#FABCONSQLCON2026

FABCON
Microsoft Fabric
COMMUNITY CONFERENCE

SQLCON
Microsoft SQL
COMMUNITY CONFERENCE

ATLANTA MARCH 16 - 20, 2026

End-to-End Security for Data Warehousing in Microsoft Fabric

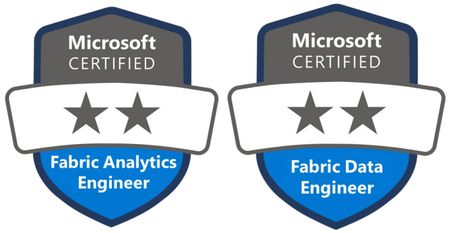
Shabnam Watson
Microsoft Data Platform MVP
Principal Consultant, ABI Cube

Shabnam Watson

Data Consultant,

Speaker, author, blogger, Microsoft Data Platform MVP

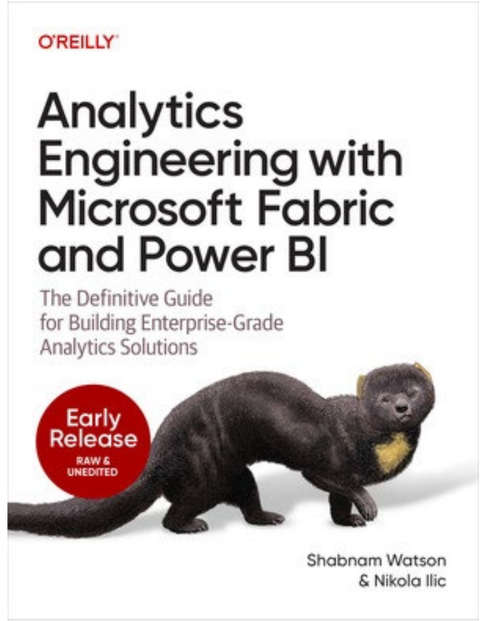
Azure Data & AI, Power BI & Fabric



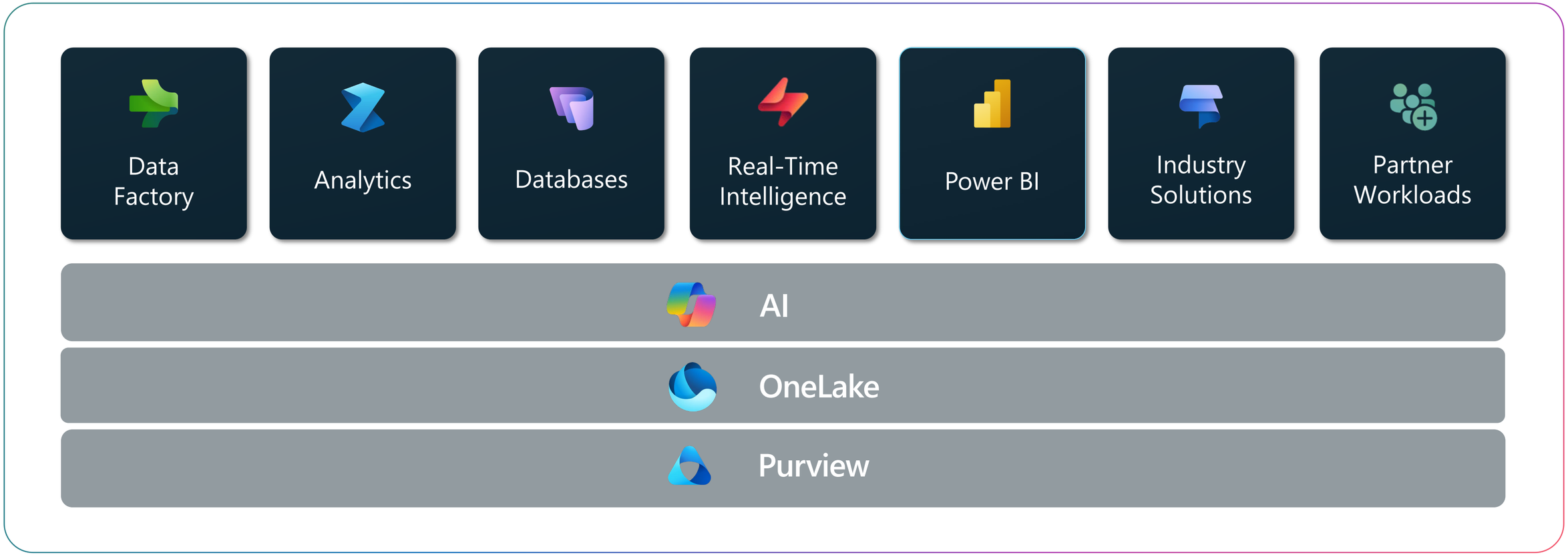
www.shabnamwatson.com

/ShabnamWatson

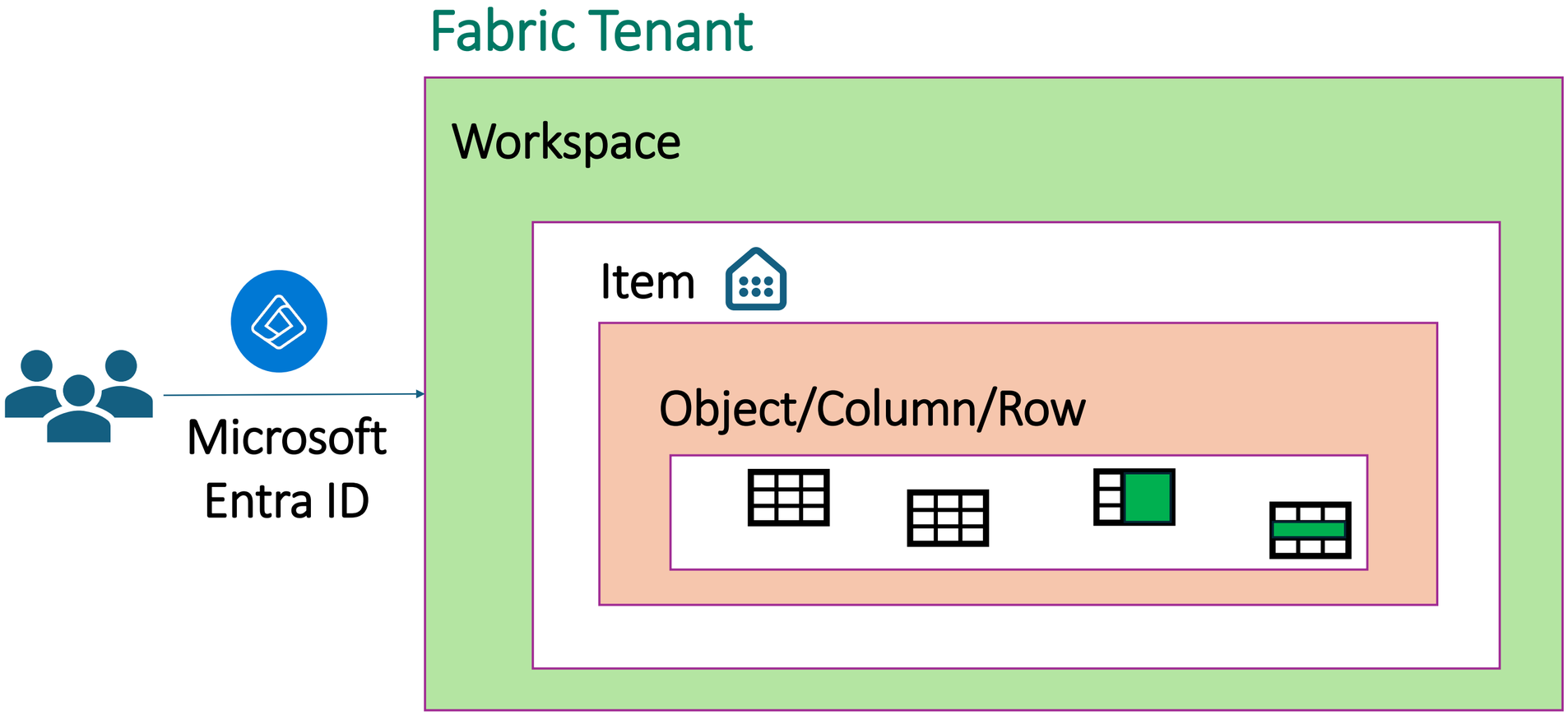
https://www.youtube.com/@ShabnamWatson



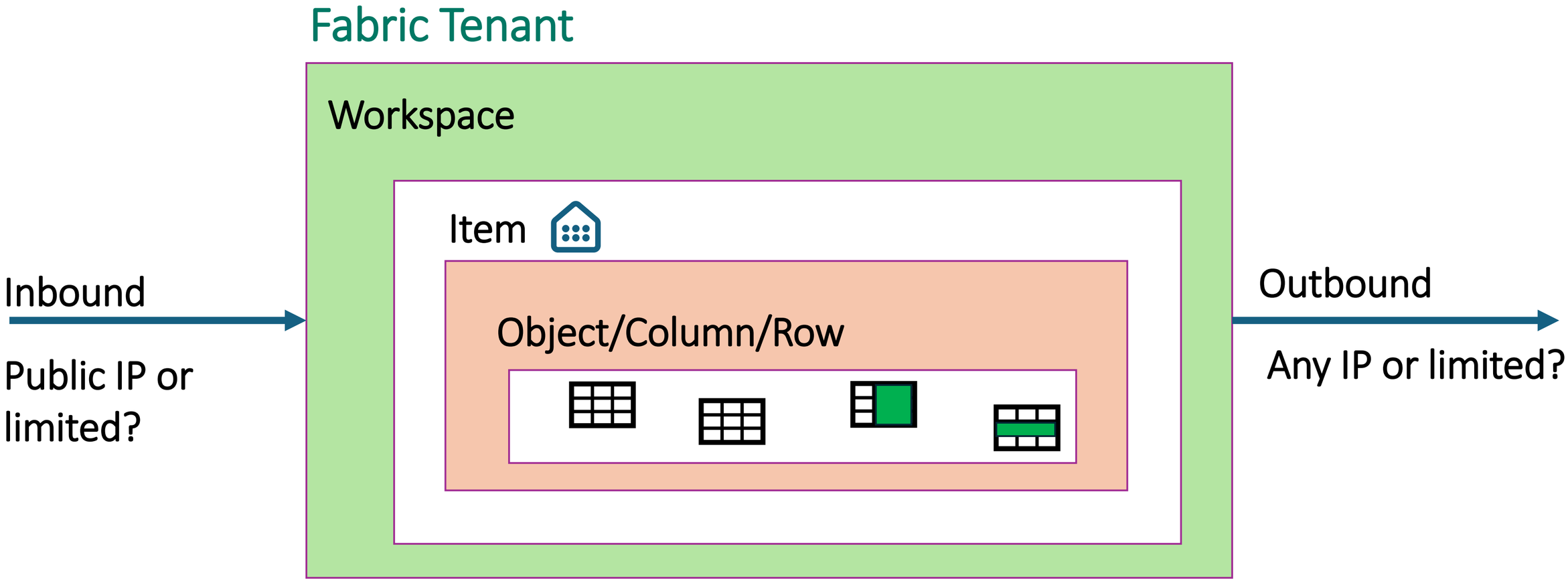
Microsoft Fabric



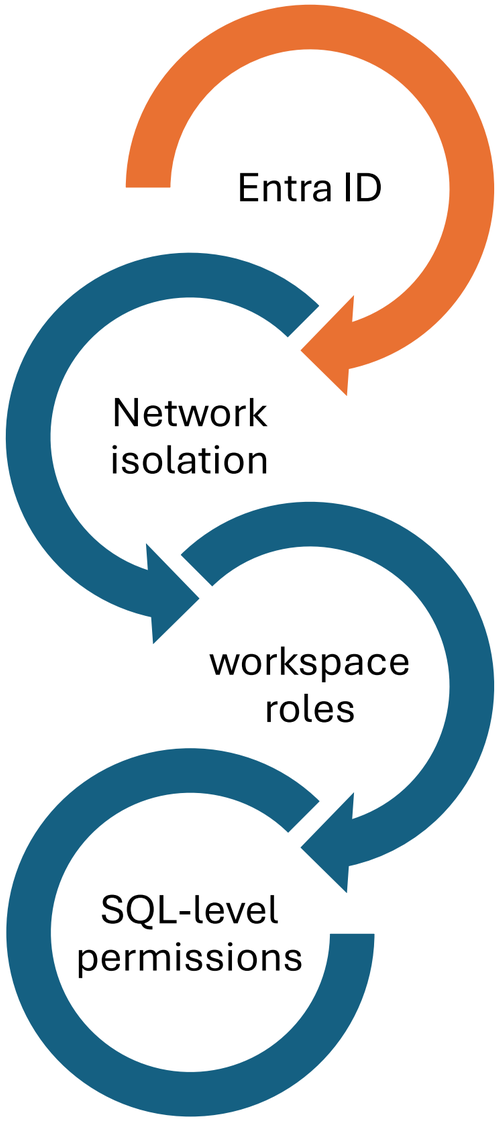
Access Control



Network Security



Warehouse Secured with



EntraID

Identity Management in Microsoft Fabric

User Authentication: Microsoft Entra ID.

SSO Integration: Users log in with their Microsoft 365 credentials.

Token-Based Access: Entra ID issues OAuth 2.0 / OpenID Connect tokens to authorize actions.

Conditional Access in Entra ID

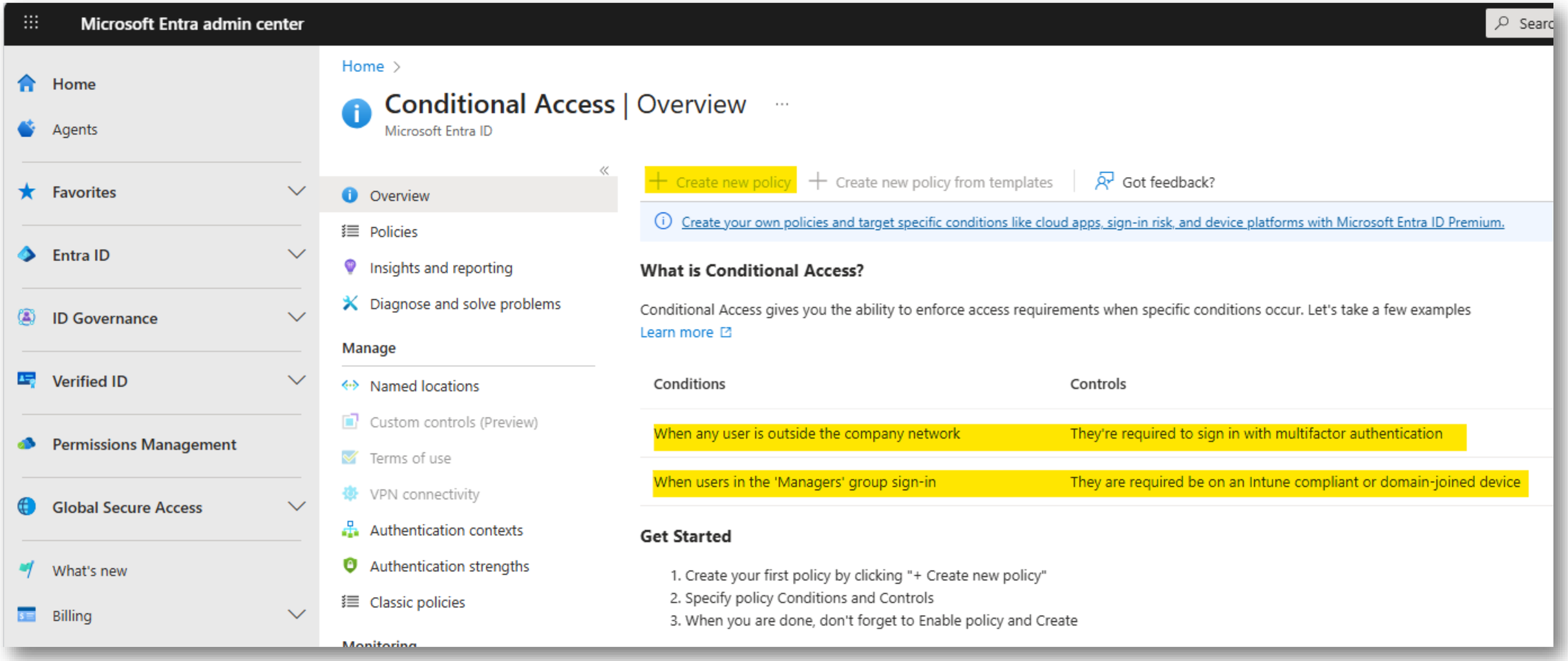
Policy Engine*: Enforces context-aware access controls.

- **Who**: User or group identity.
- **Where**: Location/IP restrictions.
- **What**: Device compliance (e.g., managed device).
- **Risk**: Sign-in risk level (e.g., unfamiliar behavior).
- **Session Controls**: Limit access duration or require re-authentication.

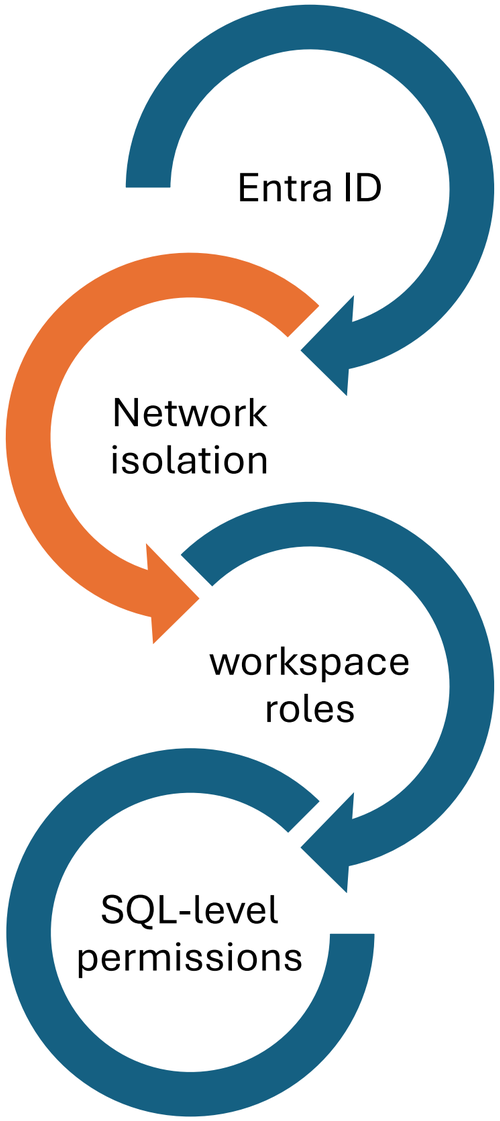
* Requires Microsoft Entra ID P1 licenses or Microsoft 365 Business Premium licenses

What is Conditional Access in Microsoft Entra ID? - Microsoft Entra ID | Microsoft Learn

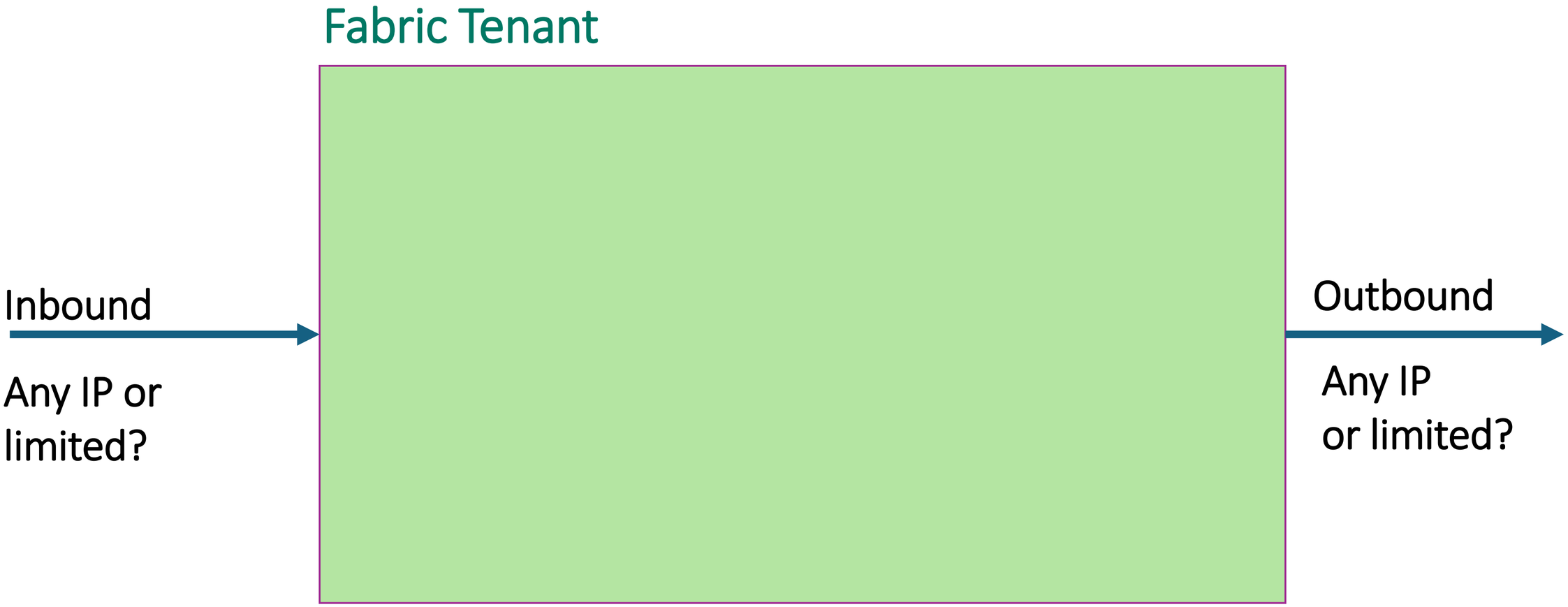
Conditional Access Policy



Warehouse Secured with



Network Security

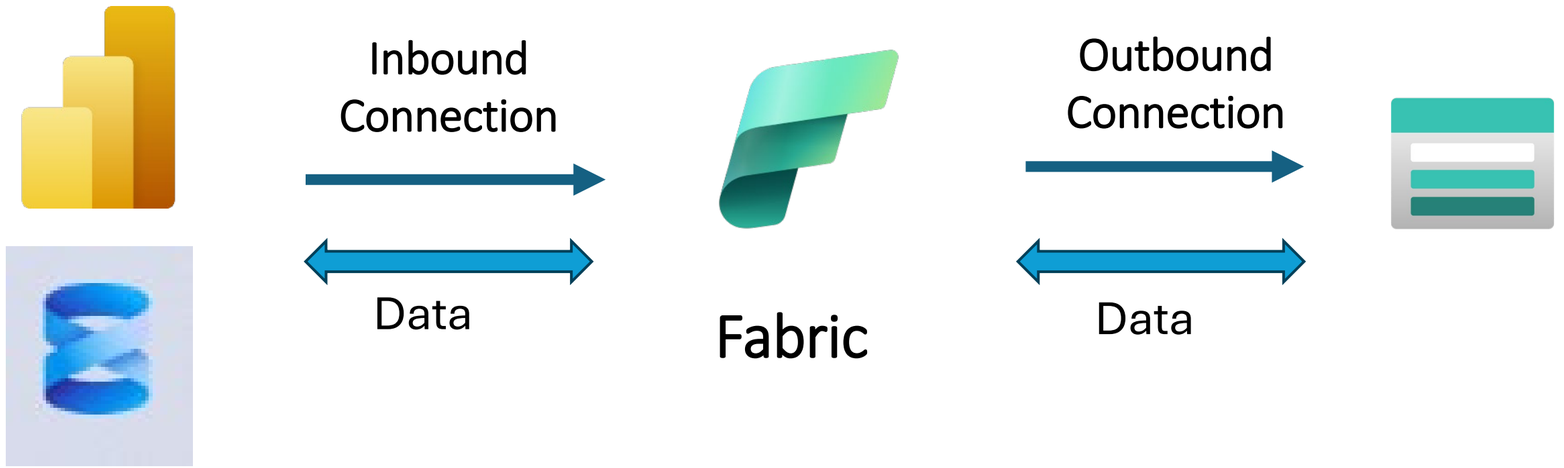


Network Security

- **Inbound Security**
  Protects internal data from external threats.

- **Outbound Security**
  Ensures secure sharing of data outside workspace boundaries.

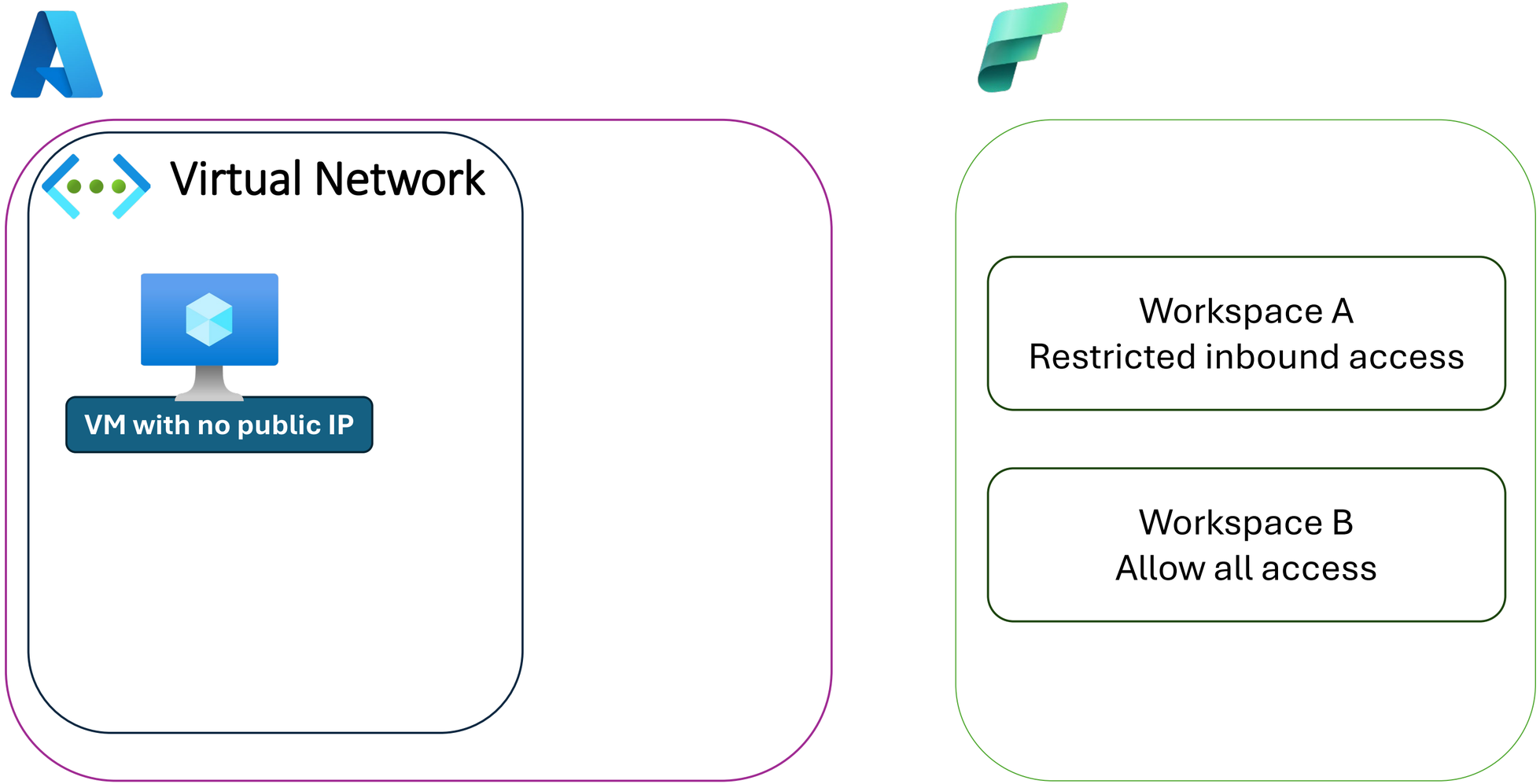
Network Security: All about connections



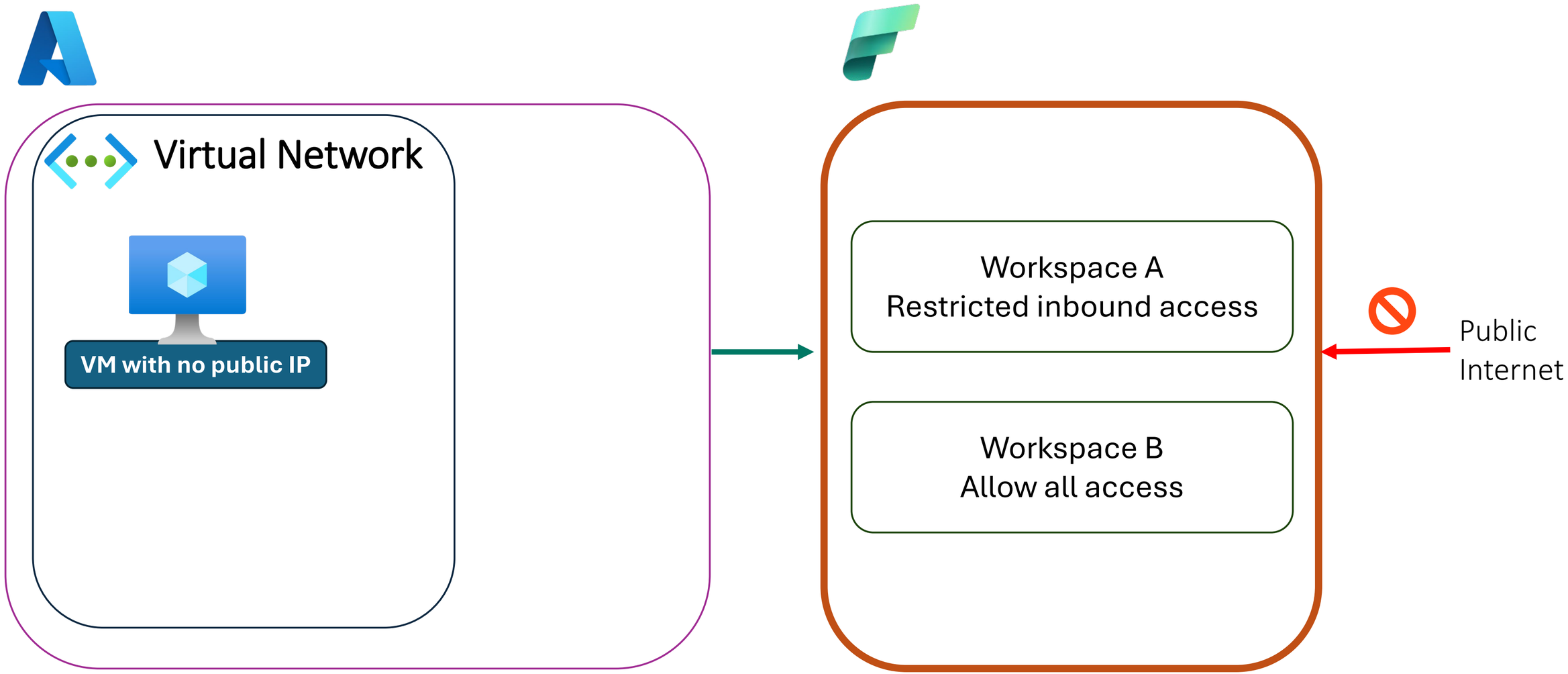
Inbound Security

- Protects internal data from external threats
- Tenant and workspace levels
- Secure access to Fabric items from trusted networks
- Blocks unauthorized inbound traffic

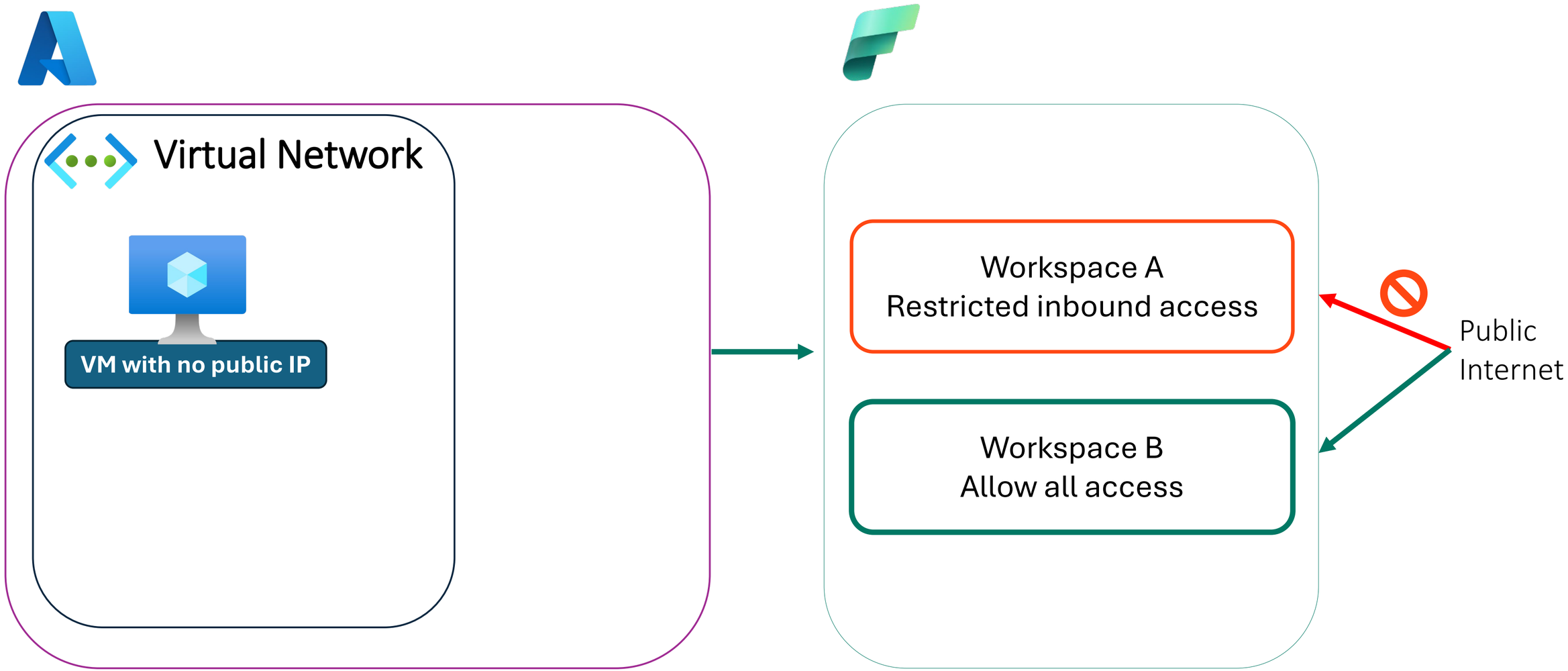
Big Picture


Virtual Network
VM with no public IP
Workspace A
Restricted inbound access
Workspace B
Allow all access
Public
Internet

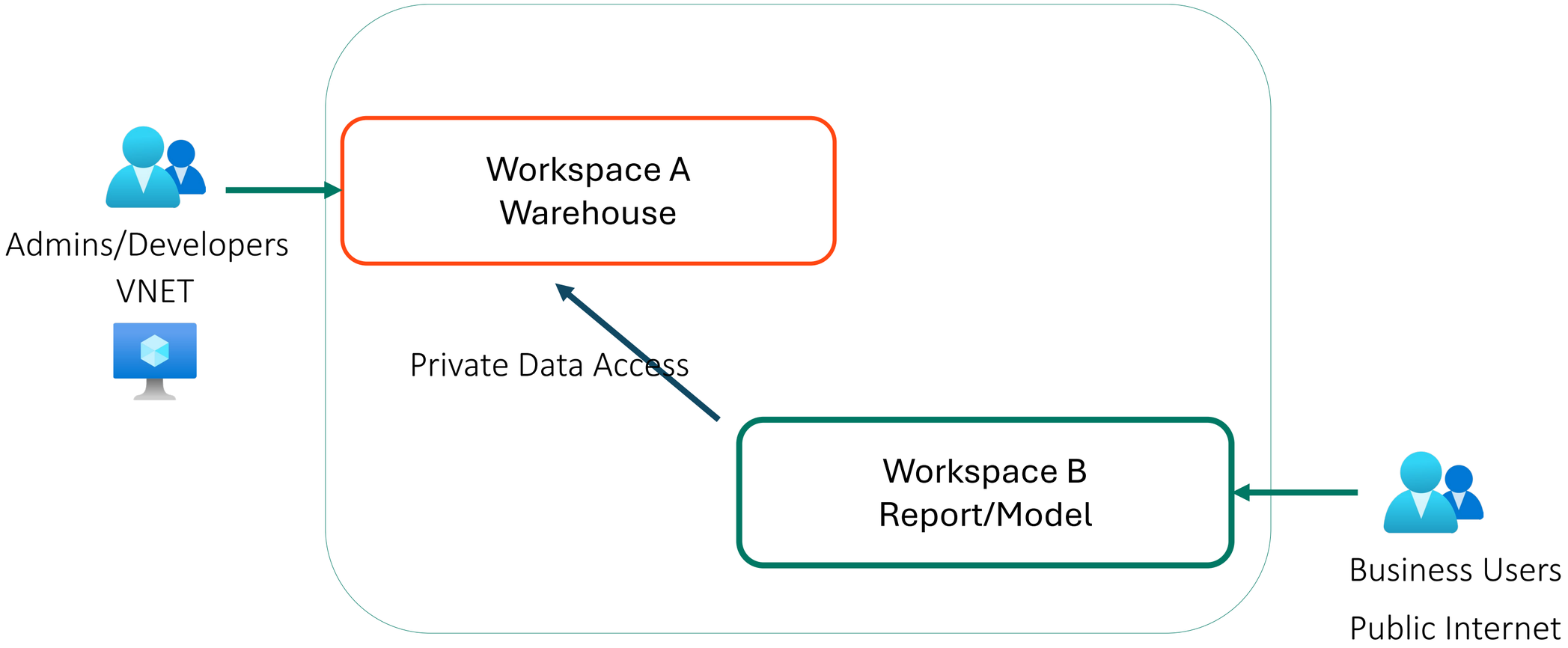
Tenant Level Control



Workspace Level Control



Workspace Level Pattern

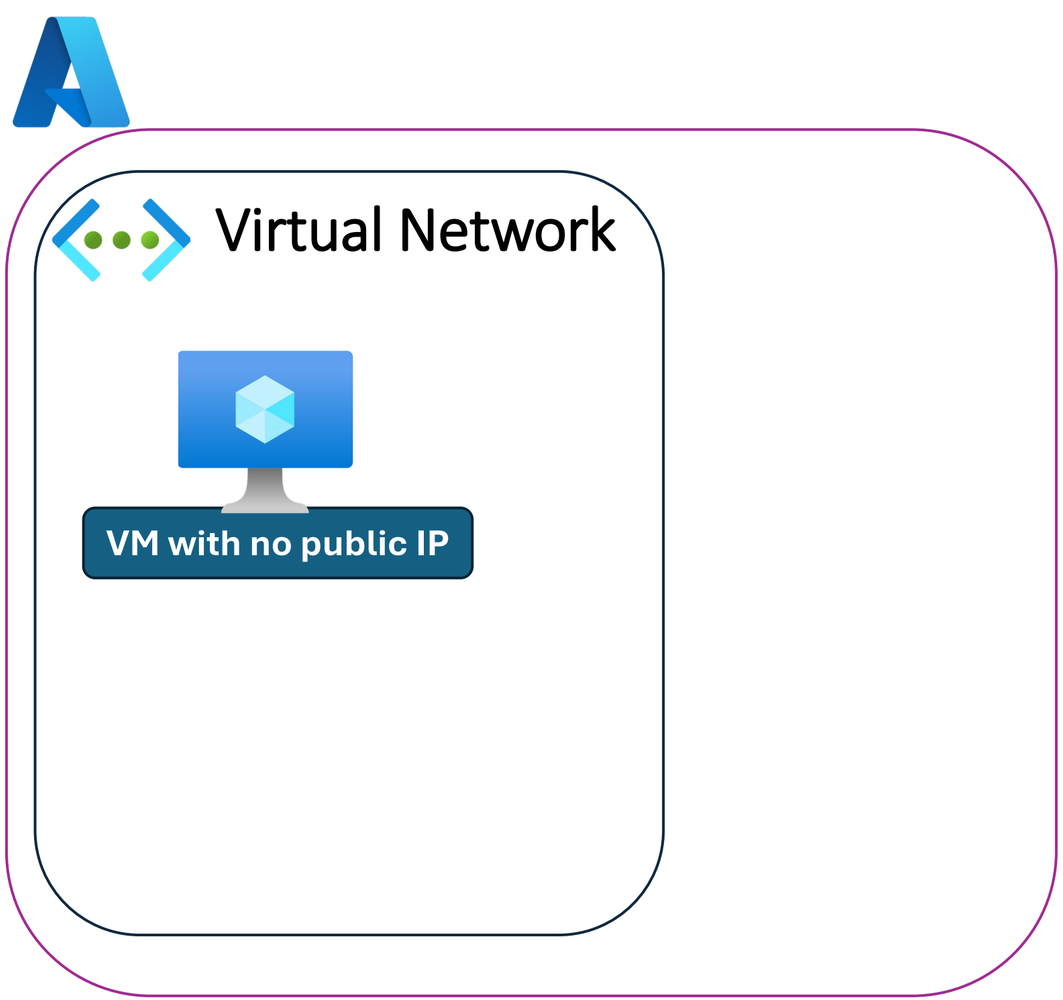


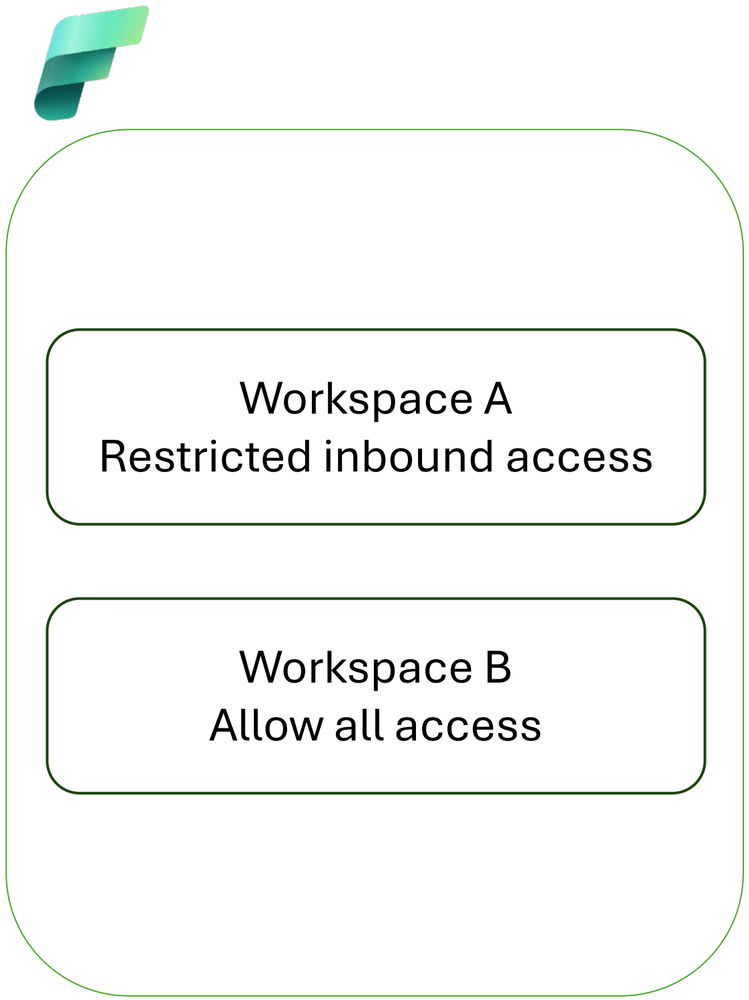
Workspace level wins over Tenant level

Tenant Public Access	Workspace Public Access	Private Link in Effect
Allowed	Blocked	Workspace
Blocked	Allowed	Tenant
Blocked	Blocked	Workspace

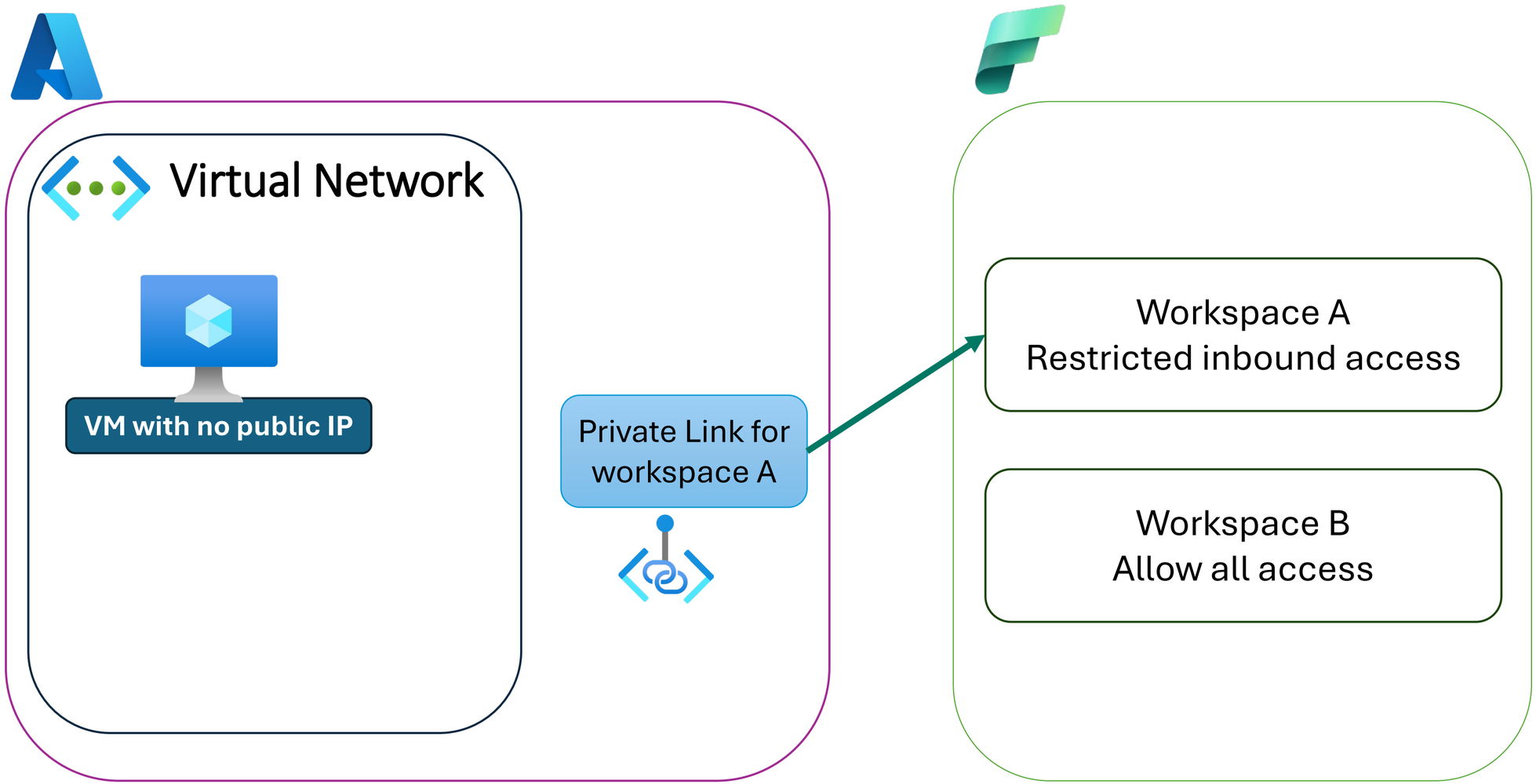
Use tenant and workspace private links - Microsoft Fabric | Microsoft Learn

Workspace Level Control

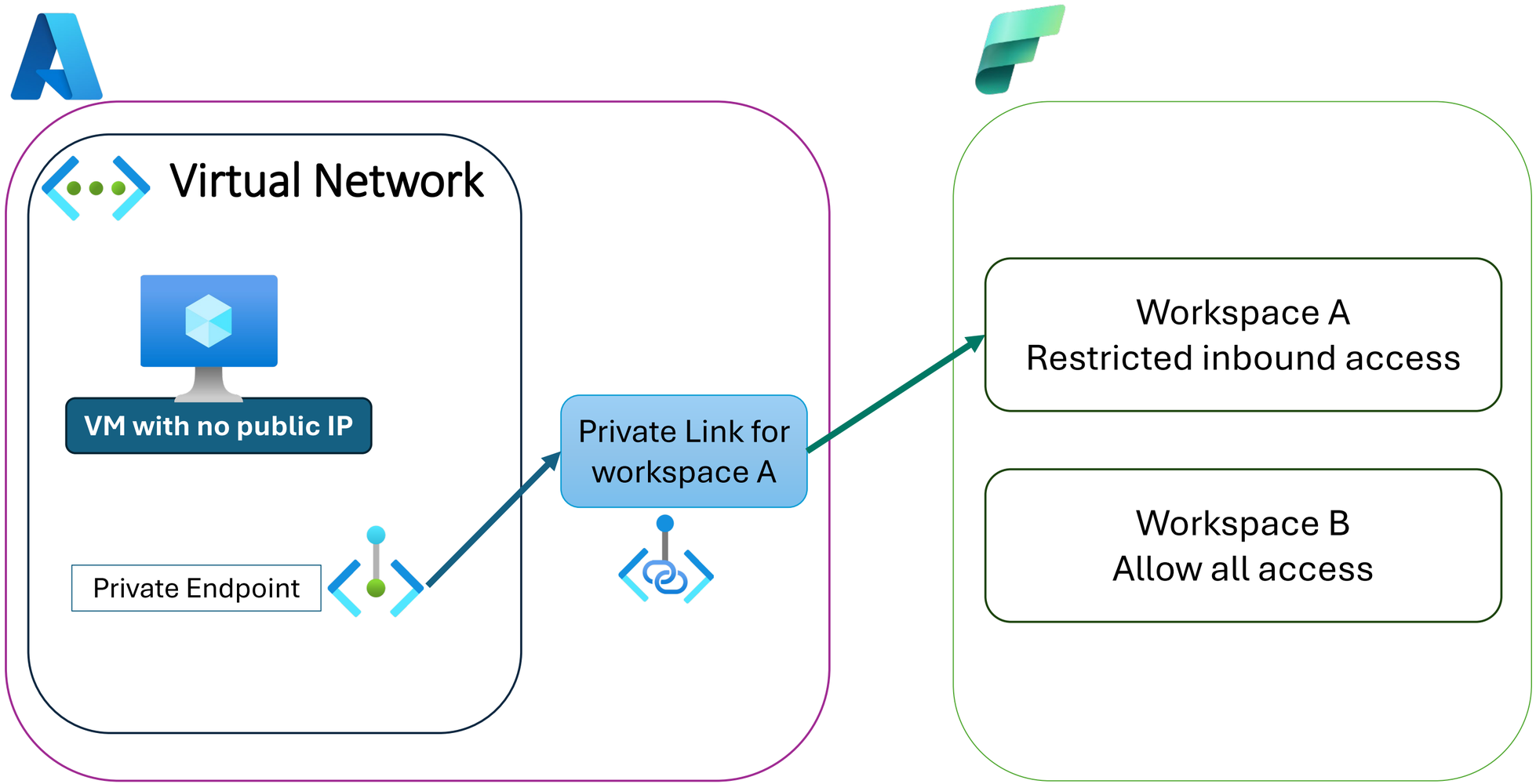




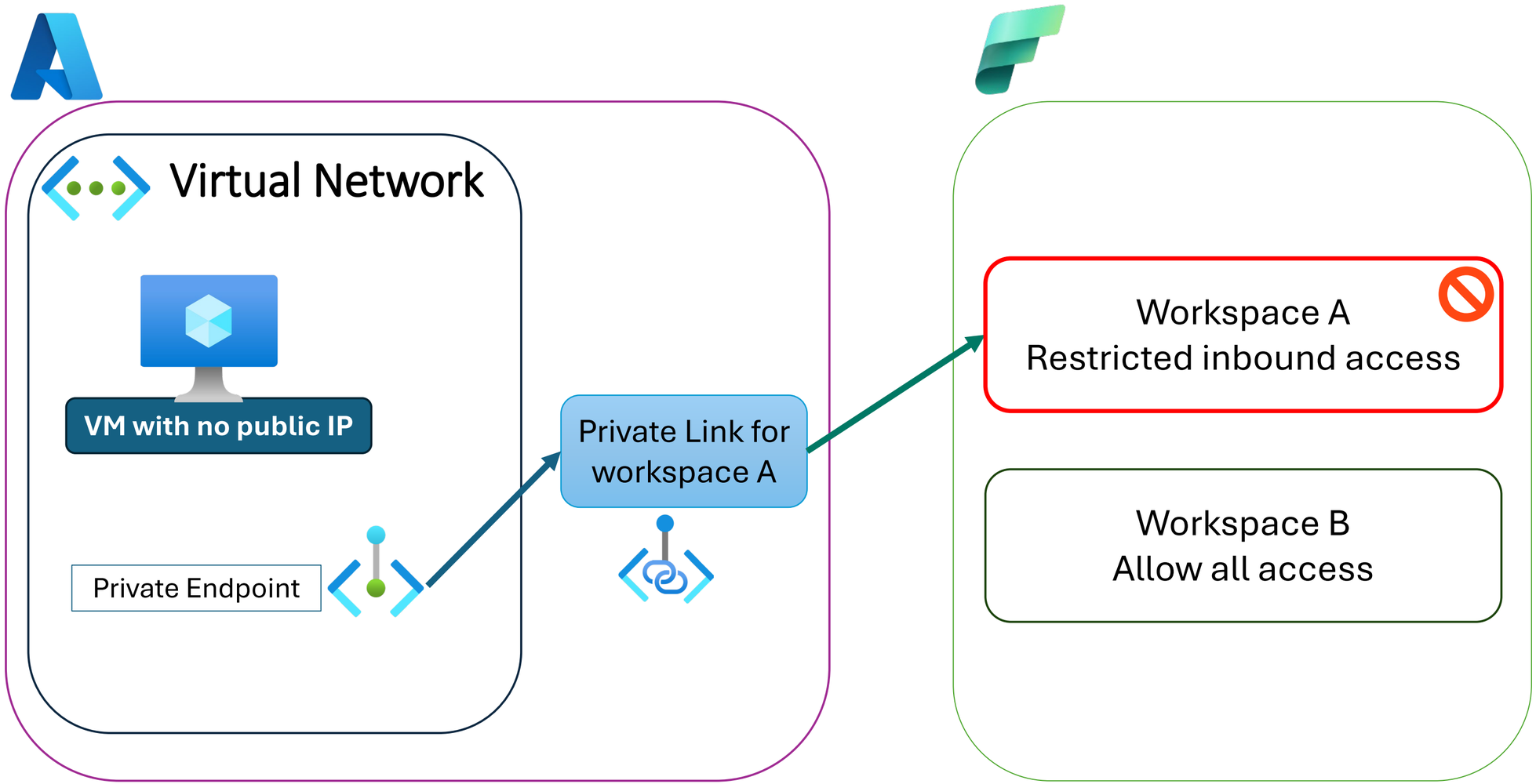
Workspace Level Control



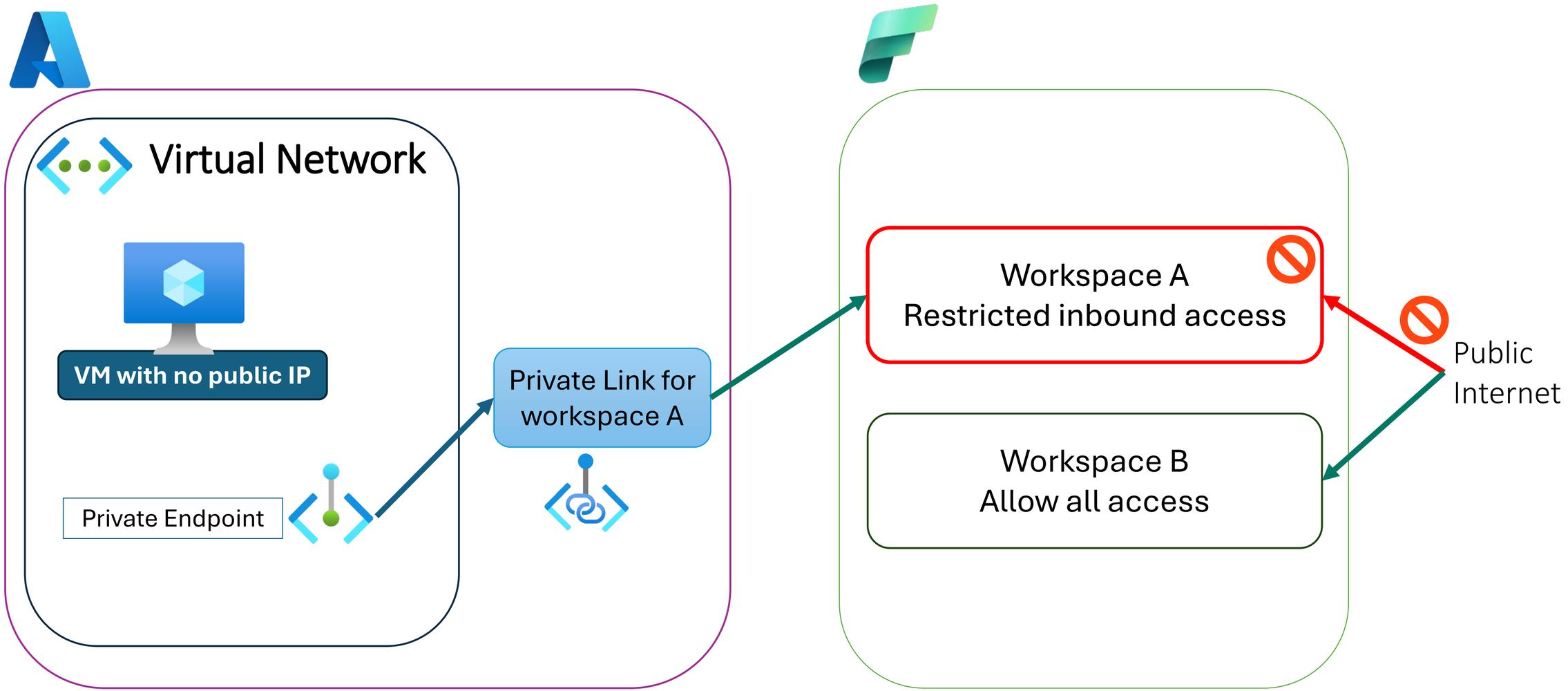
Workspace Level Control



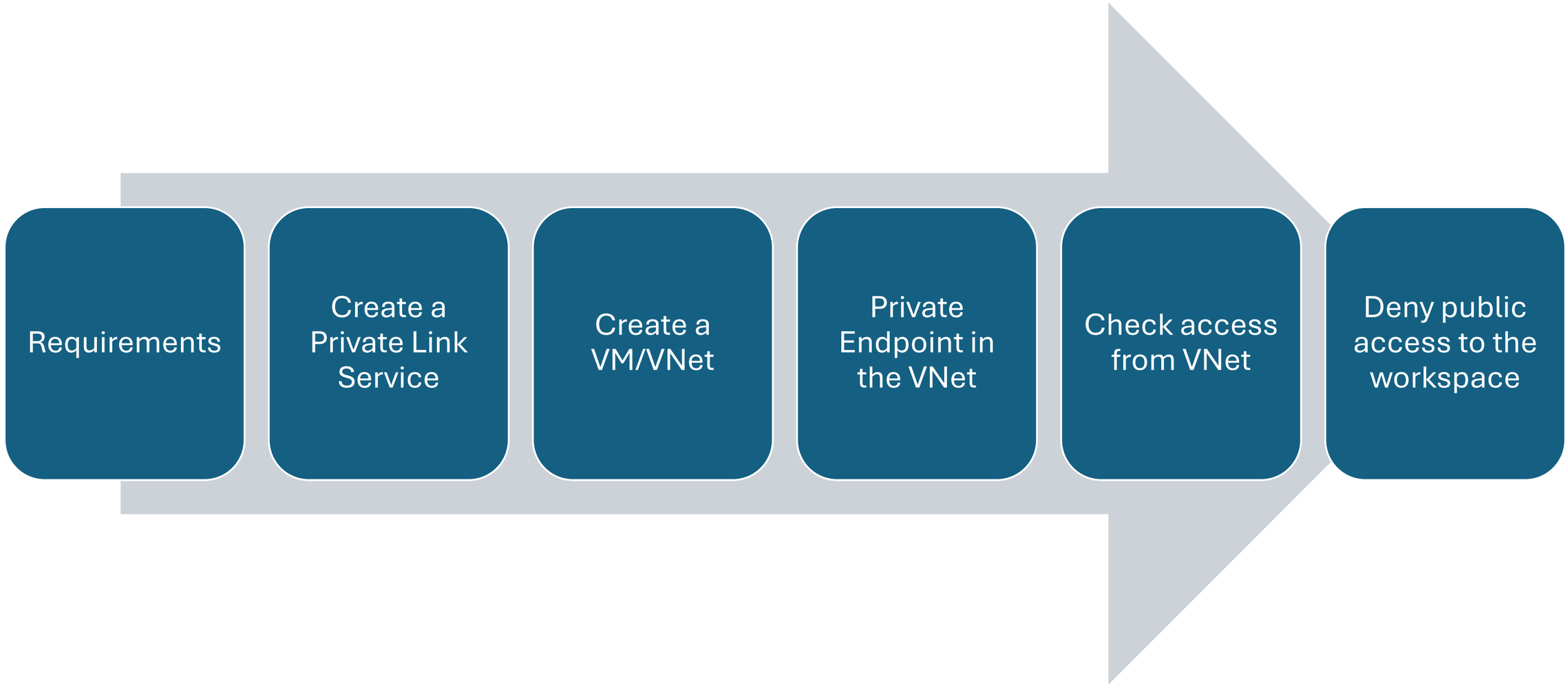
Workspace Level Control



Workspace Level Control



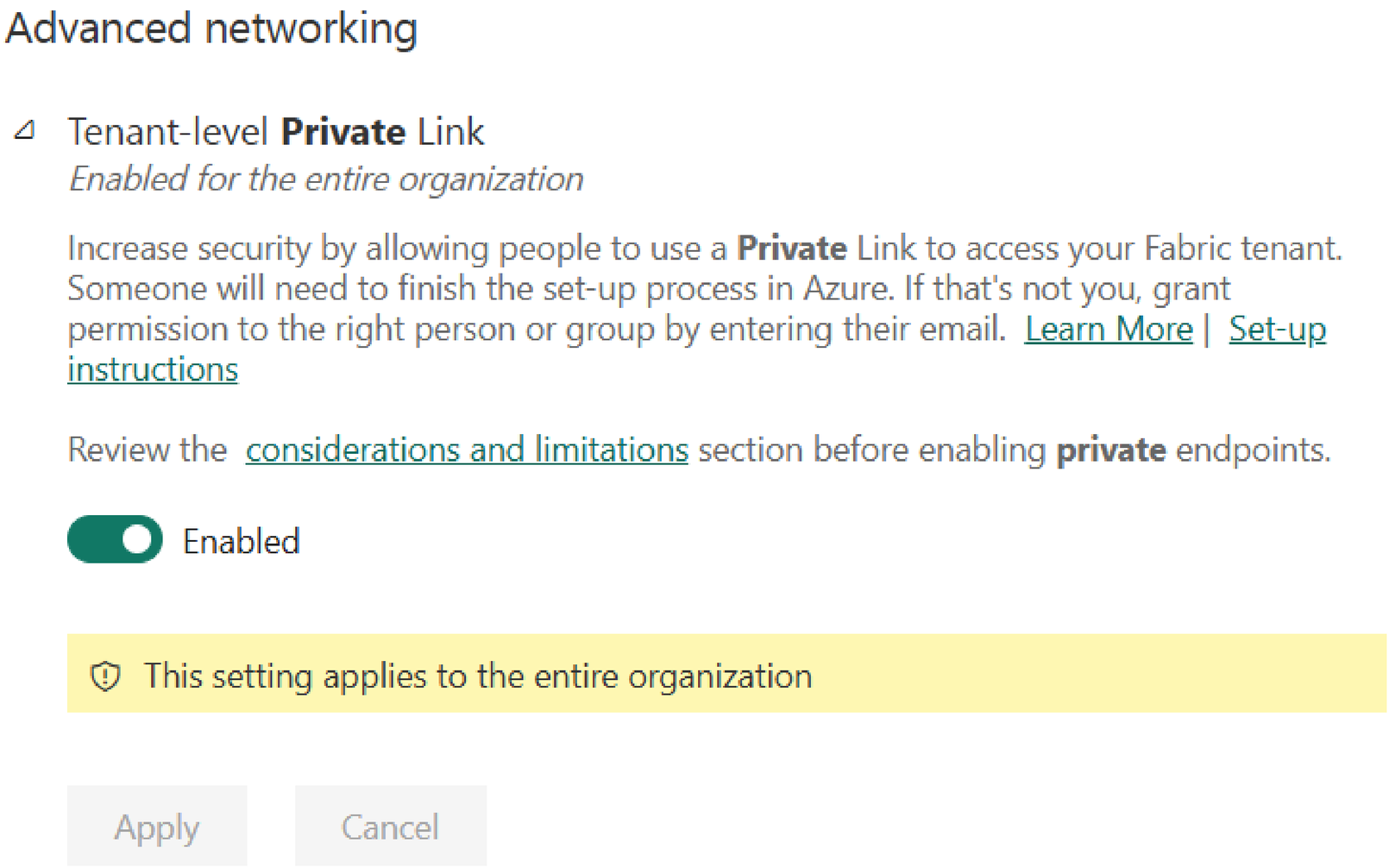
Steps to Limit Inbound Connectivity



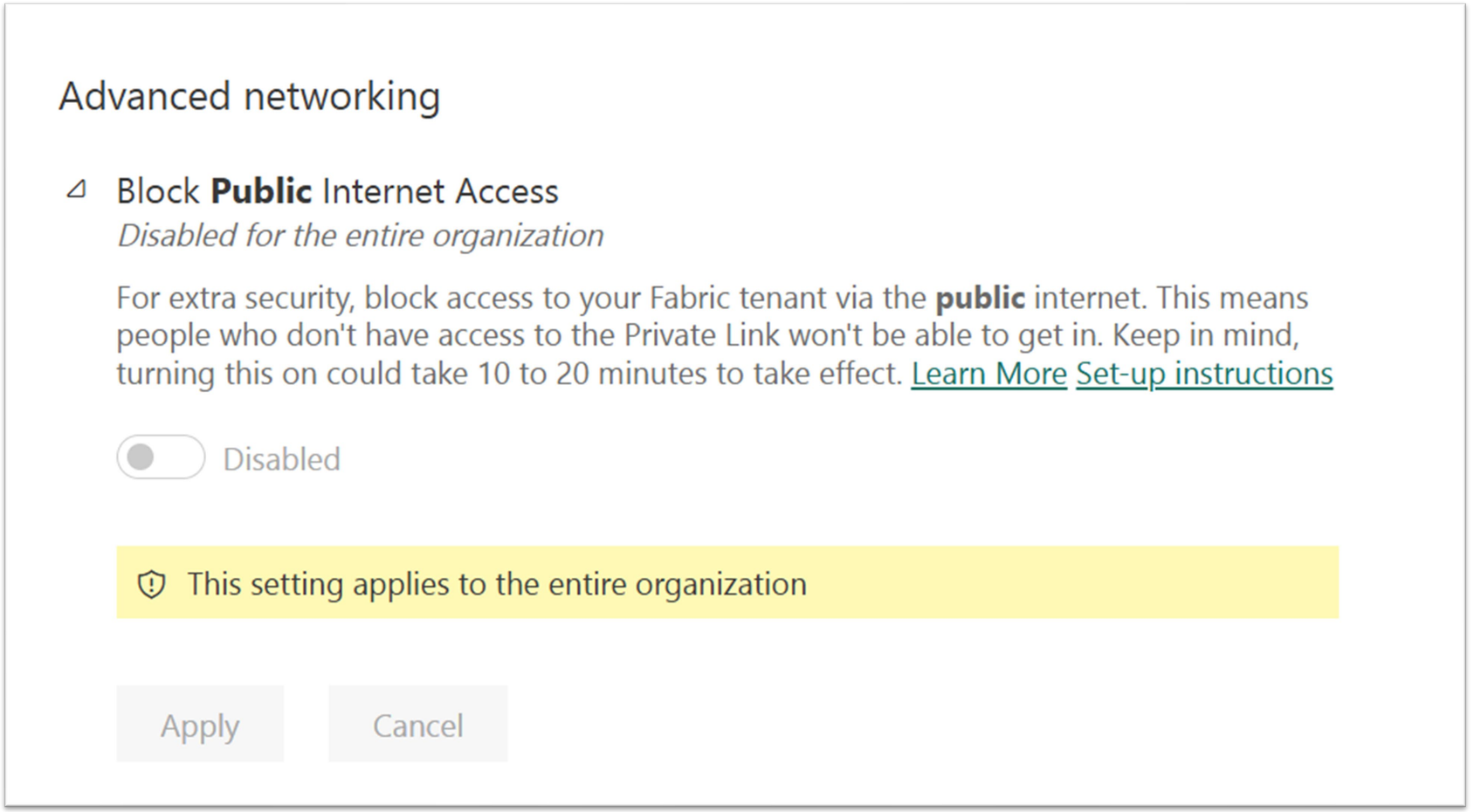
Before you get started

- Make sure you have enough permissions!
- Make sure you have an Azure (tenant or lower) admin ready to work with you!

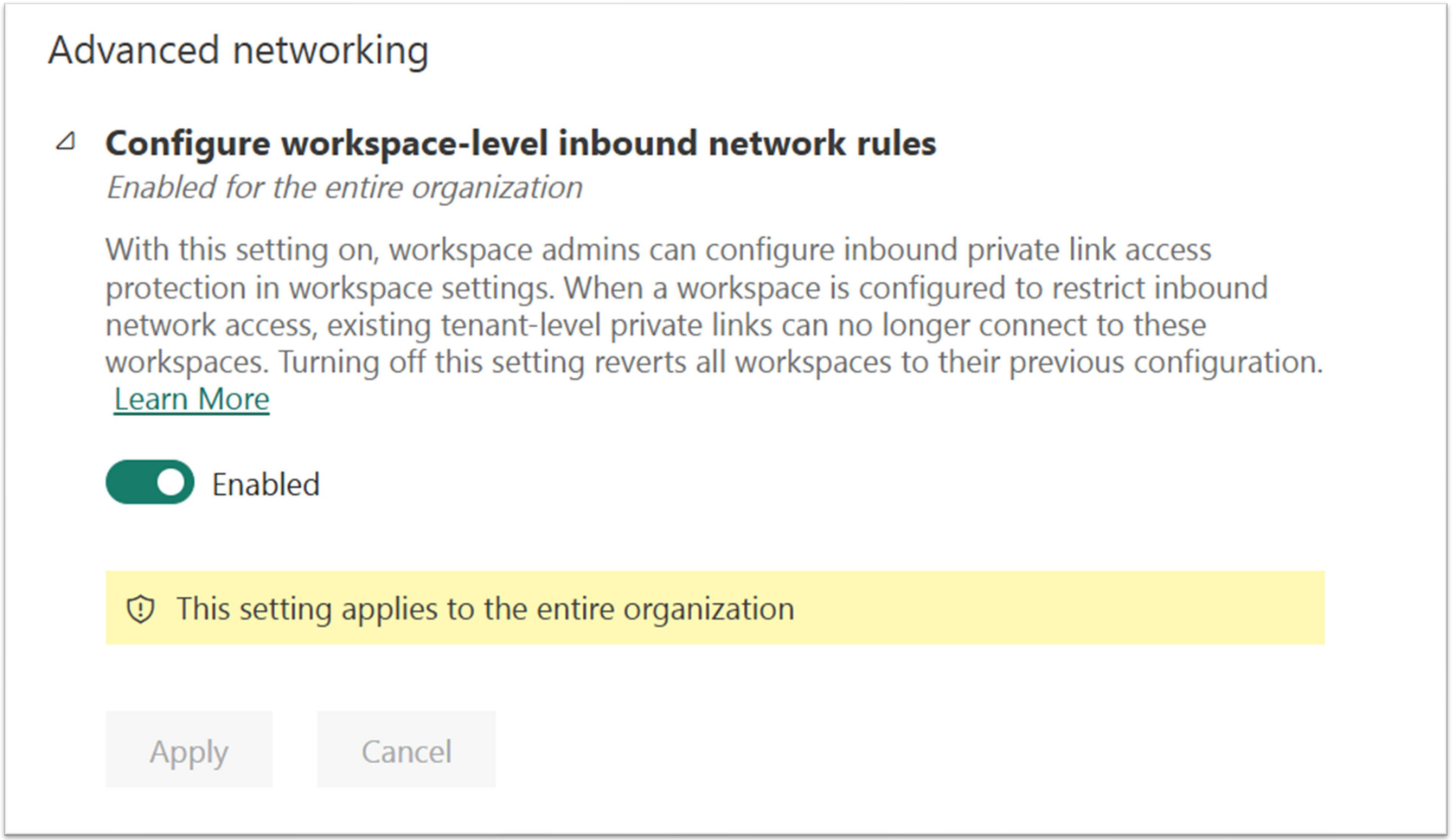
Tenant-level Private Link



Block Public Internet Access to tenant



Workspace-level Private Links



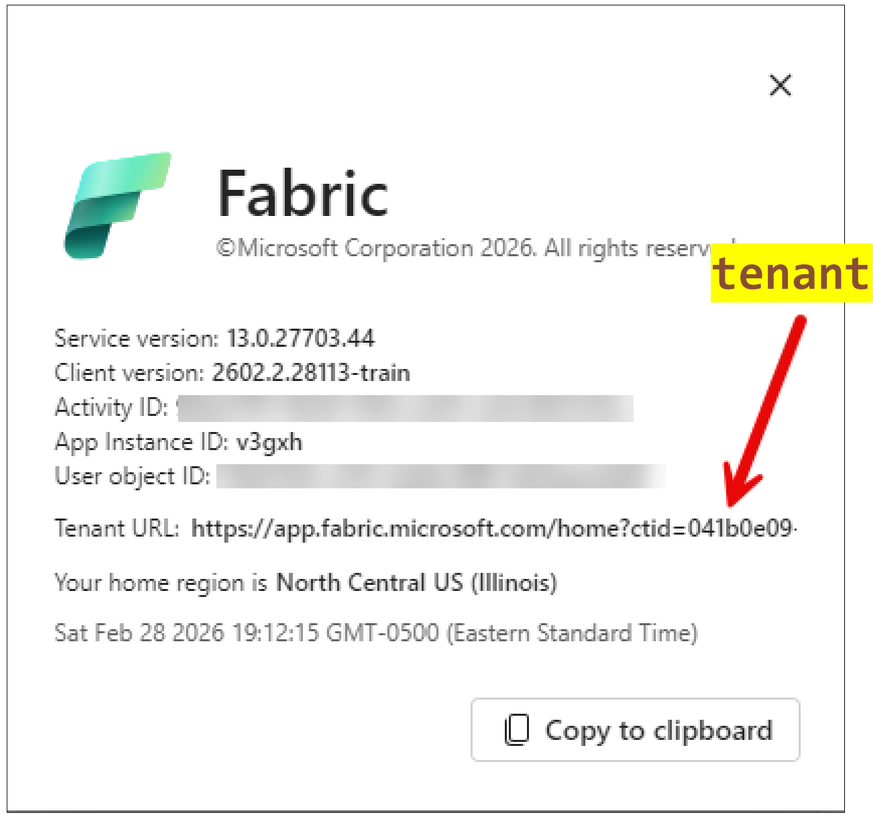
Private Link JSON

```
{
      "$schema": "http://schema.management.azure.com/schemas/2015-01-01/deploymentTemplate.json#",
      "contentVersion": "1.0.0.0",
      "parameters": {},
      "resources": [
        {
          "type": "Microsoft.Fabric/privateLinkServicesForFabric",
          "apiVersion": "2024-06-01",
          "name": "<resource-name>",
          "location": "global",
          "properties": {
            "tenantId": "<tenant-id>",
            "workspaceId": "<workspace-id>"
          }
        }
      ]
    }
```

Private Link JSON

```
{
      "$schema": "http://schema.management.azure.com/schemas/2015-01-01/deploymentTemplate.json#",
      "contentVersion": "1.0.0.0",
      "parameters": {},
      "resources": [
        {
          "type": "Microsoft.Fabric/privateLinkServicesForFabric",
          "apiVersion": "2024-06-01",
          "name": “TheSeventhLink",
          "location": "global",
          "properties": {
            "tenantId": “039487-98233-…",
            "workspaceId": “4783adv-…"
          }
        }
      ]
    }
```

Private Link JSON



workspace-id

Tenant Level Private Link

```
{
  "$schema": "http://schema.management.azure.com/schemas/2015-01-01/deploymentTemplate.json#",
  "contentVersion": "1.0.0.0",
  "parameters": {},
  "resources": [
    {
      "type":"Microsoft.PowerBI/privateLinkServicesForPowerBI",
      "apiVersion": "2020-06-01",
      "name" : "<resource-name>",
      "location": "global",
      "properties" :
      {
          "tenantId": "<tenant-object-id>"
      }
    }
  ]
}
```

Private Endpoint

- **Private IP Address**
  Connects services to your virtual network using a private IP.

- **Brings Services into Your VNet**
  Treats external services as part of your internal network.

Create a private endpoint ...

✓ Basics | 2 Resource | 3 Virtual Network | 4 DNS | 5 Tags | 6 Review + create

Private Link offers options to create private endpoints for different Azure resources, like your private link service, a SQL server, or an Azure storage account. Select which resource you would like to connect to using this private endpoint. Learn more

Connection method
- (●) Connect to an Azure resource in my directory.
- ( ) Connect to an Azure resource by resource ID or alias.

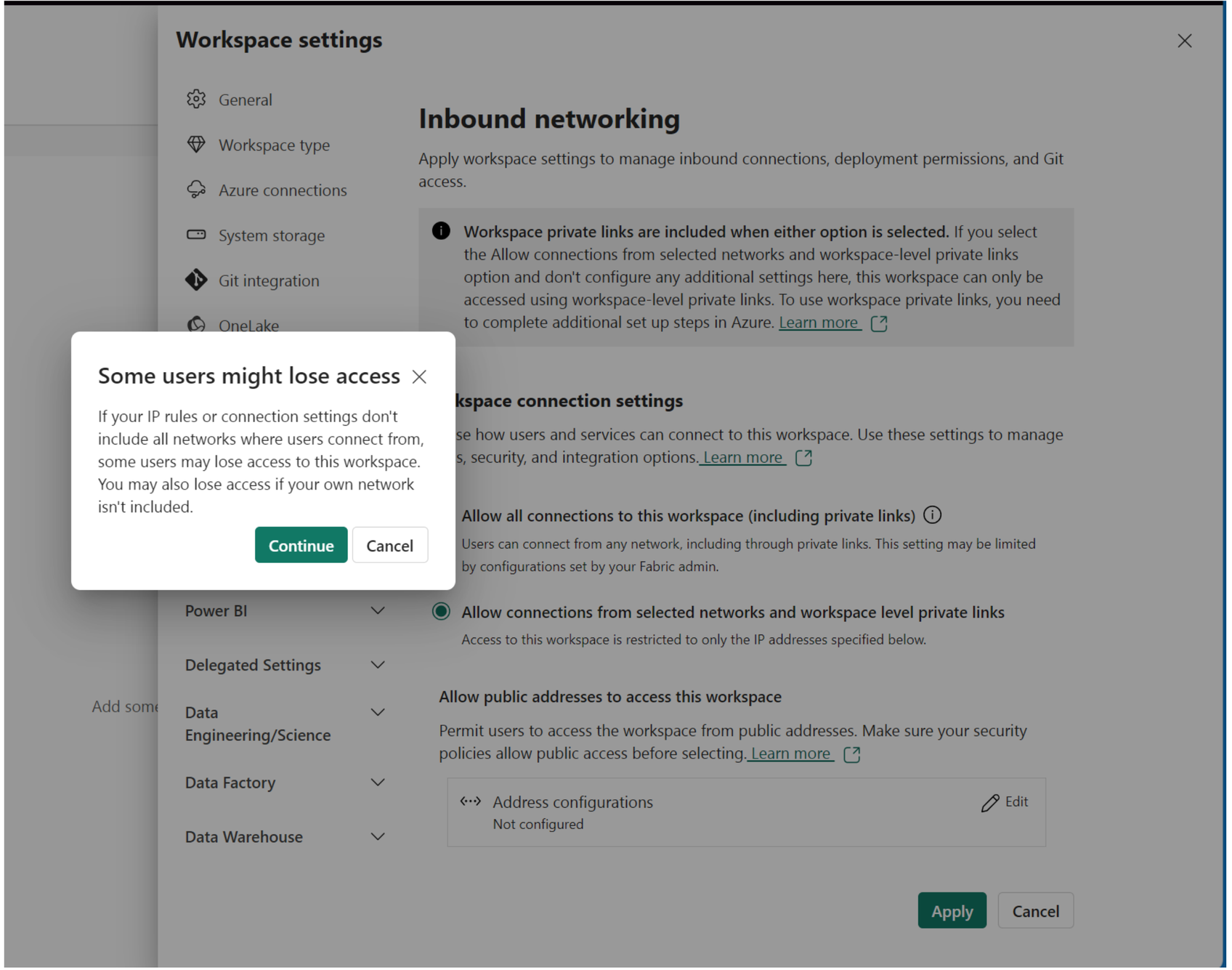
Subscription * : Main One

Resource type * : Microsoft.Fabric/privateLinkServicesForFabric

Resource * : TheSeventhLink

Target sub-resource * : workspace

Disabling Public Access from Workspace



Disabling Public Access with Code

```powershell
$url = "https://api.fabric.microsoft.com/v1/workspaces/$($workspaceID)/networking/communicationPolicy"

# Full policy body (must include both inbound and outbound)
$body = @{
    inbound = @{
        publicAccessRules = @{
            defaultAction = "Deny"
        }
    }
    outbound = @{
        publicAccessRules = @{
            defaultAction = "Allow"
        }
    }
} | ConvertTo-Json -Depth 5

# Make PUT request
$response = Invoke-RestMethod -Uri $url -Method Put -Headers @{
    Authorization = "Bearer $($token.accessToken)"
    "Content-Type" = "application/json"
} -Body $body
```

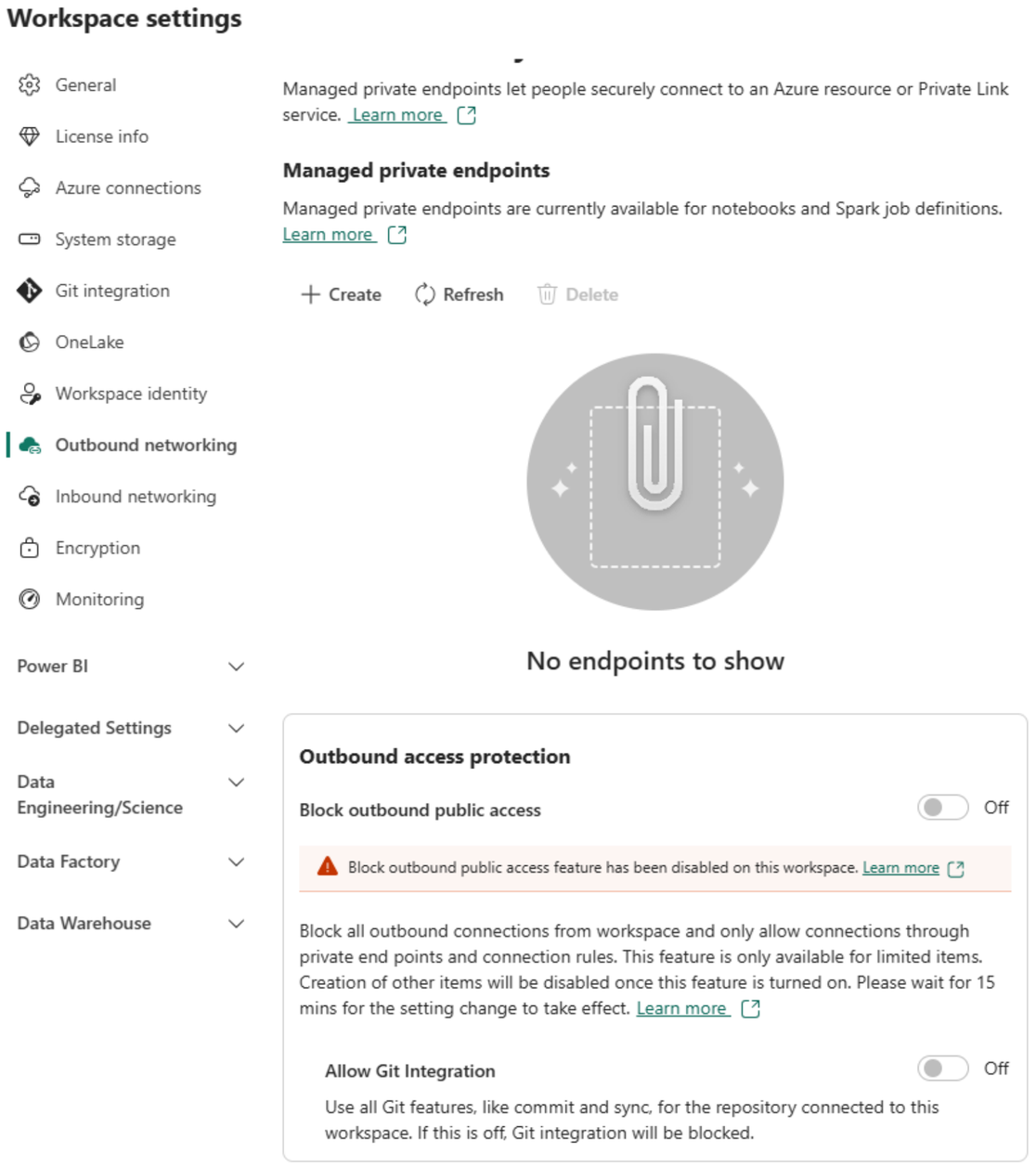
Supported Item Types

- Lakehouse, SQL Endpoint, Shortcut
- Notebook
- Pipeline, Copy Job, Dataflows Gen2 (CI/CD)
- **Warehouse**
- Mirrored database
- Eventstream, Eventhouse

Outbound Security

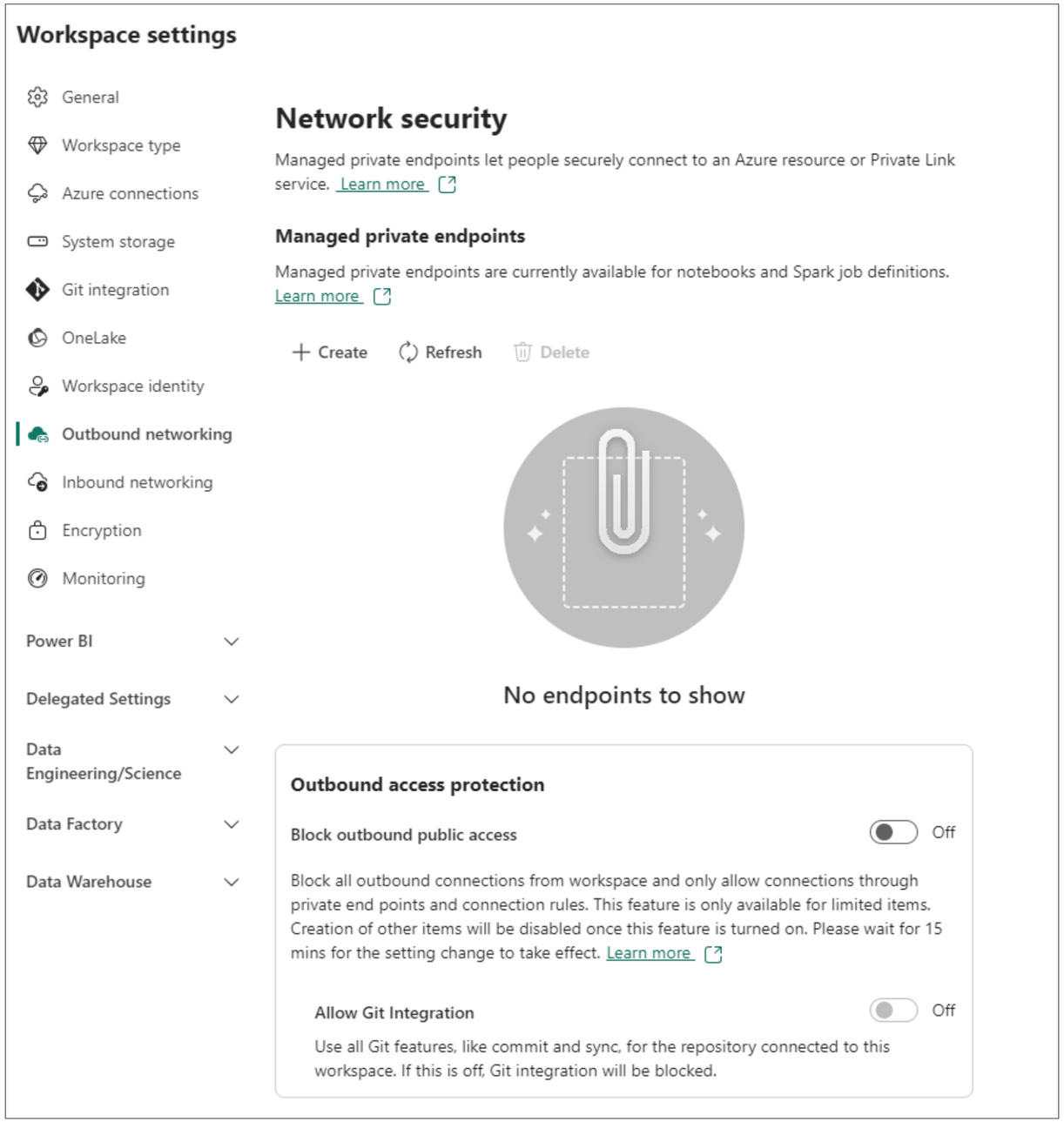
- Enforces **workspace outbound access protection**
- Routes outbound traffic through managed private endpoints to a virtual network.
- Prevents unsecured connections from public IPs
- Enables protection per workspace

Outbound Access Protection



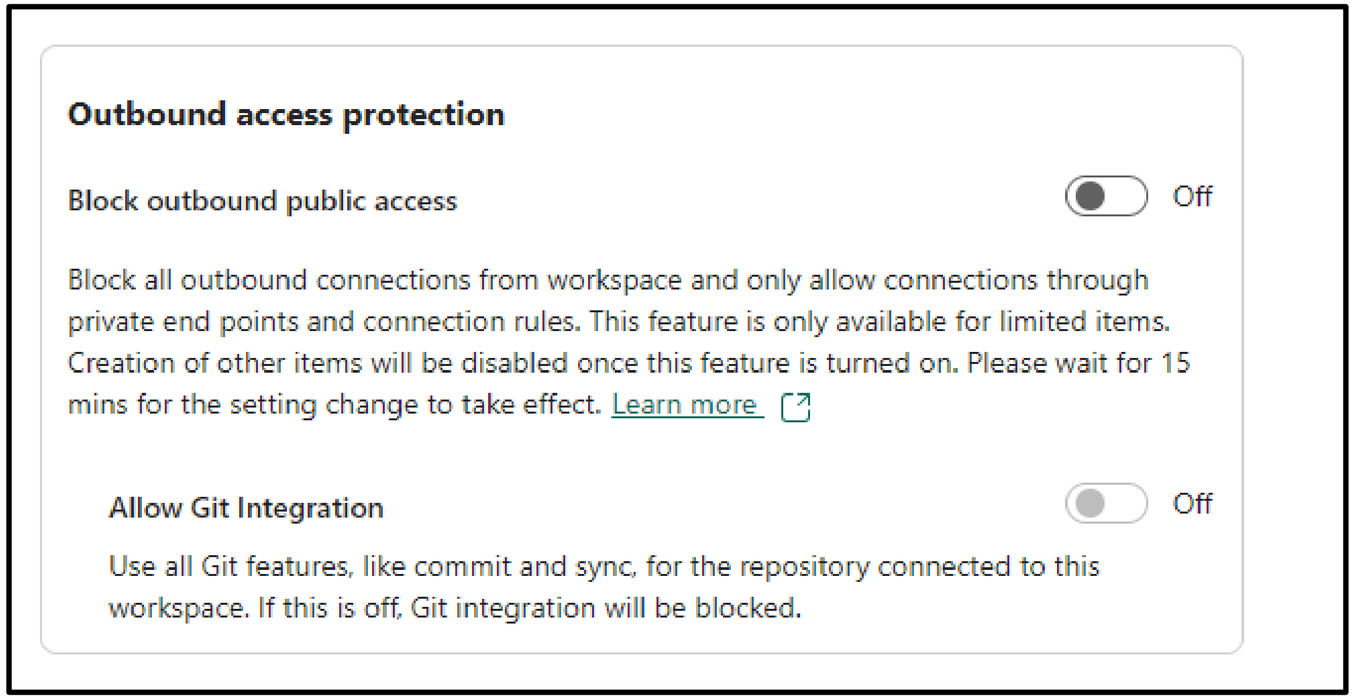
https://learn.microsoft.com/en-us/fabric/security/workspace-outbound-access-protection-overview

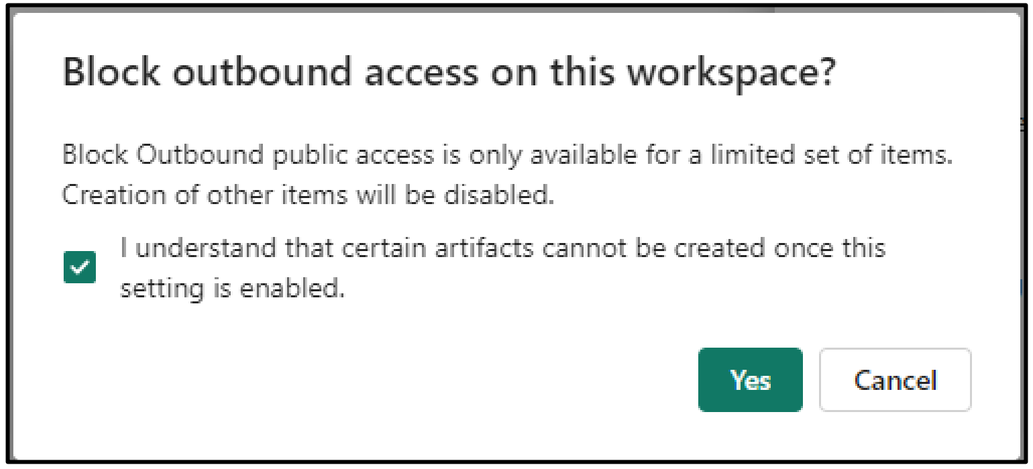
Outbound Access Protection



https://learn.microsoft.com/en-us/fabric/security/workspace-outbound-access-protection-overview

Outbound Access Protection





Workspace Managed Identity

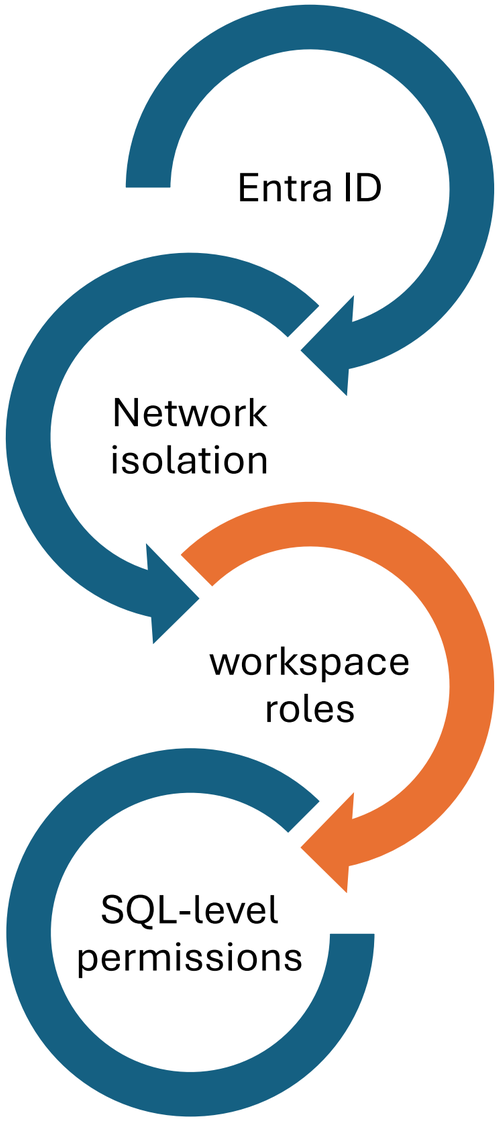
Secure Access to External Data

Enables Copy Into and Shortcuts without using user credentials

Works with ADLS Securely

Supports public, firewall-restricted, and block public access storage

Warehouse Secured with



Workspace Roles

Development Team Collaboration

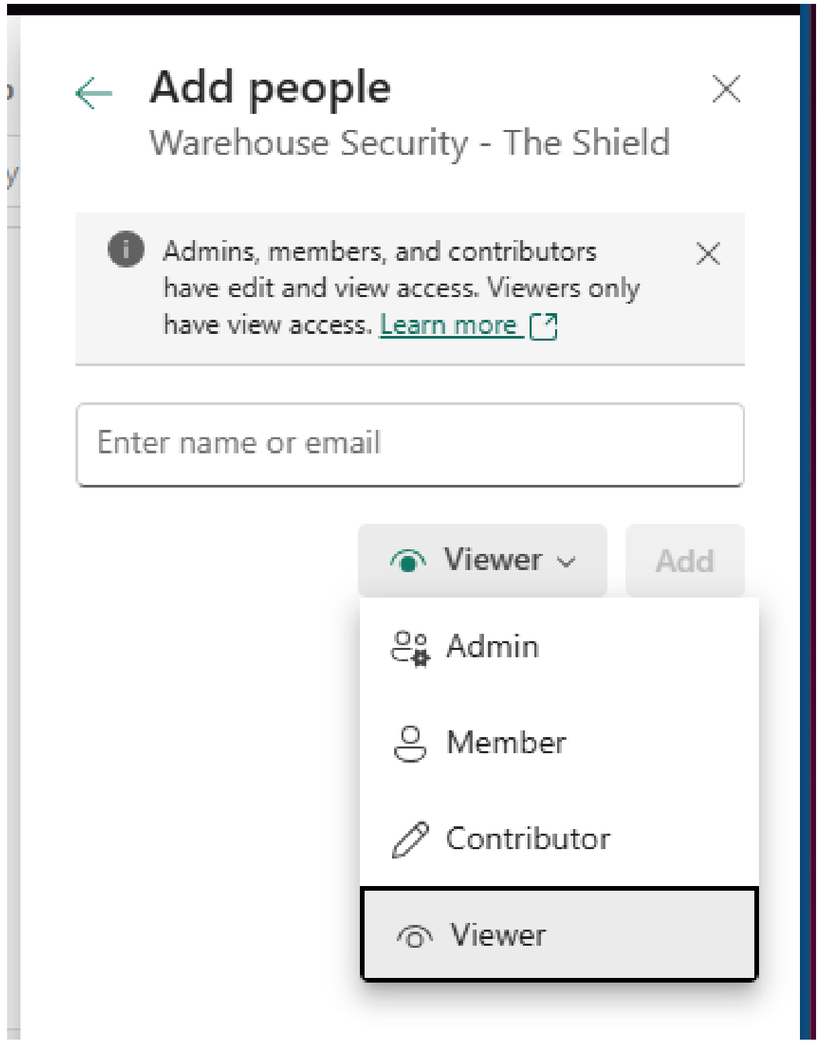
Admin

Member

Contributor

Viewer

Workspace: Manage Access



Workspace Roles

Workspace Roles

Capability	Admin	Member	Contributor	Viewer
Update and delete the workspace.	✅			
Add or remove people, including other admins.	✅			
Add members or others with lower permissions.	✅	✅		
Allow others to reshare items.[1]	✅	✅		
Create or modify warehouse items.	✅	✅	✅	

[1] Reshare allows Contributors and Viewers to share.

https://learn.microsoft.com/en-us/fabric/fundamentals/roles-workspaces

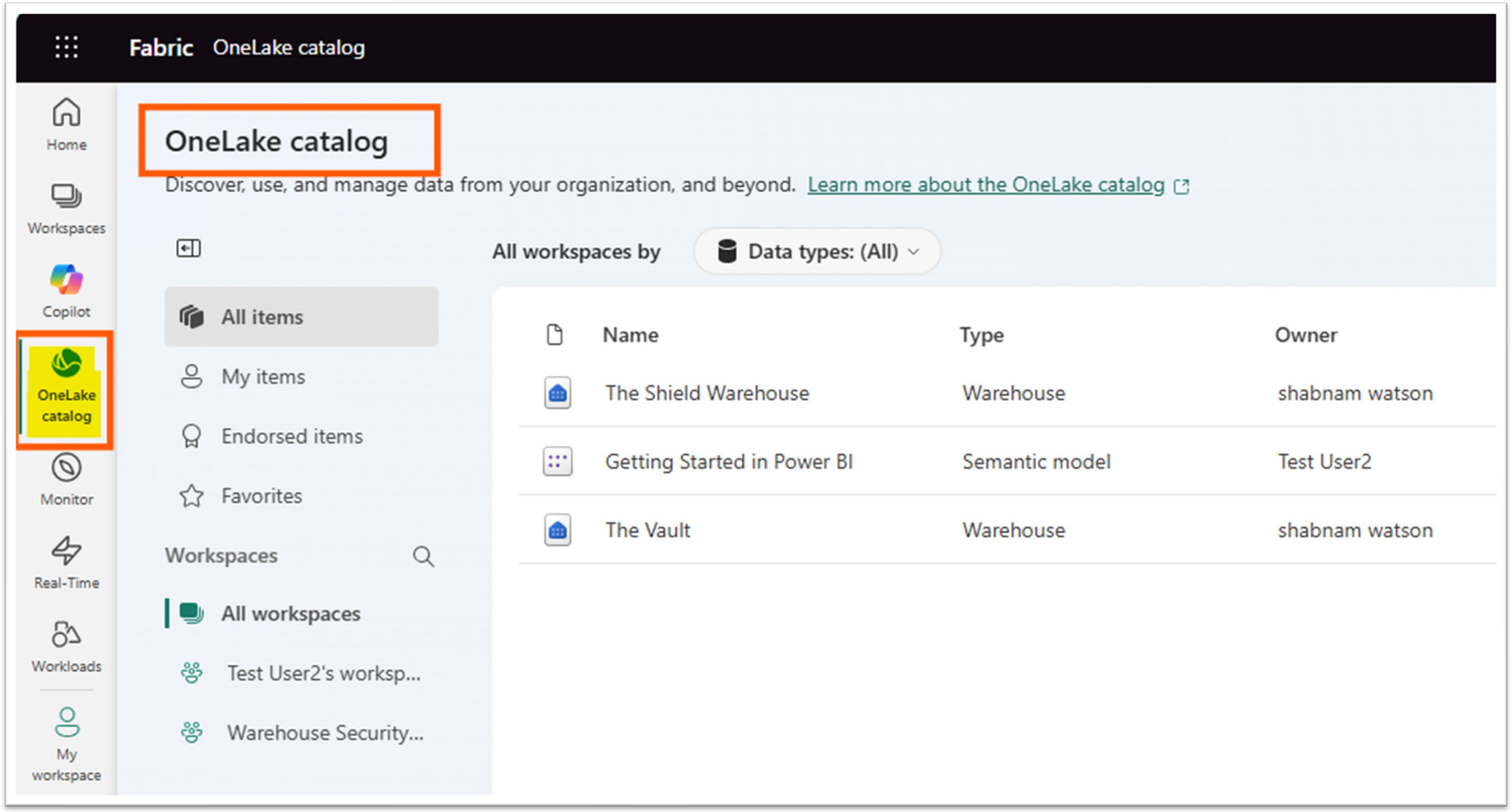
Workspace Roles

Capability	Admin	Member	Contributor	Viewer
Connect to SQL analytics endpoint of Lakehouse or Warehouse	✅	✅	✅	✅
Read data with T-SQL through TDS endpoint (**ReadData**).	✅	✅	✅	✅
Read data through OneLake APIs and Spark (**ReadAll**).	✅	✅	✅	

https://learn.microsoft.com/en-us/fabric/fundamentals/roles-workspaces

Sharing with users outside workspace

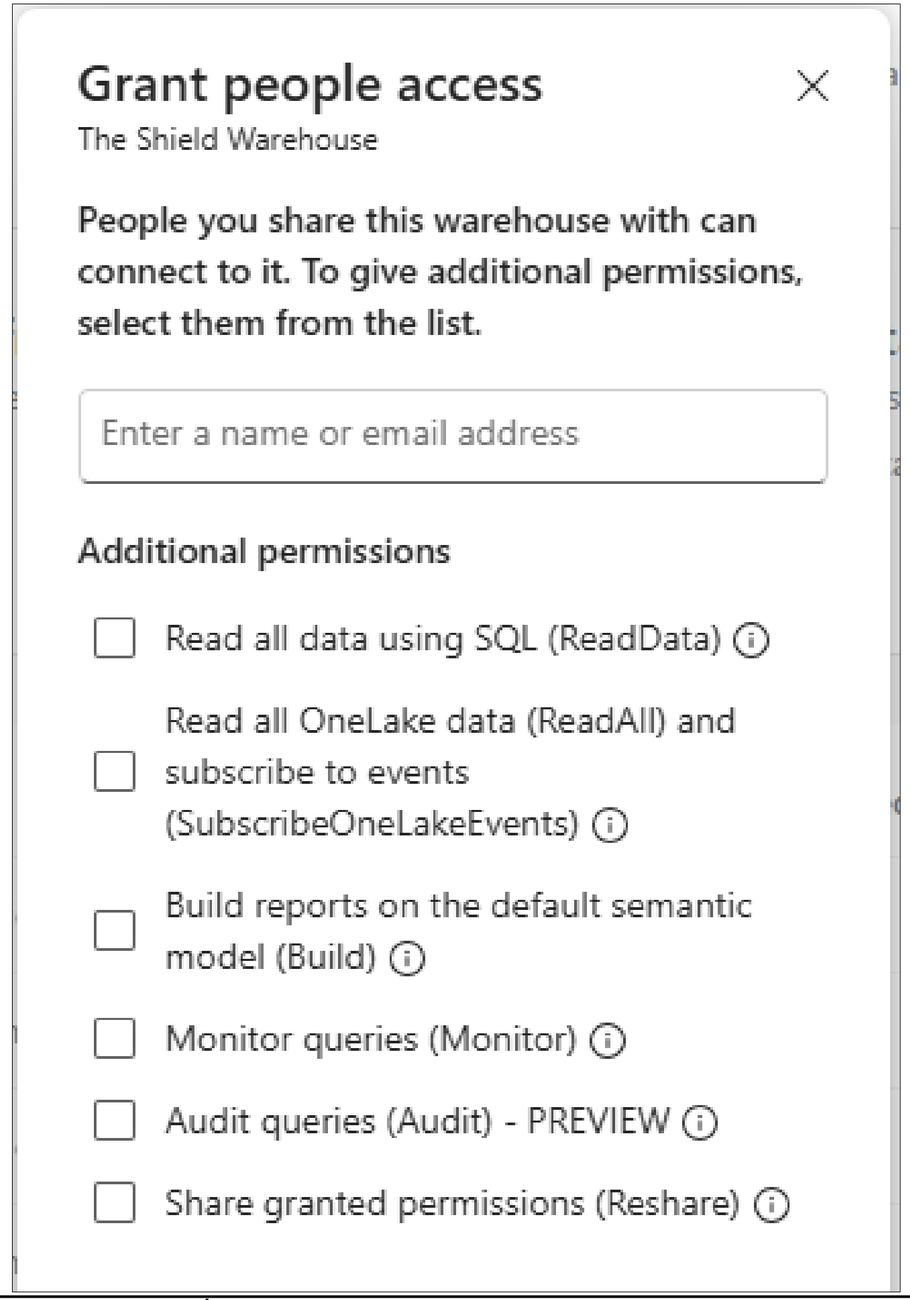
- Use case:
  - Not immediate development team
  - SQL Analysts
  - Report Developers
  - QA testers



https://learn.microsoft.com/en-us/fabric/fundamentals/roles-workspaces

Warehouse Item level Permissions

Connect
ReadData (SQL)
ReadAll (Files)
Monitor
Audit
Reshare

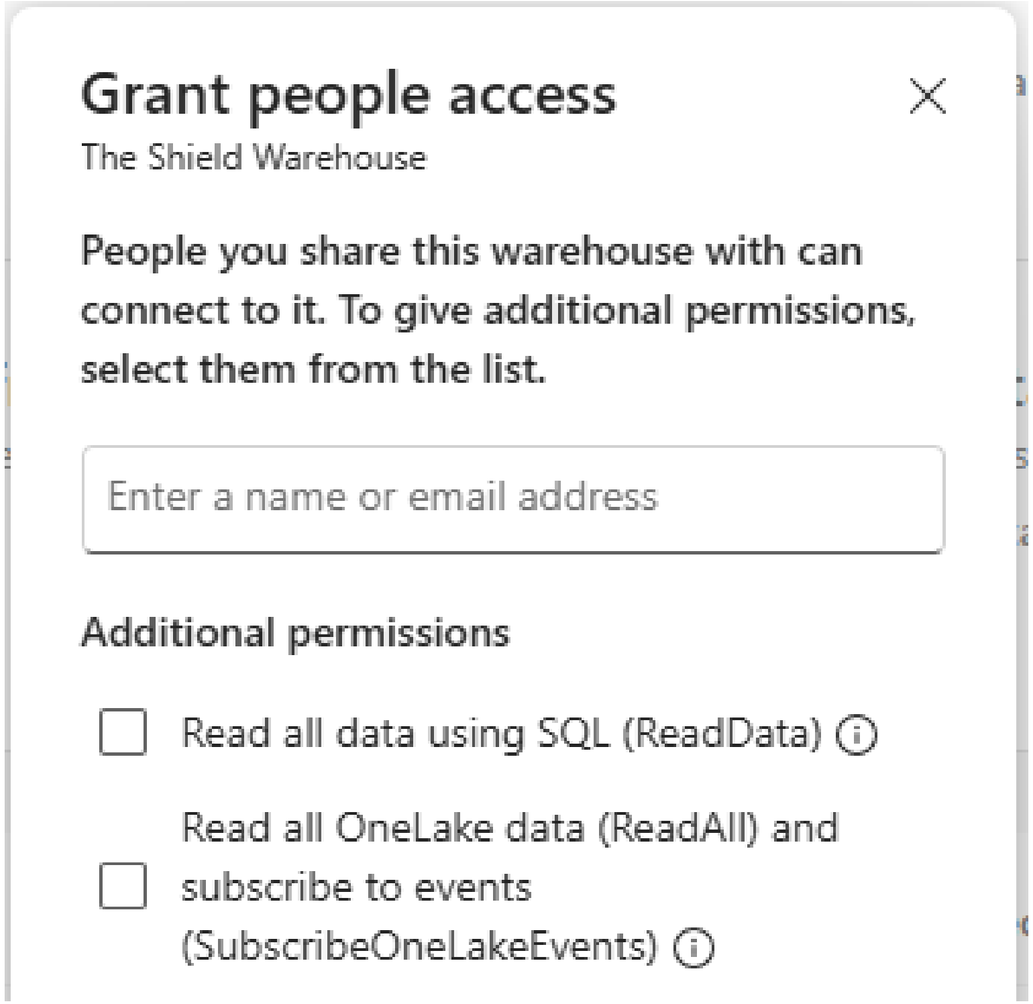


SQL Endpoint Item level Permissions

Connect

ReadData → All SQL data

ReadAll → All OneLake

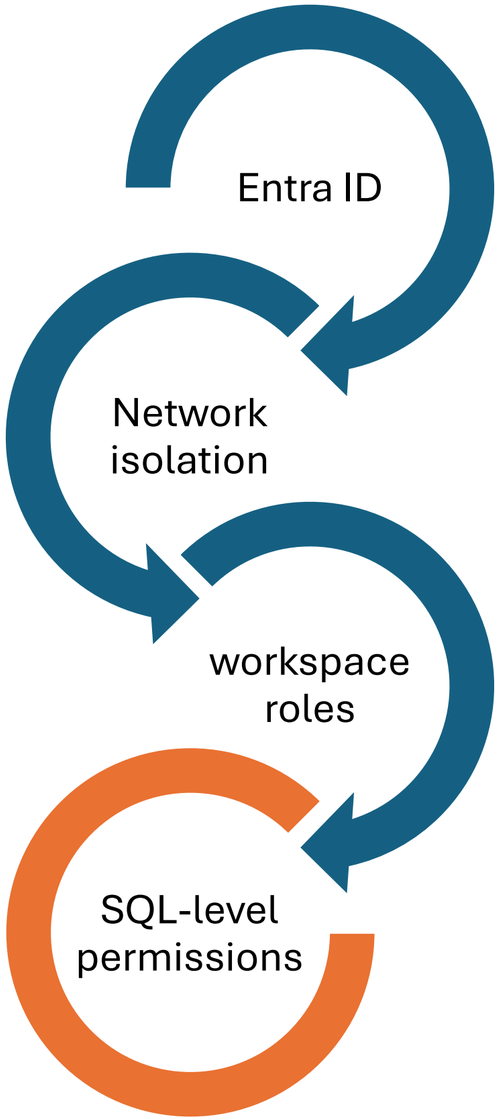


Workspace Roles

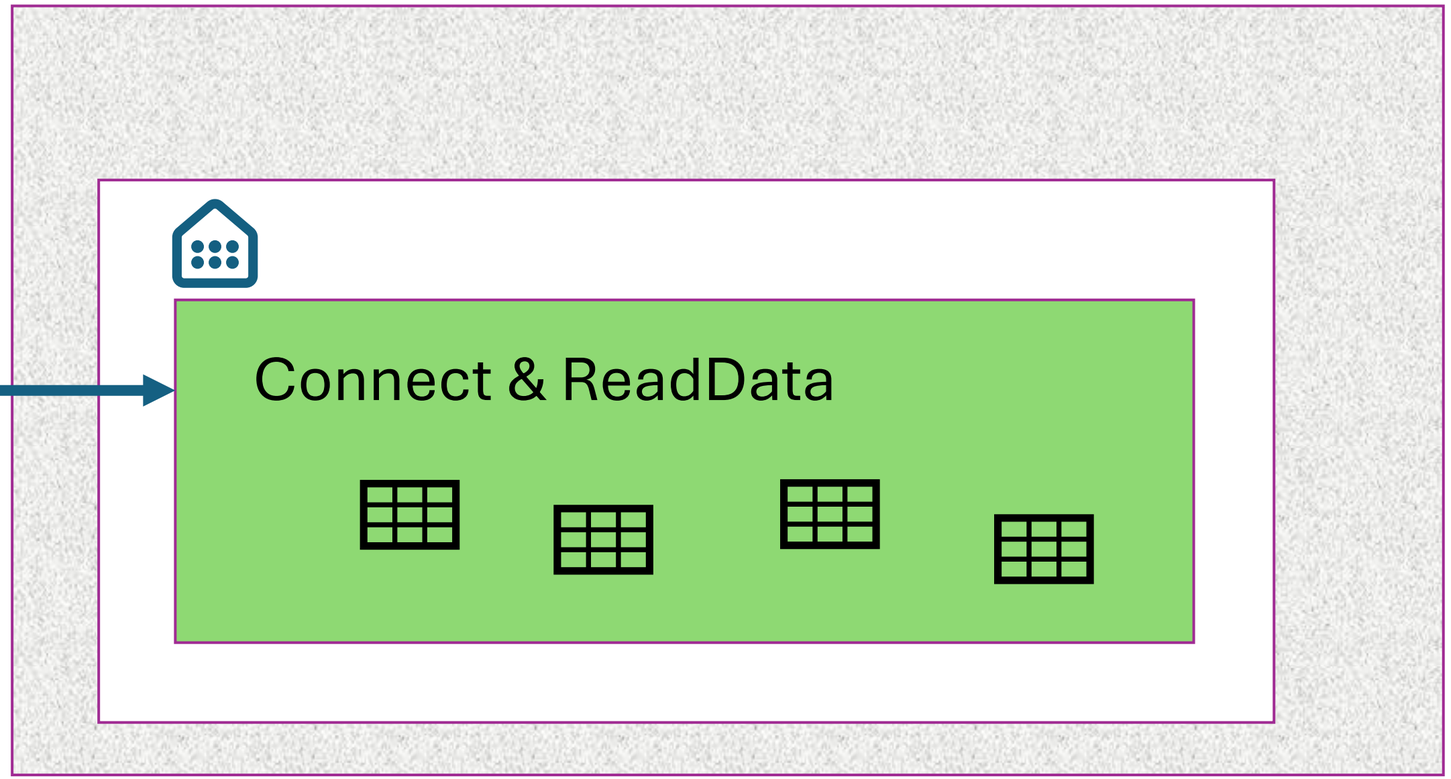
Capability	Admin	Member	Contributor	Viewer
Connect to SQL analytics endpoint of Lakehouse or Warehouse	✅	✅	✅	✅
Read data with T-SQL through TDS endpoint (**ReadData**).	✅	✅	✅	✅
Read data through OneLake APIs and Spark (**ReadAll**).	✅	✅	✅	

https://learn.microsoft.com/en-us/fabric/fundamentals/roles-workspaces

Warehouse Secured with

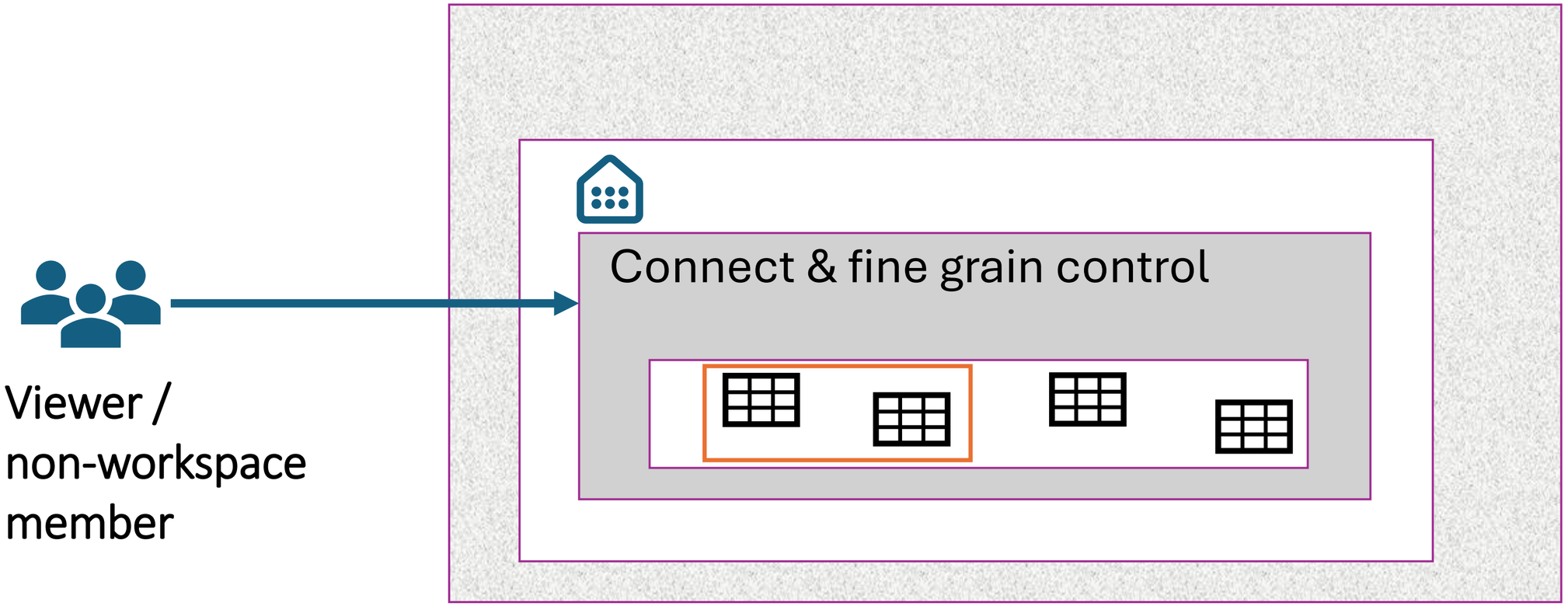


SQL Level Permissions

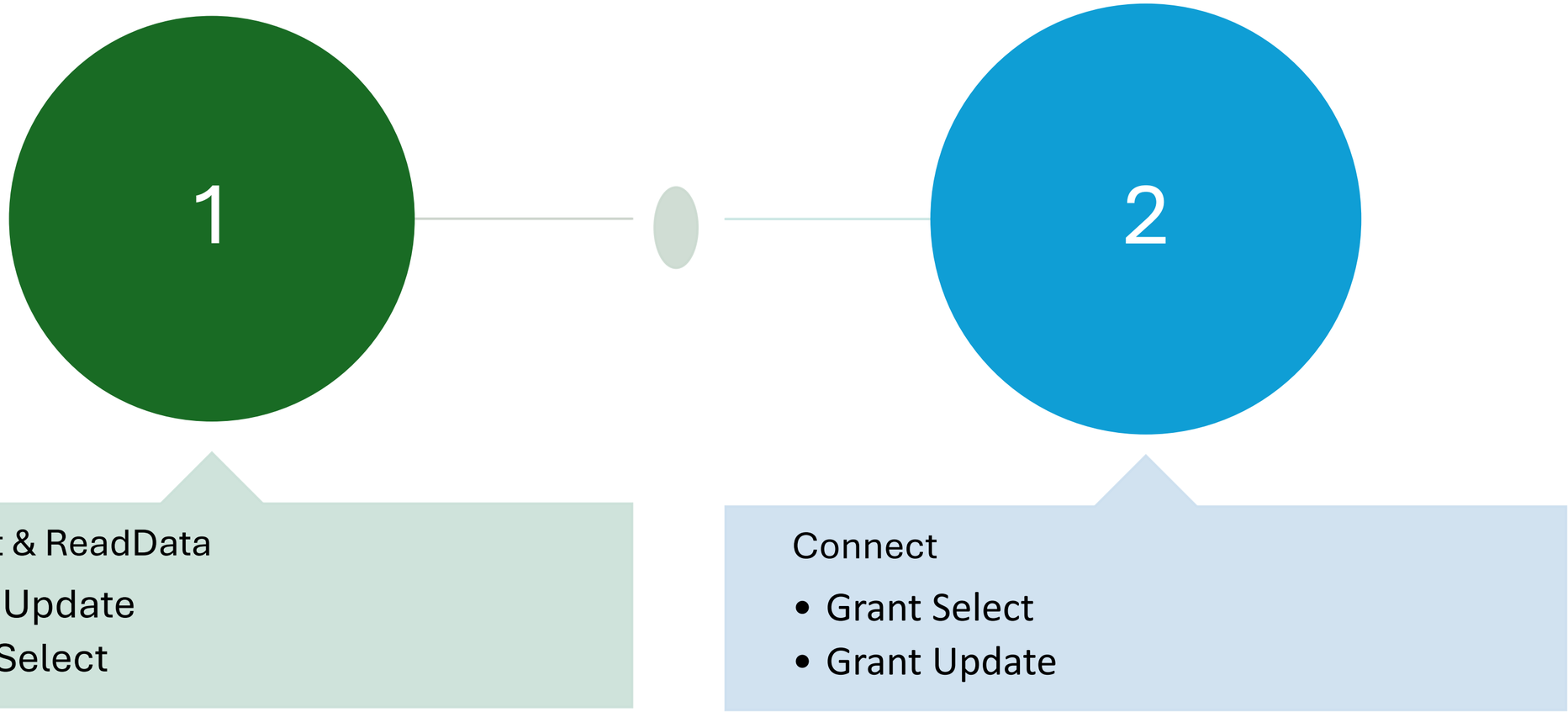


Viewer / non-workspace member with Connect and ReadData

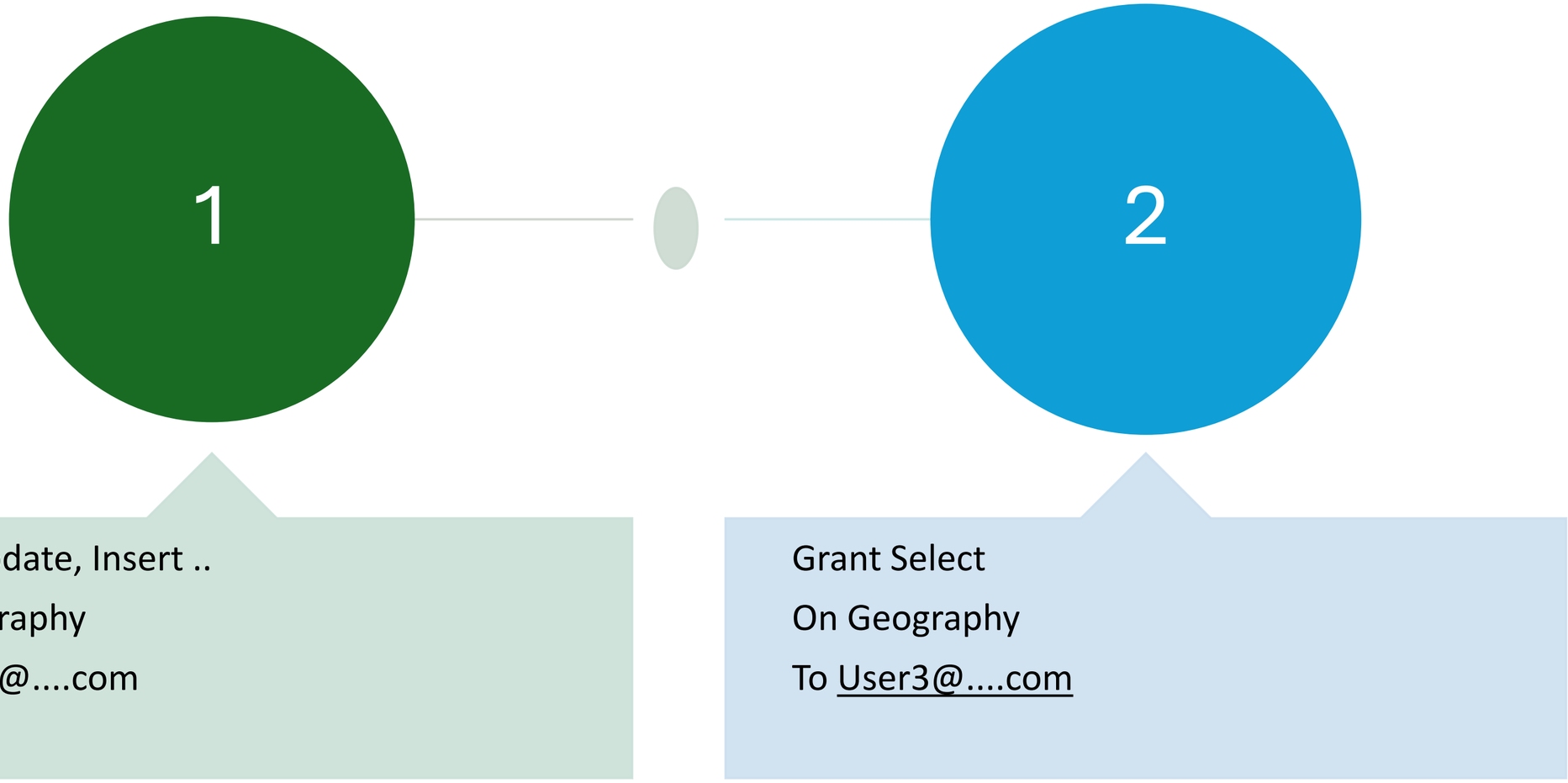
SQL Level Permissions: Object Level Security (OLS)



SQL-Level Permissions

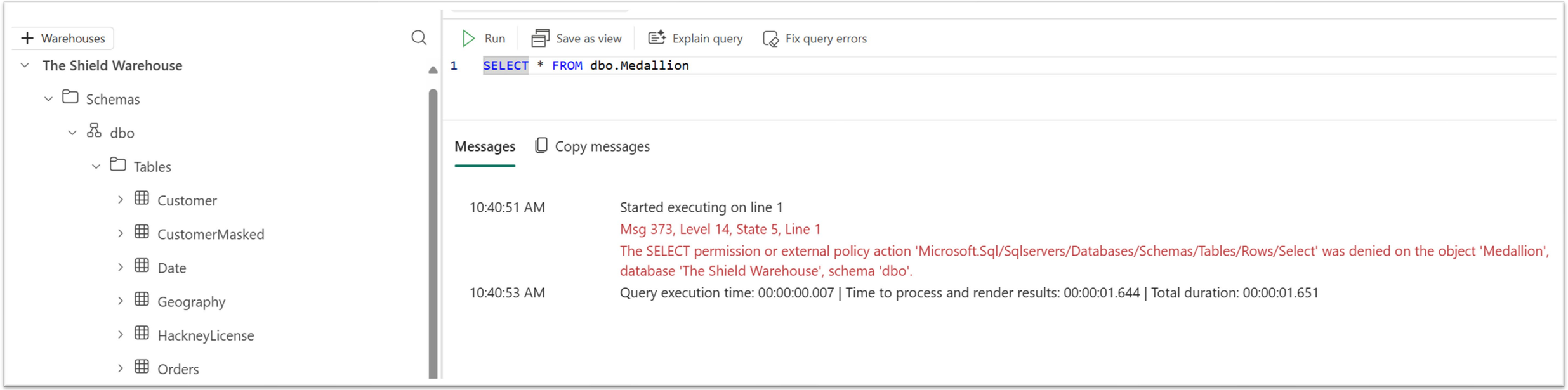


SQL-Level Permissions



DENY

- Deny Select on dbo.Medallion to TestUser1@....com
- Deny has precedence over ReadData even for workspace viewers



REVOKE

Remove a previously granted permission.

Revoke Select On MyTable To [UserA];

CONTROL

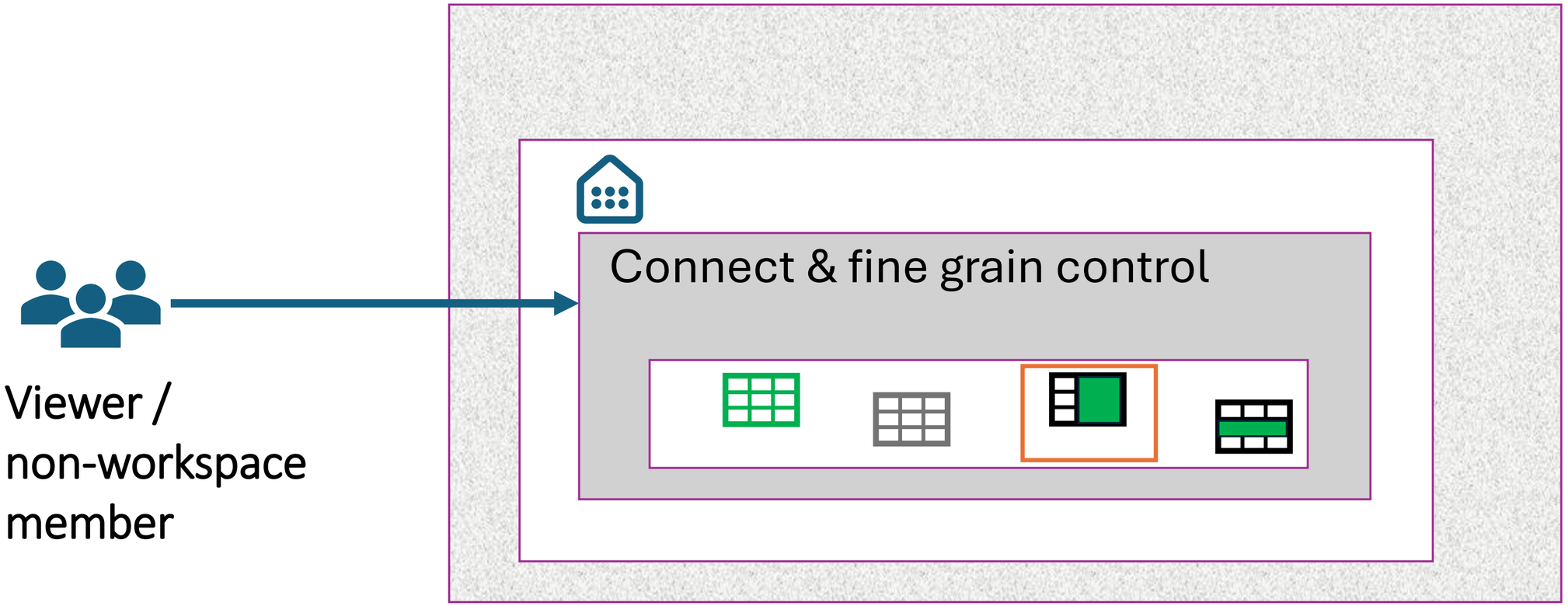
Gives a principal (user or role) **full access** to a securable

Grant Control on Table to User

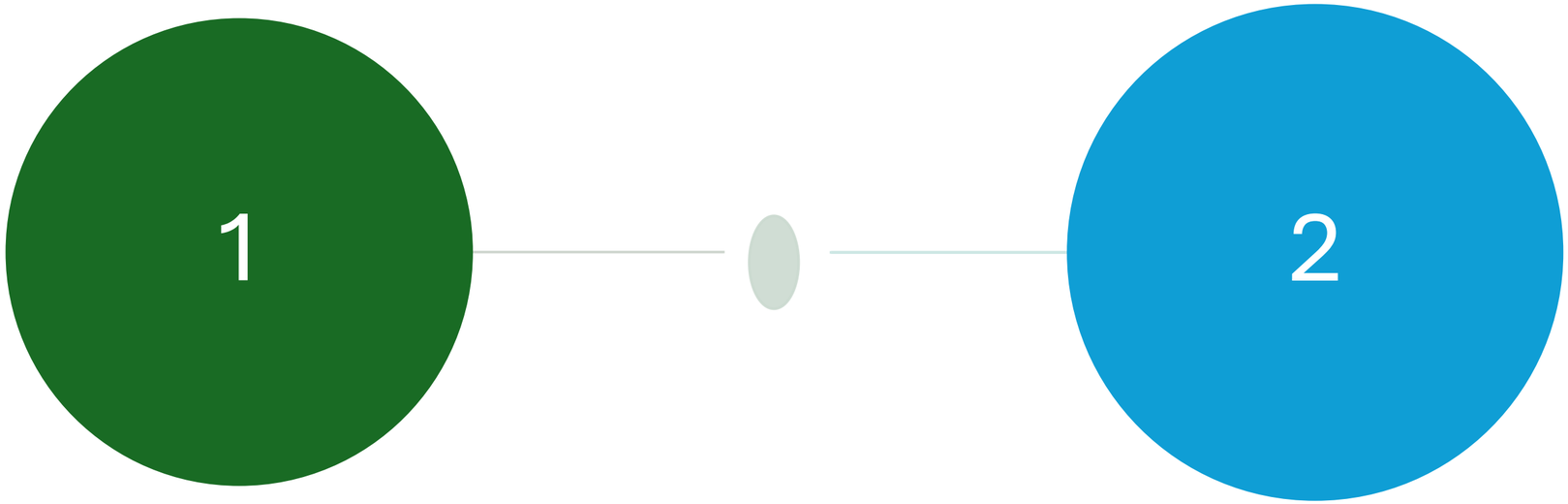
Use sparingly

Does not overwrite Deny

SQL Level Permissions: Column Level Security (CLS)



SQL-Level Permissions



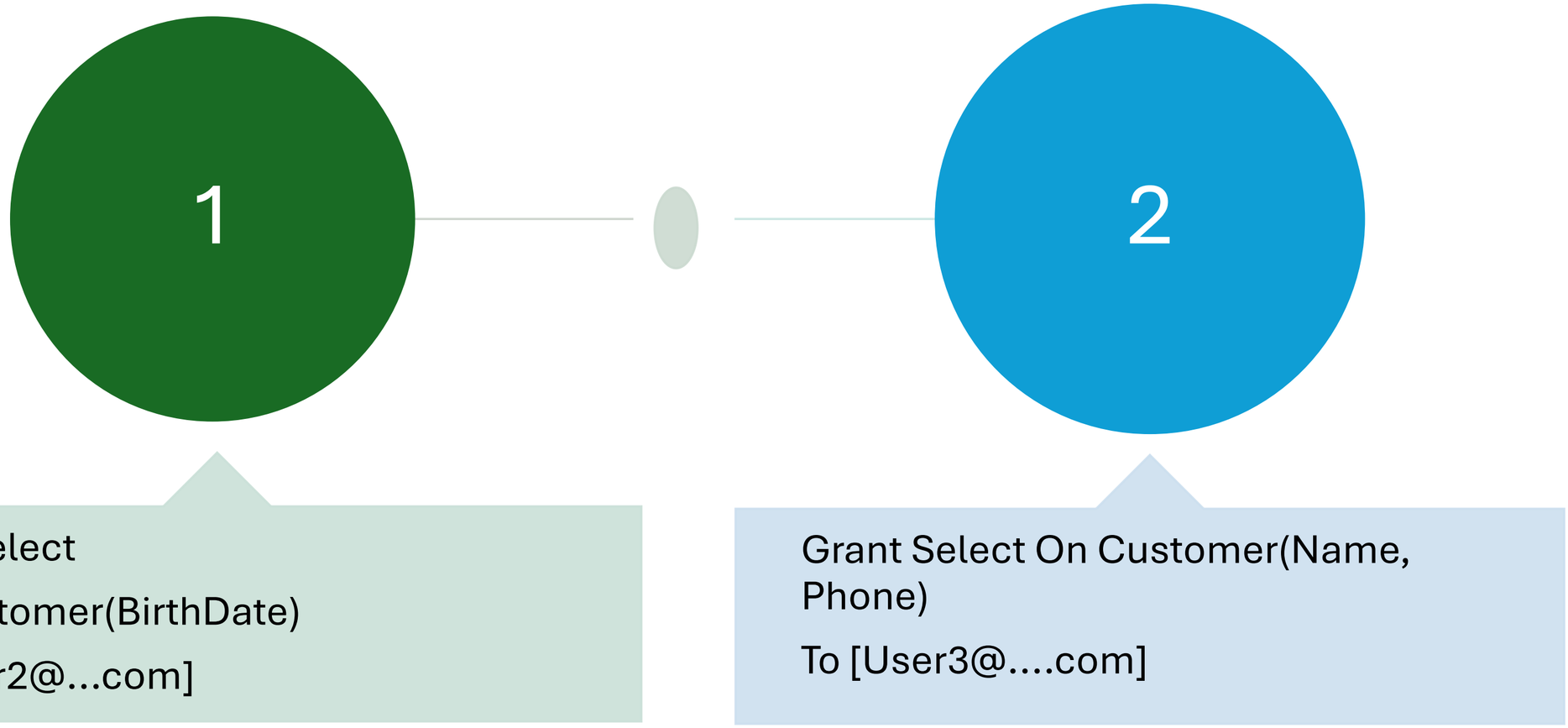
Connect & ReadData

- Grant Update
- Deny Select

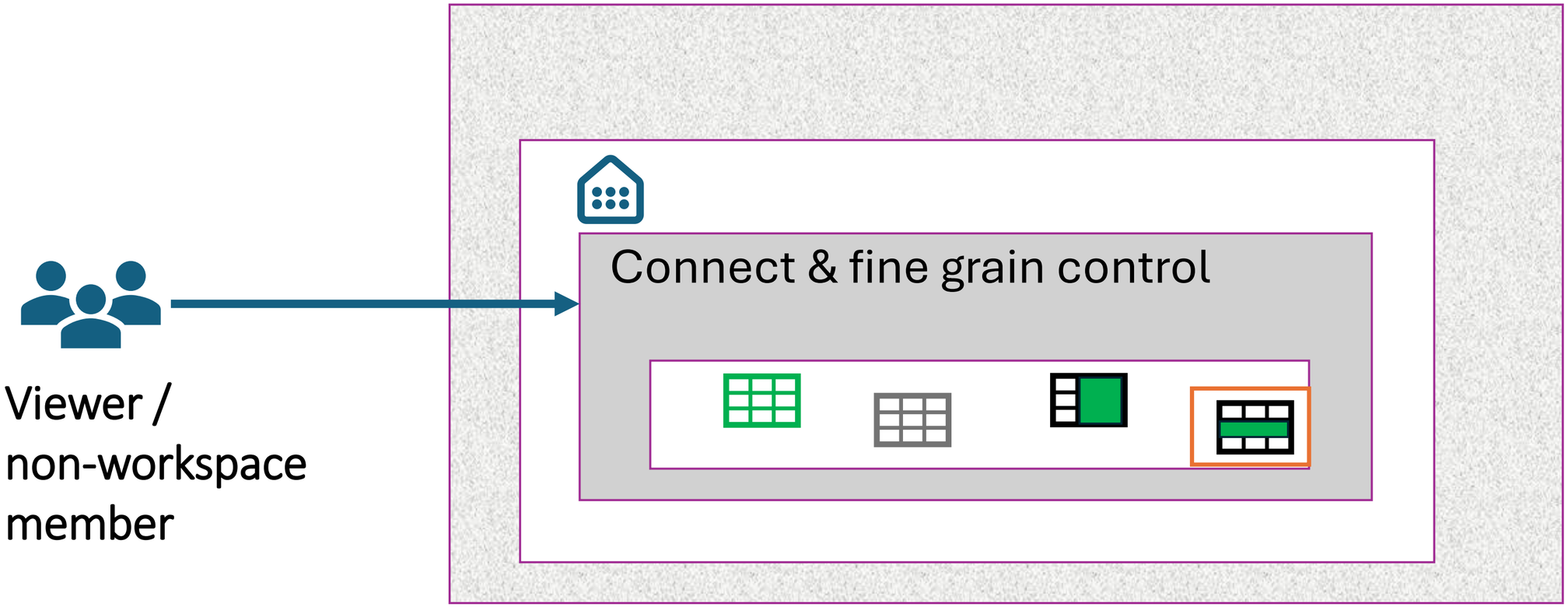
Connect

- Grant Select
- Grant Update

SQL-Level Permissions



SQL Level Permissions: Column Level Security (RLS)



Row Level Security

Different users see different rows

123 SaleID	ABC SalesRep	ABC ProductName	e^x SaleAmount
1	TestUser1@: com	Smartphone	500.00
2	TestUser2@: com	Laptop	1000.00
3	TestUser1@: com	Headphones	120.00
4	TestUser2@: com	Tablet	800.00
5	TestUser1@: com	Smartwatch	300.00
6	TestUser2@: com	Gaming Console	400.00
7	TestUser1@: com	TV	700.00
8	TestUser2@: com	Wireless Earbuds	150.00
9	TestUser1@: com	Fitness Tracker	80.00
10	TestUser2@: com	Camera	600.00

Row Level Security

Schema

Function

Security Policy

Row Level Security: Schema

```
CREATE SCHEMA
Security;
```

Row Level Security: Function

```
Create Function Security.RLSFunction
(@SalesRep AS nvarchar(50))
Returns Table
With SCHEMABINDING
AS
    Return Select 1 as RLSFunction_result
    Where @SalesRep = USER_NAME()
    Or USER_NAME() = admin@....com';
```

Row Level Security: Security Policy

```
Create SECURITY POLICY SalesRLS
Add Filter PREDICATE
    [Security].[RLSFunction](SalesRep)
On dbo.Orders
With (State = On);
```

Row Level Security: Warning

```
SELECT 1/(Salary – 100,000)
FROM EmployeeSalaries
Where Name = ‘Bob Jones’
```

It is possible to leak some data.

Row-Level Security in Fabric Data Warehousing - Microsoft Fabric | Microsoft Learn

OLS, RLS, CLS

Can we get even more fine grain?

What if we want User 1 to only see the last 4 characters of a column?

Dynamic Data Masking (DDS)

With DDS, users see different values in the same column.

```
COLUMN MASKED WITH (FUNCTION = '……................')
                               default(),
                               random(18, 100)
                               partial(0,"XXXXXXXXXXX",4)
                               email()
```

Dynamic Data Masking Example

```
CREATE TABLE dbo.CustomerMasked (
    CustomerID INT,
    FirstName VARCHAR(100) MASKED WITH (FUNCTION = 'partial(1,"-",2)') ,
    LastName VARCHAR(100) MASKED WITH (FUNCTION = 'default()') ,
    Age INT MASKED WITH (FUNCTION = 'random(18, 100)'),
    BirthDate DATE MASKED WITH (FUNCTION = 'default()') ,
    CreditCardNumber VARCHAR(16) MASKED WITH (FUNCTION =
'partial(0,"XXXXXXXXXXX",4)'),
    PhoneNumber VARCHAR(15) MASKED WITH (FUNCTION =
'partial(0,"XXXXXXXXXXX",4)') ,
    EmailAddress VARCHAR(100) MASKED WITH (FUNCTION = 'email()')
);
```

Dynamic Data Masking Example

	CustomerID	FirstName	LastName	Age	BirthDate	CreditCardNumber	PhoneNumber	EmailAddress
1	25	Sarah	Smith	68	1957-07-03	3328244935928628	+1-950-400-2586	sarah.smith@mocksite.xyz
2	122	Adam	Smith	44	1981-06-22	6997198094538311	+1-706-701-8784	adam.smith@example.org
3	131	Bradley	Smith	50	1975-03-22	9458474556051140	+1-604-532-6448	bradley.smith@example....
4	146	Lindsay	Smith	48	1977-07-20	1020809259711497	+1-376-292-6488	lindsay.smith@testdomai..
5	211	Patricia	Smith	30	1995-03-15	8439785037202282	+1-975-593-4161	patricia.smith@testdoma...

	CustomerID	FirstName	LastName	Age	BirthDate	CreditCardNumber	PhoneNumber	EmailAddress
1	25	S-ah	xxxx	26	1900-01-01	XXXXXXXXXXX8628	XXXXXXXXXXX2586	sXXX@XXXX.com
2	122	A-am	xxxx	100	1900-01-01	XXXXXXXXXXX8311	XXXXXXXXXXX8784	aXXX@XXXX.com
3	131	B-ey	xxxx	79	1900-01-01	XXXXXXXXXXX1140	XXXXXXXXXXX6448	bXXX@XXXX.com
4	146	L-ay	xxxx	91	1900-01-01	XXXXXXXXXXX1497	XXXXXXXXXXX6488	lXXX@XXXX.com
5	211	P-ia	xxxx	93	1900-01-01	XXXXXXXXXXX2282	XXXXXXXXXXX4161	pXXX@XXXX.com

Dynamic Data Masking: Warning

```
SELECT ID, Name, Salary
FROM EmployeeSalaries
Where Salary > 99,999 and Salary <100,001
```

Data is masked but is still accessible in the where clause.
It is possible to infer some data.

Dynamic data masking in Fabric Data Warehouse - Microsoft Fabric | Microsoft Learn

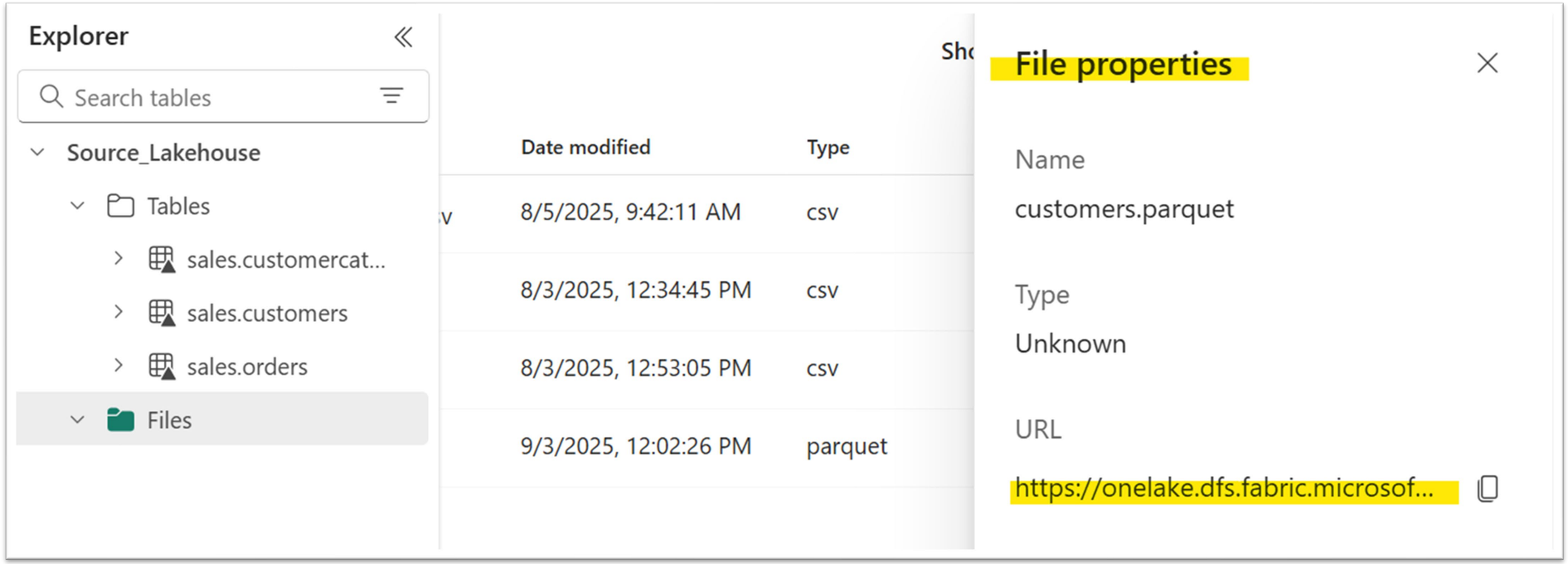
Warning!

Removing a user from a workspace role / sharing items does not remove the SQL Logins!

OPENROWSET

```
SELECT *
FROM OPENROWSET(
    BULK
'https://onelake.dfs.fabric.microsoft.com/<workspace>/<lakehouse>/Files/file',
    FORMAT = 'PARQUET’or CSV
);
```

OPENROWSET




```
SELECT *
FROM OPENROWSET(
    BULK 'https://onelake.dfs.fabric.microsoft.com/Workspace-ID/Lakehouse-ID/Files/customers.parquet',
    FORMAT = 'PARQUET'
);
```

PARQUET is case sensitive.

Audit Logs

What it Tracks: Data access, schema & permission changes, and sign-ins
Where it Lives: Stored in OneLake, queried with T-SQL
How It Works: Select specific actions to log (SELECT, INSERT, EXECUTE)
Security Value: Supports compliance and detects suspicious activity
Setup Required: Not enabled by default; requires Audit permission

Best Practices

Control Access: Use Conditional Access and Private Links
Limit Exposure: Restrict outbound connectivity
Least Privilege: Grant only required workspace and SQL permissions
Layered Protection: Apply RLS, CLS, and object-level security
Monitor & Audit: Track activity with audit logs

Shabnam Watson

Data Consultant,

Speaker, author, blogger, Microsoft Data Platform MVP

Azure Data & AI, Power BI & Fabric

www.shabnamwatson.com

/ShabnamWatson

https://www.youtube.com/@ShabnamWatson

@shbWatson

Sound off.
The mic is all yours.
Influence the product roadmap.

Join the Fabric User Panel

Share your feedback directly with our Fabric product group and researchers.

https://aka.ms/JoinFabricUserPanel

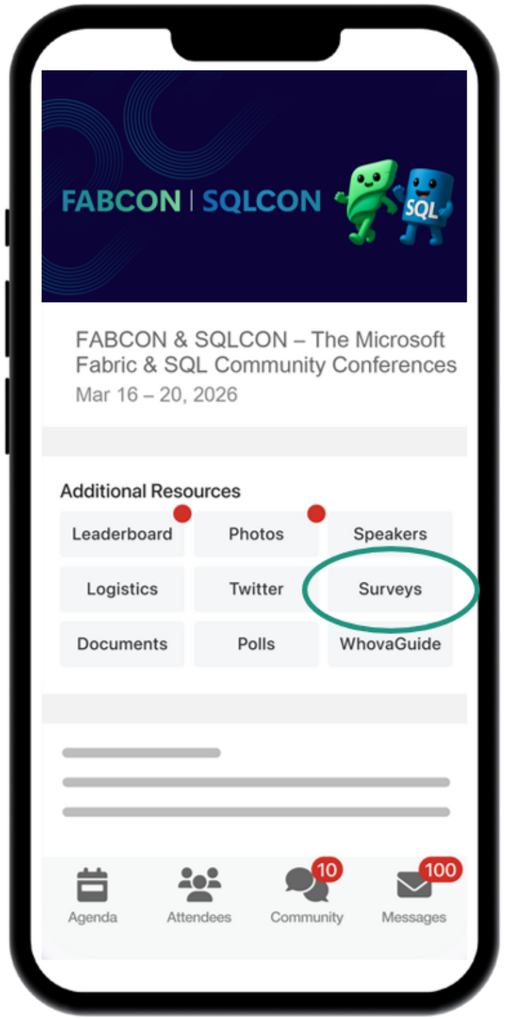
Join the SQL User Panel

Influence our SQL roadmap and ensure it meets your real-life needs

https://aka.ms/JoinSQLUserPanel

How was the session?

Complete Session Surveys in Whova for your chance to WIN PRIZES!



Two Fabric Certifications, One FREE Exam Included

Attendees can take the Fabric Analytics Engineer or Fabric Data Engineer exam for free. Be part of the 2 fastest growing role-based certifications in Microsoft history.

Request your voucher by March 31, 2026.

https://aka.ms/GetDataCertified