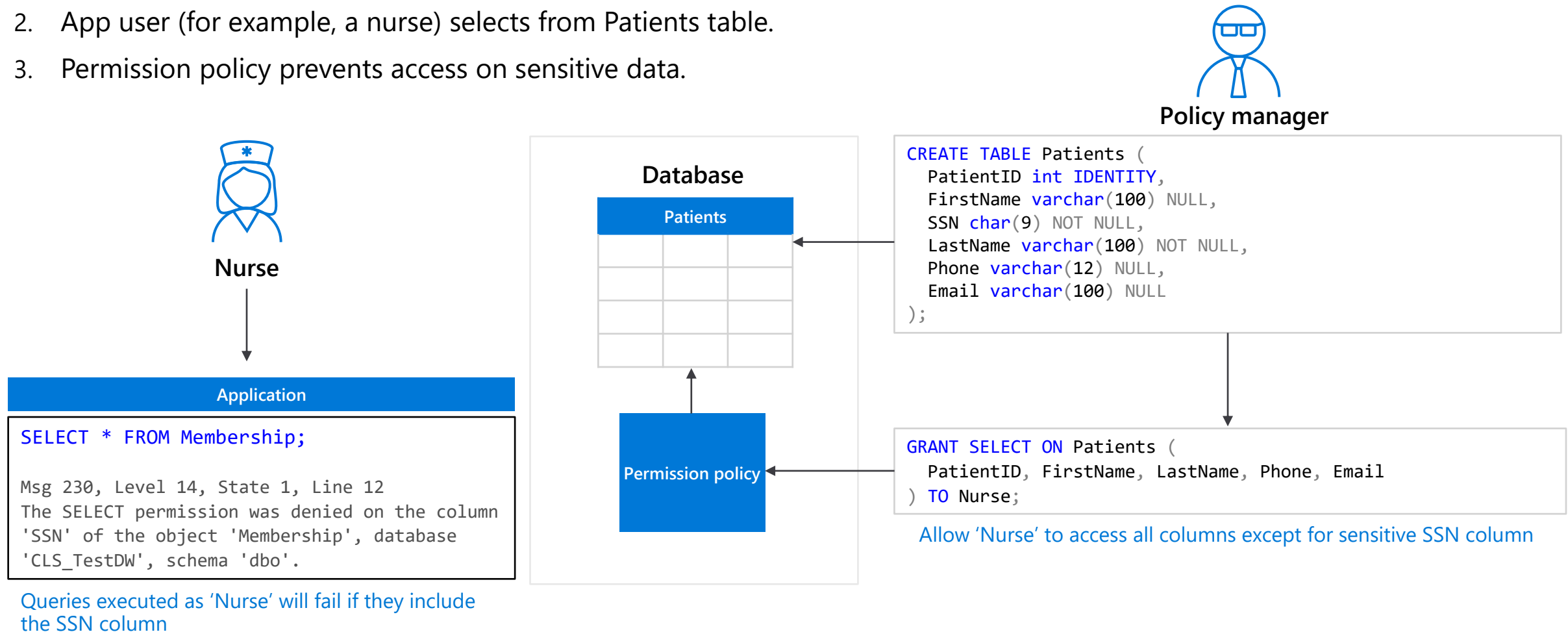
```
SELECT * FROM Patients
SEMIJOIN APPLY dbo.fn_securitypredicate(patients.Wing);
```

```
SELECT Patients.* FROM Patients,
  StaffDuties d INNER JOIN Employees e ON (d.EmpId = e.EmpId)
  WHERE e.UserID = SUSER_SID() AND Patients.wing = d.Wing;
```

Column-level security

Three steps:

1. Policy manager creates permission policy in T-SQL, binding the policy to the Patients table on a specific group.
2. App user (for example, a nurse) selects from Patients table.
3. Permission policy prevents access on sensitive data.



Dynamic Data Masking

Three steps

1. Security officer defines dynamic data masking policy in T-SQL over sensitive data in the Employee table. The security officer uses the built-in masking functions (default, email, random)
2. The app-user selects from the Employee table
3. The dynamic data masking policy obfuscates the sensitive data in the query results for non-privileged users



Security officer

1

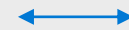
```

ALTER TABLE [Employee]
ALTER COLUMN [SocialSecurityNumber]
ADD MASKED WITH (FUNCTION = 'DEFAULT()')

ALTER TABLE [Employee]
ALTER COLUMN [Email]
ADD MASKED WITH (FUNCTION = 'EMAIL()')

ALTER TABLE [Employee]
ALTER COLUMN [Salary]
ADD MASKED WITH (FUNCTION = 'RANDOM(1,20000)')

GRANT UNMASK to admin1
  
```



2

```

SELECT [First Name],
       [Social Security Number],
       [Email],
       [Salary]
FROM   [Employee]
  
```

Non-masked data (admin login)

	First Name	Social Security Num...	Email	Salary
1	LILA	758-10-9637	lila.barnett@comcast.net	1012794
2	JAMIE	113-29-4314	jamie.brown@ntlworld.com	1025713
3	SHELLEY	550-72-2028	shelley.lynn@charter.net	1040131
4	MARCELLA	903-94-5665	marcella.estrada@comcast.net	1040753
5	GILBERT	376-79-4787	gilbert.juarez@verizon.net	1041308

Masked data (admin1 login)

	First Name	Social Security Number	Email	Salary
1	LILA	XXX-XX-XX37	lXX@XXXX.net	8940
2	JAMIE	XXX-XX-XX14	jXX@XXXX.com	19582
3	SHELLEY	XXX-XX-XX28	sXX@XXXX.net	3713
4	MARCELLA	XXX-XX-XX65	mXX@XXXX.net	11572
5	GILBERT	XXX-XX-XX87	gXX@XXXX.net	4487

Column Level Encryption

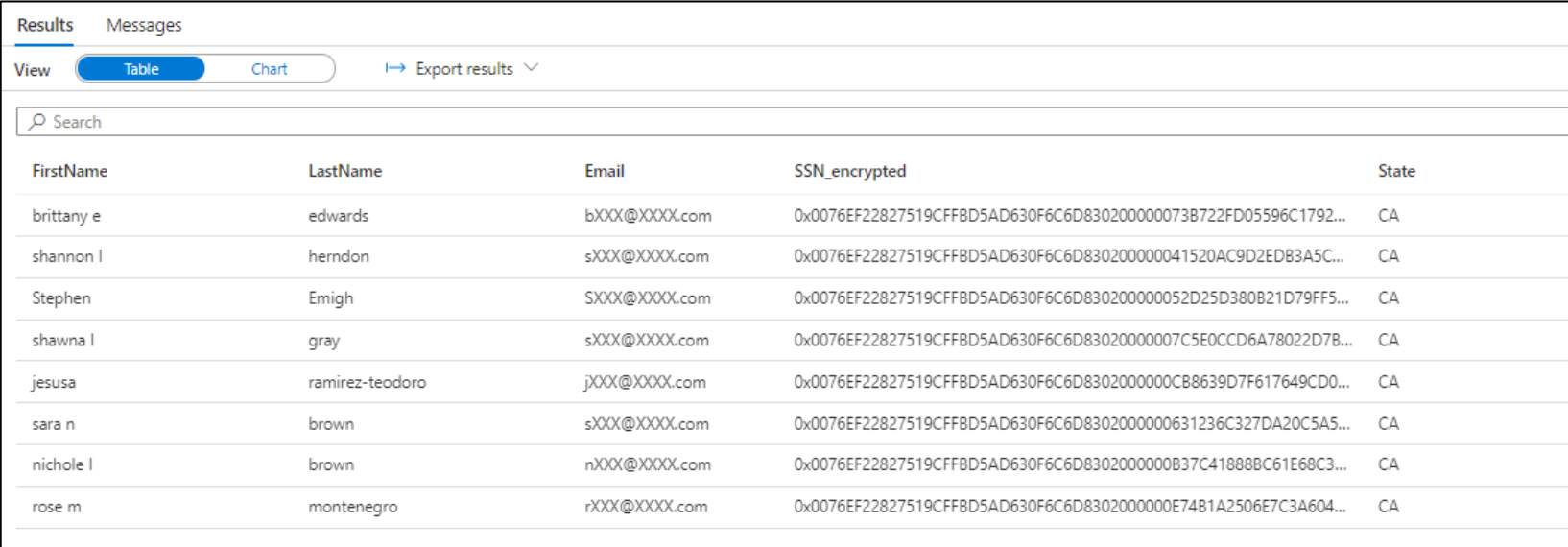
Overview

It helps to implement fine-grained protection of sensitive data within a table in dedicated SQL pool.

The data in CLE enforced columns is encrypted on disk. User need to use DECRYPTBYKEY function to decrypt it.

5 step process to set up CLE

1. Create master key
2. Create certificate
3. Configure symmetric key for encryption
4. Encrypt the column data
5. Close symmetric key



The screenshot shows a SQL query results window with a 'Results' tab selected. The window displays a table with five columns: FirstName, LastName, Email, SSN_encrypted, and State. The SSN values are encrypted and displayed as long hexadecimal strings. The interface includes a search bar, view options (Table, Chart), and an export results button.

FirstName	LastName	Email	SSN_encrypted	State
brittany e	edwards	bXXX@XXX.com	0x0076EF22827519CFFBD5AD630F6C6D830200000073B722FD05596C1792...	CA
shannon l	herndon	sXXX@XXX.com	0x0076EF22827519CFFBD5AD630F6C6D830200000041520AC9D2EDB3A5C...	CA
Stephen	Emigh	SXXX@XXX.com	0x0076EF22827519CFFBD5AD630F6C6D830200000052D25D380B21D79FF5...	CA
shawna l	gray	sXXX@XXX.com	0x0076EF22827519CFFBD5AD630F6C6D83020000007C5E0CCD6A78022D7B...	CA
jesusa	ramirez-teodoro	jXXX@XXX.com	0x0076EF22827519CFFBD5AD630F6C6D8302000000C88639D7F617649CD0...	CA
sara n	brown	sXXX@XXX.com	0x0076EF22827519CFFBD5AD630F6C6D8302000000631236C327DA20C5A5...	CA
nichole l	brown	nXXX@XXX.com	0x0076EF22827519CFFBD5AD630F6C6D8302000000B37C41888BC61E68C3...	CA
rose m	montenegro	rXXX@XXX.com	0x0076EF22827519CFFBD5AD630F6C6D8302000000E74B1A2506E7C3A604...	CA



Azure Synapse Analytics

Authentication

Authentication Methods

SQL Authentication

With this authentication method, the user submits a user account name and associated password to establish a connection. This password is stored in the master database for user accounts linked to a login

Azure Active Directory Authentication

With this authentication method, the user submits a user account name and requests that the service use the credential information stored in Azure Active Directory (Azure AD).

Contained Database User

In the contained database user model, the login in the master database is not present. Instead, the authentication process occurs at the user database, and the database user in the user database does not have an associated login in the master database.

In Azure Synapse Analytics contained database users are supported only with Azure Active Directory authentication.

Contained database users are **not supported for SQL Server authentication**.

SQL Authentication **does not support** password policy enforcement and expiration

[ALTER LOGIN \(Transact-SQL\) - SQL Server | Microsoft Docs](#)

[LOGINPROPERTY \(Transact-SQL\) - SQL Server | Microsoft Docs](#)

Login

A login is an individual account in the master database, to which a user account in one or more databases can be linked. With a login, the credential information for the user account is stored with the login.

User

A user account is an individual account in any database that may be, but does not have to be, linked to a login. With a user account that is not linked to a login, the credential information is stored with the user account.

Azure Active Directory authentication

Overview

Manage user identities in one location.

Enable access to Azure Synapse Analytics and other Microsoft services with Azure Active Directory user identities and groups.

Benefits

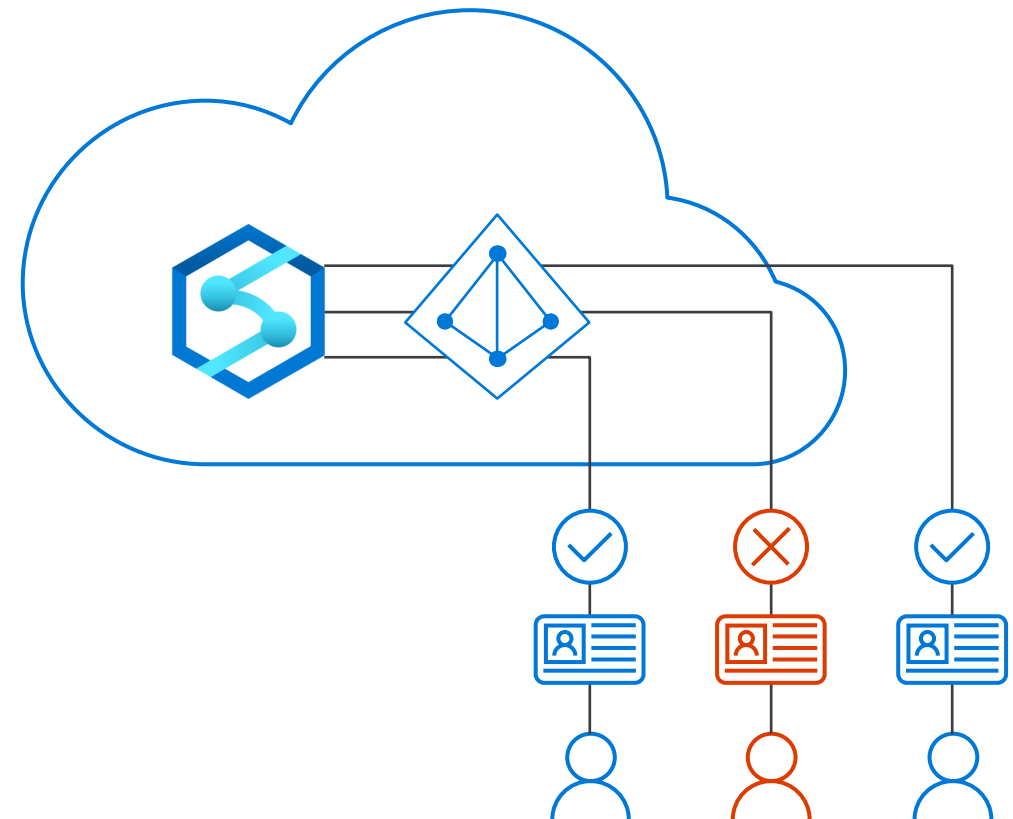
Enables management of database permissions by using external Azure Active Directory groups

Allows password rotation in a single place



Alternative to SQL Server authentication

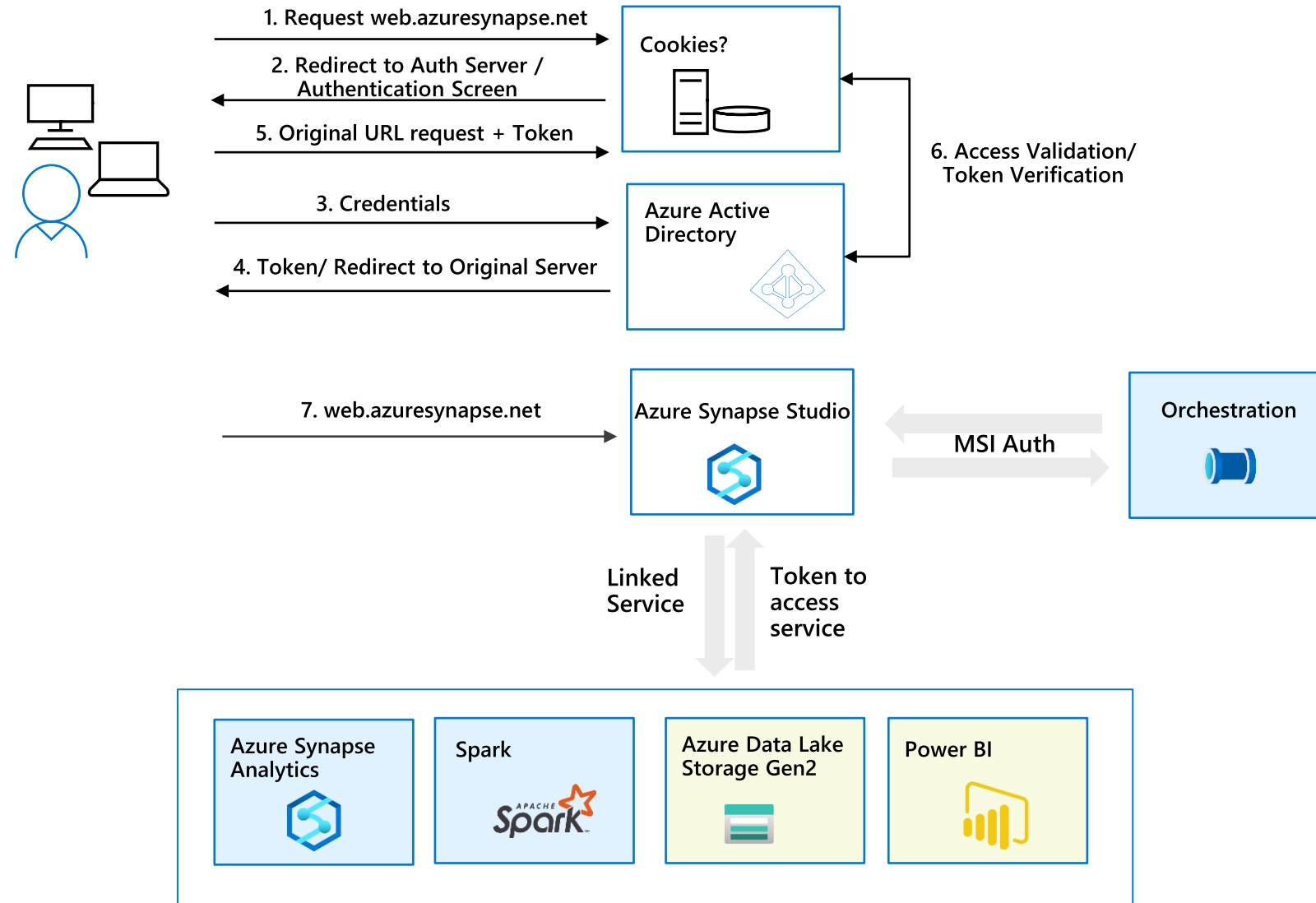
Eliminates the need to store passwords

Azure Synapse Analytics



Single Sign-On

 Synapse Foundation Components
 Synapse Linked Services



Implicit authentication - User provides login credentials once to access Azure Synapse Workspace

AAD authentication - Azure Synapse Studio will request token to access each linked services as user. A separate token is acquired for each of the below services:

1. ADLS Gen2
2. Azure Synapse Analytics
3. Power BI
4. Spark – Spark Livy API
5. `management.azure.com` – resource provisioning
6. Develop artifacts – `dev.workspace.net`
7. Graph endpoints

MSI authentication - Orchestration uses workspace MSI auth for automation



Azure Synapse Analytics

Access Control

Access Control

Overview

Azure Synapse provides a comprehensive and fine-grained access control system, that integrates:

- ❑ **Azure roles** for resource management and access to data in storage
- ❑ **Synapse roles** for managing live access to code and execution
- ❑ **SQL roles** for data plane access to data in SQL pools
- ❑ **Git permissions** for source code control, including continuous integration and deployment support

Synapse Roles

Overview

It provides access control management to workspace resources and artifacts

Add role assignment

Grant others access to this workspace by assigning roles to users, groups, and/or service principals.
[Learn more](#)

Scope *

☒ Workspace ☐ Workspace item

Role *

Select a role

Filter...

- Synapse Administrator
- Synapse SQL Administrator
- Synapse Apache Spark Administrator
- Synapse Contributor (preview)
- Synapse Artifact Publisher (preview)
- Synapse Artifact User (preview)
- Synapse Compute Operator (preview)
- Synapse Credential User (preview)

Microsoft Azure | internalsandbox

» [Publish all](#) [Validate all](#) [Refresh](#) [Discard all](#)

Access control

Grant access to Synapse workspace and resources by assigning a role to a user, group, service principal, or managed identity.

[+ Add](#) [Refresh](#) [Remove access](#)

Showing 1 - 3 of 3 items

NAME	TYP	ROLE
------	-----	------

Add role assignment

Grant others access to this workspace by assigning roles to users, groups, and/or service principals.
[Learn more](#)

Scope *

☐ Workspace ☒ Workspace item

Item type *

Apache Spark pools

Item *

analytics1

Role *

Synapse Compute Operator (preview)

Filter...

- Synapse Administrator
- Synapse Contributor (preview)
- Synapse Compute Operator (preview)

Synapse RBAC Roles and permitted actions

Actions -> Roles	Synapse Administrator	Spark Administrator	SQL Administrator	Synapse Contributor	Artifact Publisher	Artifact User	Compute Operator	Credential User	Linked Data Manager	Synapse User
workspaces/read	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
workspaces/roleAssignments/write, delete	Yes									
workspaces/managedPrivateEndpoint/write, delete	Yes								Yes	
workspaces/bigDataPools/useCompute/action	Yes	Yes		Yes			Yes			
workspaces/bigDataPools/viewLogs/action	Yes	Yes		Yes			Yes			
workspaces/integrationRuntimes/useCompute/action	Yes			Yes			Yes			
workspaces/integrationRuntimes/viewLogs/action	Yes			Yes			Yes			
workspaces/artifacts/read	Yes	Yes	Yes	Yes	Yes	Yes				
workspaces/notebooks/write, delete	Yes	Yes		Yes	Yes					
workspaces/sparkJobDefinitions/write, delete	Yes	Yes		Yes	Yes					
workspaces/sqlScripts/write, delete	Yes		Yes	Yes	Yes					
workspaces/kqlScripts/write, delete	Yes			Yes	Yes					
workspaces/dataFlows/write, delete	Yes			Yes	Yes					
workspaces/pipelines/write, delete	Yes			Yes	Yes					
workspaces/triggers/write, delete	Yes			Yes	Yes					
workspaces/datasets/write, delete	Yes			Yes	Yes					
workspaces/libraries/write, delete	Yes	Yes		Yes	Yes					
workspaces/linkedServices/write, delete	Yes	Yes	Yes	Yes	Yes				Yes	
workspaces/credentials/write, delete	Yes		Yes	Yes	Yes				Yes	
workspaces/notebooks/viewOutputs/action	Yes	Yes		Yes	Yes	Yes				
workspaces/pipelines/viewOutputs/action	Yes			Yes	Yes	Yes				
workspaces/linkedServices/useSecret/action	Yes							Yes		
workspaces/credentials/useSecret/action	Yes	Yes						Yes		

Synapse RBAC Roles and permitted actions

Roles -> Scope	Workspace	Apache Spark pool	Integration runtime	Linked service	Credential
Synapse Administrator	Yes	Yes	Yes	Yes	Yes
Synapse Apache Spark Administrator	Yes				
Synapse SQL Administrator	Yes				
Synapse Contributor	Yes	Yes	Yes		
Synapse Artifact Publisher	Yes				
Synapse Artifact User	Yes				
Synapse Compute Operator	Yes	Yes	Yes		
Synapse Credential User	Yes			Yes	Yes
Synapse Linked Data Manager	Yes				
Synapse User	Yes				

SQL Roles & Permissions

Fixed Database Roles and Permissions

db_owner	Super user role – all activities
db_securityadmin	Can modify role membership for custom roles
db_accessadmin	Can add or remove access to the database
db_backupoperator	Can back up the database.
db_ddladmin	Can run any Data Definition Language (DDL) command in a database.
db_datawriter	Can add, delete, or change data in all user tables.
db_datareader	Can read all data from all user tables and views. except sys and <i>INFORMATION_SCHEMA</i> .
db_denydatawriter	Cannot add, modify, or delete any data in the user tables within a database.
db_denydatareader	Cannot read any data from the user tables and views within a database.

Custom Database Roles

A custom role enables you to create your own user-defined database roles and carefully grant each role the least permissions necessary for the business need. You can then add users to the custom role.

Object Level Permissions

There are over 200 permissions that can be individually granted or denied in SQL Database. Many of these permissions are nested. Applied using GRANT, REVOKE, and DENY statements.

```
GRANT SELECT ON SCHEMA::HumanResources TO role_HumanResourcesDept;
```

```
REVOKE SELECT ON SCHEMA::HumanResources TO role_HumanResourcesDept;
```

<https://aka.ms/sql-permissions-poster>

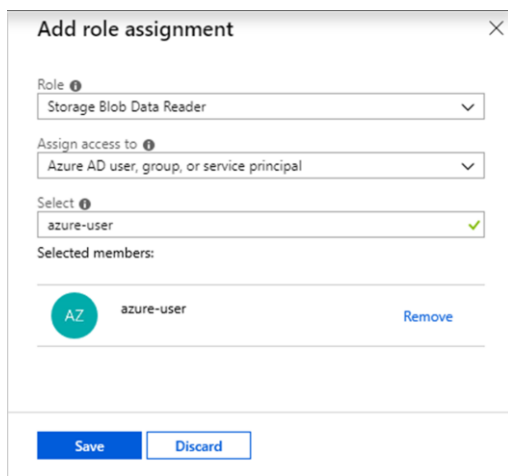
Access control – serverless SQL pool

Overview

Enterprise-grade security model enables you to control who can access data.

Benefits

- Use Azure Active Directory users or native SQL logins.
- SAS tokens, AAD or workspace identity access
- Specify access methods in credential
- Grant access to storage by referencing storage credential
- Enable some logins to access external tables
- Add AAD role assignments directly on Azure storage.



--Create Login to a a single serverless SQL pool database

```
CREATE LOGIN [alias@domain.com] FROM EXTERNAL PROVIDER;
```

-- create user under that login

```
use yourdb -- Use your DB name
```

```
go
```

```
CREATE USER alias FROM LOGIN [alias@domain.com];
```

To grant full access to a user to all serverless SQL pool databases

```
CREATE LOGIN [alias@domain.com] FROM EXTERNAL PROVIDER;
```

```
ALTER SERVER ROLE sysadmin ADD MEMBER [alias@domain.com];
```

-- enable impersonation using workspace Managed Identity

```
CREATE CREDENTIAL [ManagedIdentity]
```

```
WITH IDENTITY = 'Managed Identity'
```

-- enable access to specified storage using SAS token

```
CREATE CREDENTIAL [https://XXX.blob.core.windows.net/csv]
```

```
WITH IDENTITY = 'SHARED ACCESS SIGNATURE',
```

```
SECRET = 'sv=2014-02-
```

```
14&sr=b&si=TestPolicy&sig=o%2B5%2F0C%2BLm7tWWft'
```

-- grant login1 to use SAS token defined in credential for storage account

```
GRANT REFERENCES CREDENTIAL::[https://XXX.blob.core.windows.net/csv]
```

```
TO LOGIN = 'login1'
```

-- grant login2 to use Managed Identity

```
GRANT REFERENCES CREDENTIAL::[ManagedIdentity]
```

```
TO LOGIN = 'login2'
```

-- grant login2 to select external data via table

```
GRANT SELECT ON OBJECT::[dbo.population] TO LOGIN = 'login2'
```

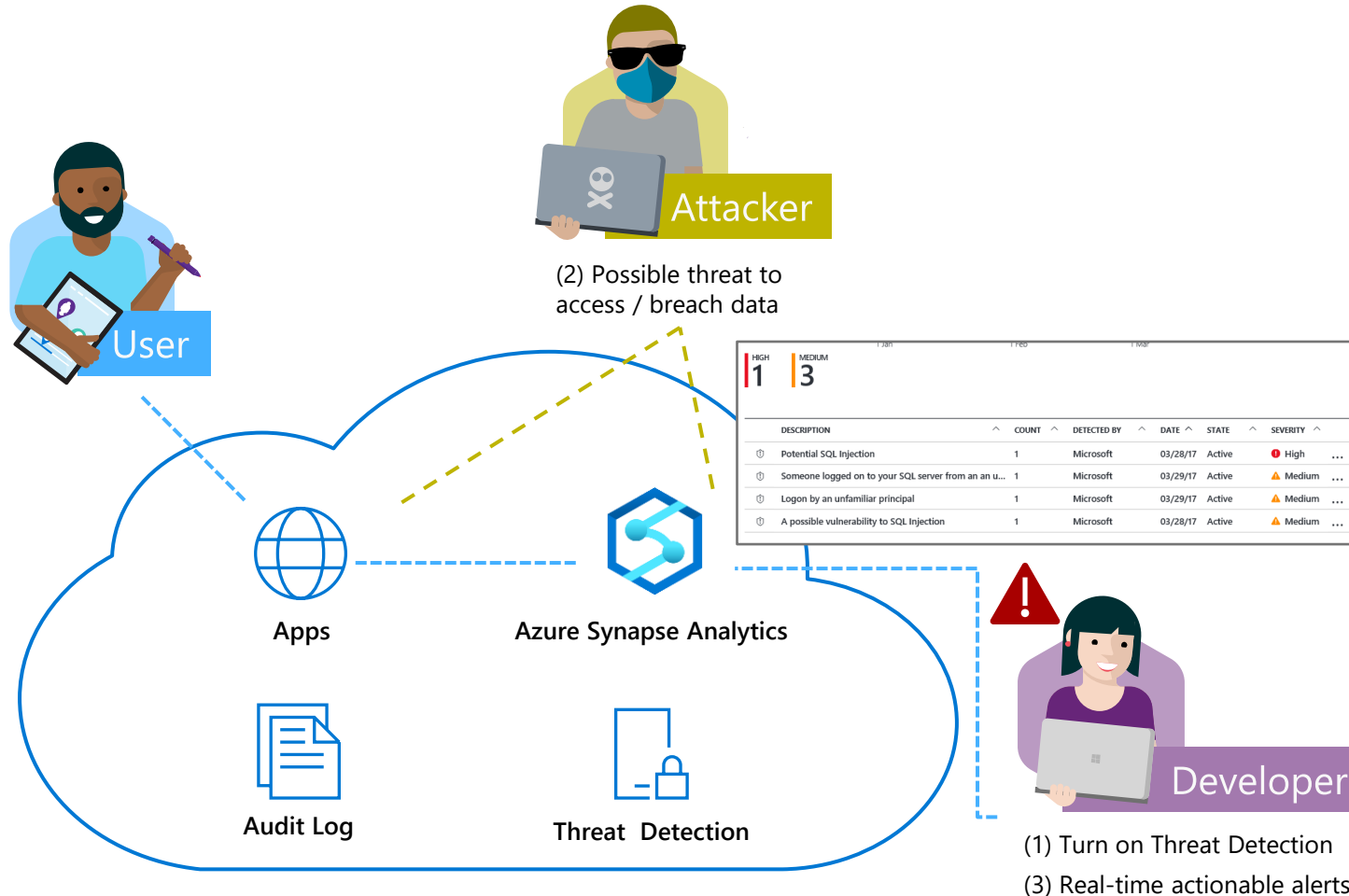


Azure Synapse Analytics

Threat Protection

SQL threat detection

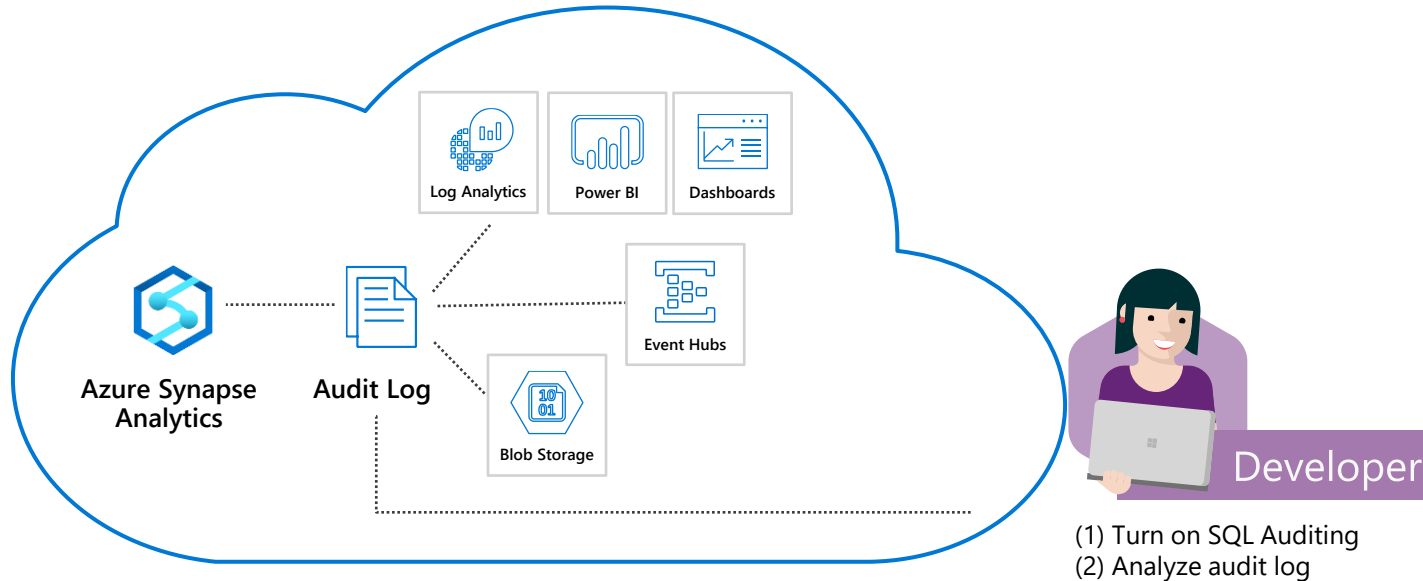
Detect and investigate anomalous database activity



- ✓ Detects potential SQL injection attacks
- ✓ Detects unusual access & data exfiltration activities
- ✓ Actionable alerts to investigate & remediate
- ✓ View alerts for your entire Azure tenant using Azure Security Center

SQL auditing in Azure Log Analytics and Event Hubs

Gain insight into database audit log



✓ Configurable via audit policy

✓ SQL audit logs can reside in

- Azure [Storage account](#)
- Azure Log Analytics
- Azure Event Hubs

✓ Rich set of tools for

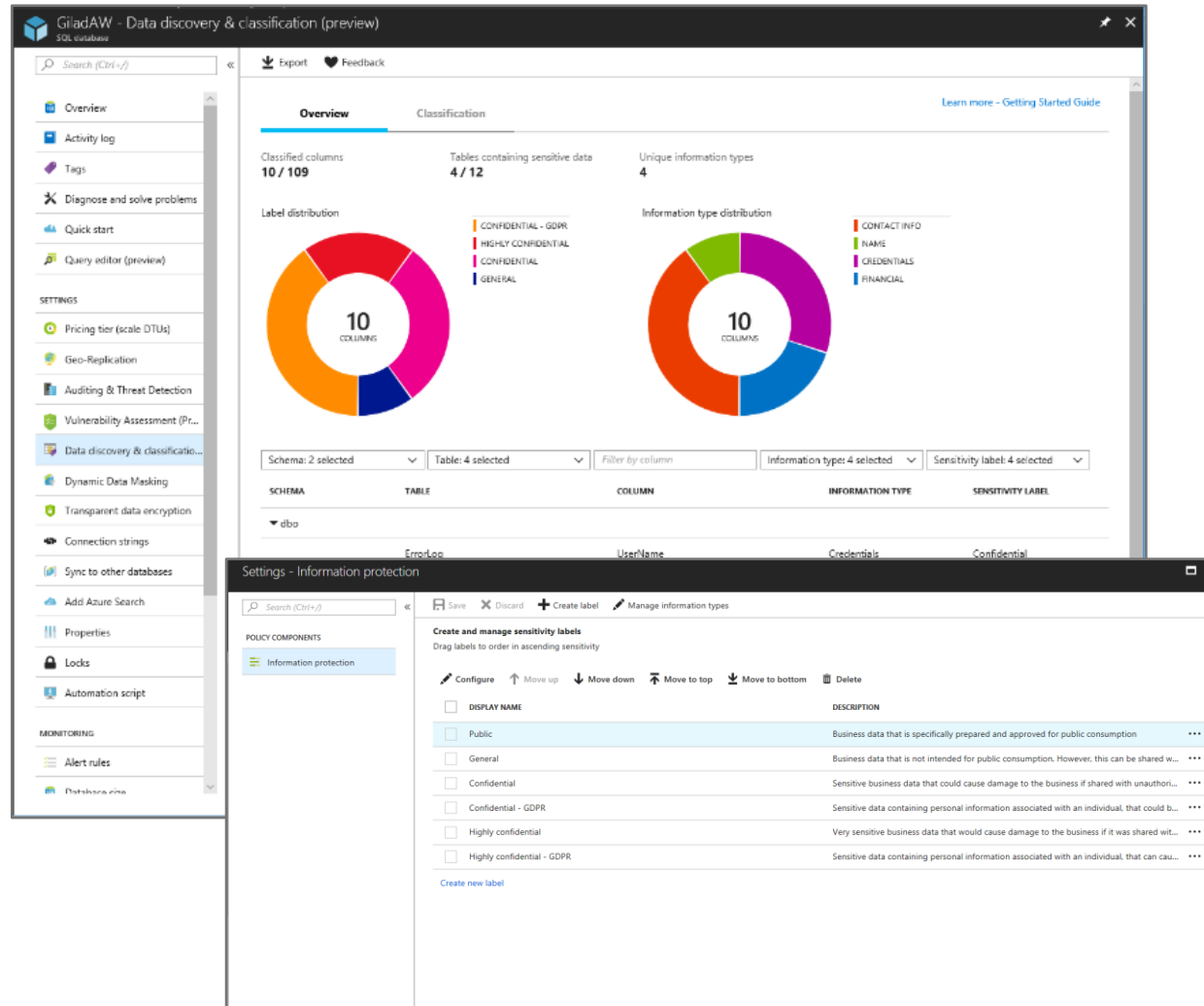
- [Investigating](#) security alerts
- Tracking [access](#) to sensitive data

The screenshot shows the Azure Log Analytics interface. On the left, there's a sidebar with filters for TYPE (1), LOGICALSERVERNAME_S (1), and CATEGORY (1). The main area shows a search query: `search "where Category == 'SQLSecurityAuditEvents' | project TimeGenerated, server_principal_name_s, statement_s, affected_rows_d, SeverityLevel | sort by TimeGenerated asc"`. The results are displayed in a table with 62 results.

TimeGenerated	server_principal_name_s	statement_s	affected_rows_d	SeverityLevel
8/15/2018 12:00:22.521 AM	admin1		0	
8/15/2018 12:00:22.521 AM	admin1	exec sp_executesql N'SELECT tbl.name AS [Name], SCHEMA_NAME(tbl...	0	
8/15/2018 12:00:22.521 AM	admin1	exec sp_executesql N'SELECT ISNULL(HAS_PERMS_BY_NAME(QUOTEN...	1	
8/15/2018 12:00:22.521 AM	admin1	DECLARE @edition sysname: SET @edition = cast(SERVERPROPERTY(N...	4	
8/15/2018 12:00:22.521 AM	admin1		0	
8/15/2018 12:00:22.521 AM	admin1	exec sp_executesql N'SELECT CAST((this_enabled AS bit) AS [isDisabled]...	0	
8/15/2018 12:00:22.521 AM	admin1	IF OBJECT_ID (N'[sys].[database_query_store_options]') IS NOT NULL BE...	2	

SQL Data Discovery & Classification

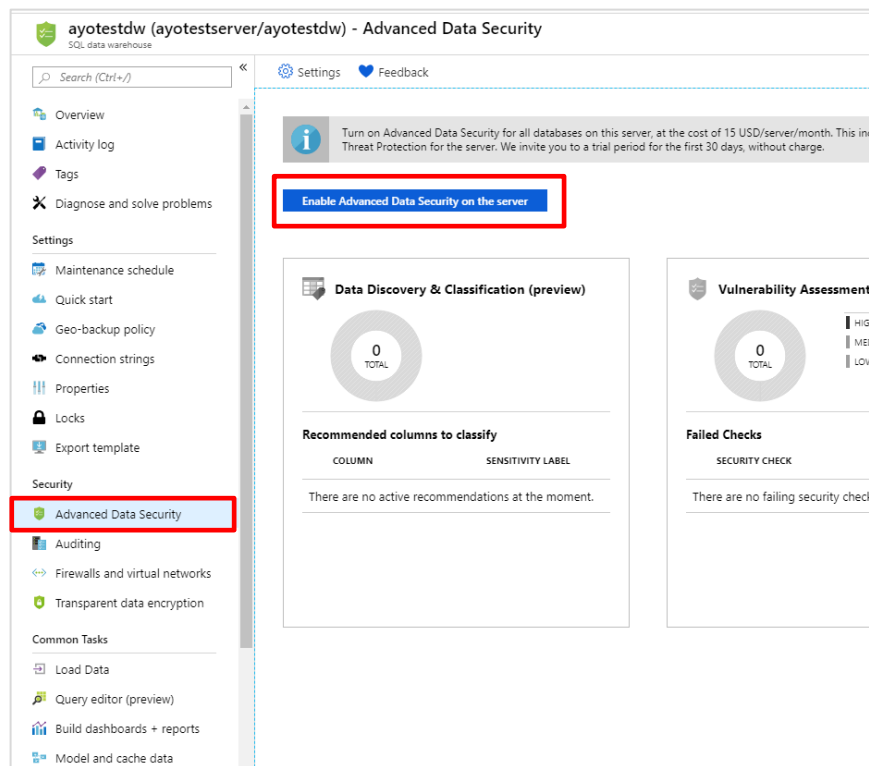
Discover, classify, protect and track access to sensitive data



- ✓ Automatic **discovery** of columns with sensitive data
- ✓ Add **persistent** sensitive data labels
- ✓ **Audit** and **detect** access to the sensitive data
- ✓ **Manage labels** for your entire Azure tenant using Azure Security Center

SQL Data Discovery & Classification - setup

Step 1: Enable Advanced Data Security on the logical SQL Server



ayotestdw (ayotestserver/ayotestdw) - Advanced Data Security

SQL data warehouse

Search (Ctrl+/)

Settings Feedback

Turn on Advanced Data Security for all databases on this server, at the cost of 15 USD/server/month. This includes Threat Protection for the server. We invite you to a trial period for the first 30 days, without charge.

Enable Advanced Data Security on the server

Data Discovery & Classification (preview)

0 TOTAL

Recommended columns to classify

COLUMN	SENSITIVITY LABEL
There are no active recommendations at the moment.	

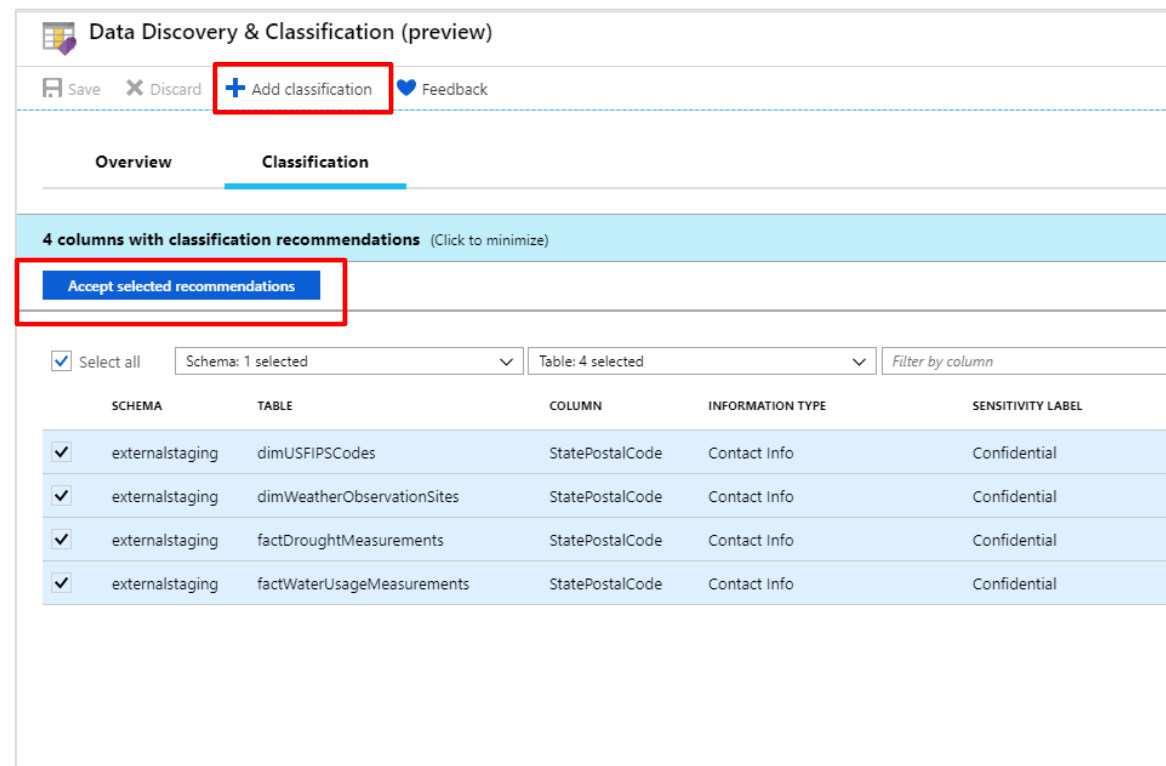
Vulnerability Assessment

0 TOTAL

Failed Checks

SECURITY CHECK
There are no failing security checks.

Step 2: Use recommendations and/or manual classification to classify all the sensitive columns in your tables



Data Discovery & Classification (preview)

Save Discard **+ Add classification** Feedback

Overview **Classification**

4 columns with classification recommendations (Click to minimize)

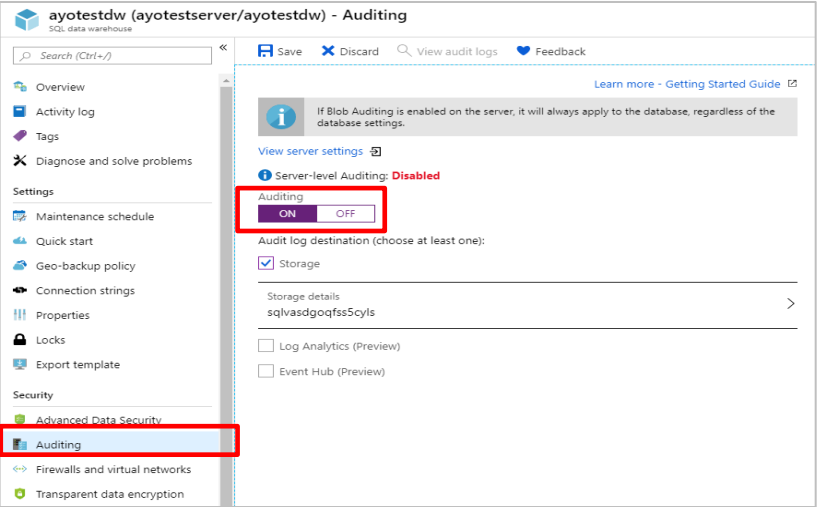
Accept selected recommendations

☒ Select all Schema: 1 selected Table: 4 selected Filter by column

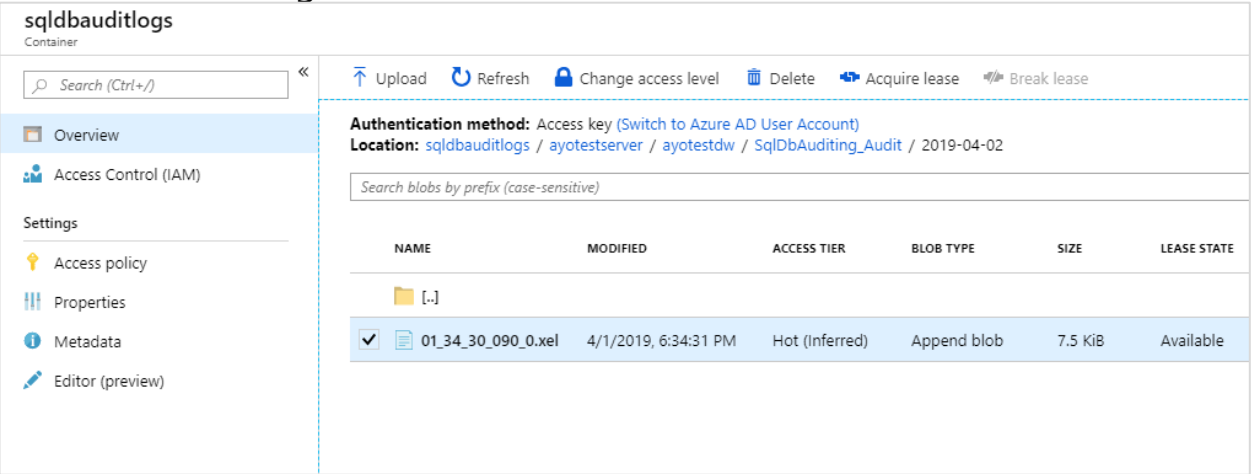
	SCHEMA	TABLE	COLUMN	INFORMATION TYPE	SENSITIVITY LABEL
<input checked="" type="checkbox"/>	externalstaging	dimUSFIPSCodes	StatePostalCode	Contact Info	Confidential
<input checked="" type="checkbox"/>	externalstaging	dimWeatherObservationSites	StatePostalCode	Contact Info	Confidential
<input checked="" type="checkbox"/>	externalstaging	factDroughtMeasurements	StatePostalCode	Contact Info	Confidential
<input checked="" type="checkbox"/>	externalstaging	factWaterUsageMeasurements	StatePostalCode	Contact Info	Confidential

SQL Data Discovery & Classification – audit sensitive data access

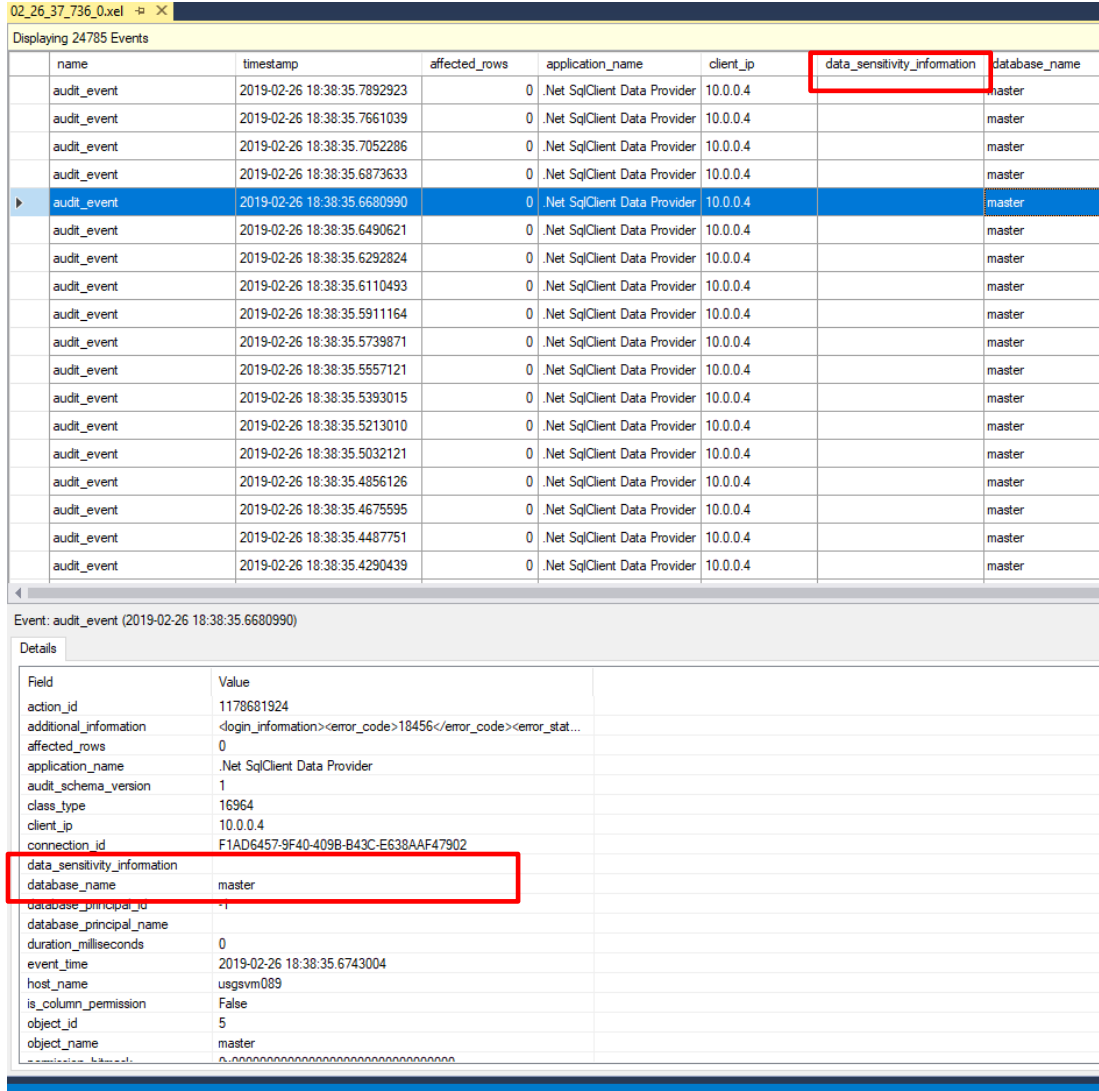
Step 1: Configure auditing for your target Data warehouse. This can be configured for just a single data warehouse or all databases on a server.



Step 2: Navigate to audit logs in storage account and download 'xel' log files to local machine.



Step 3: Open logs using extended events viewer in SSMS. Configure viewer to include 'data_sensitivity_information' column



Thank You – Q&A