





Building a Fortress of Your Fabric Environment: Security Best Practices for

Erwin de Kreuk

Technology Lead Data
InSpark



Dutchfabricusergroup.com



linkedin.com/in/erwindekreuk



erwindekreuk.com



github.com/edkreuk

Let's connect



Thank you to our Fabric February Friends!

bouvet



twoday

KOKDI

sopra  steria

 Evidi

 Crayon
CONSULTING

 Profisee
Master Data Management

 Tabular Editor

 ANALYTICS
masterminds

 VASS

 Fraktal

 Microsoft

KURANT

ARROW

 EUROPEAN
MICROSOFT
FABRIC
Community Conference
BARCELONA 28 SEPT - 01 OCT 2024

 profitbase
PART OF HYPERGENE

 Capgemini

 fabric
FEBRUARY





Cybercriminals are
getting more
creative just like us



Data culture and AI transformation are happening now



78%

of organizations are implementing or developing a company wide data foundation¹



75%

of knowledge workers already using AI at work (doubled in the past 6 months)²



DATA SECURITY



Data is most secure if no one can access it.

DATA SECURITY



But...if no one can access data then you can't use it for anything.

Achieving both goals can prove challenging



Ensuring your data is secure

Fostering a data-driven culture



Agenda

Introduction

Challenges

Inbound Connections

Private Links

Outbound connections

Q & A



Fabric Security Whitepaper

Who has ever heard of the
Fabric Security Whitepaper?

Only 127 pages

[Microsoft Fabric security
white paper - Microsoft
Fabric | Microsoft Learn](#)

Introduction

Security is a top priority for any organization that wants to succeed in the digital age. You need to safeguard your assets from threats and follow your organization's security policies. This whitepaper serves as an end-to-end security overview for Microsoft Fabric. It covers details on how Microsoft secures your data by default as a SaaS service and how you can secure, manage, and govern the data stored in Microsoft Fabric as an organization.

The contents of this whitepaper is created by combining several security related online documents into a single whitepaper for reading convenience. This whitepaper will be updated regularly, but the online documentation will always be up to date. You can find the online documentation here: [Microsoft Fabric security - Microsoft Fabric | Microsoft Learn](#)

“

In the era of AI, security and governance practices are prerequisites for extracting valuable insights from data.¹

”



¹Chandana Gopal, Research Director, Enterprise Intelligence, IDC



AI & Data



AI is transforming the world





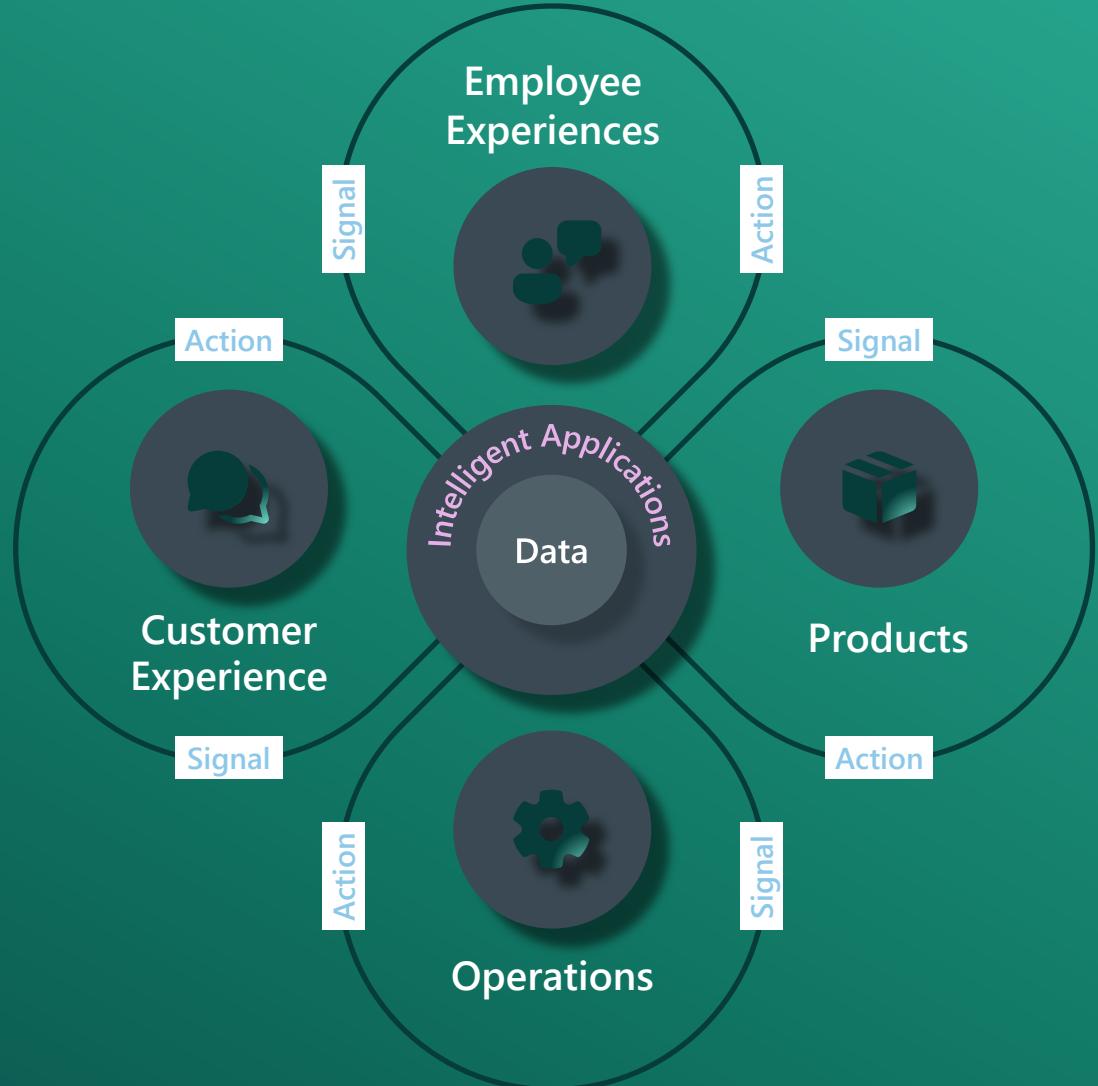
Data is the fuel
that *powers* AI



Data is the oxygen of our digital transformation

"A new kind of company — we call them insights driven businesses — has formed. They are growing at an average of more than 30% annually"

Forrester Analytics Business Technographics Global Data & Analytics Survey



Security : The Cornerstone of Microsoft Fabric

Security is paramount in the digital age, and Microsoft Fabric ensures your data is protected at every stage. By using Fabric, organizations can trust that their data is secure, allowing them to focus on innovation and growth.

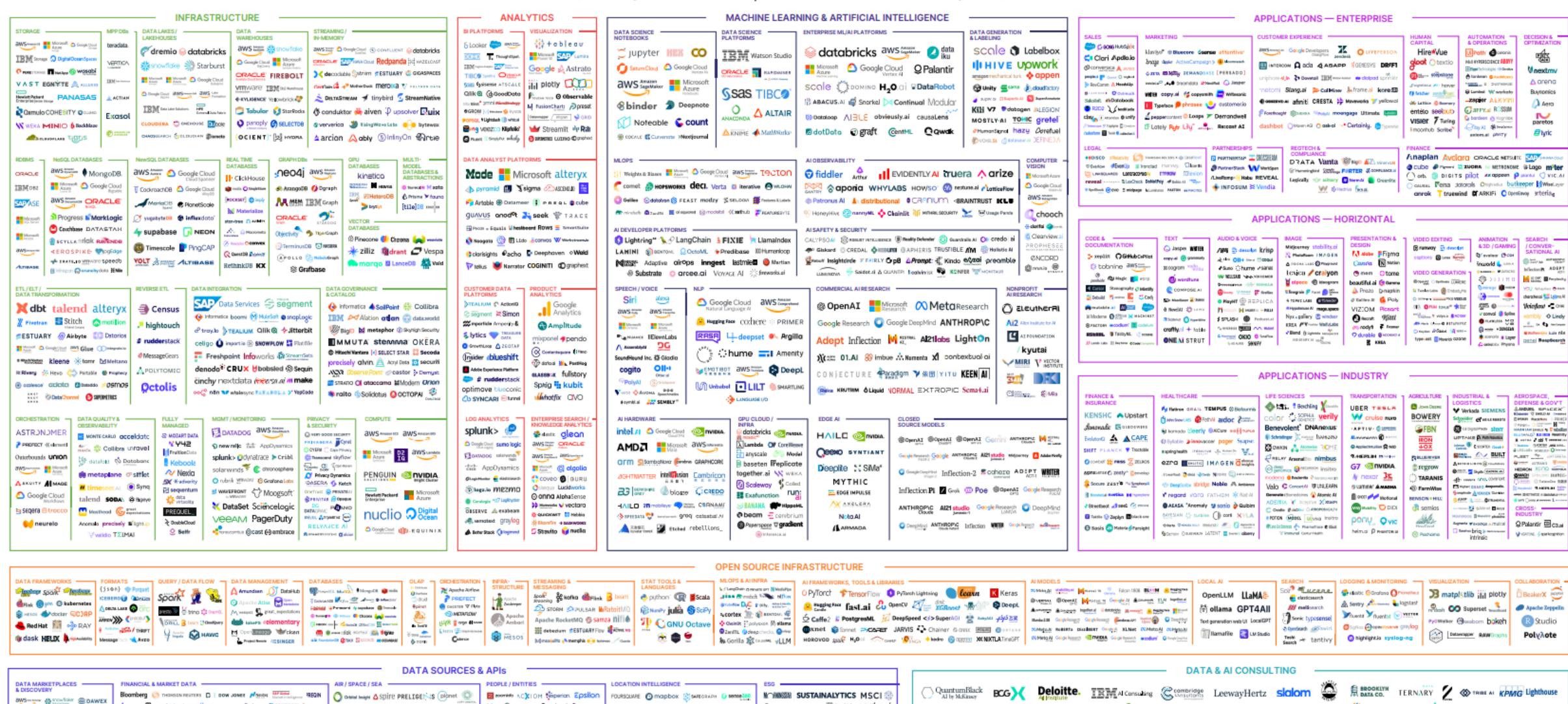


How do you translate data into competitive advantage



The 2025 ML, AI, and Data Landscape

THE 2024 MAD (MACHINE LEARNING, ARTIFICIAL INTELLIGENCE & DATA) LANDSCAPE





Microsoft Fabric

The unified data platform for AI transformation



Data
Factory



Analytics



Databases



Real-Time
Intelligence



IQ



Power BI



Copilot



OneLake

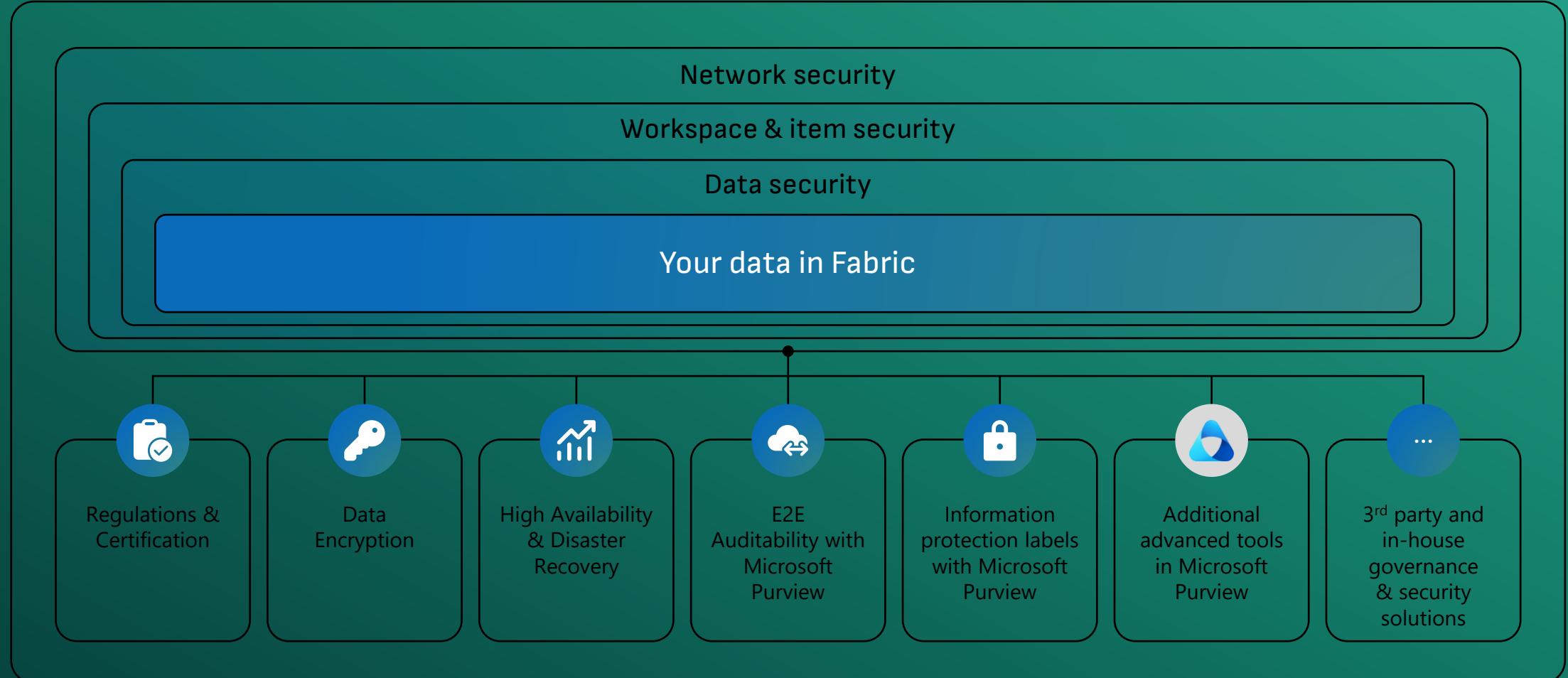


Governance

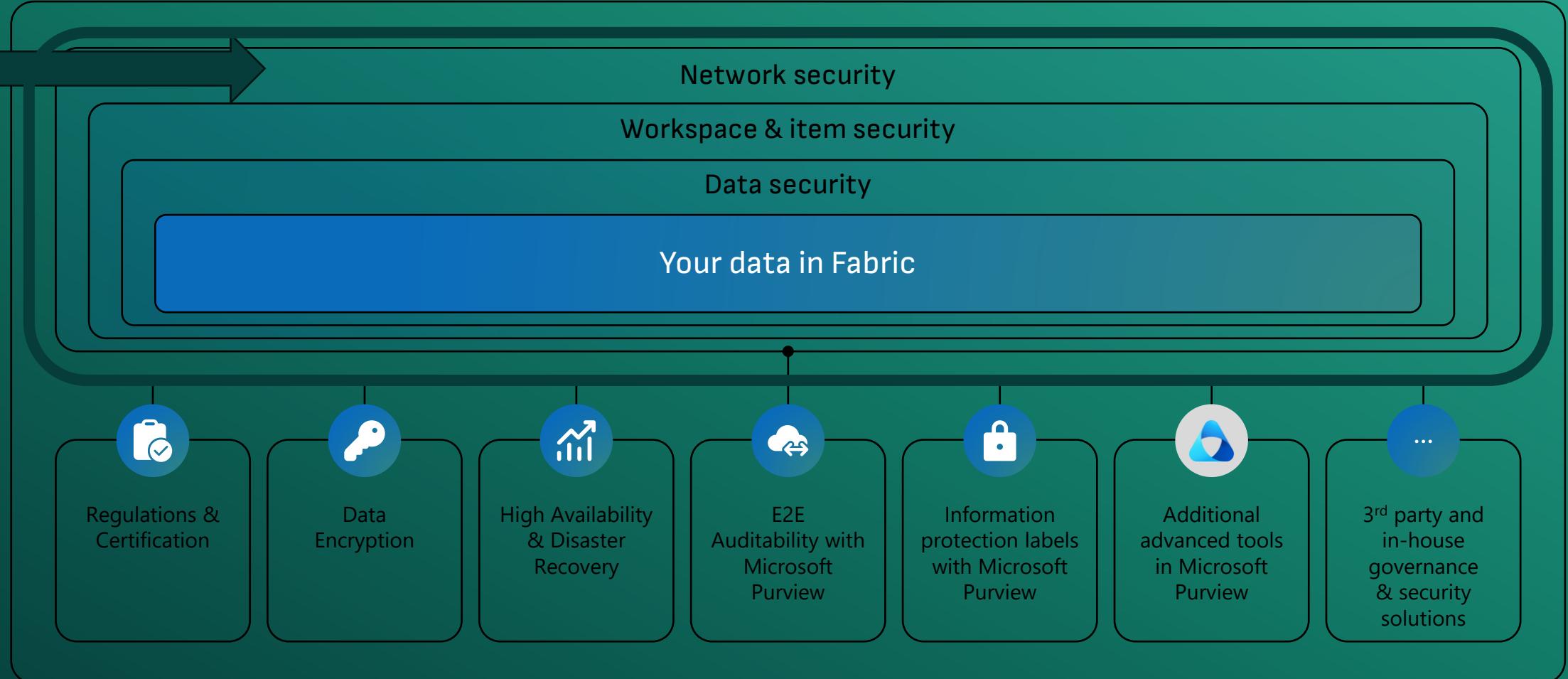
Fabric Platform



Security layers in Microsoft Fabric



Security layers in Microsoft Fabric

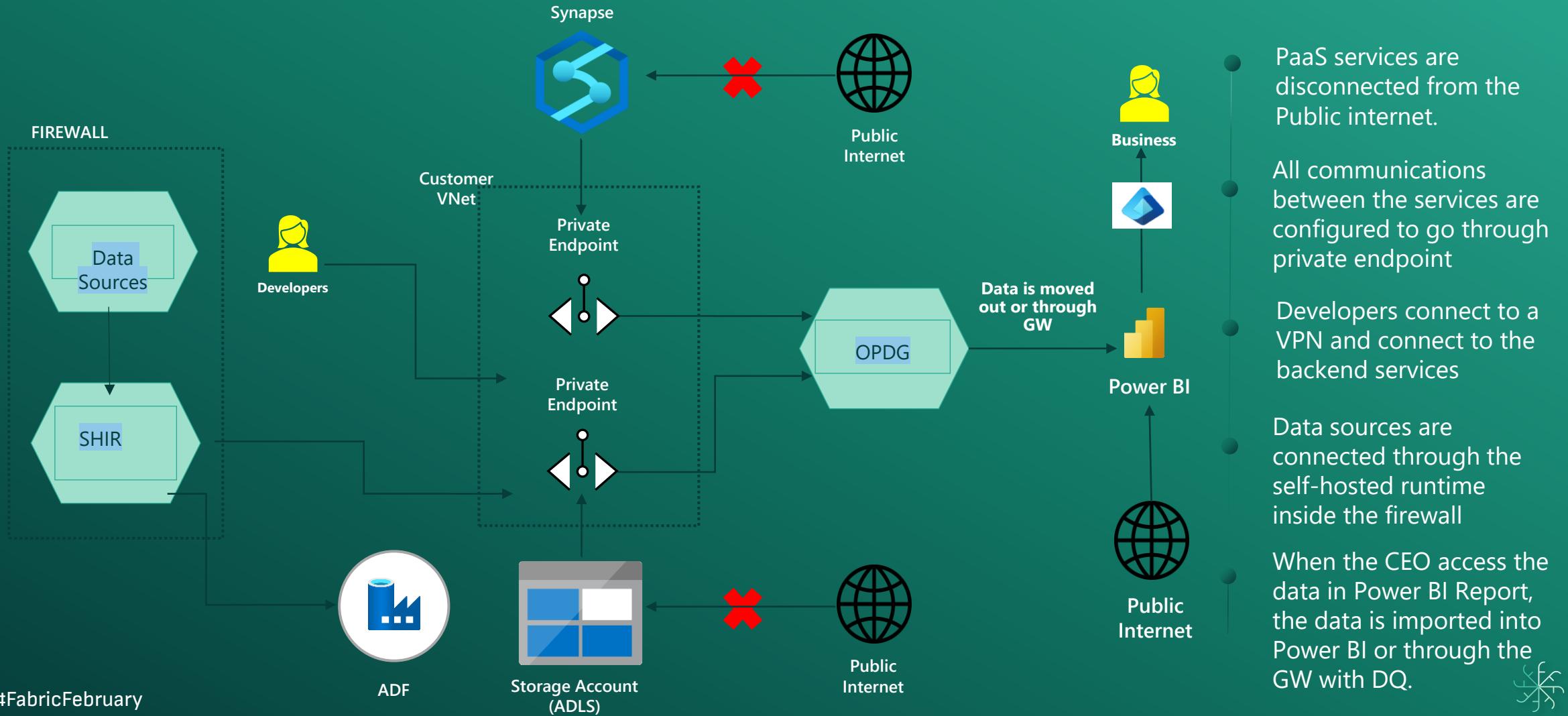


Modern data challenges

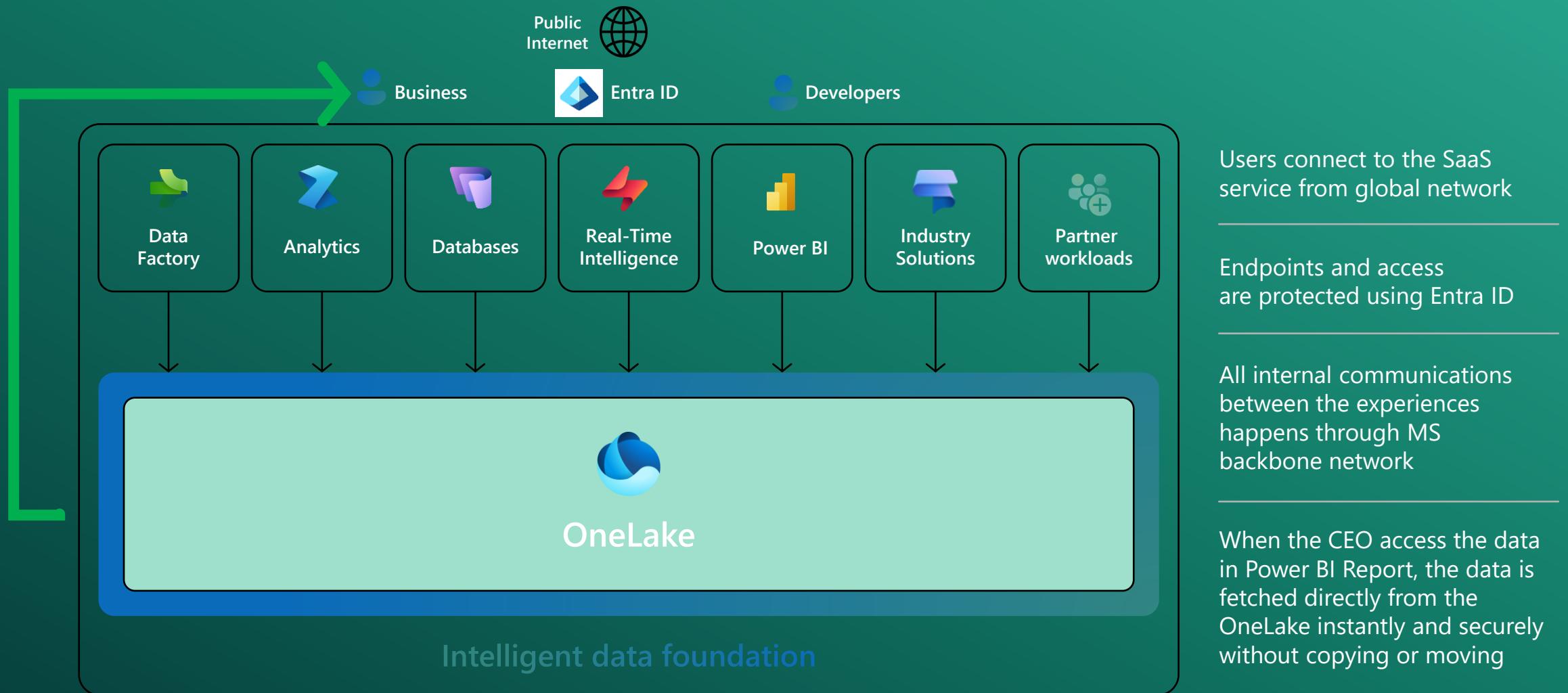
- Bring data to the masses, everyone should have access to data to make decisions
- Instant access to the latest data, no copying around
- Modern workforce, anywhere, any device
- At the same time, you need to secure, govern and audit your data to protect customers and the company
- SaaS platforms are designed with these challenges in mind.
- Shift from siloed PaaS to integrated SaaS



Existing PaaS World



Microsoft Fabric – SaaS World



Common network security requirements



- Secure access to your data in Fabric (Inbound Protection)
 - Conditional Access Policies
 - Private Link at a Tenant Level
 - Private Link at a Workspace level
 - Workspace IP Firewall



Restrict outbound access from a Fabric workspace (Outbound Protection)



Securely connect to data behind a firewall\private link from Fabric (Outbound Access)



Inbound protection options

Perimeter Network Security



From limited known locations

Zero Trust Approach



to unknown locations



New principles for Zero Trust in today's reality



Verify explicitly



Use least privilege access

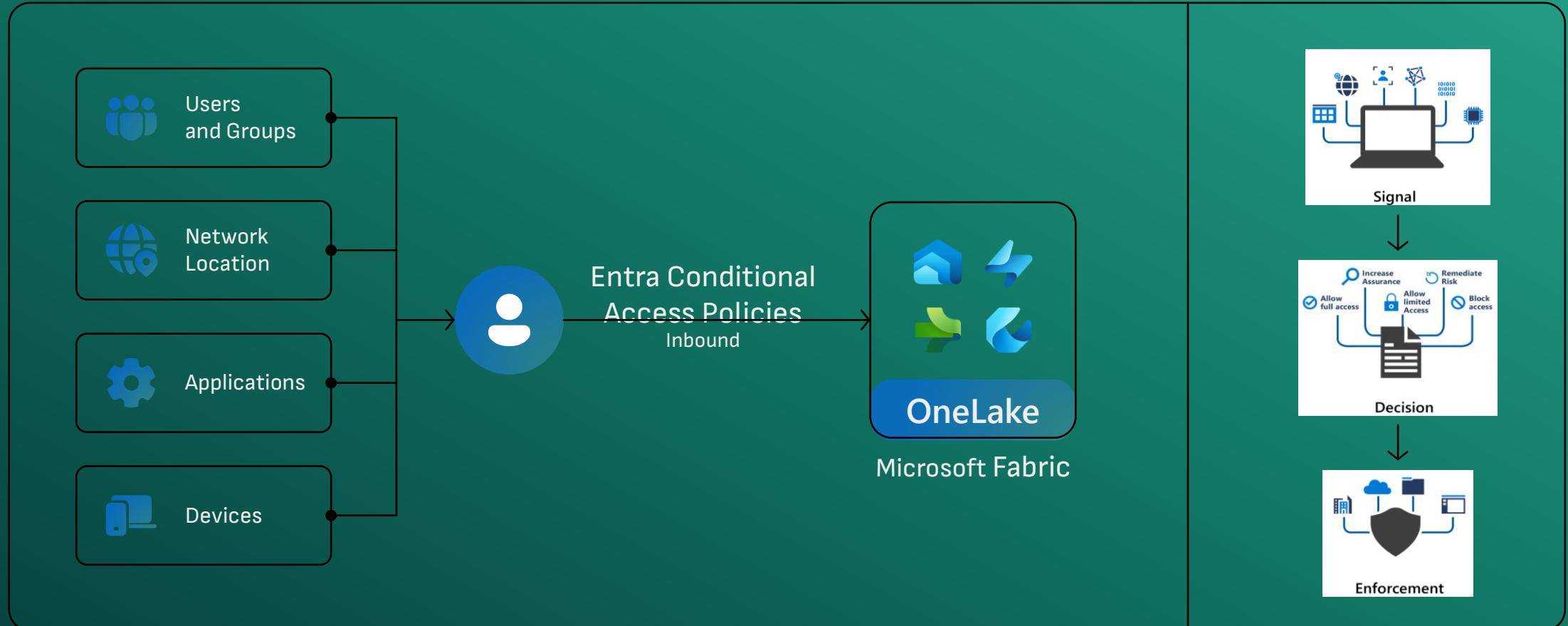


Assume breach



Conditional Access Policies

Common Decisions – Block, Grant, Require MFA



Entra ID Conditional Access



- Applications
- Protection
- Identity Governance
- External Identities
- ...

Protection

- Identity Protection
- Conditional Access
- Authentication methods
- Password reset
- Custom security attributes
- Risky activities
- ...

Identity Governance

Verified ID

Permissions Management

Global Secure Access

Microsoft Entra



InSpark Labs
(InSpark B.V.)

Tenant ID cd004ec9-bc4b-4...

Primary domain insparklab...

399

572

239

560

[View users](#)

[View groups](#)

[View devices](#)

[View apps](#)



Erwin de Kreuk
Global Administrator

a79b59b2-3de7-4c48-b6c8-...

[View user profile](#)

My role assignments



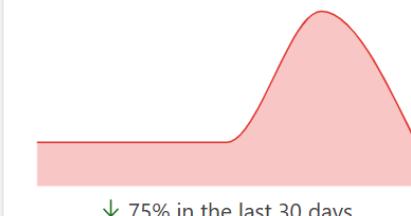
- High privileged role assignments
- Other role assignments

[Manage my roles](#)

Users at high risk

8 user detections with risk level "high" in the last 6 months.

[Learn more](#)



[View high risk users](#)

Tenant status



Identity Secure
Score
77.90%

[View recommendations](#)



Microsoft Entra
Connect
Enabled

[View Entra Connect](#)

Shortcuts

Add

User sign-ins

Audit logs

Authentication Methods

Blocked users

Domain names

Unused service principals

Manage tenants

Named locations

Cross-tenant Access Policies

Tenant restrictions

Risk Based Conditional Access policies

Risky sign-ins

Lifecycle workflows

Get the most out of your licenses and subscriptions

Deployment guides

Use these deployment guides to plan, configure and deploy Microsoft Entra capabilities

Microsoft Entra plan Entra Suite

Applications

Protection

Identity Governance

External Identities

Show more

Protection

Identity Protection

Conditional Access

Authentication methods

Password reset

Custom security attributes

Risky activities

Show more

Identity Governance

Verified ID

Permissions Management

Global Secure Access

Home > Conditional Access

Conditional Access | Named locations

Microsoft Entra ID

Overview

Policies

Insights and reporting

Diagnose and solve problems

Manage

Named locations

Custom controls (Preview)

Terms of use

VPN connectivity

Authentication contexts

Authentication strengths

Classic policies

Monitoring

Sign-in logs

Audit logs

Troubleshooting + Support

New support request

[Countries location](#) [IP ranges location](#)[Configure multi...](#)

Named locations are used by Microsoft Entra security reports to reduce the number of locations that are marked Trusted or configured in Conditional Access Policies cannot be trusted.

All Named Locations

Search by name

3 named locations found

Name	Location type
Block countries	Countries (IP)
The Netherlands	Countries (IP)
Untrusted Countries	Countries (IP)

New location (IP ranges)

[Upload](#) [Download](#)Configure named location IPv4 and IPv6 ranges. [Learn more](#)

Name *

 Mark as trusted location

Enter a new IPv4 or IPv6 range

ex: 40.77.182.32/27 or 2a01:111::/32

[Add](#)[Cancel](#)

- Applications
- Protection
- Identity Governance
- External Identities
- ... Show more

Protection

- Identity Protection
- Conditional Access
- Authentication methods
- Password reset
- Custom security attributes
- Risky activities
- ... Show more

Identity Governance

- Verified ID
- Permissions Management
- Global Secure Access

Home > Conditional Access | Overview

Microsoft Entra ID

[Overview](#)[Create new policy](#)[Create new policy from templates](#)

[Getting started](#)[Overview](#)[Coverage](#)[Monitoring \(Preview\)](#)[Tutorials](#)

[Refresh](#)[Got feedback?](#)

Policy Summary

Policy Snapshot

23 Enabled 23 Report-only 7 off

[View all policies](#)

Devices

100% of sign-ins in the last 7 days were from unmanaged or non-compliant devices

[See all noncompliant devices](#) [See all unmanaged devices](#)

Users

5 users signed in during the last 7 days without any policy coverage

[See all unprotected sign-ins](#)

Applications

Browse a list of applications that are not protected by your policies.

[View top unprotected apps](#)

What's new

The approved client app grant in Conditional Access is retiring in March 2026.

This control will no longer be enforced after March 2026. [Update your policy](#) to stay up to date.

[Learn more](#)

Named Locations

Microsoft Entra ID now supports IPv6! Update your Named locations with IPv6 ranges.

[Learn more](#)

4 policies have a Named Location condition

Applications

Protection

Identity Governance

External Identities

... Show more

Protection

Identity Protection

Conditional Access

Authentication methods

Password reset

Custom security attributes

Risky activities

... Show more

Identity Governance

Verified ID

Permissions Management

Global Secure Access

Home > Conditional Access | Overview >

New

...

Conditional Access policy

Control access based on Conditional Access policy to bring signals together, to make decisions, and enforce organizational policies.

[Learn more](#)

Name *

Example: 'Device compliance app policy'

Assignments

Users

0 users and groups selected

Target resources

No target resources selected

Network NEW

Not configured

Conditions

0 conditions selected

Access controls

Grant

0 controls selected

Session

0 controls selected

Enable policy

Grant

Control access enforcement to block or grant access. [Learn more](#)

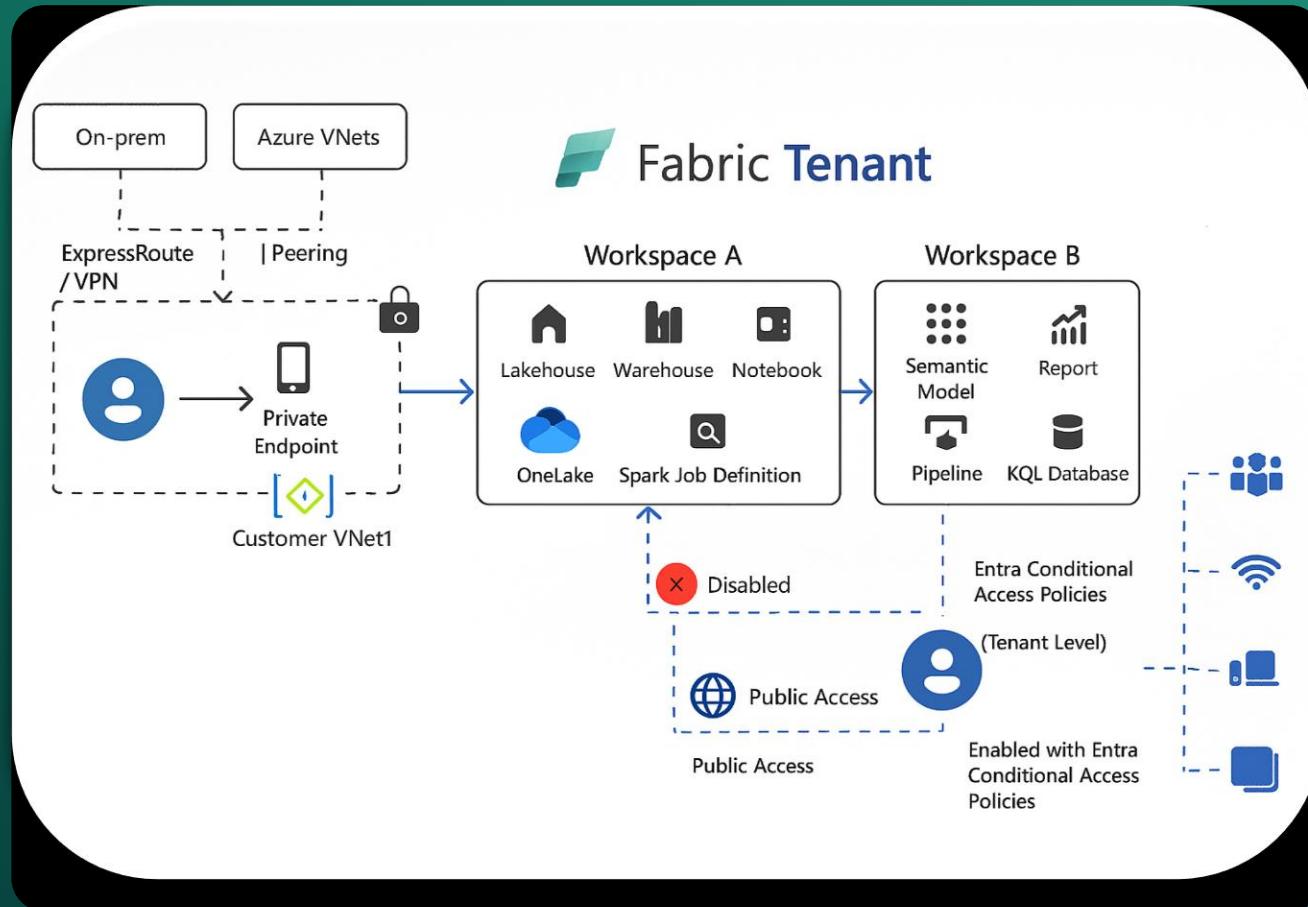
 Block access Grant access Require multifactor authentication Require authentication strength Require device to be marked as compliant Require Microsoft Entra hybrid joined device Require approved client app [See list of approved client apps](#) Require app protection policy [See list of policy protected client apps](#) Require password change All users term of use Guests term of use (Jeffrey TEST)

For multiple controls

 Require all the selected controls Require one of the selected controls

Private Link for Fabric Tenant

Perimeter Network Security for your tenant



What it means:

1. Fabric is disconnected from the public internet
2. Every user needs to connect to the private network to get access on every device
3. No longer able to load resources locally (slower reports)
4. Increases ExpressRoute bandwidth and added costs for Private Links
5. Several product limitations (like on-prem data gateway)



Private Link for Fabric

Perimeter Network Security for your tenant

Private Link for Fabric (Admin Portal)



Azure Private Link

Disabled 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**.



 This setting applies to the entire organization

Apply

Cancel

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](#)



 This setting applies to the entire organization

Apply

Cancel



Private Link for Fabric

Perimeter Network Security for your tenant

Private Link for Fabric (Azure Portal)

Dashboard >

Custom deployment ...

Deploy from a custom template

X

Select a template Basics Review + create

Automate deploying resources with Azure Resource Manager templates in a single, coordinated operation. Create or select a template below to get started. [Learn more about template deployment](#)

 Build your own template in the editor

Common templates

 Create a Linux virtual machine

 Create a Windows virtual machine

 Create a web app

 Create a SQL database

 Azure landing zone

Start with a quickstart template or template spec

Template source (1)

Quickstart template

Template spec

Quickstart template (disclaimer) (1)

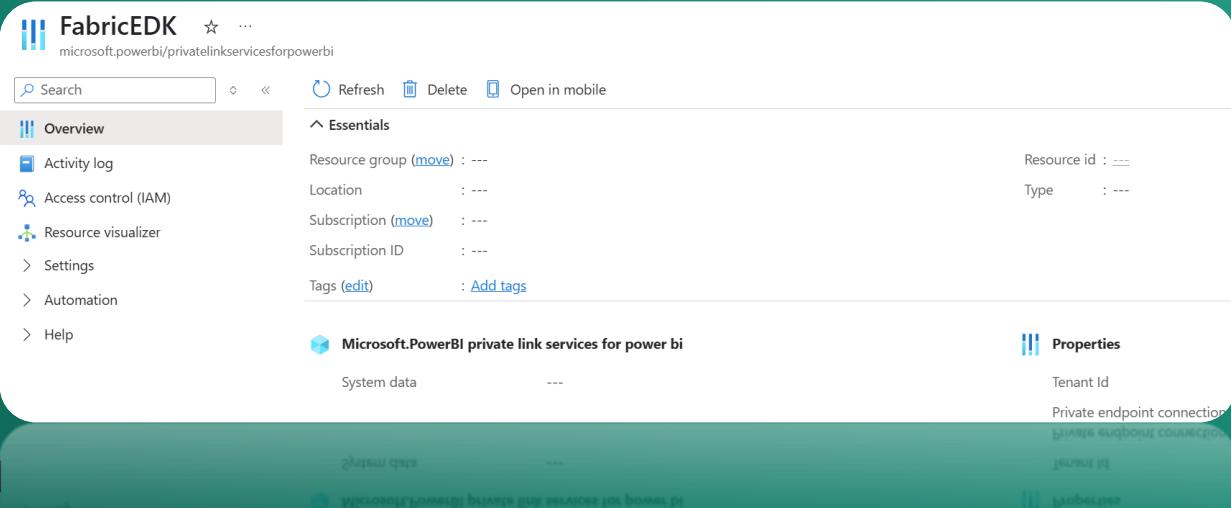
Private Link for Fabric

Perimeter Network Security for your tenant

Private Link for Fabric (Azure Portal)

- <resource-name> is the name you choose for the Fabric resource.
- <tenant-object-id> is your Microsoft Entra tenant ID. See [How to find your Microsoft Entra tenant ID](#).

```
{  
  "$schema": "http://schema.management.azure.com/schemas/2015-01-01/deploy  
  "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 Link for Fabric

Perimeter Network Security for your tenant

Private Link for Fabric (Azure Portal)

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

Resource type	Instance name	
Microsoft.Fabric/workspaces	35bb742f-4dee-437e-b51d-55efaec91cae	
Select a resource type	Select one or more instances	

Exceptions

Allow Azure services on the trusted services list to access this storage account. (i)

Allow read access to storage logging from any network

Allow read access to storage metrics from any network

Allow Azure services on the trusted services list to access this storage account. (i)

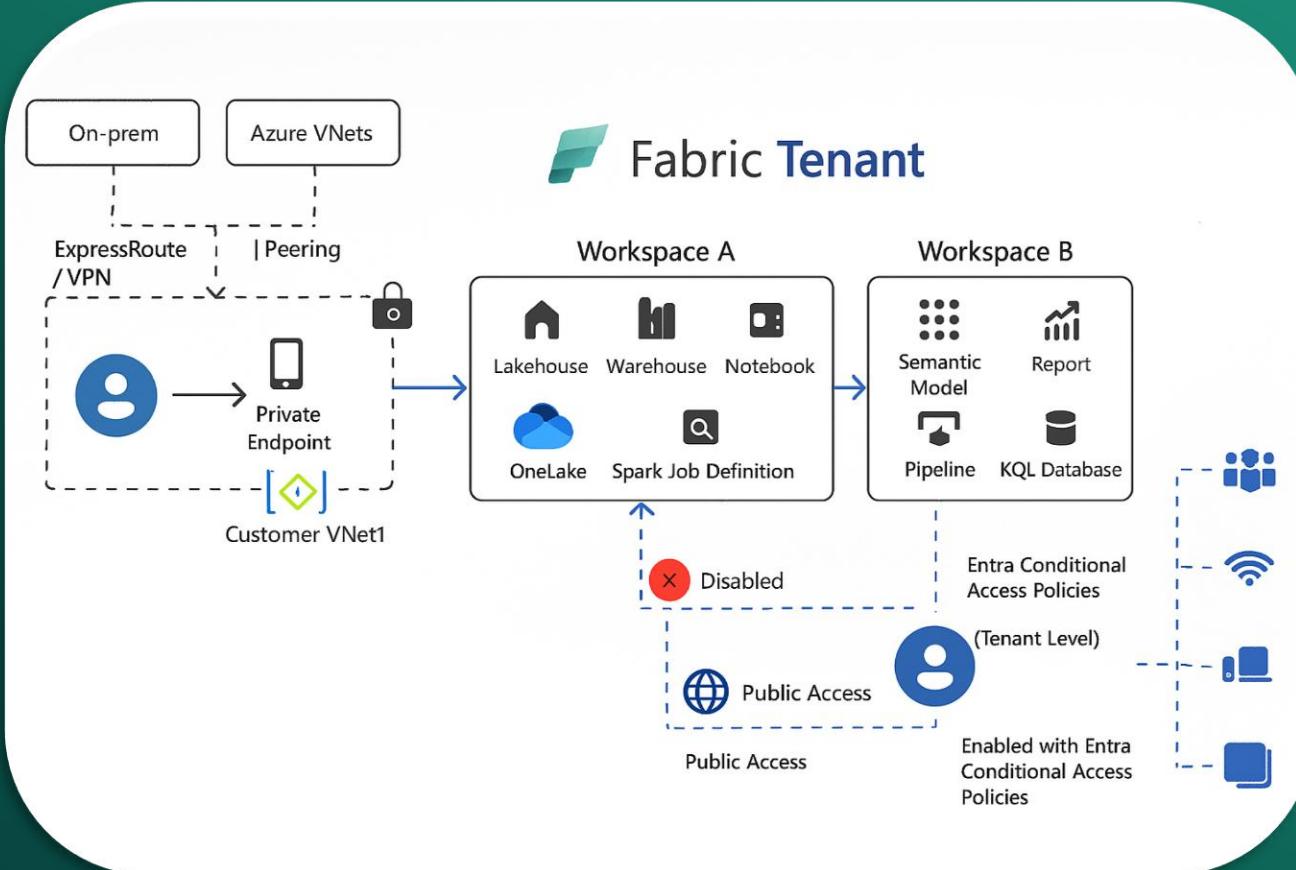
Allow read access to storage logging from any network

Allow read access to storage metrics from any network



Workspace Private Link for Fabric

Perimeter Network Security for your workspace



What it means:

1. Selected workspaces can be protected using Private Links and closed from public internet.
2. Create a secure connection between public and private workspaces using private data access.
3. Public workspaces can be secured using Entra policies or IP filtering to use Power BI.



Workspace Private Link for Fabric

Perimeter Network Security for your workspace



Private Link for Workspace (Admin Portal)

Inbound Networking Workspace

Configure workspace-level inbound network rules (preview)

Unapplied changes

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

Workspace connection settings

Choose how users and services can connect to this workspace. Use these settings to manage access, security, and integration options. [Learn more](#)

Allow all connections to this workspace (including private links)

Users can connect from any network, including through private links. This setting may be limited by configurations set by your Fabric admin.

Allow connections only from workspace level private links

Public access to this workspace is denied when this option is selected.

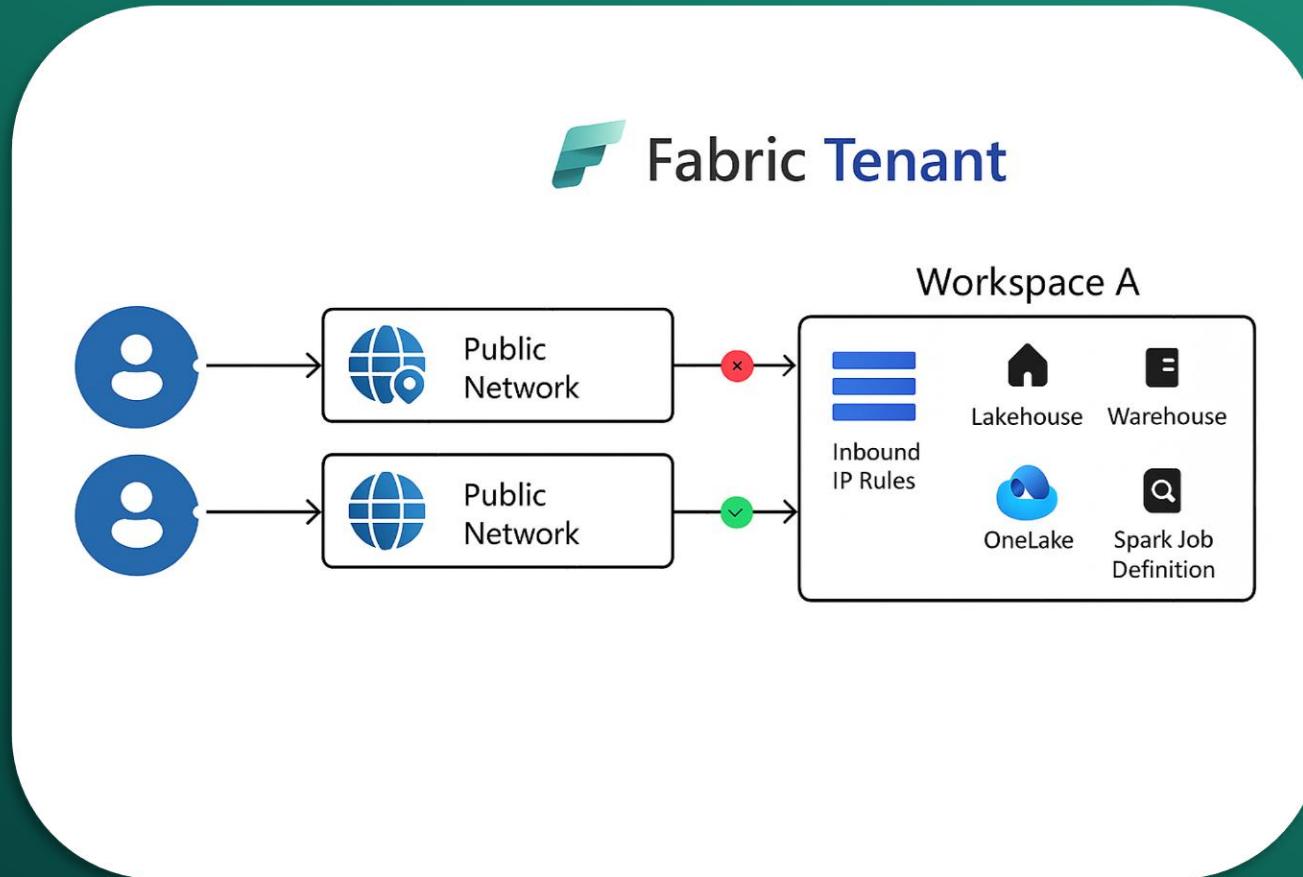
Apply

Cancel



Workspace IP Firewall for Fabric

Perimeter Network Security for your workspace



What it means:

1. Fabric workspace is accessible only from specific public IP or IP Ranges
2. Simple setup.



Fabric Outbound Security



Common network security requirements

→ Secure access to your data in Fabric (Inbound Protection)

↓ Restrict outbound access from a Fabric workspace (Outbound Protection)

- Outbound Access Policies + Inbound network security features
-

→ Securely connect to data behind a firewall\private link from Fabric (Outbound Access)



Workspace outbound access protection



What it means:

1. Workspace level control to restrict outbound access to Public network
2. Restrict outbound connections to permitted destinations only
3. Use in conjunction with other security features to achieve robust outbound control



Workspace outbound access protection

Outbound rules (Admin Portal)

Configure workspace-level outbound **network rules**
Enabled for the entire organization

With this setting on, workspace admins can configure outbound access protection in workspace settings. Turning off this tenant setting also turns off outbound access protection in all the workspaces in the tenant. [Learn More](#)

Enabled

⚠ This setting applies to the entire organization

Apply Cancel

Data connection rules (preview)

+ Add new cloud connection rule Save

Cloud connection policies

✓ Azure Data Factory Allowed >Delete
This connection kind does not support endpoints.

➤ FabricSqlEndpointMetadata Allowed Delete

✓ All other connection kinds Allowed
This connection kind does not support endpoints.

Gateway connection policies

Workspace outbound access protection

Store data

Organize, query, and store your ingested data in an easily retrievable format.

Cosmos DB database



Build modern apps using fully managed NoSQL database



Datamart (preview)



Provide strategic insights from multiple sources into your business-focused or departmental data.



Eventhouse



Rapidly load structured, unstructured and streaming data for querying.



Lakehouse



Store big data for cleaning, querying, reporting, and sharing.



Sample warehouse



Start a new warehouse with sample data already loaded



Semantic model



Combine data sources in a semantic model to visualize or share it.



Snowflake database (Preview)



Link to a Snowflake database comprised of apache Iceberg tables.



SQL database



Build modern cloud apps that scale on an intelligent, fully managed database.



Warehouse

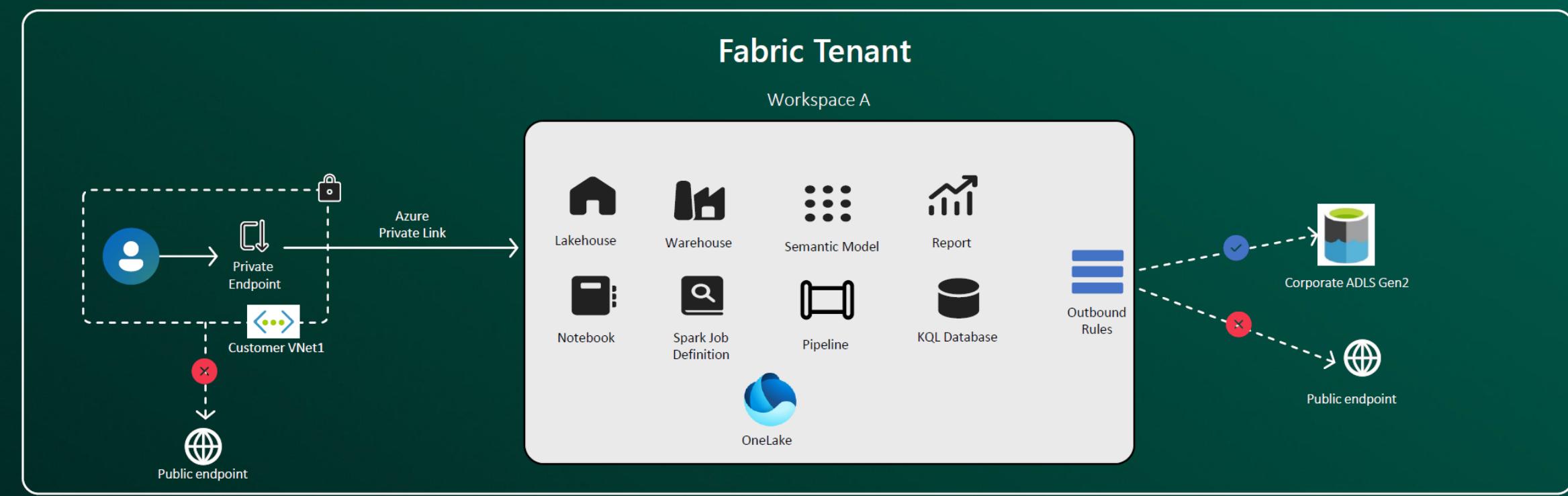


Provide strategic insights from multiple sources into your entire business.



Data Exfiltration Protection

DEP = Outbound + Inbound protection



Inbound security features like private link allow you to restrict who can access your data and from where, reducing risks of data exfiltration



Outbound security make sure that malicious users cannot exfiltrate data

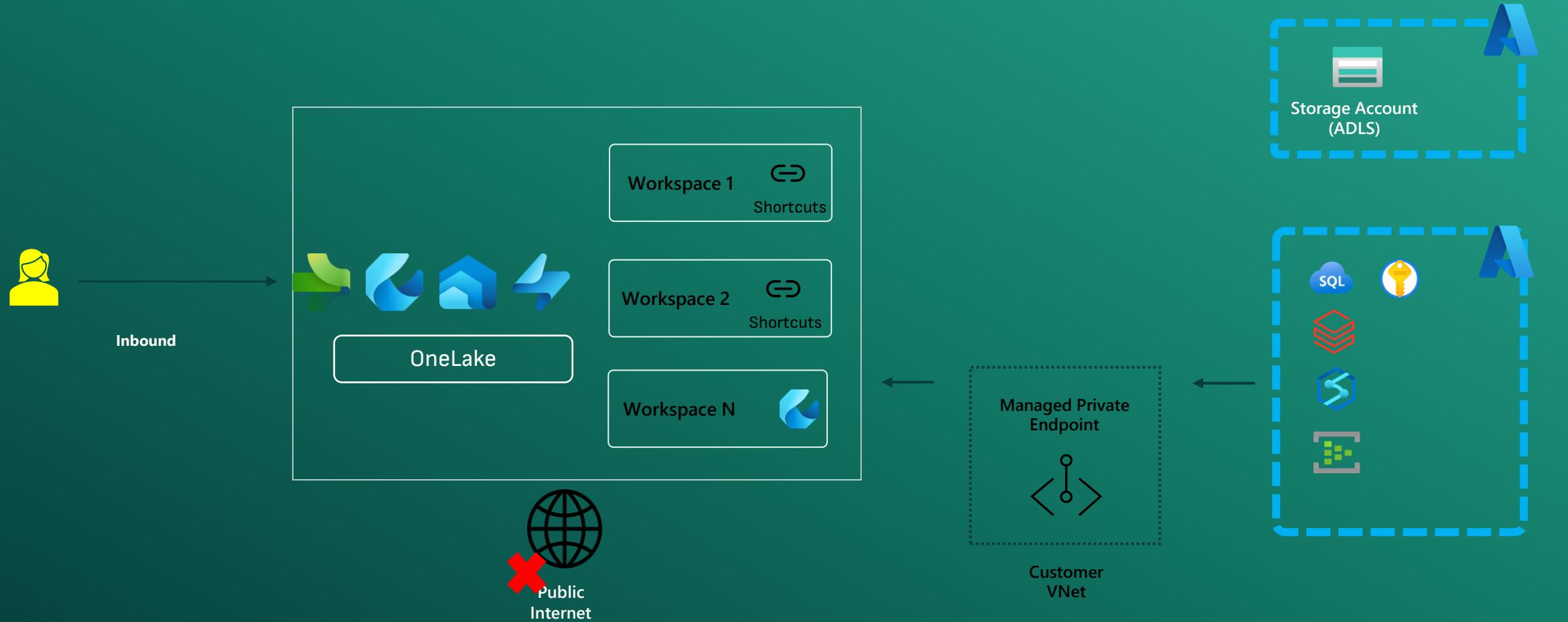


Common network security requirements

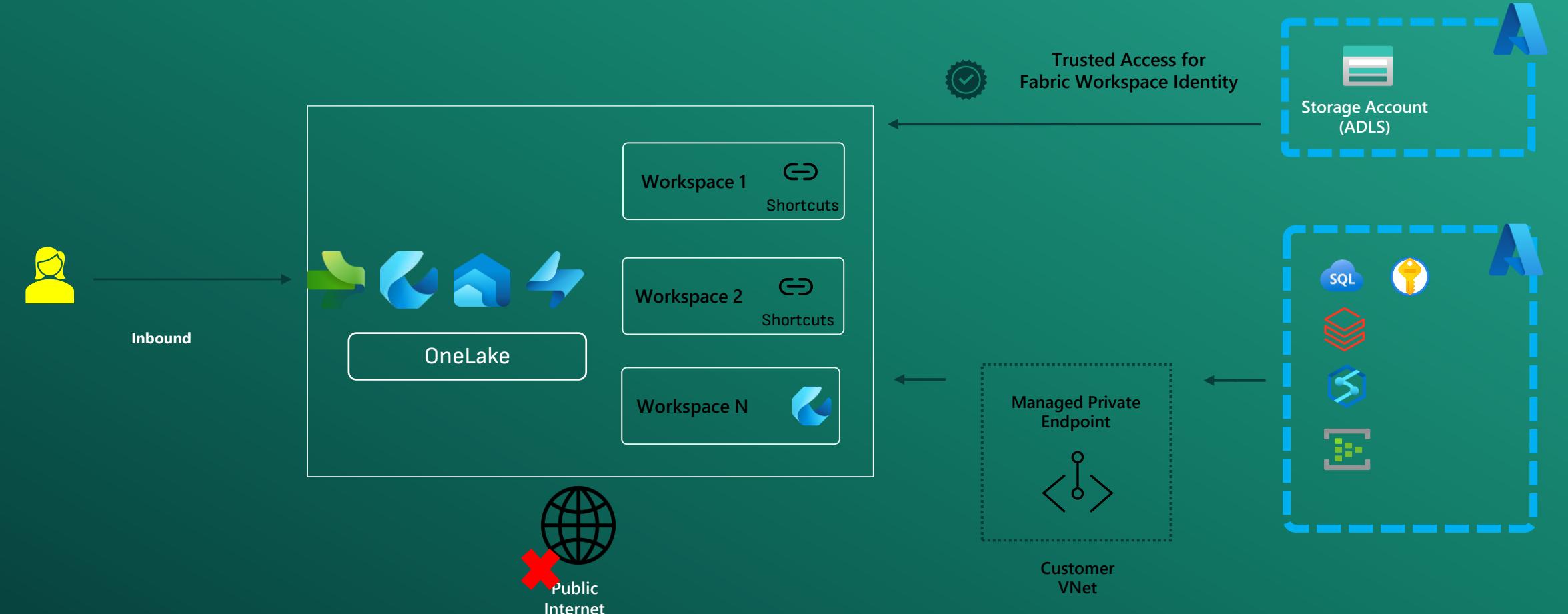
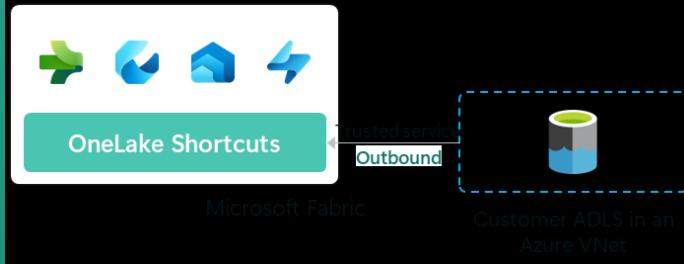
- Secure access to your data in Fabric (Inbound Protection)
- Restrict outbound access from a Fabric workspace (Outbound Protection)
- ↓ Securely connect to data behind a firewall\private link from Fabric (Outbound Access)
 - Trusted Access
 - Data Gateways(On-prem and VNet)
 - Managed Private Endpoints



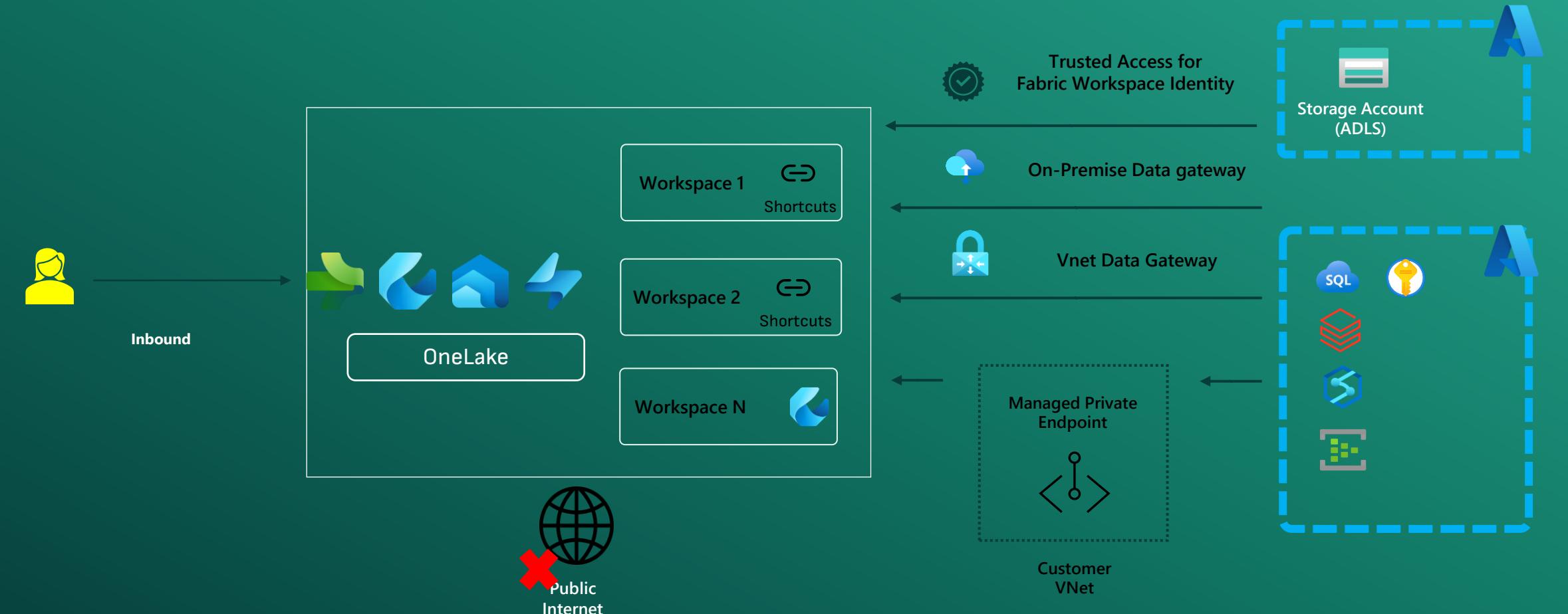
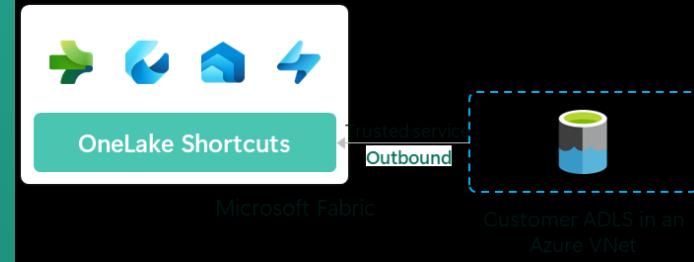
Getting data into Fabric



Getting data into Fabric



Getting data into Fabric



Getting data into Fabric

Storage account name

Region

TenantID

Workspaceld

Leave subscription for workspace as is

```
{  
    "$schema": "https://schema.management.azure.com/schemas/2019-04-01/deploymentTemplate.json#",  
    "contentVersion": "1.0.0.0",  
    "resources": [  
        {  
            "type": "Microsoft.Storage/storageAccounts",  
            "apiVersion": "2023-01-01",  
            "name": "<storage account name>",  
            "id": "/subscriptions/<subscription id of storage account>/resourceGroups/<resource group  
ame>/providers/Microsoft.Storage/storageAccounts/<storage account name>",  
            "location": "<region>",  
            "kind": "StorageV2",  
            "properties": {  
                "networkAcls": {  
                    "resourceAccessRules": [  
                        {  
                            "tenantId": "<tenantid>",  
                            "resourceId": "/subscriptions/00000000-0000-0000-0000-  
00000000/resourcegroups/Fabric/providers/Microsoft.Fabric/worksaces/<workspace-id>"  
                        }  
                    ]  
                }  
            }  
        }  
    ]  
}
```



Resource instances

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

Resource type

Microsoft.Fabric/worksaces

Instance name

05613f19-4fc0-46d0-add8-72cad691880f

Select a resource type



Select one or more instances



Common network security requirements



- Secure access to your data in Fabric (Inbound Protection)
 - Conditional Access Policies
 - Private Link at a Tenant Level
 - Private Link at a Workspace level
 - Workspace IP Firewall
-



- Restrict outbound access from a Fabric workspace (Outbound Protection)
 - Outbound Access Policies + Inbound network security features
-



- Securely connect to data behind a firewall\private link from Fabric (Outbound Access)
 - Trusted Access
 - Data Gateways(On-prem and VNet)
 - Managed Private Endpoints
-



A photograph of a person's hands holding a black smartphone, positioned in the upper left foreground. In the lower right foreground, a silver laptop is open on a dark wooden desk. A white tablet lies flat on the desk to the left of the laptop. A green textured mug sits to the left of the tablet. The background is a blurred indoor setting.

DEMO

Data Security in Fabric

Data Encryption:

Data in rest

Data in transit

Column Level encryption

Presido [Home – Microsoft Presidio](#)

Onelake Security:

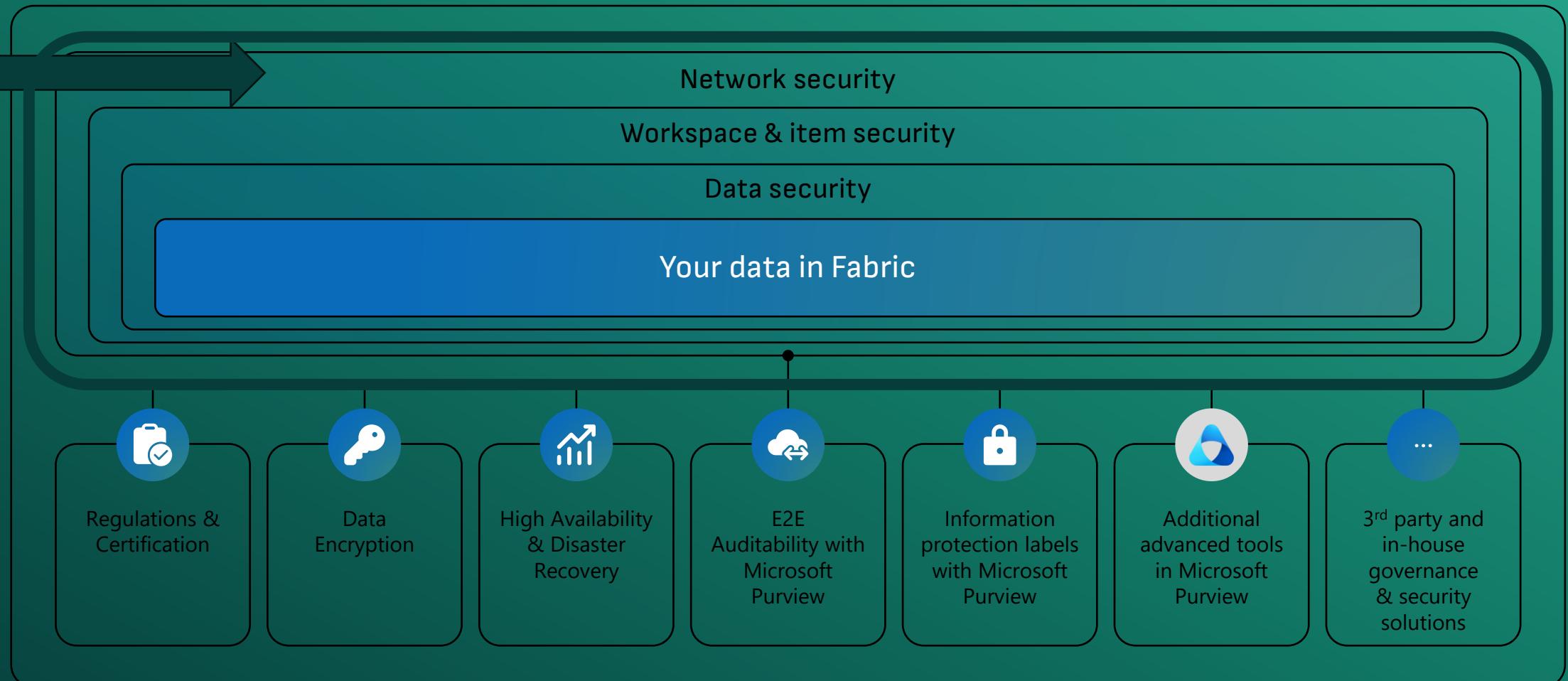
[OneLake security overview – Microsoft Fabric | Microsoft Learn](#)

Customer Managed Keys (Preview)

[Customer-managed keys for Fabric workspaces – Microsoft Fabric | Microsoft Learn](#)



Recap



Erwin de Kreuk

Technology Lead Data
InSpark



Dutchfabricusergroup.com



linkedin.com/in/erwindekreuk



erwindekreuk.com



github.com/edkreuk

Let's connect

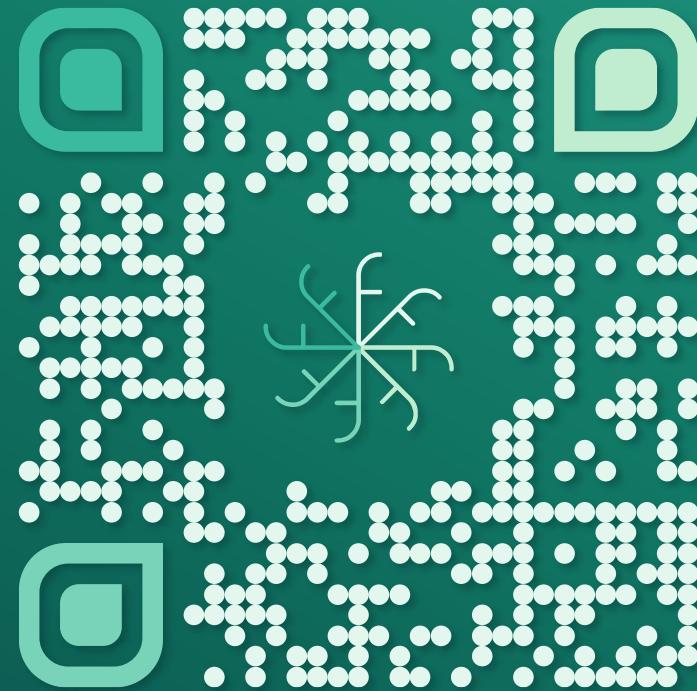


Thank you to our Fabric February Friends!

(Sponsor slide will be updated before the event!)



Share your thoughts and help our speakers!



fabfeb.app/feedback

