

#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

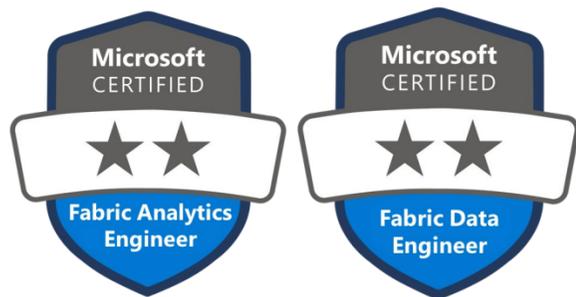
Microsoft Data Platform MVP

Principal Consultant, ABI Cube



Shabnam Watson

Data Consultant,
Speaker, author, blogger, Microsoft Data Platform MVP
Azure Data & AI, Power BI & Fabric



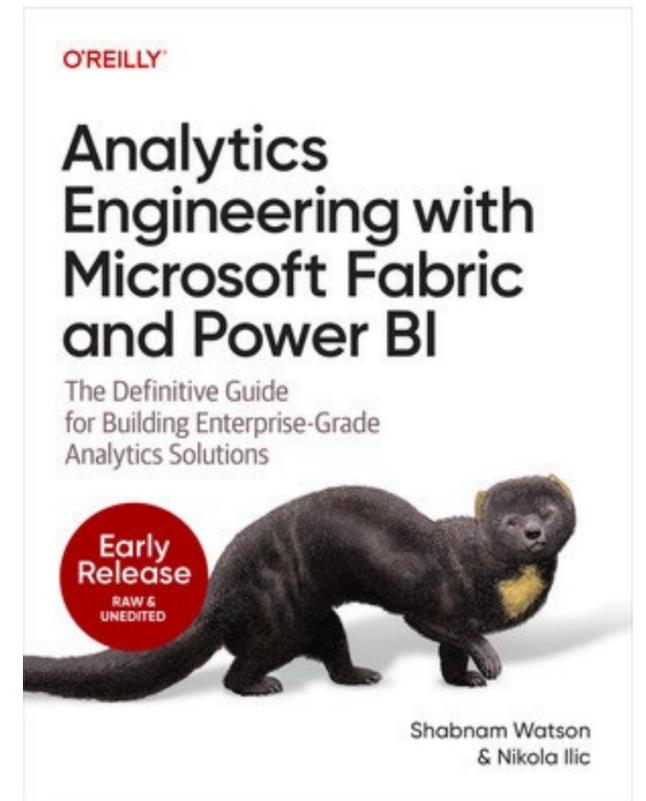
www.shabnamwatson.com



[/ShabnamWatson](https://www.linkedin.com/company/ShabnamWatson)



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



Microsoft Fabric



Data
Factory



Analytics



Databases



Real-Time
Intelligence



Power BI



Industry
Solutions



Partner
Workloads



AI



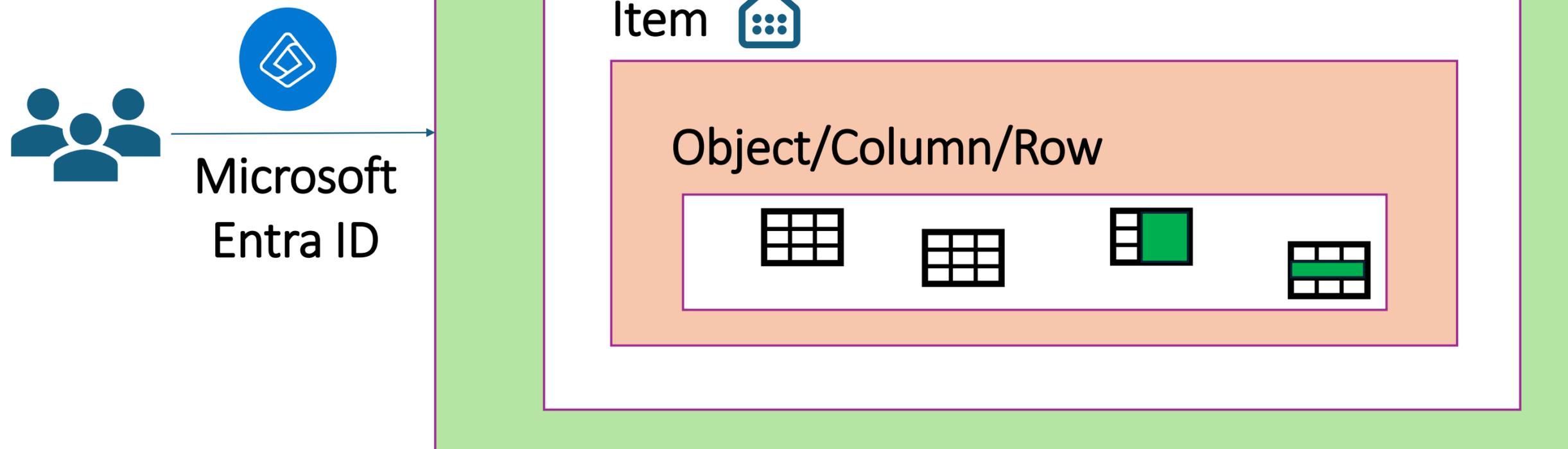
OneLake



Purview

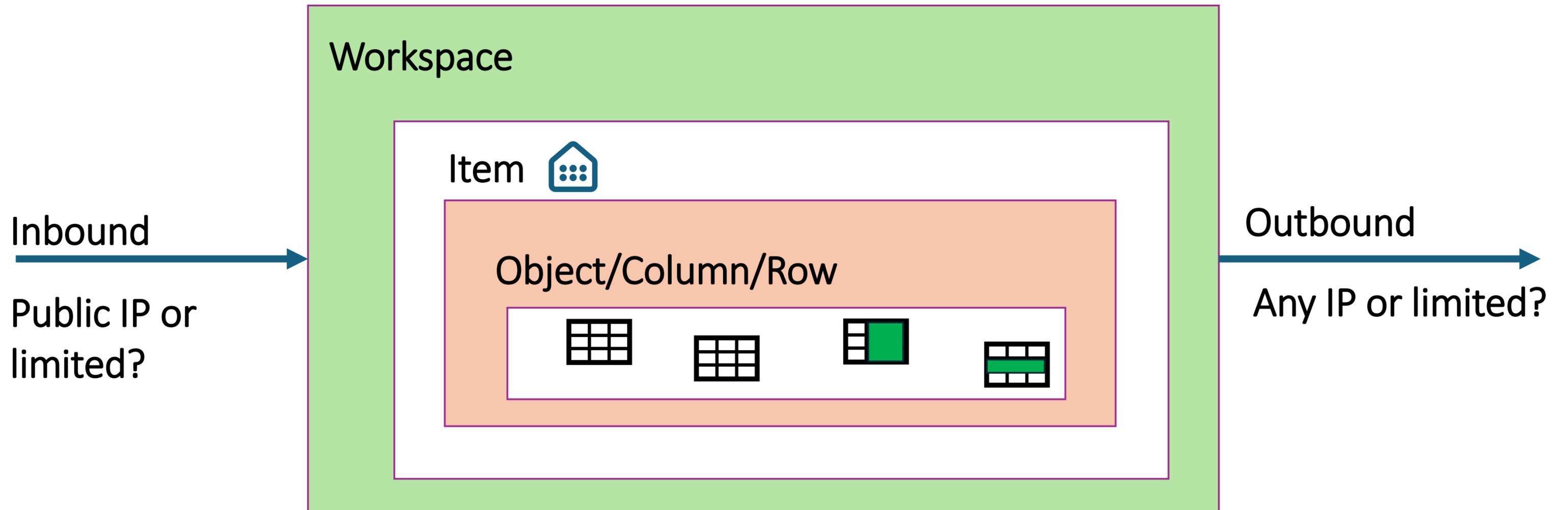
Access Control

Fabric Tenant

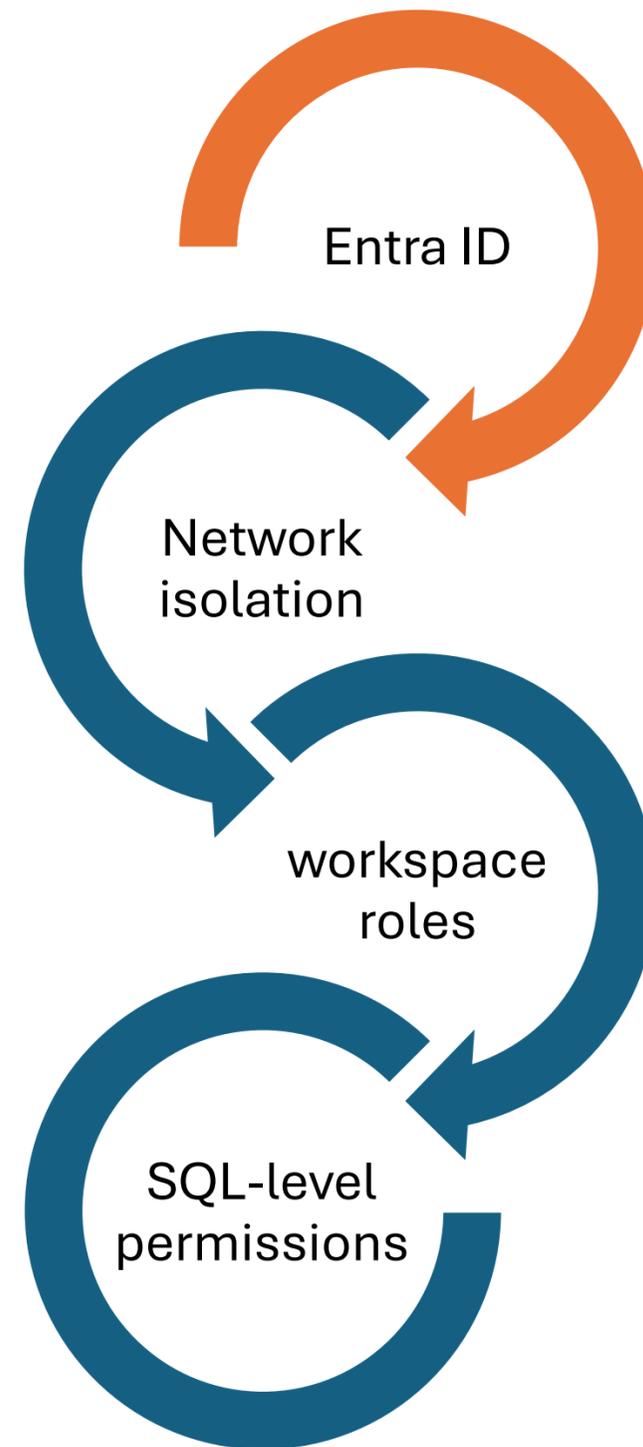


Network Security

Fabric Tenant



Warehouse Secured with



EntraID

Fabric Tenant



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

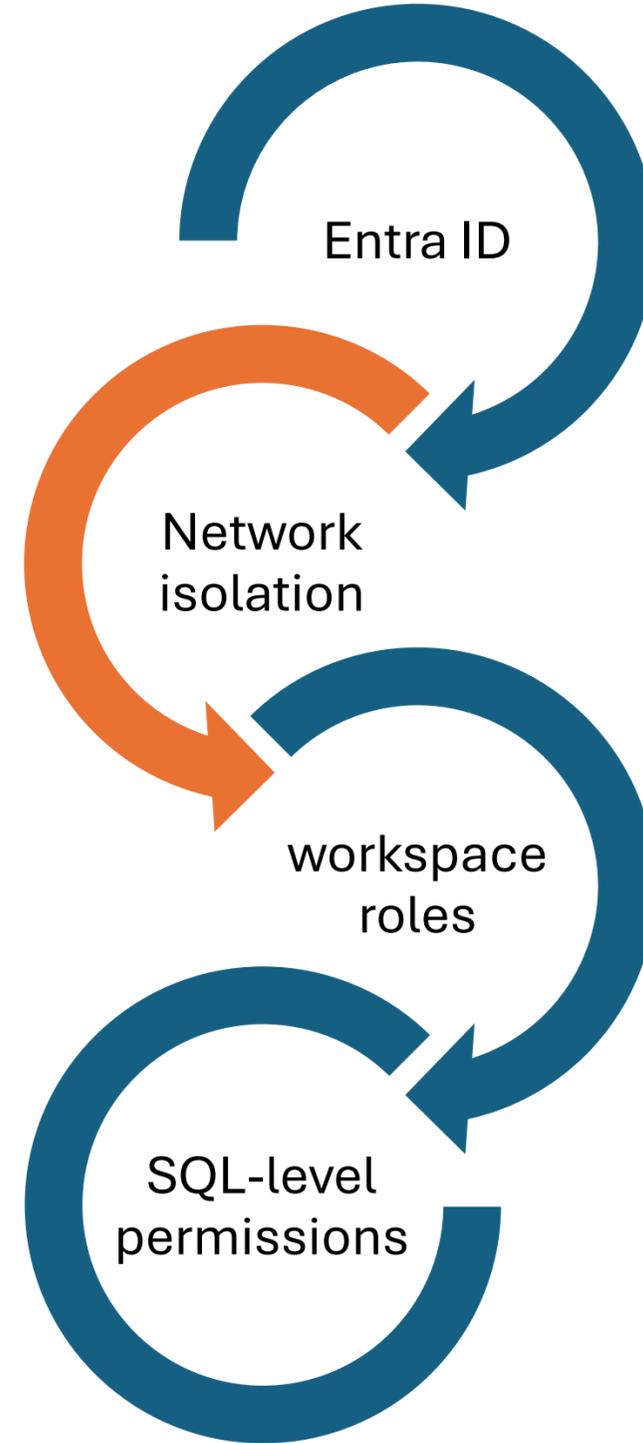
The screenshot shows the Microsoft Entra admin center interface. The left sidebar contains navigation options: Home, Agents, Favorites, Entra ID, ID Governance, Verified ID, Permissions Management, Global Secure Access, What's new, and Billing. The main content area is titled 'Conditional Access | Overview' and includes a 'Create new policy' button, a link to 'Create your own policies and target specific conditions like cloud apps, sign-in risk, and device platforms with Microsoft Entra ID Premium', and a section titled 'What is Conditional Access?' with a 'Learn more' link. Below this is a table with two columns: 'Conditions' and 'Controls'. The table lists two example policies:

Conditions	Controls
When any user is outside the company network	They're required to sign in with multifactor authentication
When users in the 'Managers' group sign-in	They are required be on an Intune compliant or domain-joined device

Below the table is a 'Get Started' section with three steps:

1. Create your first policy by clicking "+ Create new policy"
2. Specify policy Conditions and Controls
3. When you are done, don't forget to Enable policy and Create

Warehouse Secured with



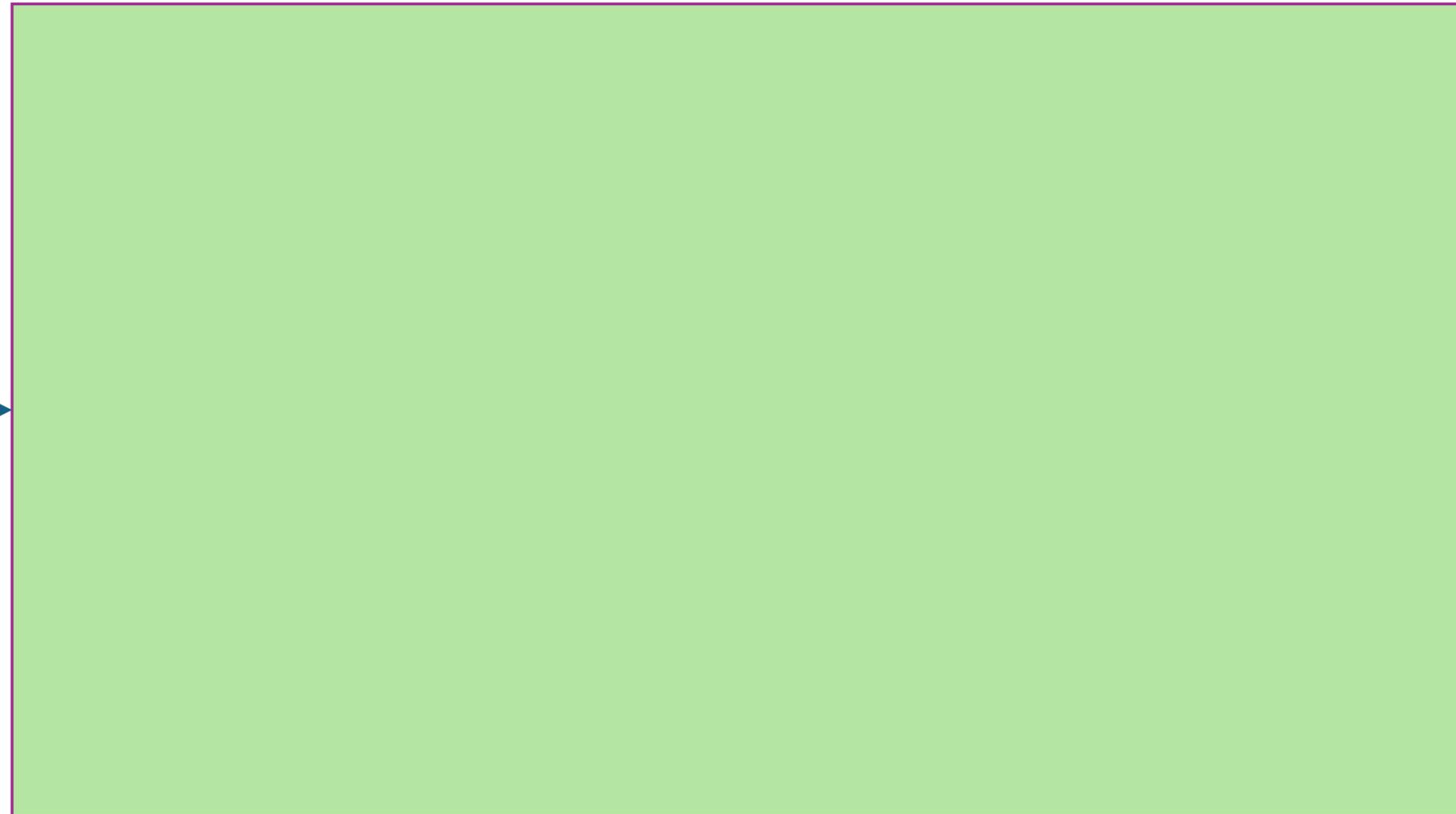
Network Security

Fabric Tenant

Inbound



Any IP or
limited?



Outbound

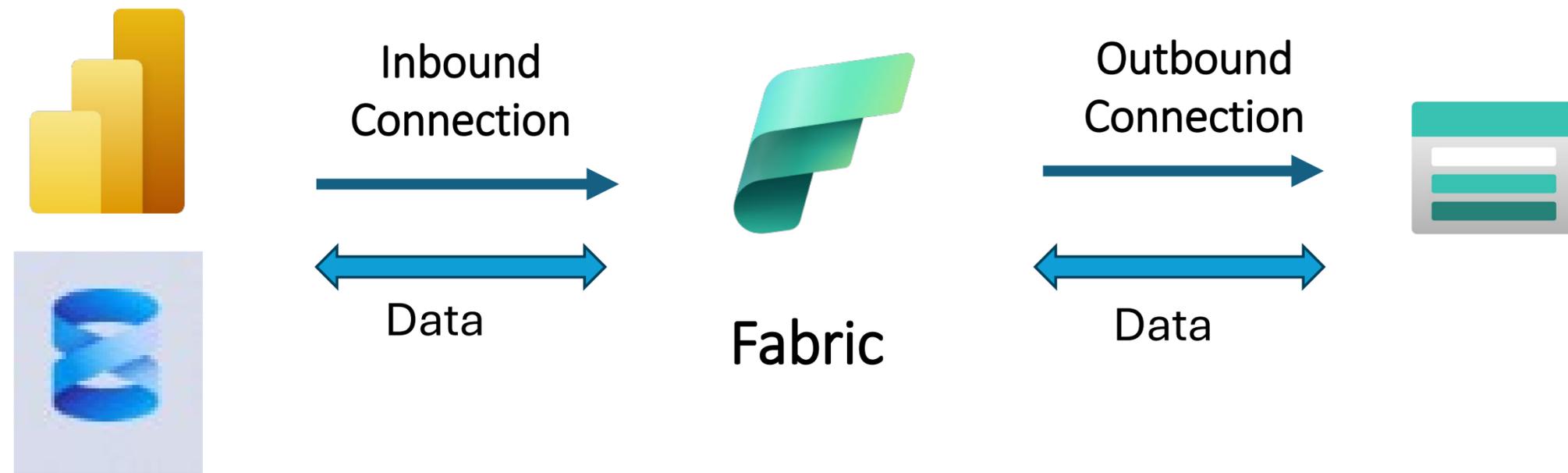


Any IP
or limited?

Network Security

- **Inbound Security**
Protects internal data from external threats.
- **Outbound Security**
Ensures secure sharing of data outside workspace boundaries.

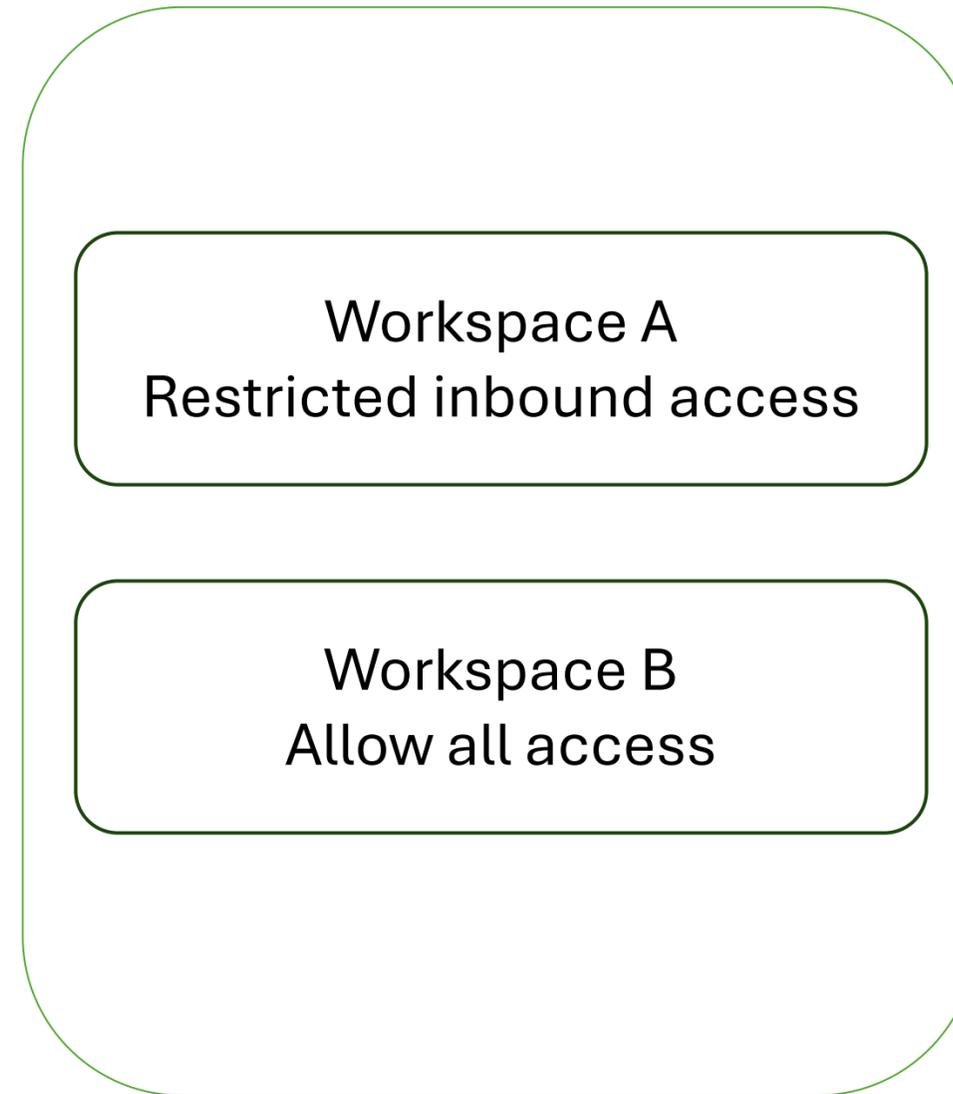
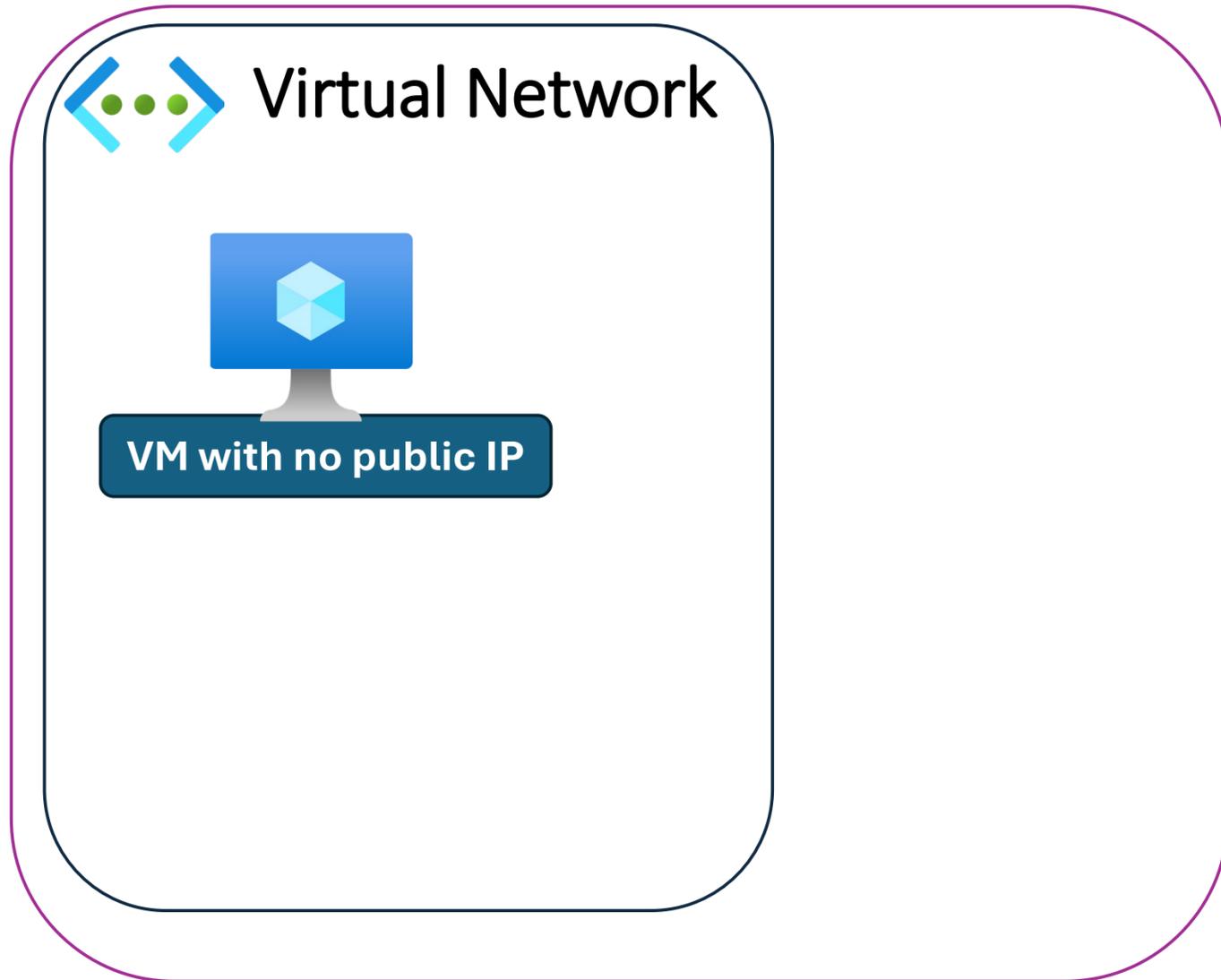
Network Security: All about connections



Inbound Security

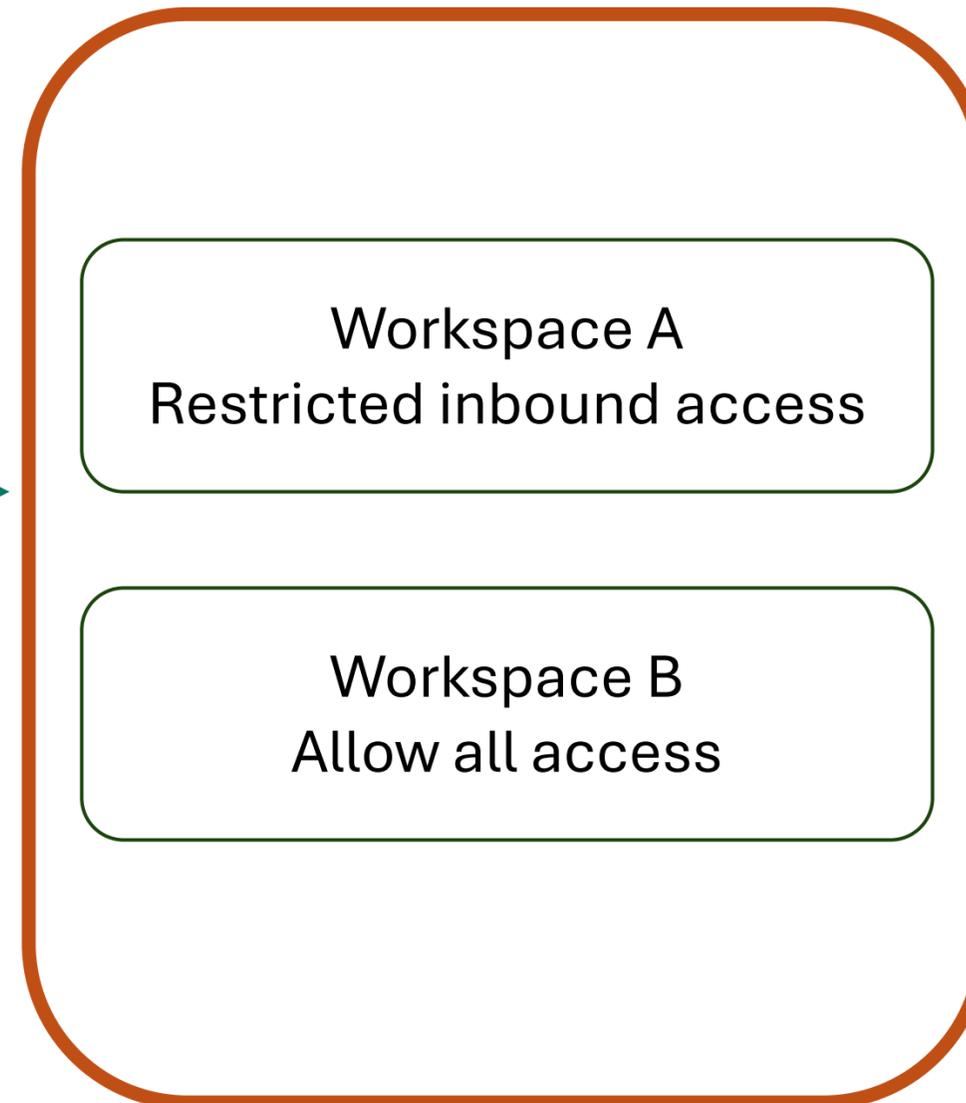
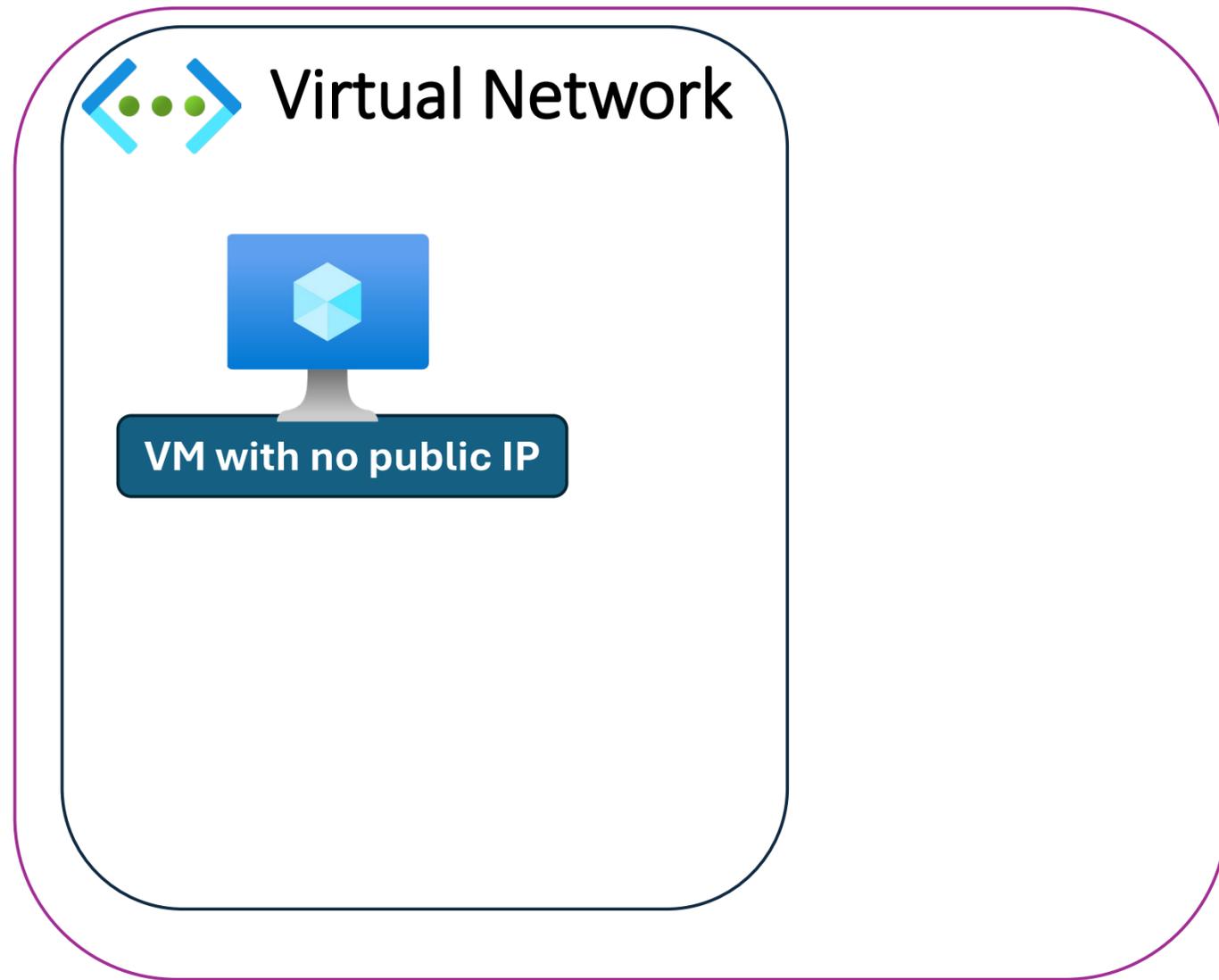
- Protects internal data from external threats
- Tenant and workspace levels
- Secure access to Fabric items from trusted networks
- Blocks unauthorized inbound traffic

Big Picture



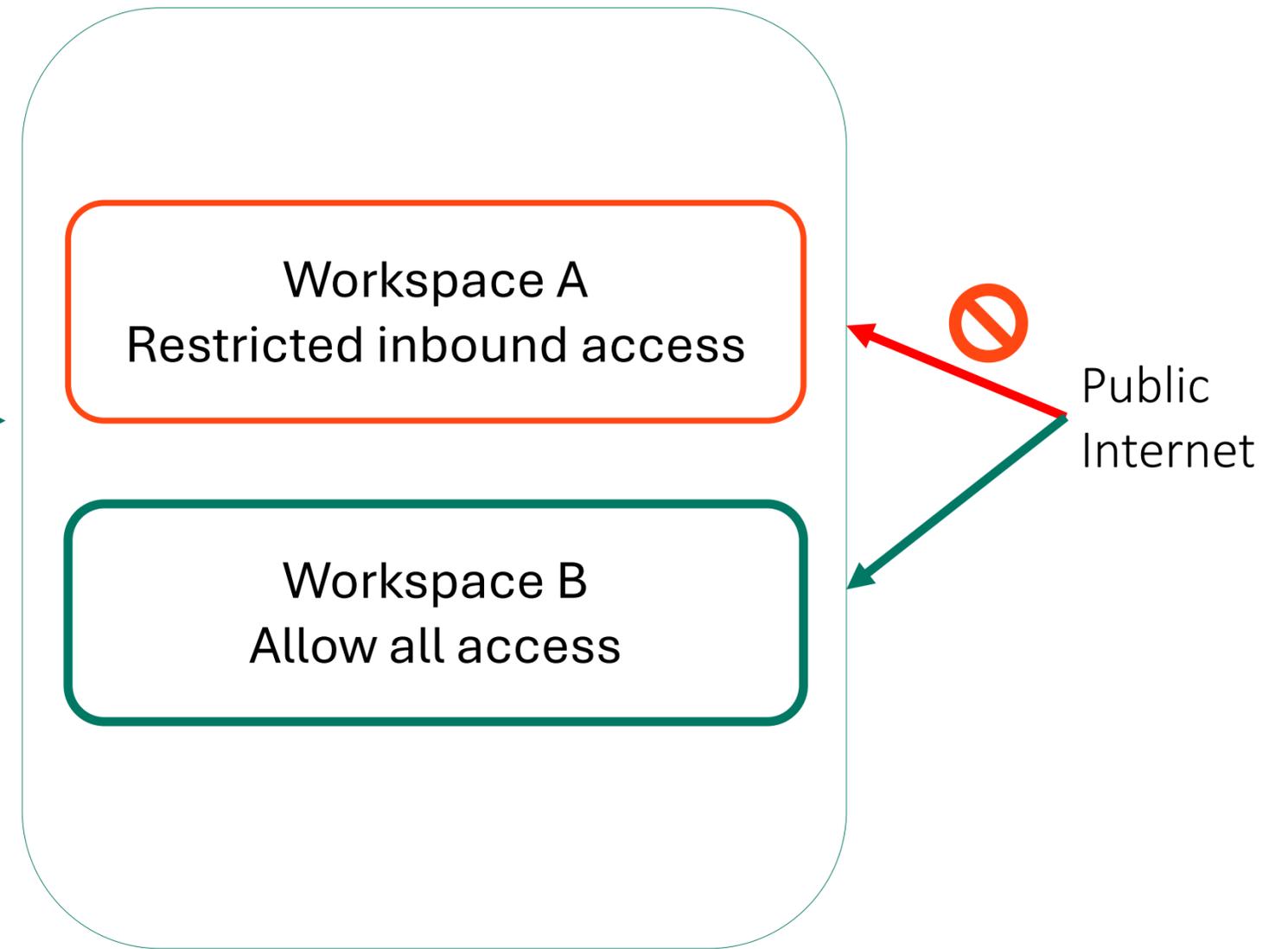
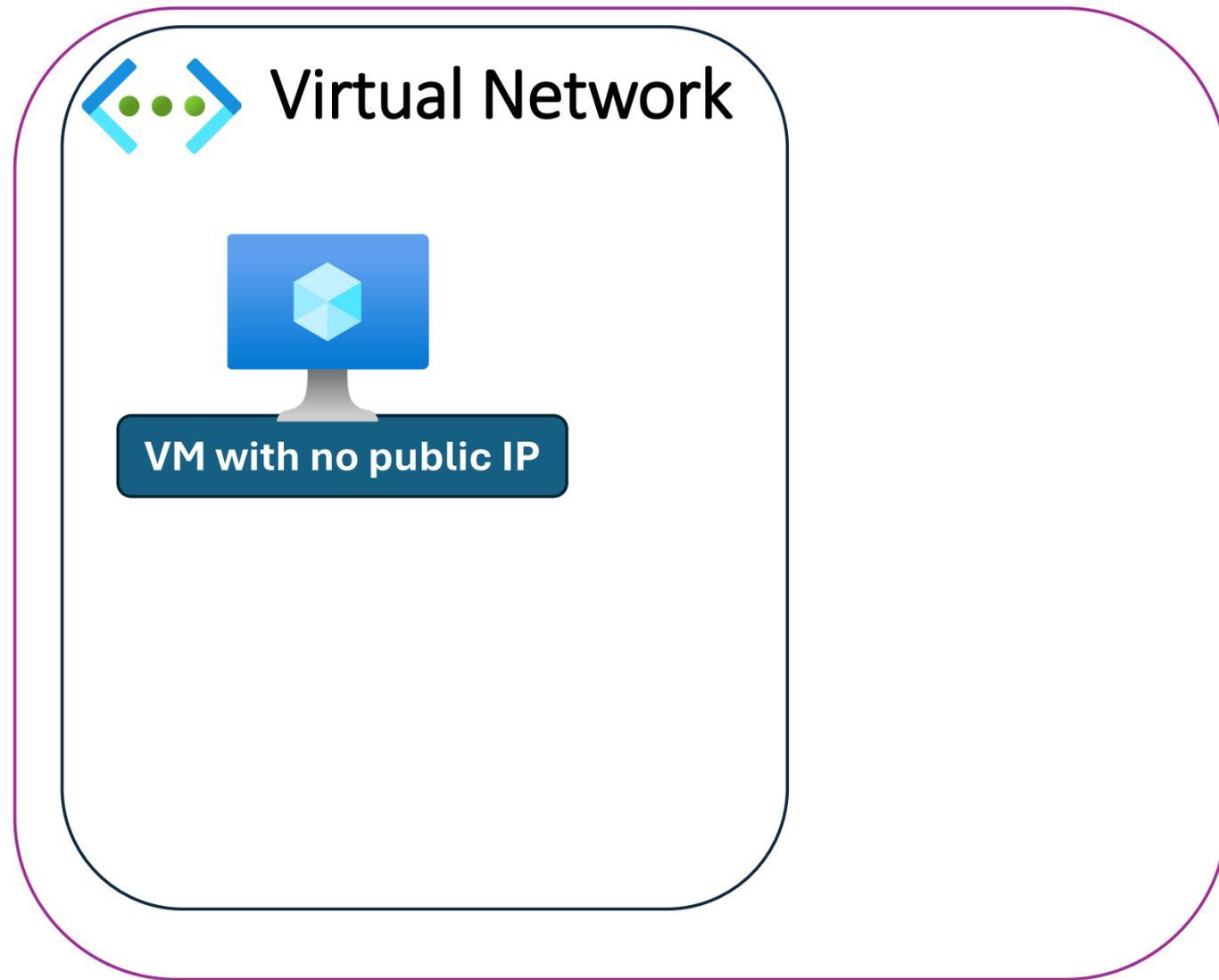
Public
Internet

Tenant Level Control

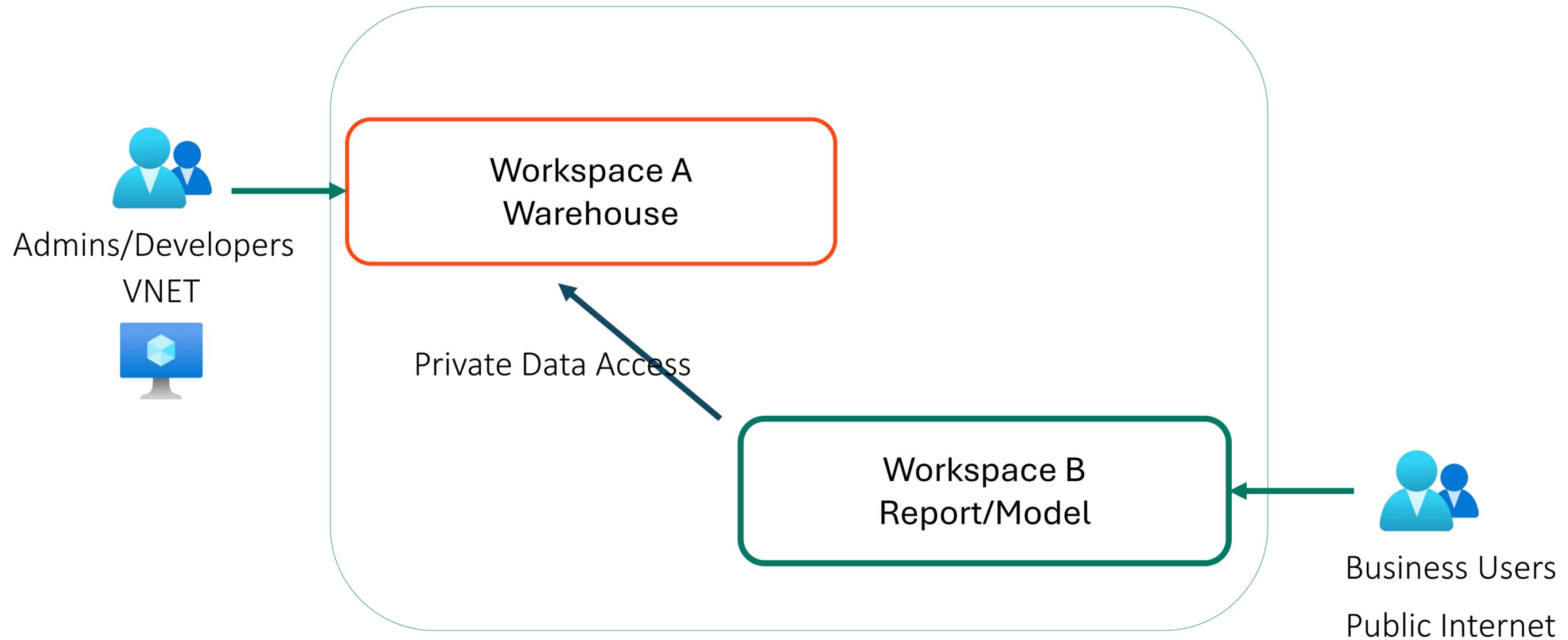


Public Internet

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



Virtual Network



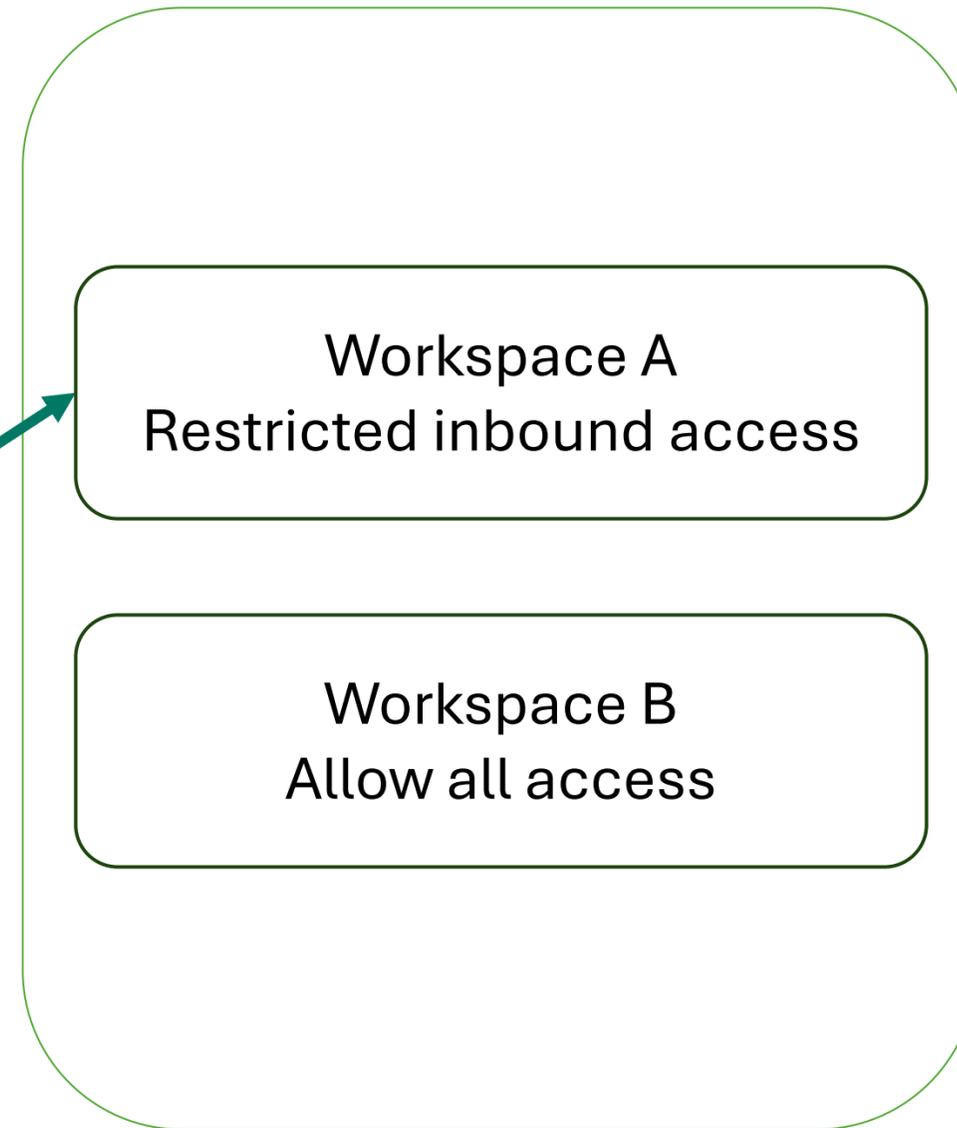
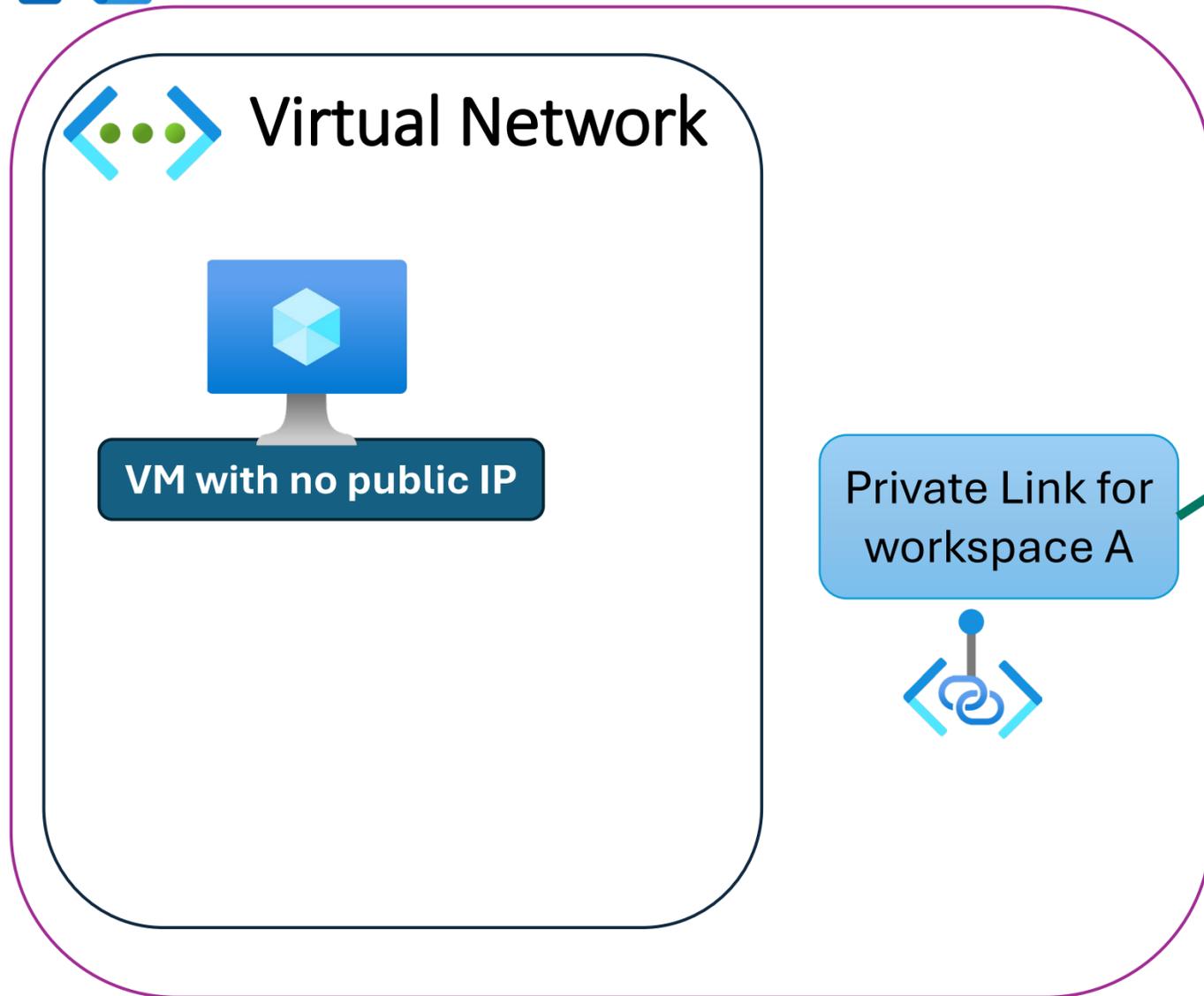
VM with no public IP



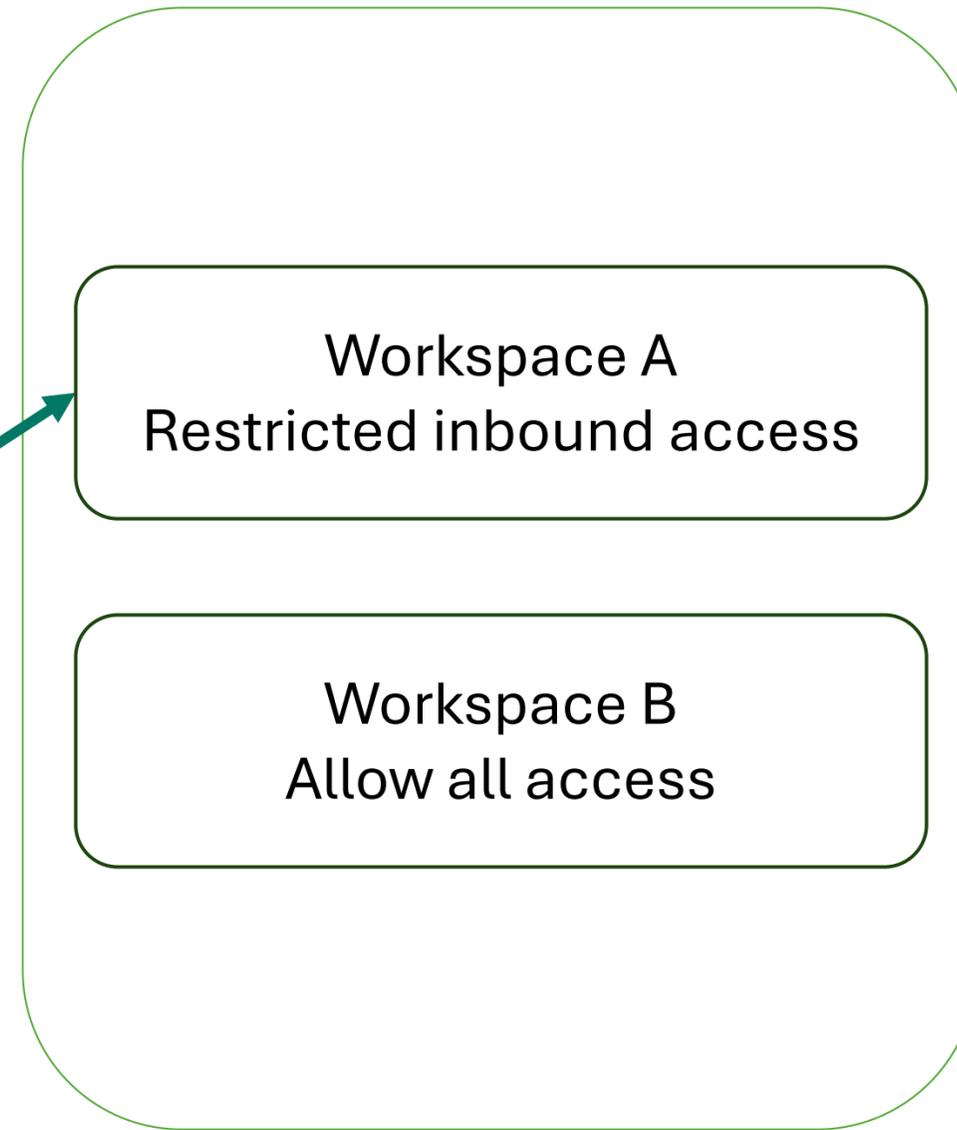
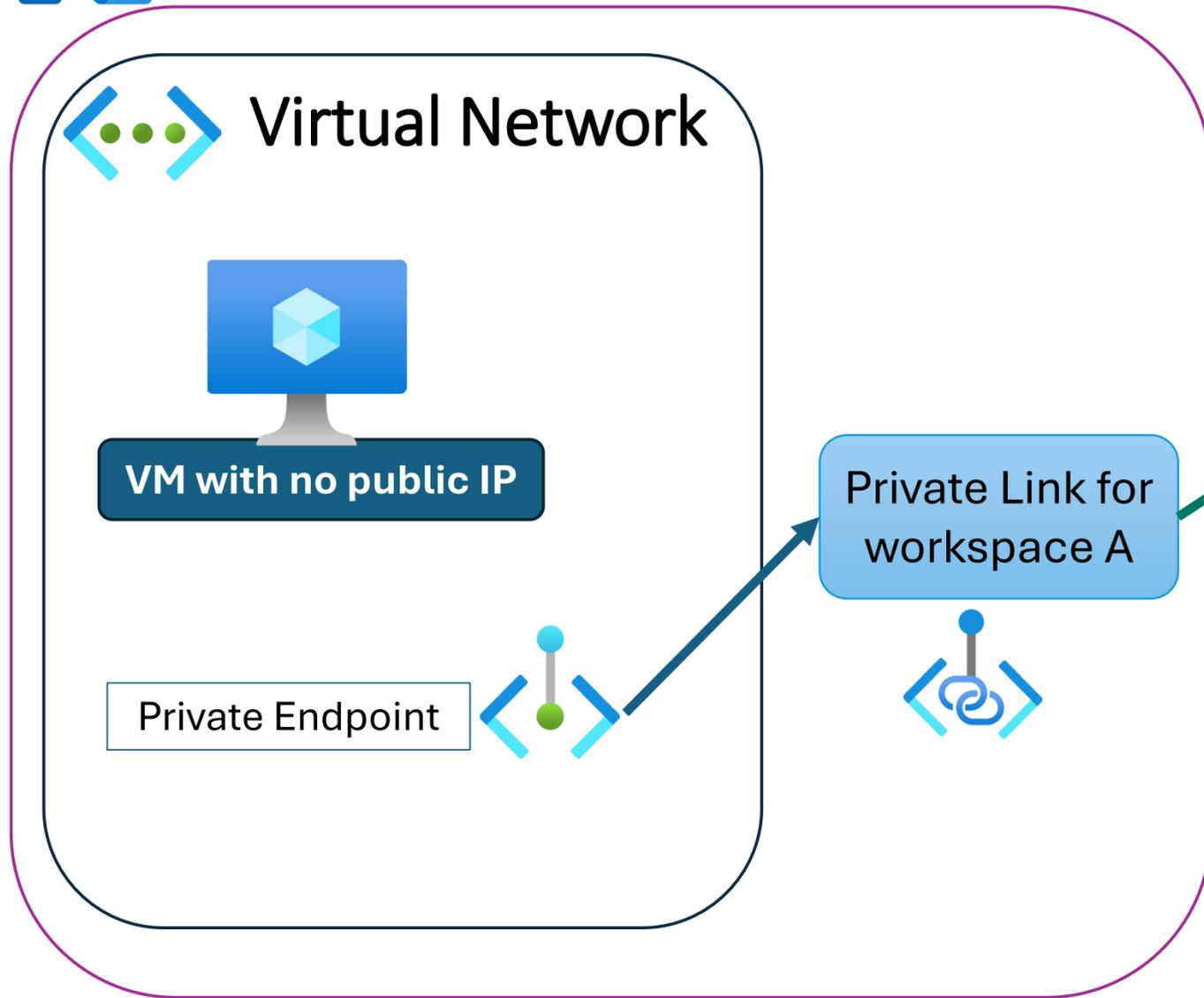
Workspace A
Restricted inbound access

Workspace B
Allow all access

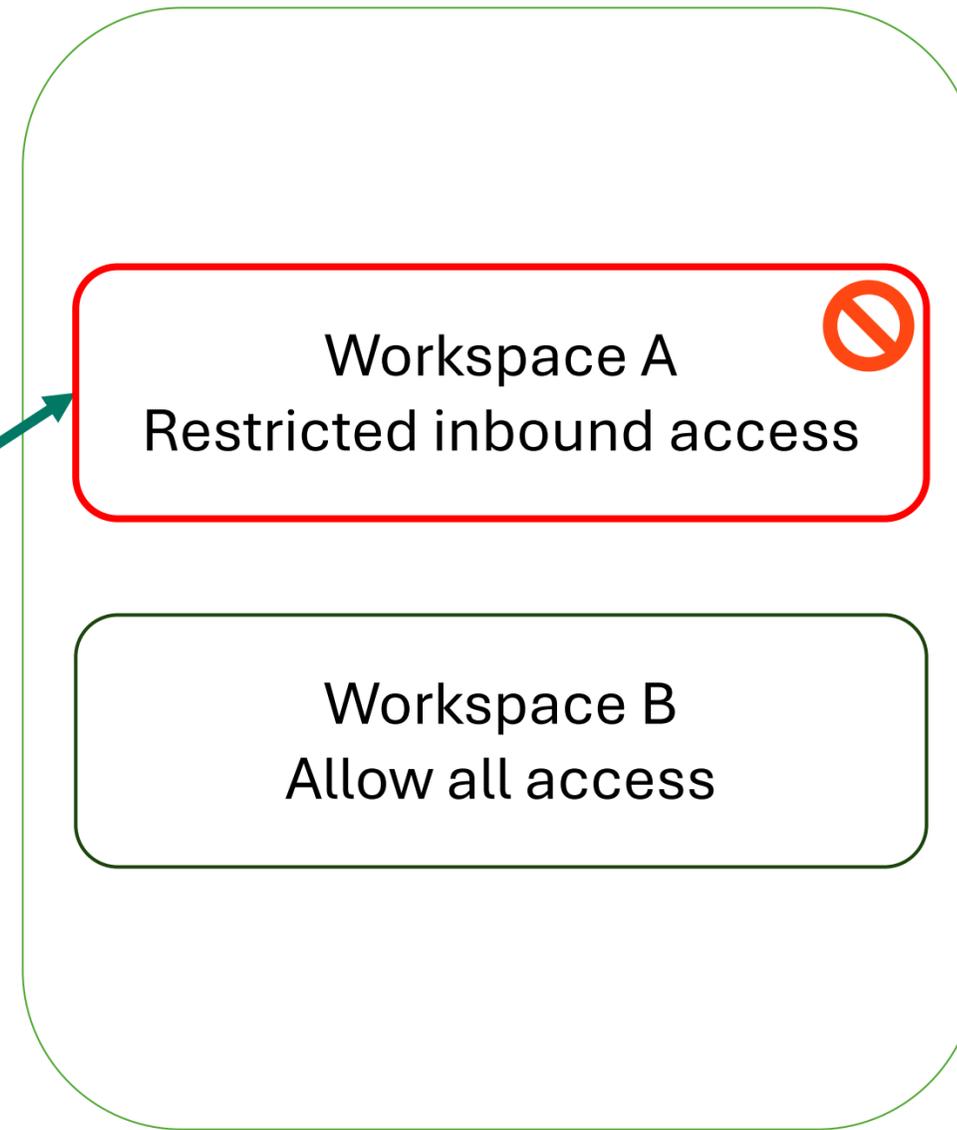
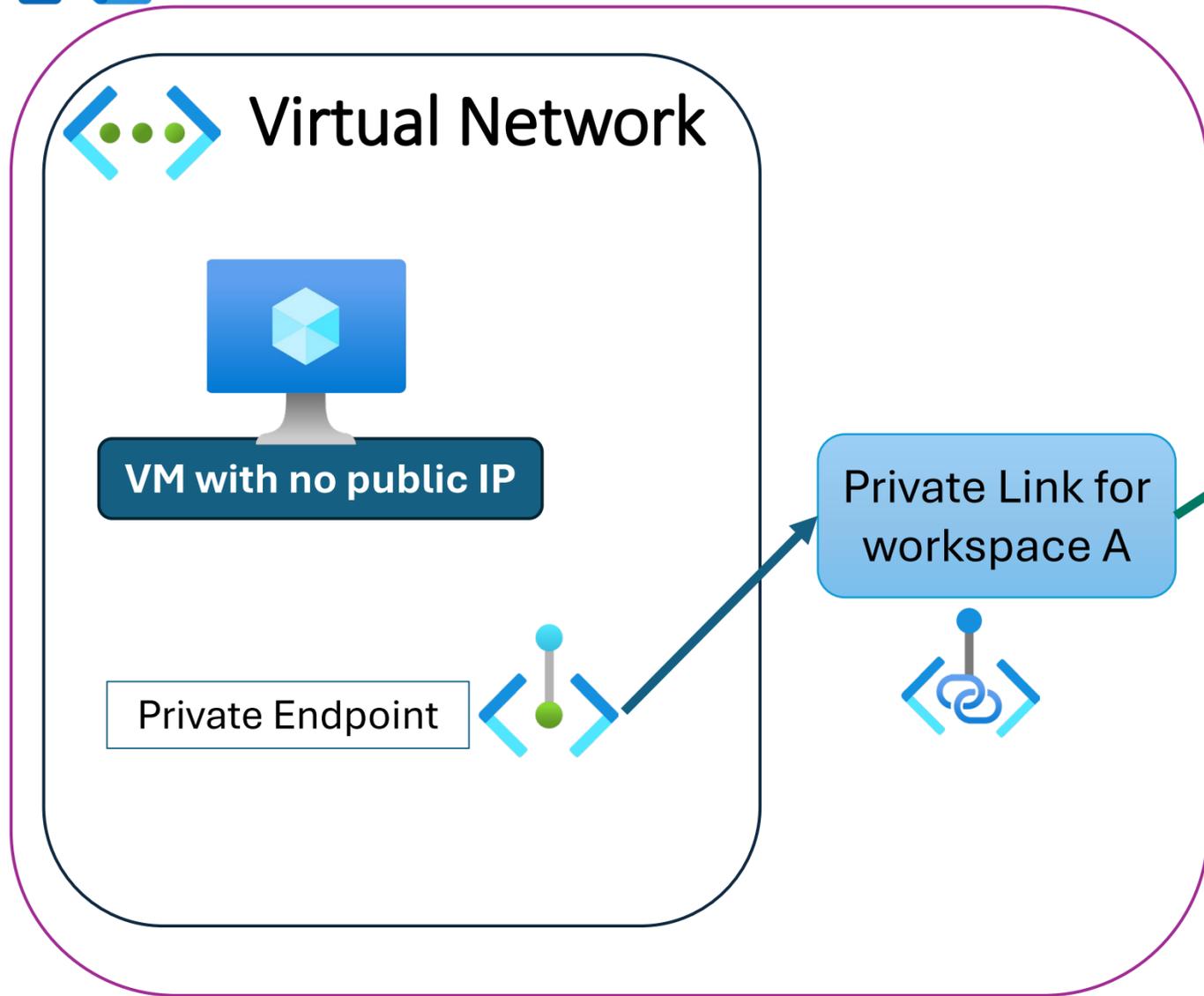
Workspace Level Control



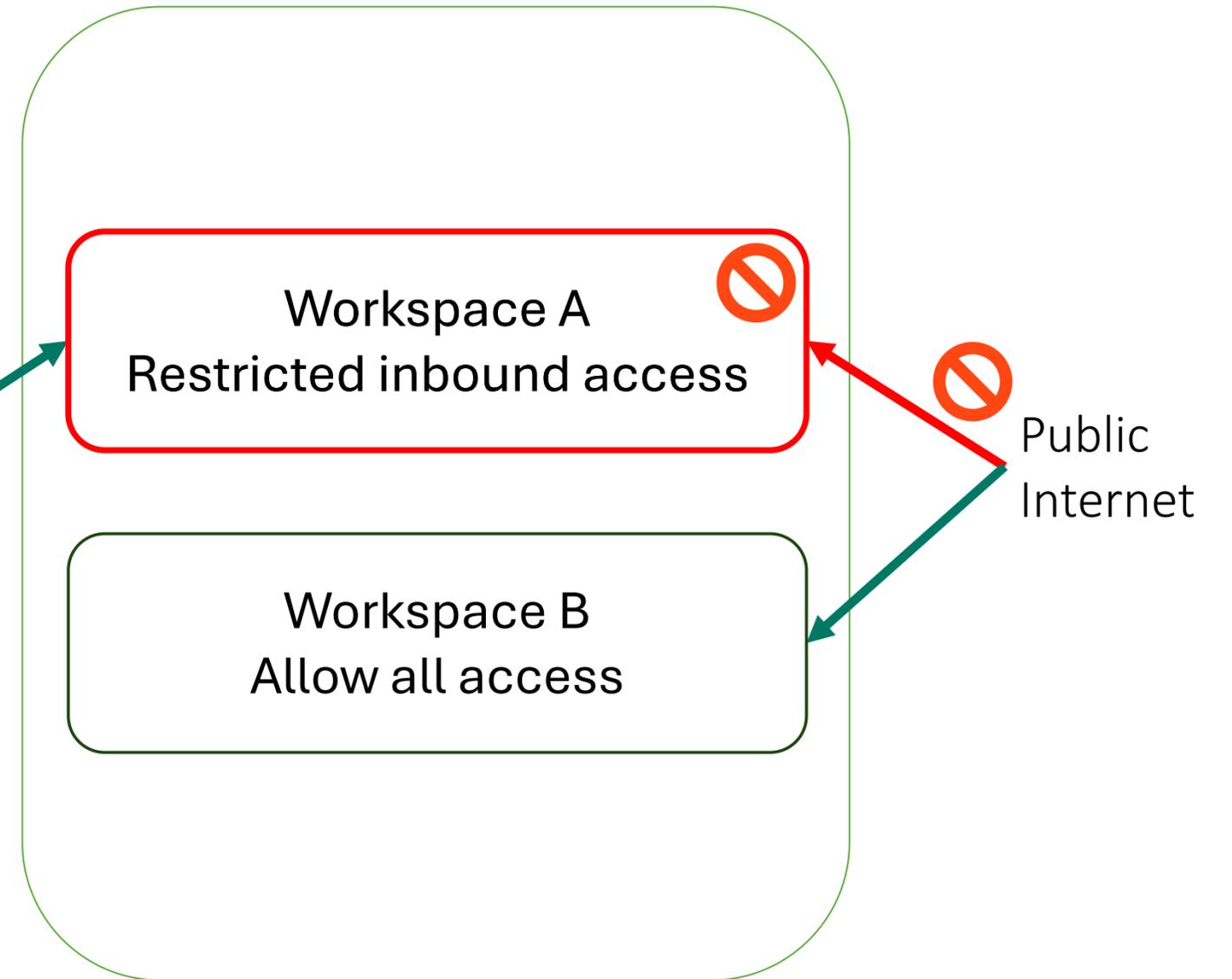
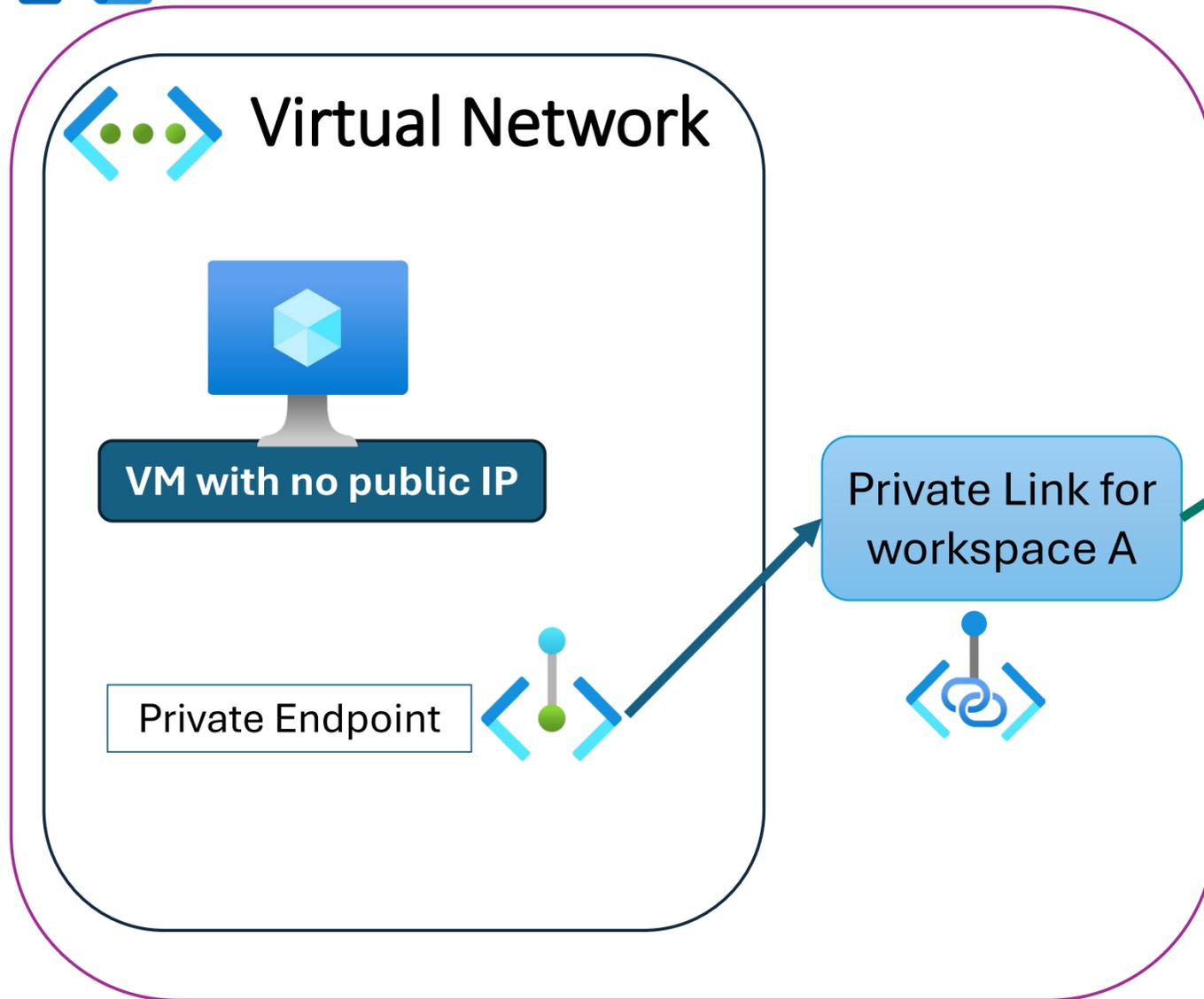
Workspace Level Control



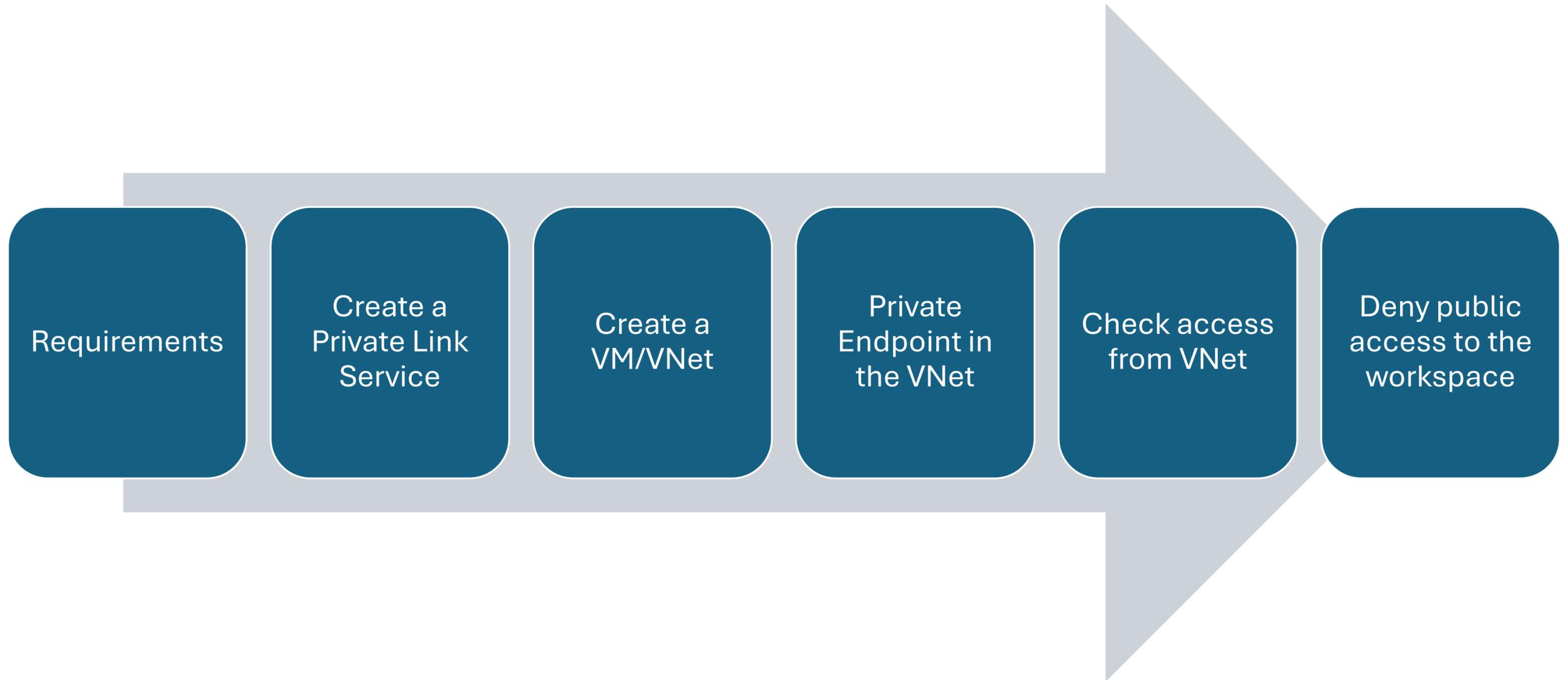
Workspace Level Control



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

Advanced networking

▾ Tenant-level **Private** Link

Enabled for the entire organization

Increase security by allowing people to use a **Private** Link to access your Fabric tenant. Someone will need to finish the set-up process in Azure. If that's not you, grant permission to the right person or group by entering their email. [Learn More](#) | [Set-up instructions](#)

Review the [considerations and limitations](#) section before enabling **private** endpoints.

Enabled

ⓘ This setting applies to the entire organization

Apply

Cancel

Block Public Internet Access to tenant

Advanced networking

⚡ Block **Public** Internet Access

Disabled for the entire organization

For extra security, block access to your Fabric tenant via the **public** internet. This means people who don't have access to the Private Link won't be able to get in. Keep in mind, turning this on could take 10 to 20 minutes to take effect. [Learn More](#) [Set-up instructions](#)

Disabled

🛡️ This setting applies to the entire organization

Apply

Cancel

Workspace-level Private Links

Advanced networking

▾ **Configure workspace-level inbound network rules**

Enabled for the entire organization

With this setting on, workspace admins can configure inbound private link access protection in workspace settings. When a workspace is configured to restrict inbound network access, existing tenant-level private links can no longer connect to these workspaces. Turning off this setting reverts all workspaces to their previous configuration.

[Learn More](#)

Enabled

🛡️ This setting applies to the entire organization

Apply

Cancel

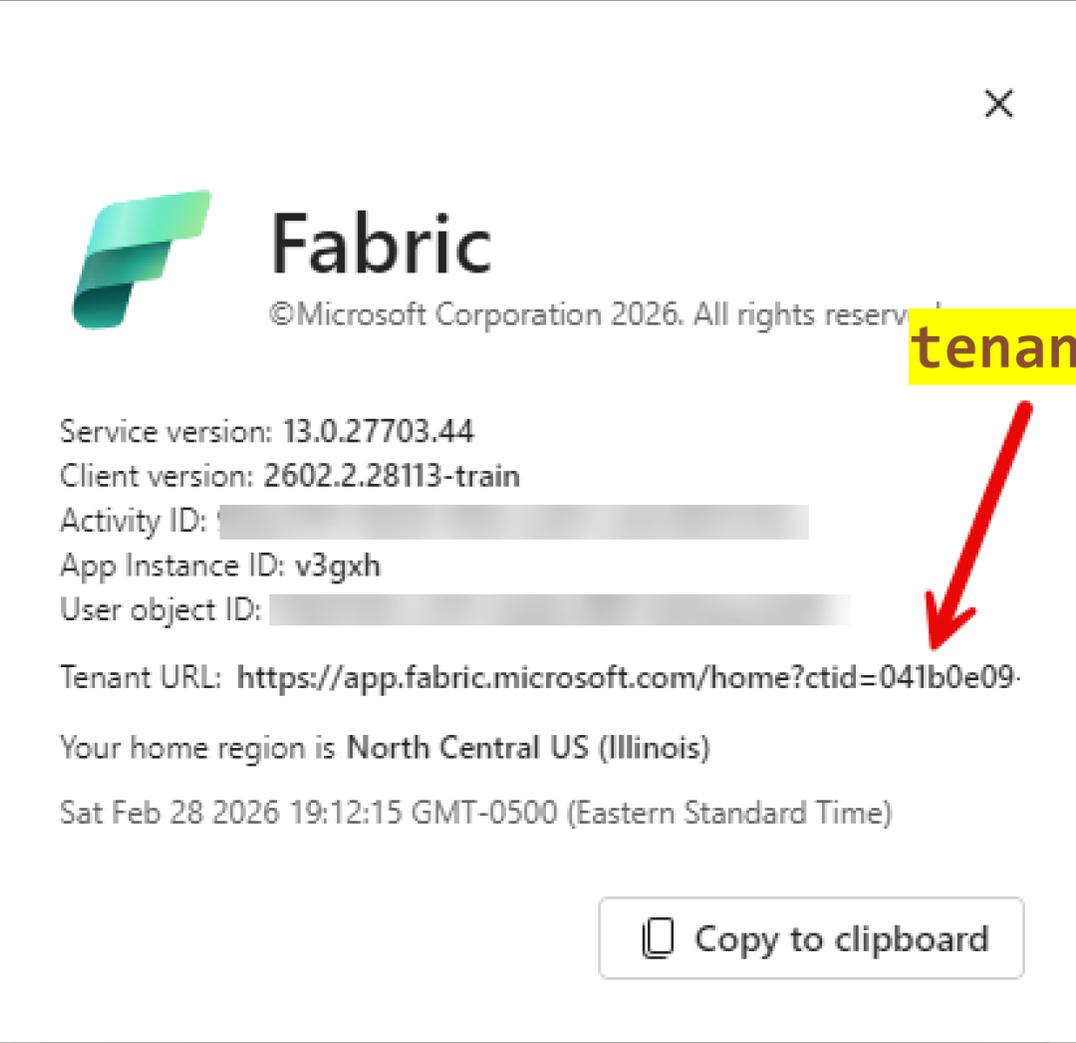
Private Link JSON

```
{
  "$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



The screenshot shows the Fabric application interface. At the top left is the Fabric logo. To its right is the word "Fabric" and the copyright notice "©Microsoft Corporation 2026. All rights reserved". Below this, the following information is displayed:

- Service version: 13.0.27703.44
- Client version: 2602.2.28113-train
- Activity ID: [redacted]
- App Instance ID: v3gxx
- User object ID: [redacted]
- Tenant URL: <https://app.fabric.microsoft.com/home?ctid=041b0e09>
- Your home region is North Central US (Illinois)
- Sat Feb 28 2026 19:12:15 GMT-0500 (Eastern Standard Time)

A "Copy to clipboard" button is located at the bottom right of the interface. A red arrow points from the "tenant-id" label to the "ctid" parameter in the Tenant URL. Another red arrow points from the "workspace-id" label to the "68" in the URL below.

tenant-id

workspace-id

<https://app.fabric.microsoft.com/groups/68> }49/list?experience=fabric-developer

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 *  

Resource type *  

Resource *  

Target sub-resource *  

Disabling Public Access from Workspace

The screenshot shows the 'Workspace settings' interface in Azure. On the left is a navigation menu with categories like 'General', 'Workspace type', 'Azure connections', 'System storage', 'Git integration', and 'OneLake'. The main area is titled 'Inbound networking' and contains a warning message: 'Workspace private links are included when either option is selected. If you select the Allow connections from selected networks and workspace-level private links option and don't configure any additional settings here, this workspace can only be accessed using workspace-level private links. To use workspace private links, you need to complete additional set up steps in Azure. [Learn more](#)'. Below this, there are two radio button options: 'Allow all connections to this workspace (including private links)' and 'Allow connections from selected networks and workspace level private links'. The second option is selected. Under the selected option, there is a section for 'Address configurations' which is currently 'Not configured'. At the bottom right, there are 'Apply' and 'Cancel' buttons. A white dialog box is overlaid on the screen with the title 'Some users might lose access' and the text: 'If your IP rules or connection settings don't include all networks where users connect from, some users may lose access to this workspace. You may also lose access if your own network isn't included.' The dialog box has 'Continue' and 'Cancel' buttons.

Disabling Public Access with Code

```
9  $url = "https://api.fabric.microsoft.com/v1/workspaces/$(workspaceID)/networking/communicationPolicy"
10
11 # Full policy body (must include both inbound and outbound)
12 $body = @{
13     inbound = @{
14         publicAccessRules = @{
15             defaultAction = "Deny"
16         }
17     }
18     outbound = @{
19         publicAccessRules = @{
20             defaultAction = "Allow"
21         }
22     }
23 } | ConvertTo-Json -Depth 5
24
25 # Make PUT request
26 $response = Invoke-RestMethod -Uri $url -Method Put -Headers @{
27     Authorization = "Bearer $($token.accessToken)"
28     "Content-Type" = "application/json"
29 } -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

Workspace settings

- General
- License info
- Azure connections
- System storage
- Git integration
- OneLake
- Workspace identity
- Outbound networking**
- Inbound networking
- Encryption
- Monitoring

- Power BI
- Delegated Settings
- Data Engineering/Science
- Data Factory
- Data Warehouse

Managed private endpoints let people securely connect to an Azure resource or Private Link service. [Learn more](#)

Managed private endpoints

Managed private endpoints are currently available for notebooks and Spark job definitions. [Learn more](#)

+ Create Refresh Delete



No endpoints to show

Outbound access protection

Block outbound public access Off

Block outbound public access feature has been disabled on this workspace. [Learn more](#)

Block all outbound connections from workspace and only allow connections through private end points and connection rules. This feature is only available for limited items. Creation of other items will be disabled once this feature is turned on. Please wait for 15 mins for the setting change to take effect. [Learn more](#)

Allow Git Integration Off

Use all Git features, like commit and sync, for the repository connected to this workspace. If this is off, Git integration will be blocked.

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

[us/fabric/security/workspace-outbound-access-protection-overview](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>

Workspace settings

- General
- Workspace type
- Azure connections
- System storage
- Git integration
- OneLake
- Workspace identity
- Outbound networking**
- Inbound networking
- Encryption
- Monitoring

- Power BI
- Delegated Settings
- Data Engineering/Science
- Data Factory
- Data Warehouse

Network security

Managed private endpoints let people securely connect to an Azure resource or Private Link service. [Learn more](#)

Managed private endpoints

Managed private endpoints are currently available for notebooks and Spark job definitions. [Learn more](#)

+ Create Refresh Delete



No endpoints to show

Outbound access protection

Block outbound public access Off

Block all outbound connections from workspace and only allow connections through private end points and connection rules. This feature is only available for limited items. Creation of other items will be disabled once this feature is turned on. Please wait for 15 mins for the setting change to take effect. [Learn more](#)

Allow Git Integration Off

Use all Git features, like commit and sync, for the repository connected to this workspace. If this is off, Git integration will be blocked.

Outbound Access Protection

Outbound access protection

Block outbound public access



Off

Block all outbound connections from workspace and only allow connections through private end points and connection rules. This feature is only available for limited items. Creation of other items will be disabled once this feature is turned on. Please wait for 15 mins for the setting change to take effect. [Learn more](#) 

Allow Git Integration



Off

Use all Git features, like commit and sync, for the repository connected to this workspace. If this is off, Git integration will be blocked.

Block outbound access on this workspace?

Block Outbound public access is only available for a limited set of items. Creation of other items will be disabled.

I understand that certain artifacts cannot be created once this setting is enabled.

Yes

Cancel

Workspace Managed Identity

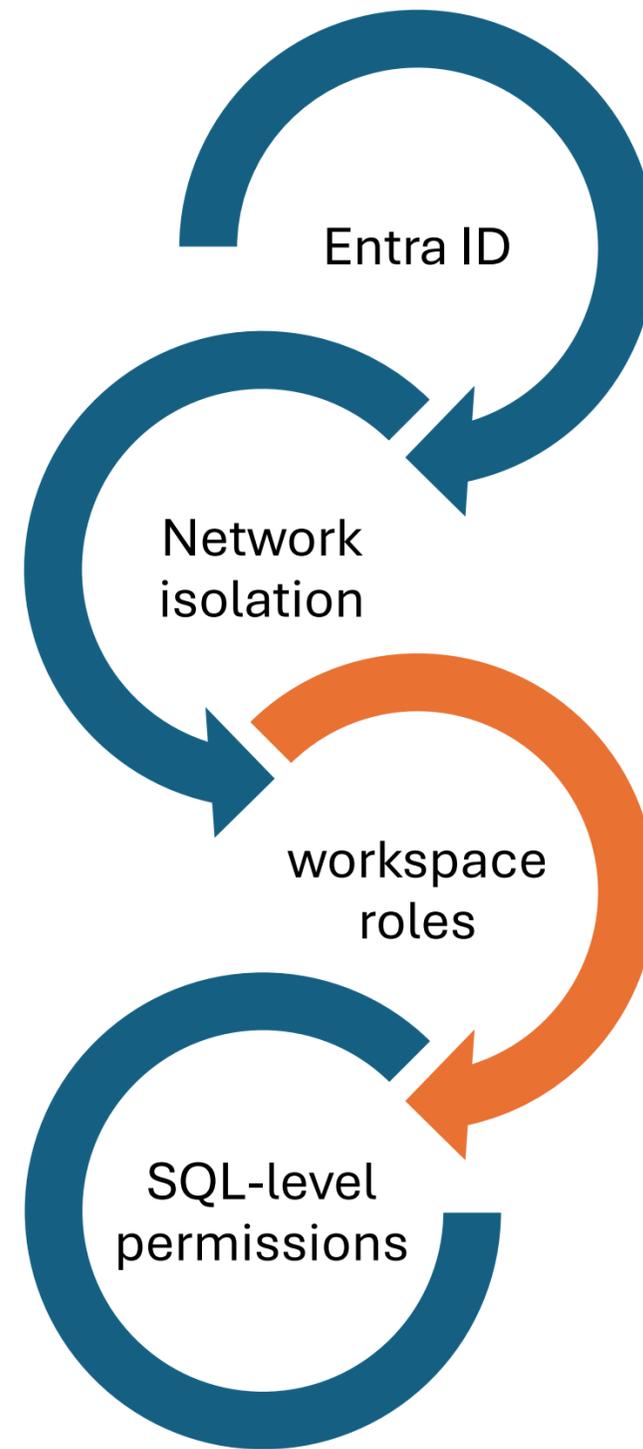
Secure Access to External Data

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

← Add people ×
Warehouse Security - The Shield

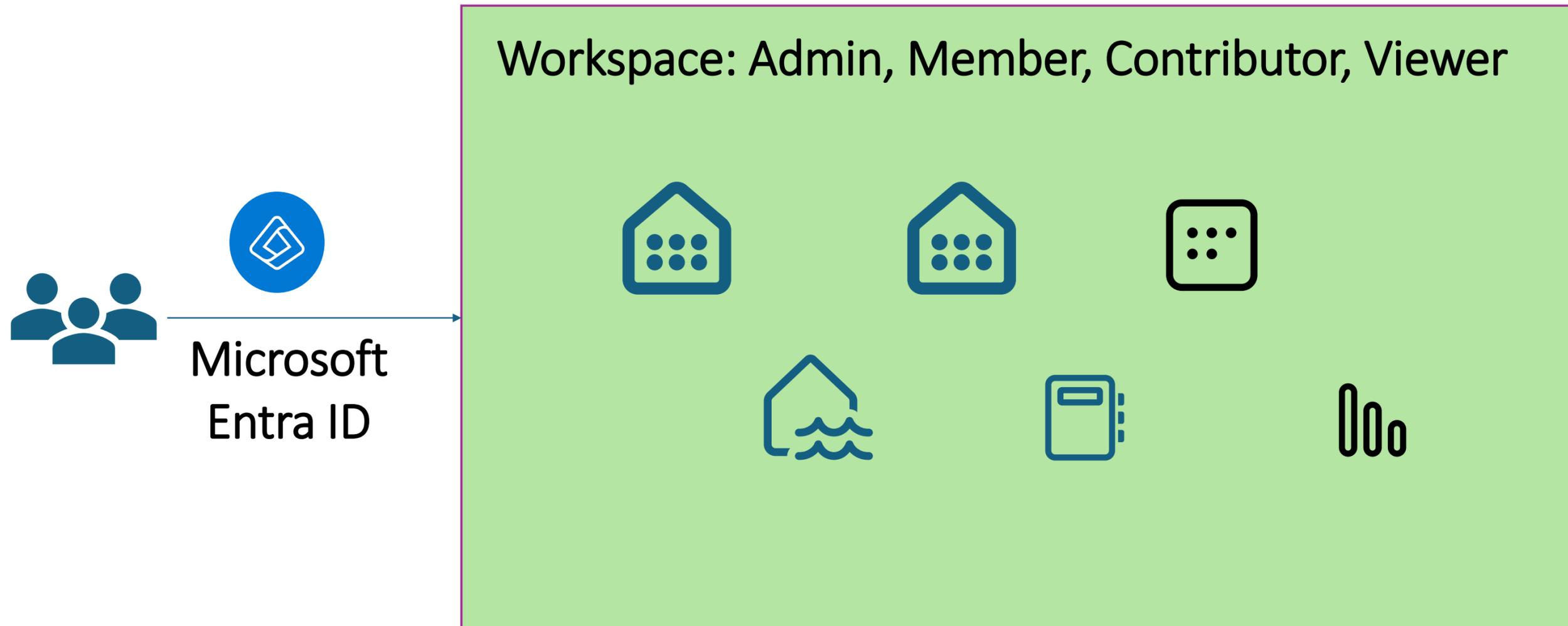
Admins, members, and contributors have edit and view access. Viewers only have view access. [Learn more](#) ↗ ×

Enter name or email

Viewer ▾ Add

- Admin
- Member
- Contributor
- Viewer

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>

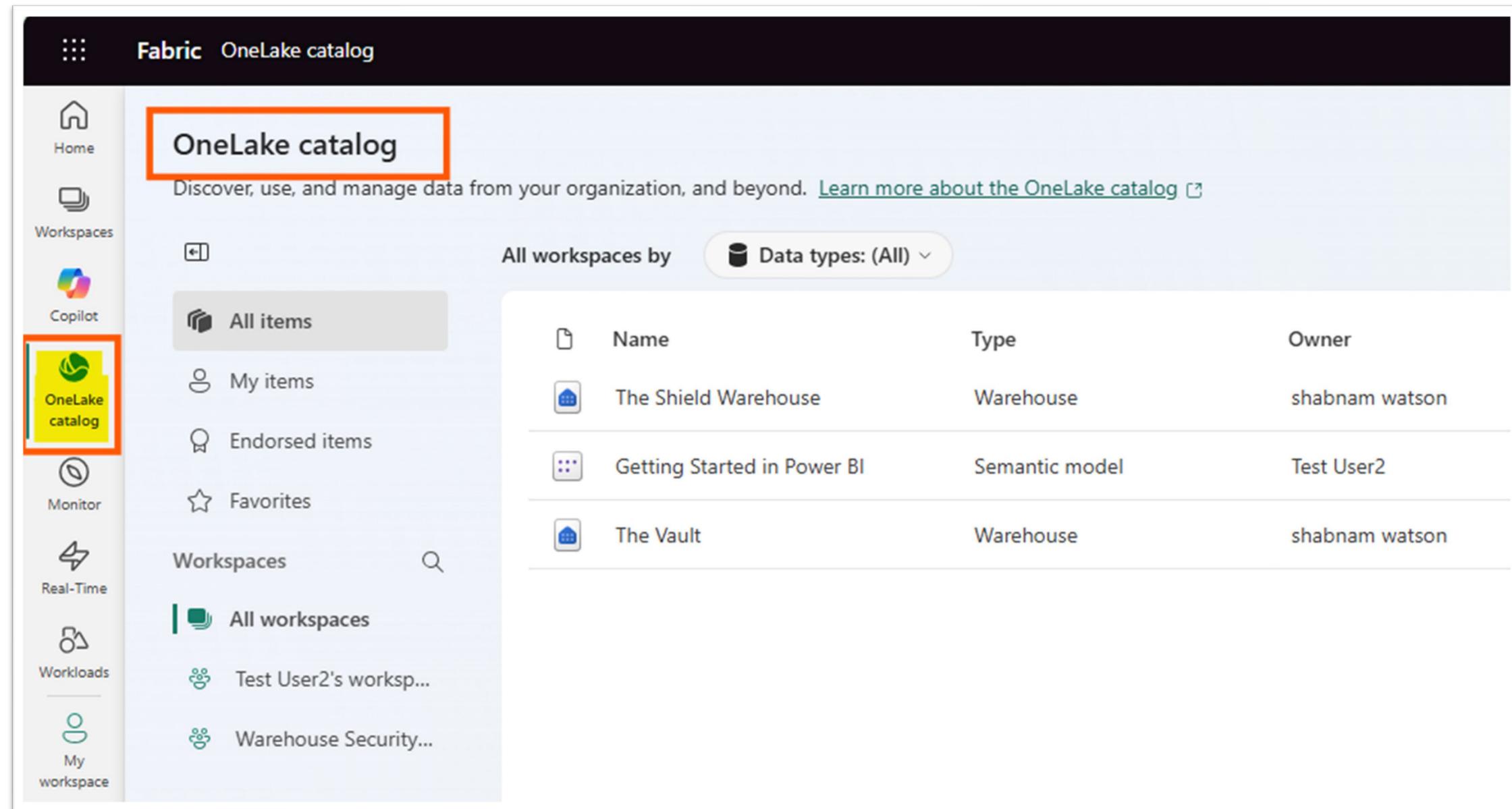
Workspace Roles

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



The screenshot displays the Microsoft Fabric OneLake catalog interface. The left sidebar contains navigation options: Home, Workspaces, Copilot, OneLake catalog (highlighted with a yellow box), Monitor, Real-Time, Workloads, and My workspace. The main content area is titled 'OneLake catalog' (highlighted with an orange box) and includes a description: 'Discover, use, and manage data from your organization, and beyond. [Learn more about the OneLake catalog](#)'. Below this, there are filters for 'All workspaces by' and 'Data types: (All)'. A table lists the workspaces:

Name	Type	Owner
The Shield Warehouse	Warehouse	shabnam watson
Getting Started in Power BI	Semantic model	Test User2
The Vault	Warehouse	shabnam watson

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

Warehouse Item level Permissions

Connect

ReadData (SQL)

ReadAll (Files)

Monitor

Audit

Reshare

Grant people access



The Shield Warehouse

People you share this warehouse with can connect to it. To give additional permissions, select them from the list.

Additional permissions

- Read all data using SQL (ReadData) ⓘ
- Read all OneLake data (ReadAll) and subscribe to events (SubscribeOneLakeEvents) ⓘ
- Build reports on the default semantic model (Build) ⓘ
- Monitor queries (Monitor) ⓘ
- Audit queries (Audit) - PREVIEW ⓘ
- Share granted permissions (Reshare) ⓘ

SQL Endpoint Item level Permissions

Connect

ReadData → All SQL data

ReadAll → All OneLake

Grant people access ×

The Shield Warehouse

People you share this warehouse with can connect to it. To give additional permissions, select them from the list.

Additional permissions

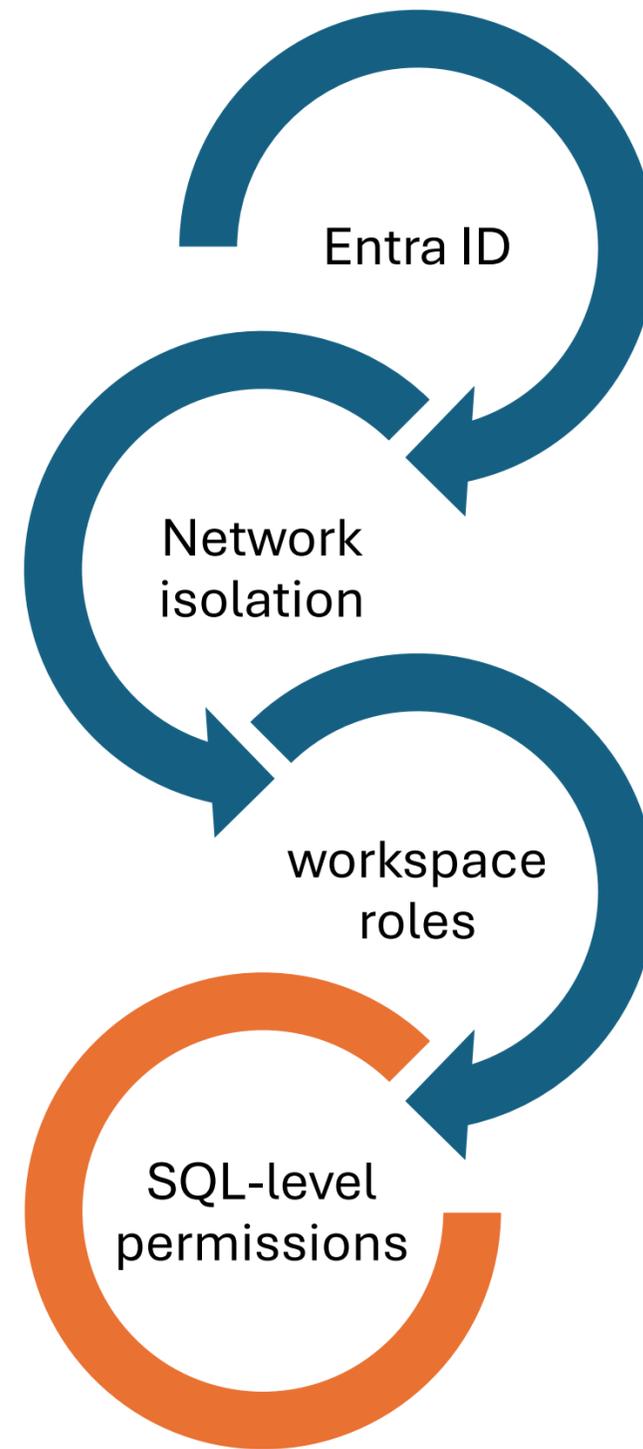
- Read all data using SQL (ReadData) ⓘ
- Read all OneLake data (ReadAll) and subscribe to events (SubscribeOneLakeEvents) ⓘ

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).	✓	✓	✓	

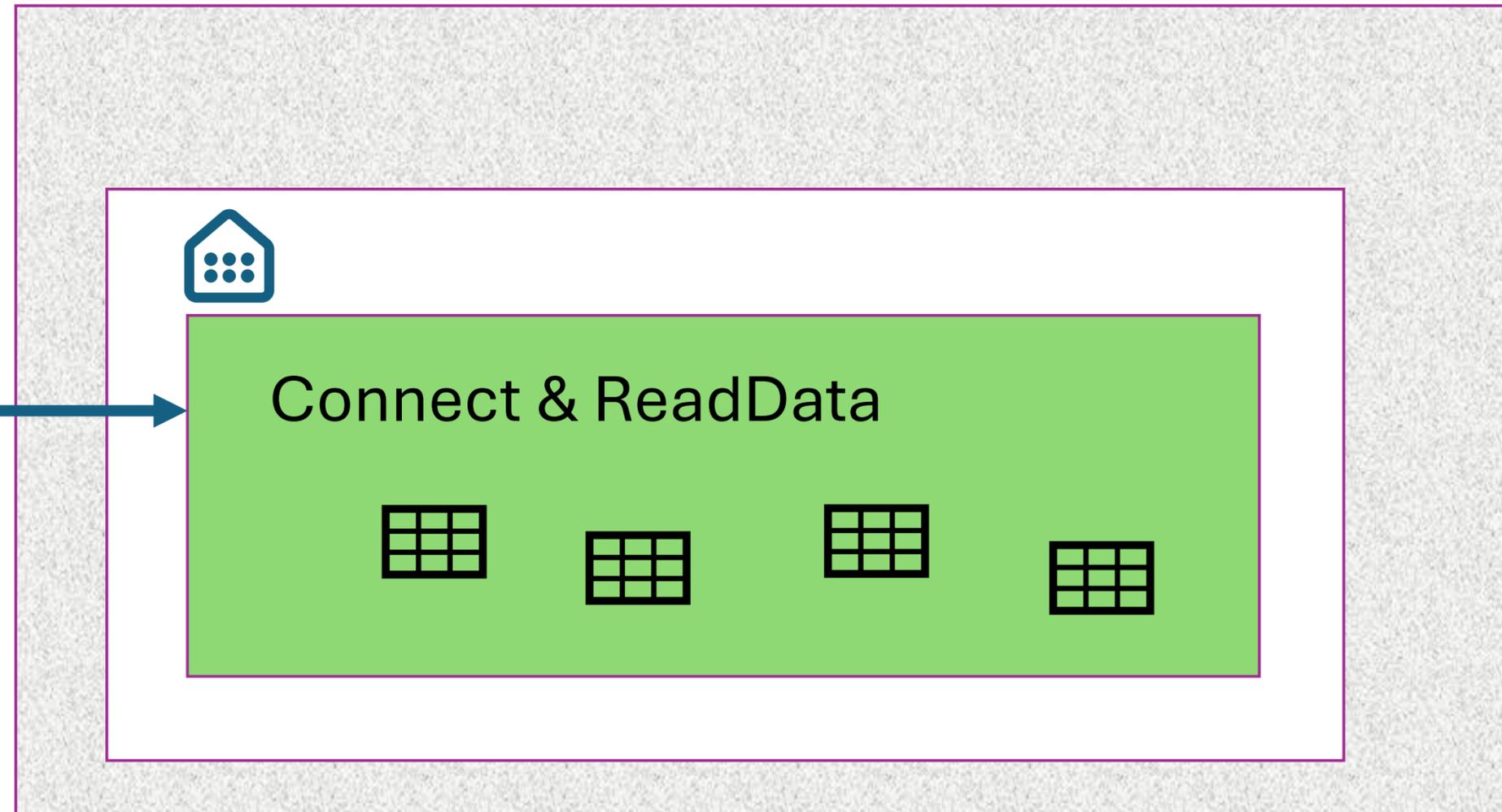
<https://learn.microsoft.com/en-us/fabric/fundamentals/roles-workspaces>

Warehouse Secured with

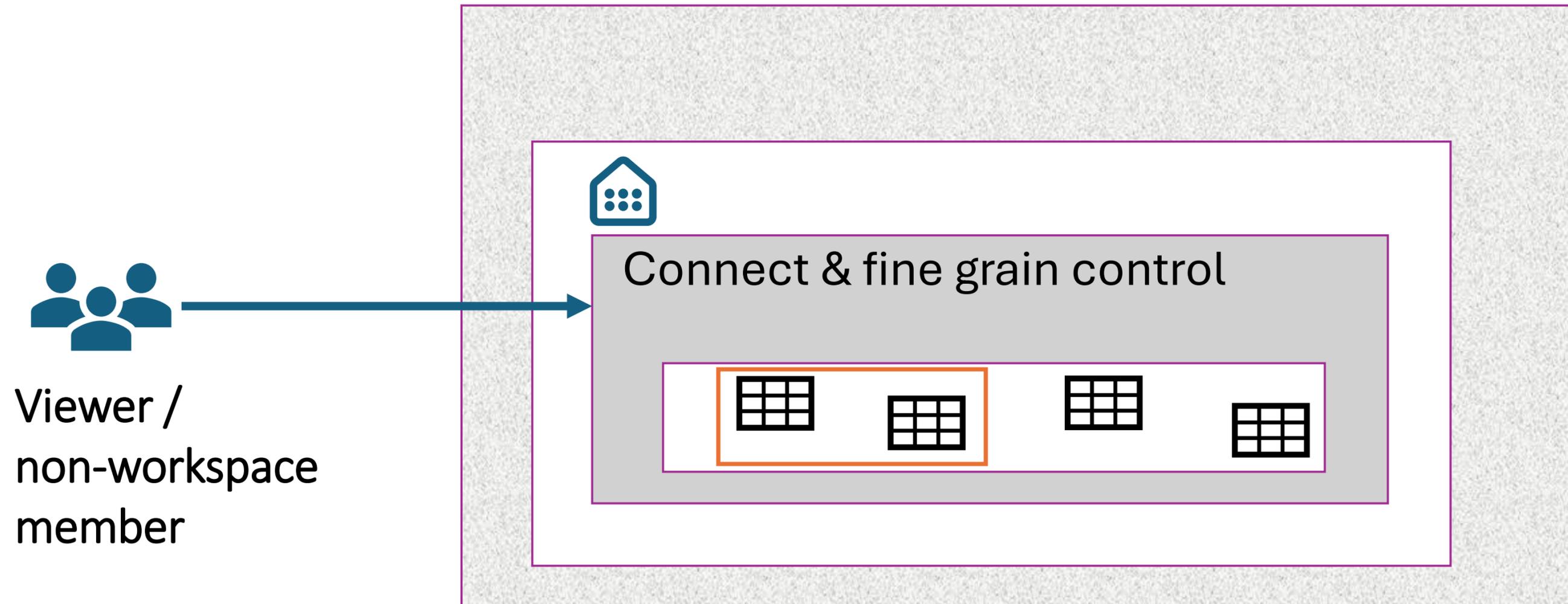


SQL Level Permissions

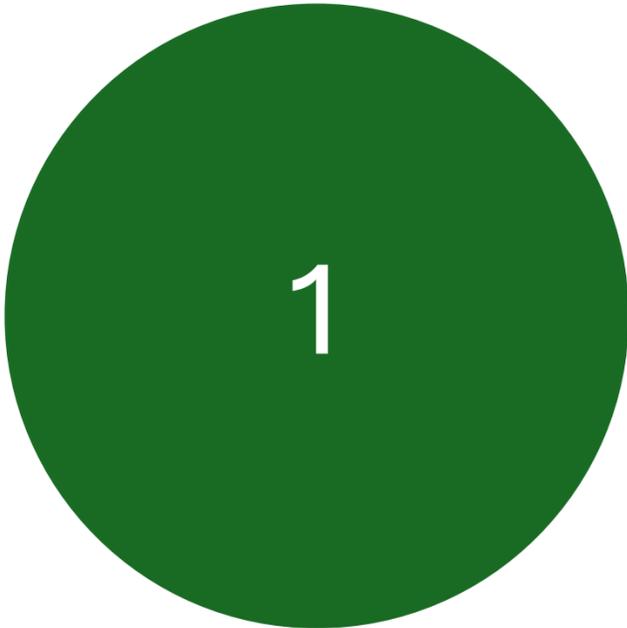
 Viewer /
non-workspace
member with
Connect and
ReadData



SQL Level Permissions: Object Level Security (OLS)



SQL-Level Permissions

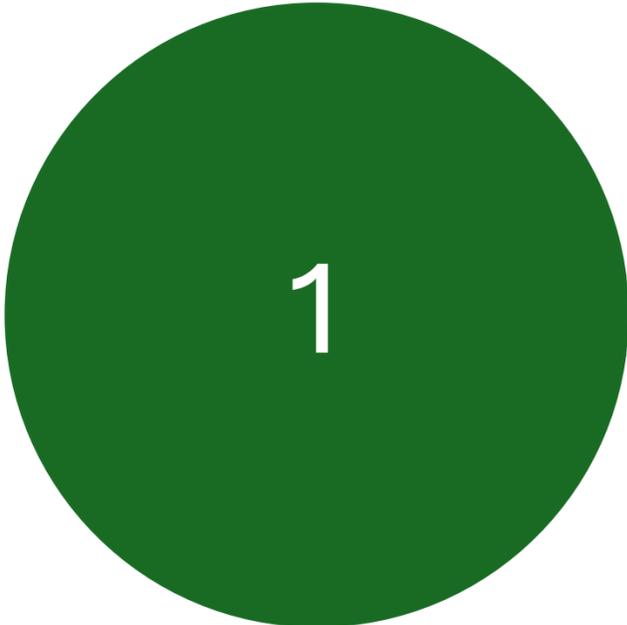


- Connect & ReadData
- Grant Update
 - Deny Select



- Connect
- Grant Select
 - Grant Update

SQL-Level Permissions



Grant Update, Insert ..
On Geography
To User1@....com



Grant Select
On Geography
To User3@....com

DENY

- Deny Select on dbo.Medallion to [TestUser1@....com](#)
- Deny has precedence over ReadData even for workspace viewers

The screenshot shows a SQL query execution interface. On the left, a tree view shows the database structure: Warehouses > The Shield Warehouse > Schemas > dbo > Tables. The tables listed are Customer, CustomerMasked, Date, Geography, HackneyLicense, and Orders. The main query editor shows the following SQL query:

```
1 SELECT * FROM dbo.Medallion
```

Below the query editor, the Messages pane shows the following error message:

10:40:51 AM Started executing on line 1
Msg 373, Level 14, State 5, Line 1
The SELECT permission or external policy action 'Microsoft.Sql/Sqlservers/Databases/Schemas/Tables/Rows/Select' was denied on the object 'Medallion', database 'The Shield Warehouse', schema 'dbo'.

10:40:53 AM Query execution time: 00:00:00.007 | Time to process and render results: 00:00:01.644 | Total duration: 00:00:01.651

REVOKE

Remove a previously granted permission.

Revoke Select On MyTable To [UserA];

CONTROL

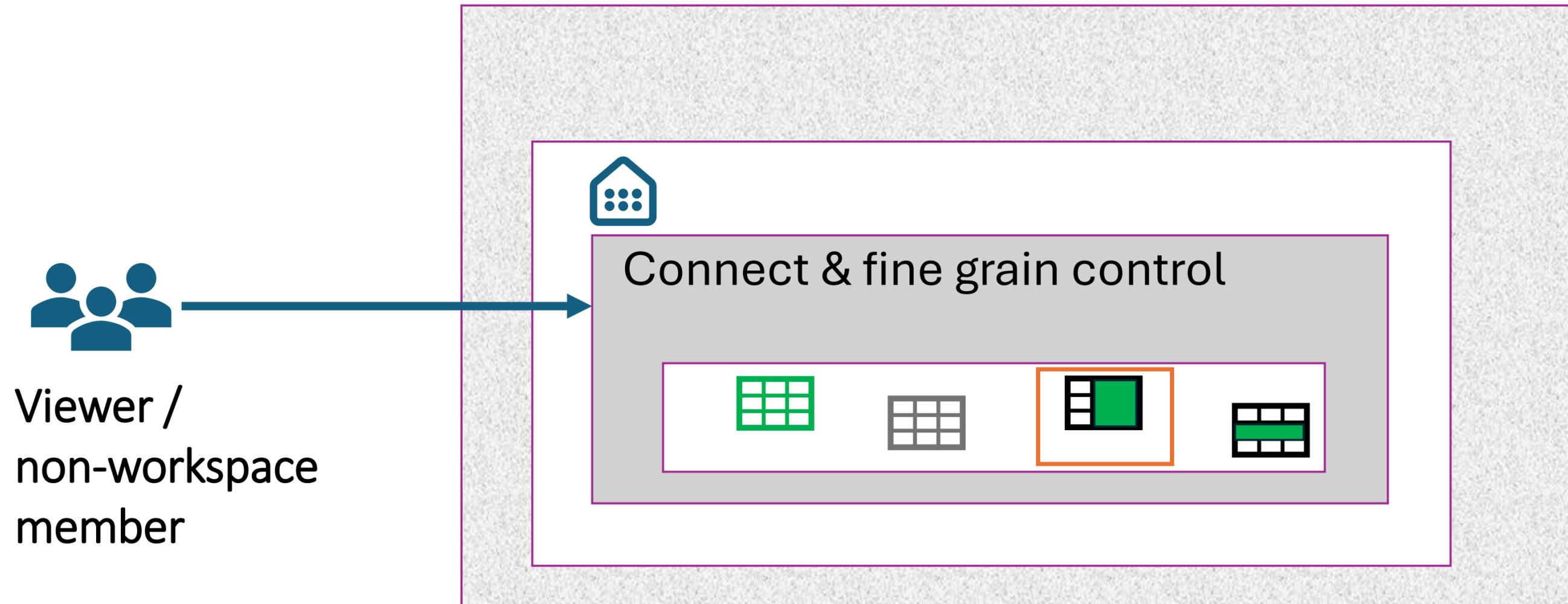
Gives a principal (user or role) **full access** to a securable

Grant Control on Table to User

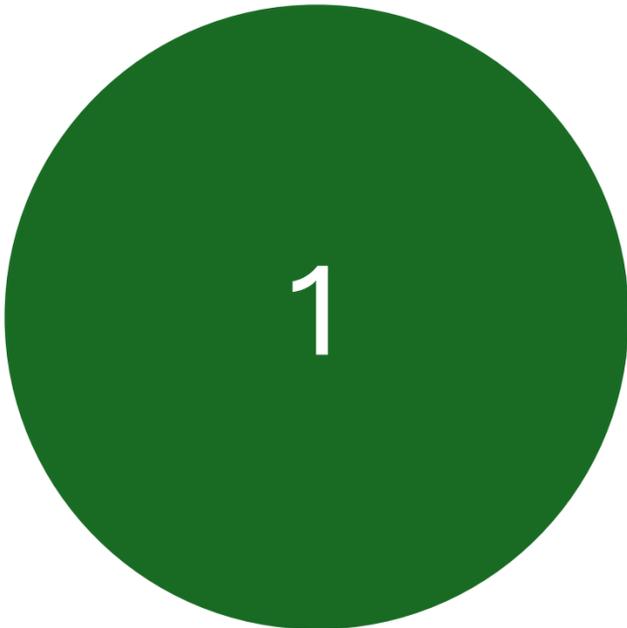
Use sparingly

Does not overwrite Deny

SQL Level Permissions: Column Level Security (CLS)



SQL-Level Permissions

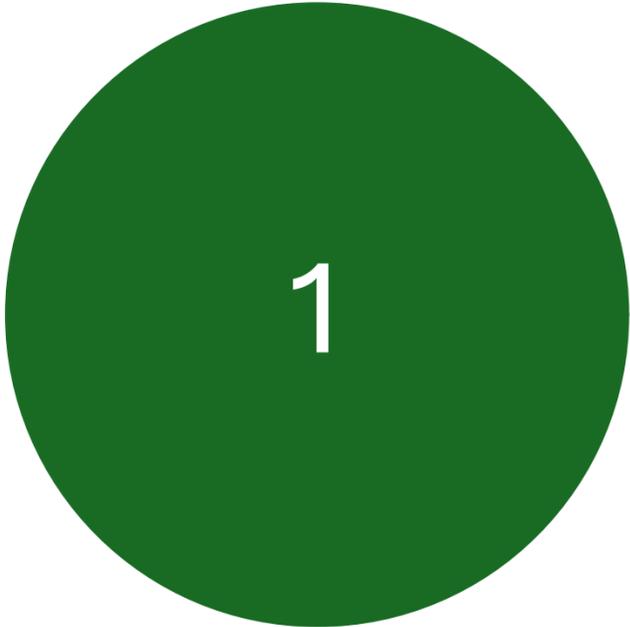


- Connect & ReadData
- Grant Update
 - Deny Select



- Connect
- Grant Select
 - Grant Update

SQL-Level Permissions

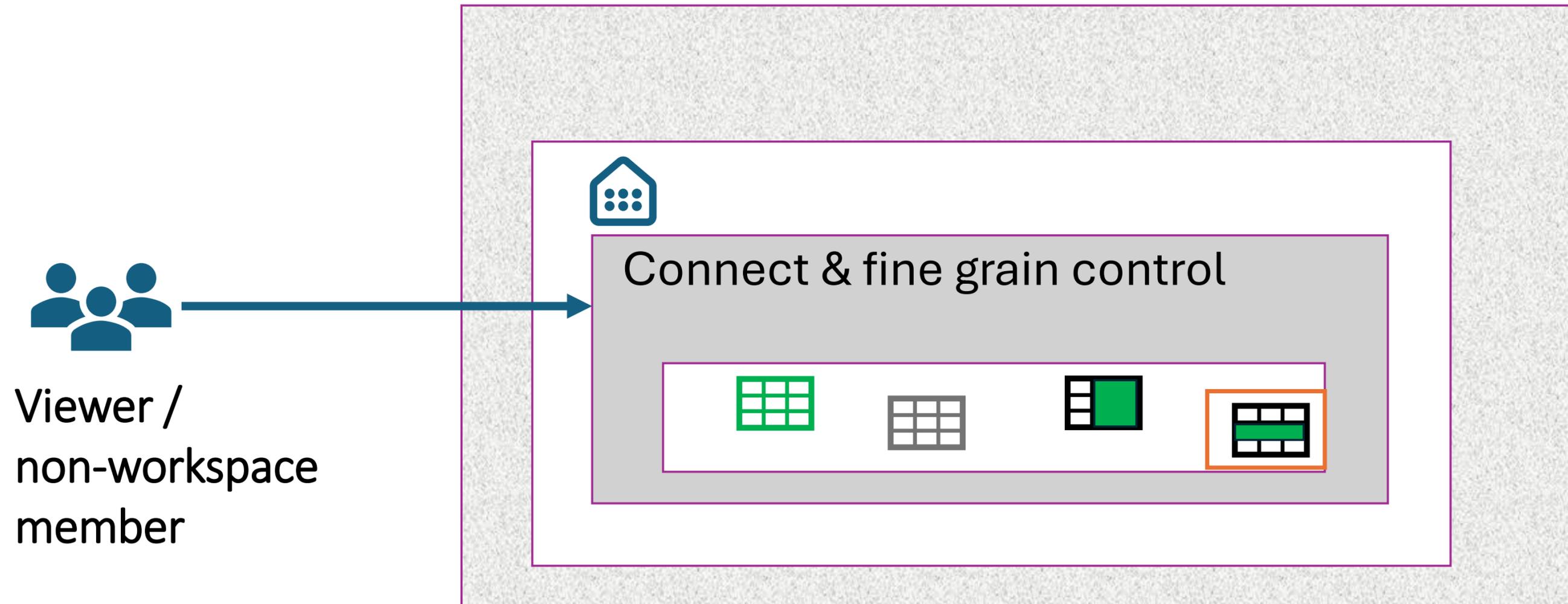


Deny Select
On Customer(BirthDate)
To [User2@...com]



Grant Select On Customer(Name,
Phone)
To [User3@....com]

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, "XXXXXXXXXXXX", 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,"XXXXXXXXXX",4)'),  
    PhoneNumber VARCHAR(15) MASKED WITH (FUNCTION =  
'partial(0,"XXXXXXXXXX",4)') ,  
    EmailAddress VARCHAR(100) MASKED WITH (FUNCTION = 'email()')  
);
```

Dynamic Data Masking Example

	123 CustomerID	ABC FirstName	ABC LastName	123 Age	BirthDate	ABC CreditCardNumber	ABC PhoneNumber	ABC 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..

	123 CustomerID	ABC FirstName	ABC LastName	123 Age	BirthDate	ABC CreditCardNumber	ABC PhoneNumber	ABC EmailAddress
1	25	S-ah	xxxx	26	1900-01-01	XXXXXXXXXXXX8628	XXXXXXXXXXXX2586	sXXX@XXXX.com
2	122	A-am	xxxx	100	1900-01-01	XXXXXXXXXXXX8311	XXXXXXXXXXXX8784	aXXX@XXXX.com
3	131	B-ey	xxxx	79	1900-01-01	XXXXXXXXXXXX1140	XXXXXXXXXXXX6448	bXXX@XXXX.com
4	146	L-ay	xxxx	91	1900-01-01	XXXXXXXXXXXX1497	XXXXXXXXXXXX6488	lXXX@XXXX.com
5	211	P-ia	xxxx	93	1900-01-01	XXXXXXXXXXXX2282	XXXXXXXXXXXX4161	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

The screenshot shows the Microsoft Fabric Explorer interface. On the left, the 'Explorer' pane shows a tree view with 'Source_Lakehouse' expanded to 'Files'. The main pane displays a table of files:

Date modified	Type
8/5/2025, 9:42:11 AM	csv
8/3/2025, 12:34:45 PM	csv
8/3/2025, 12:53:05 PM	csv
9/3/2025, 12:02:26 PM	parquet

A 'File properties' dialog box is open on the right, showing details for 'customers.parquet':

- Name: customers.parquet
- Type: Unknown
- URL: <https://onelake.dfs.fabric.microsoft.com/Workspace-ID/Lakehouse-ID/Files/customers.parquet>

```
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.linkedin.com/company/shabnamwatson/)

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

 [@shbWatson](https://twitter.com/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



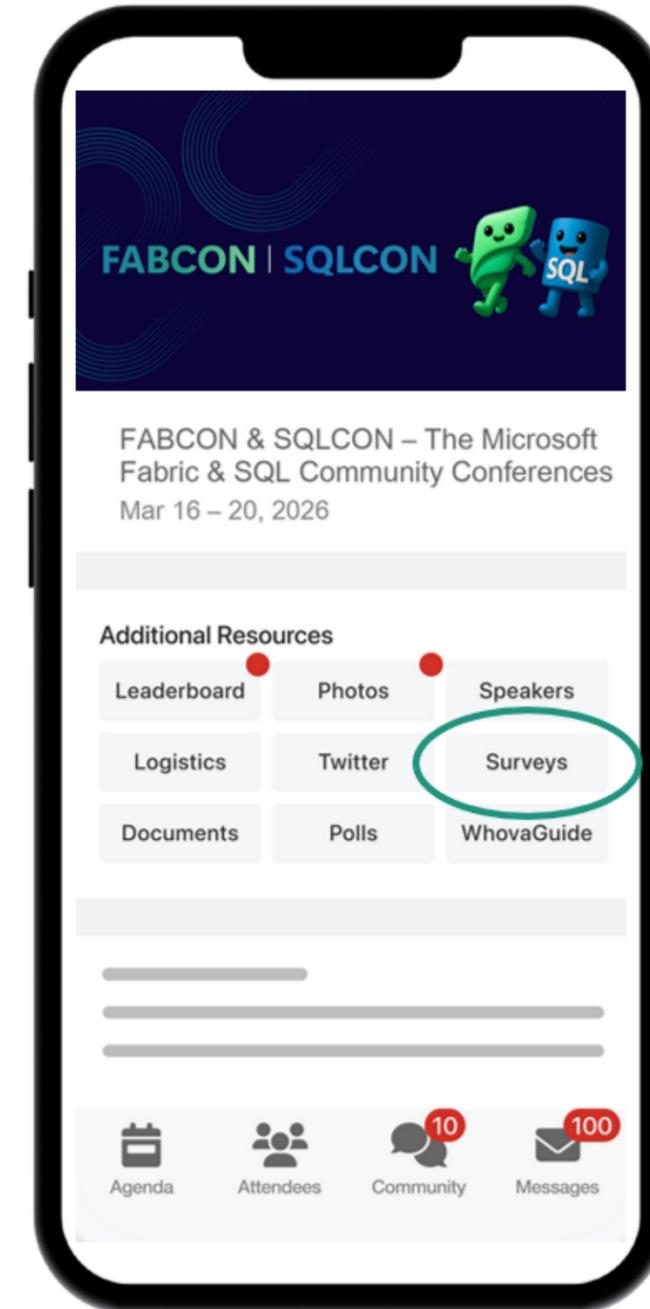
Influence our SQL roadmap and ensure it meets your real-life needs

<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>

