

Let's connect



Erwin de Kreuk
Principal Consultant
Lead Data & AI InSpark

- @erwindekreuk.bsky.social
- linkedin.com/in/erwindekreuk
- erwindekreuk.com
- github.com/edkreuk
- <https://sessionize.com/erwin-de-kreuk/>
- Dutchfabricusergroup.com





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



Winner

Partner of the
Year Awards

Country Award Data & AI
Global Award Identity





Cybercriminals are
getting more
creative just like us

AI transformation is happening **now**

95%

75%

1%

of organizations are
implementing or developing
an AI strategy¹

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

of risk leaders are thoroughly
prepared for mass GenAI
availability risks³

1. Microsoft internal research May 2023, N=638, [2. Work Trends Index](#).

3. Gartner®, Executive Pulse: Organizations are not prepared for Generative AI risks Sept 2023.

Why data security?

Data is most secure if no one can access it.

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

Agenda

Introduction

Challenges

Inbound Connections

Private Links

Outbound connections

Microsoft Purview

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

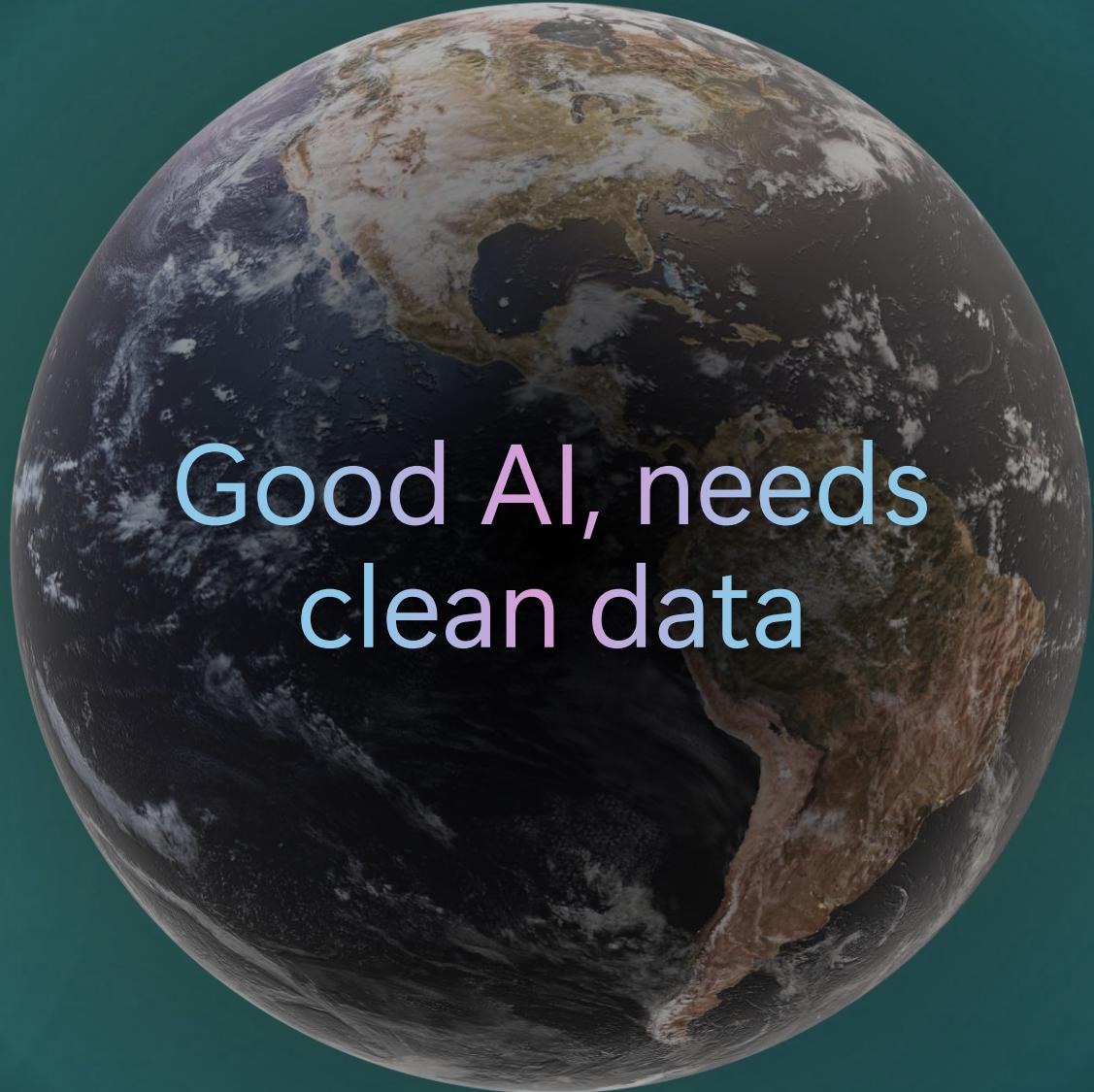
”

¹Chandana Gopal, Research Director, Enterprise Intelligence, IDC





AI is transforming the world

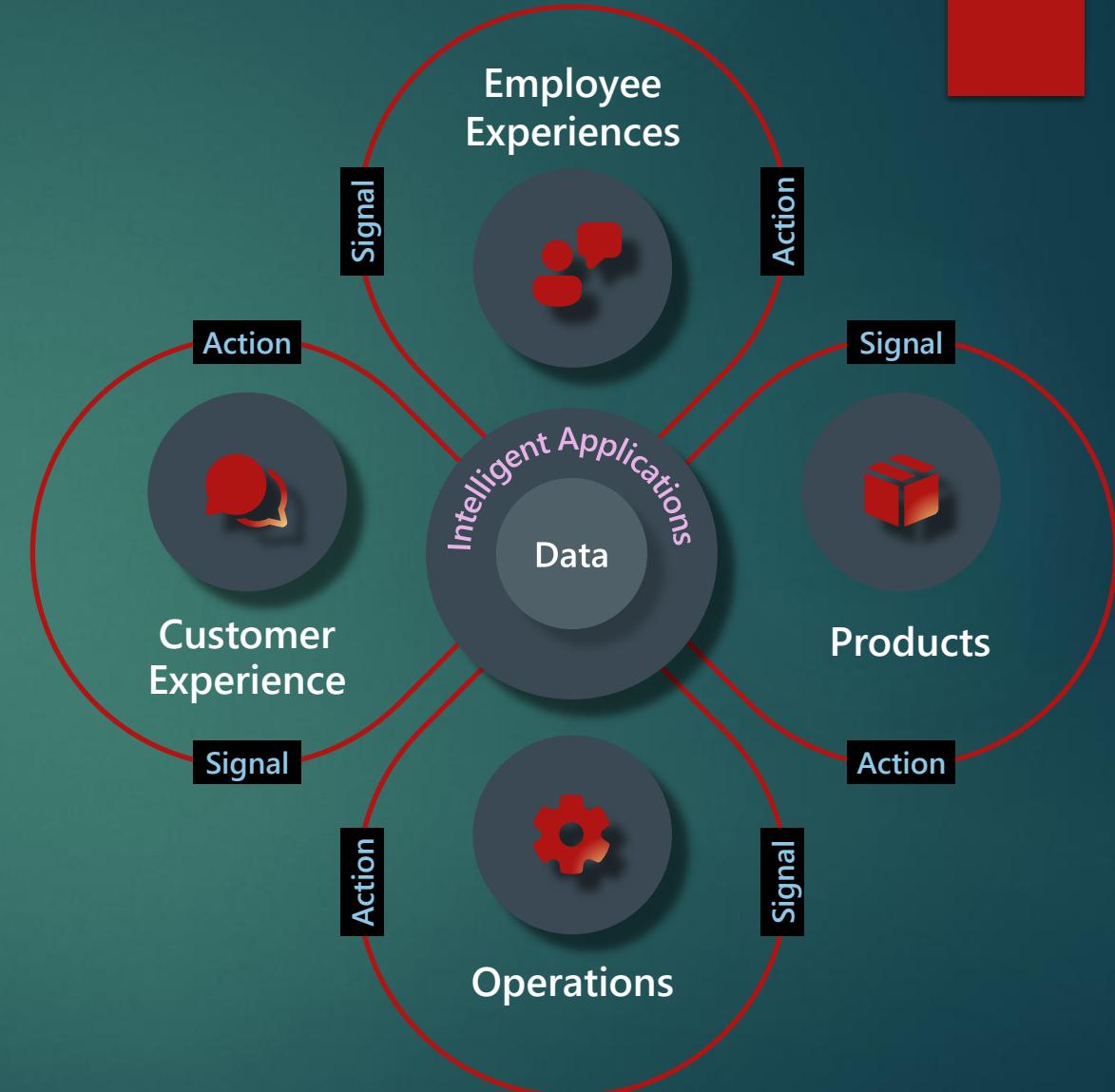


Good AI, needs
clean data

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

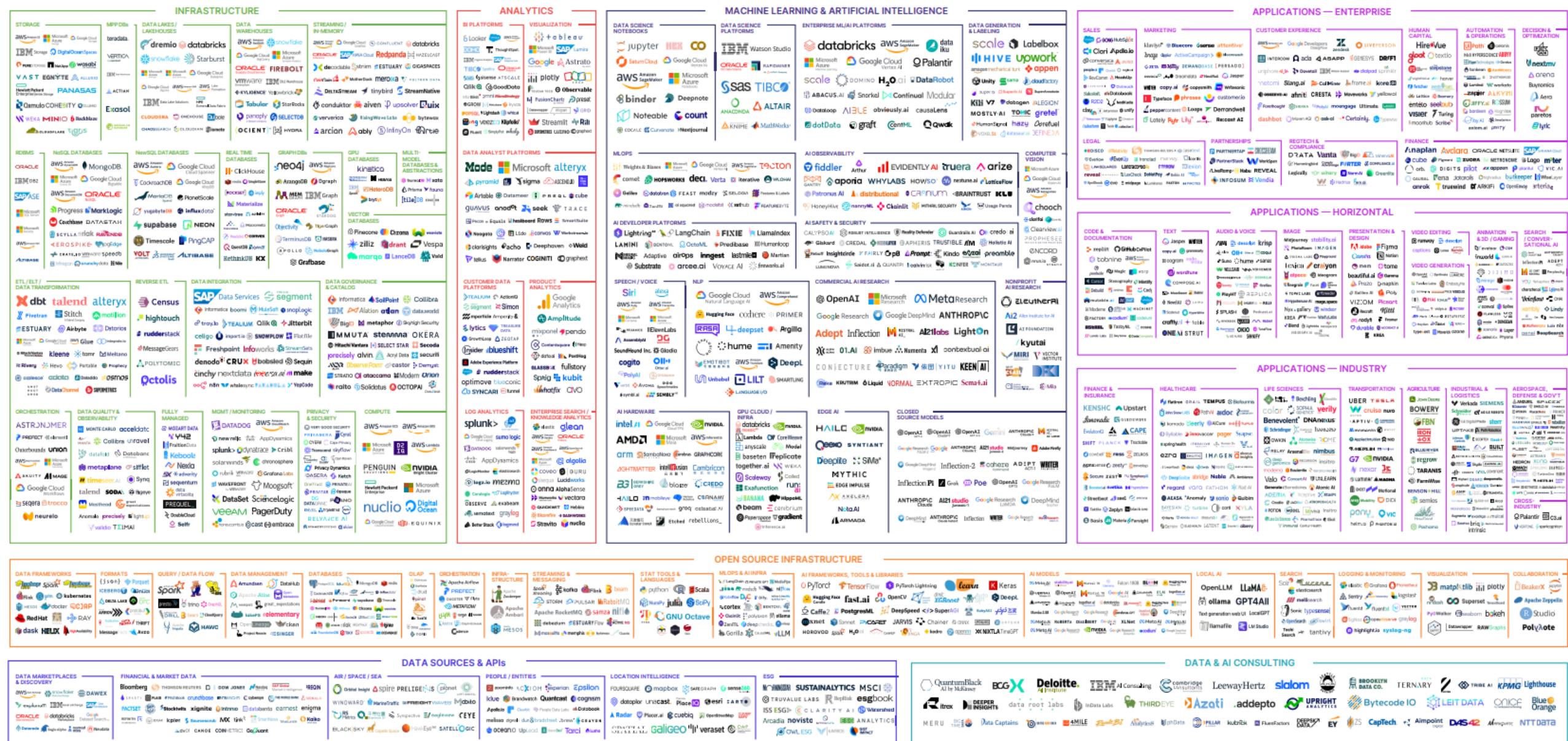
Security is paramount in the digital age, and Microsoft Fabric ensures your data is protected at every stage. By using Fabric, organizations can trust that their data is secure, allowing them to focus on innovation and growth.



How do you translate data into
competitive advantage

The 2024 ML, AI, and Data Landscape

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





Microsoft Fabric

The unified data platform for AI transformation

From

Isolated component

Single database

Gen AI Bolted-in

To

Unified stack

All the data

Gen AI built in



Microsoft Fabric

The unified data platform for AI transformation



Data
Factory



Analytics



Databases



Real-Time
Intelligence



Power BI



Industry
Solutions



Partner
workloads



AI



OneLake



Microsoft Purview

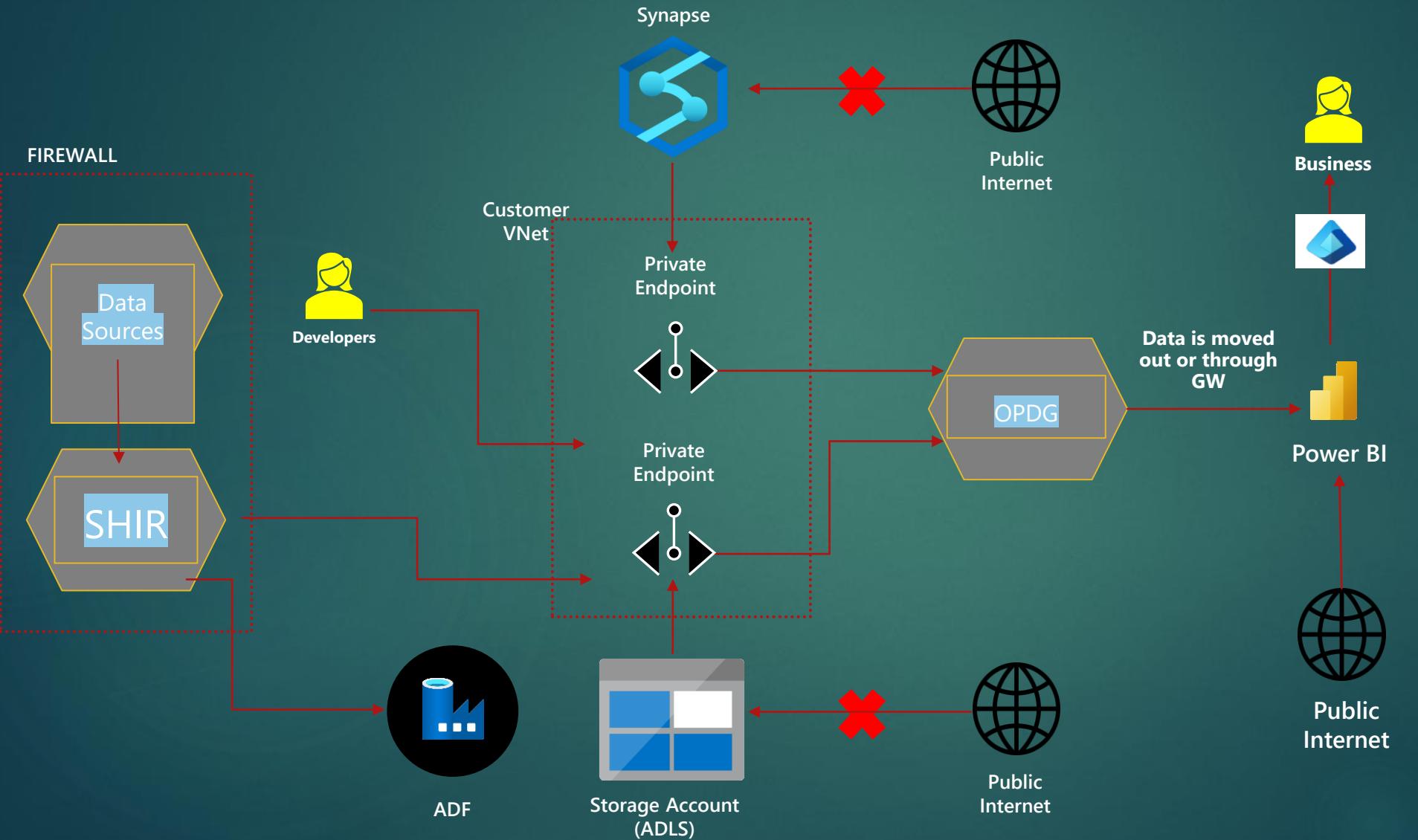
Modern data challenges

- 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

Common network security requirements

- Need to be able to connect to data inside a firewall\private link from Fabric (outbound)
- Inbound protection (restrict inbound by network location)
- Secure access to the “backend services”
- More stringent customers (FSI\HLS):
 - Traffic needs to be private (not via public internet)
 - Endpoints should not be open to the public internet

Existing PaaS World



PaaS services are disconnected from the Public internet.

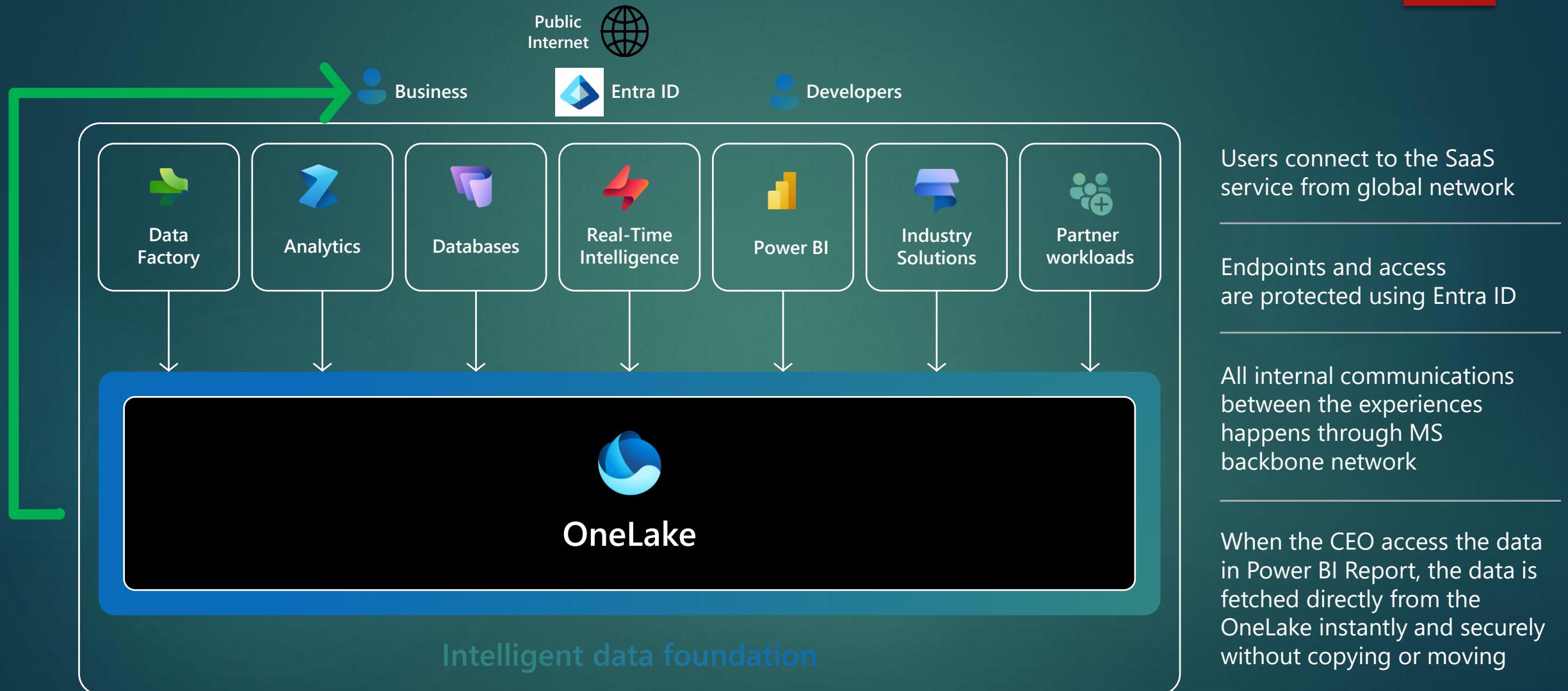
All communications between the services are configured to go through private endpoint

Developers connect to a VPN and connect to the backend services

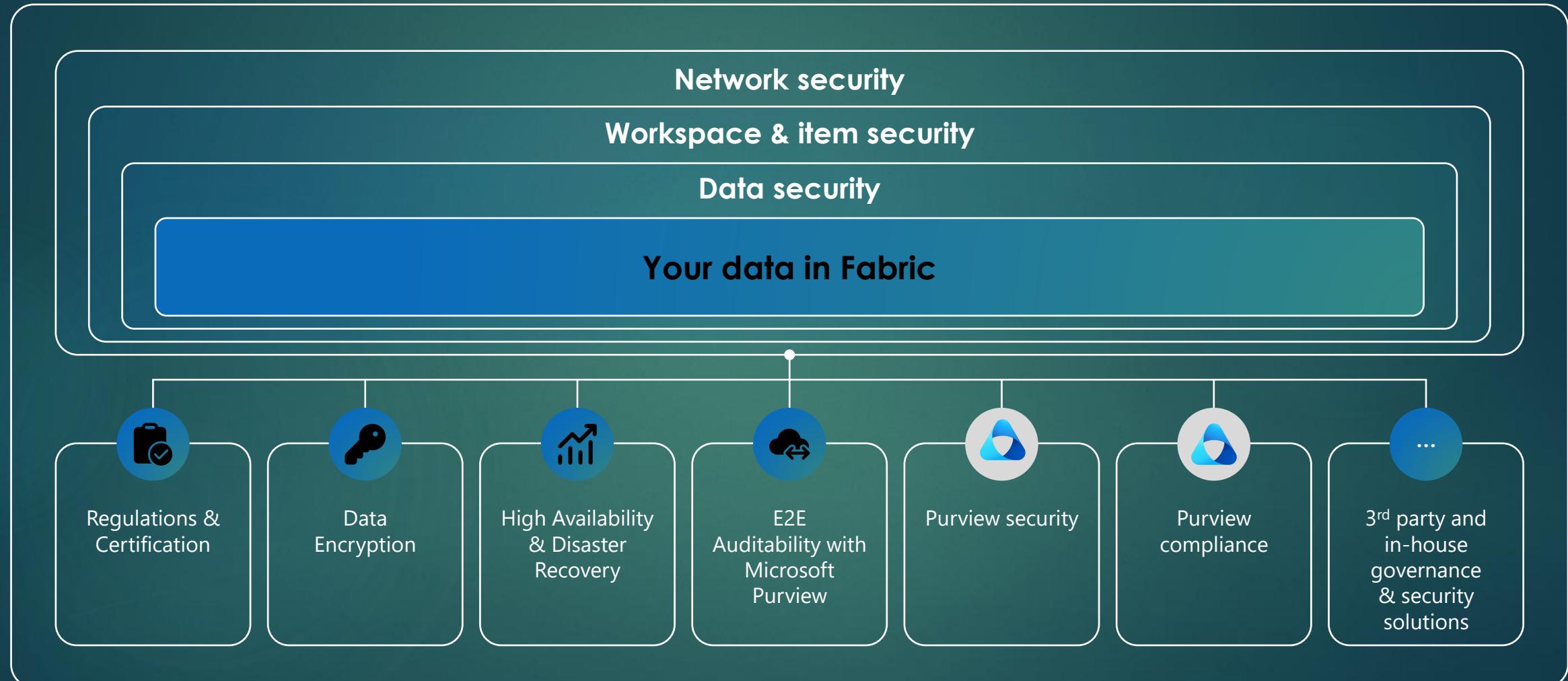
Data sources are connected through the self-hosted runtime inside the firewall

When the CEO access the data in Power BI Report, the data is imported into Power BI or through the GW with DQ.

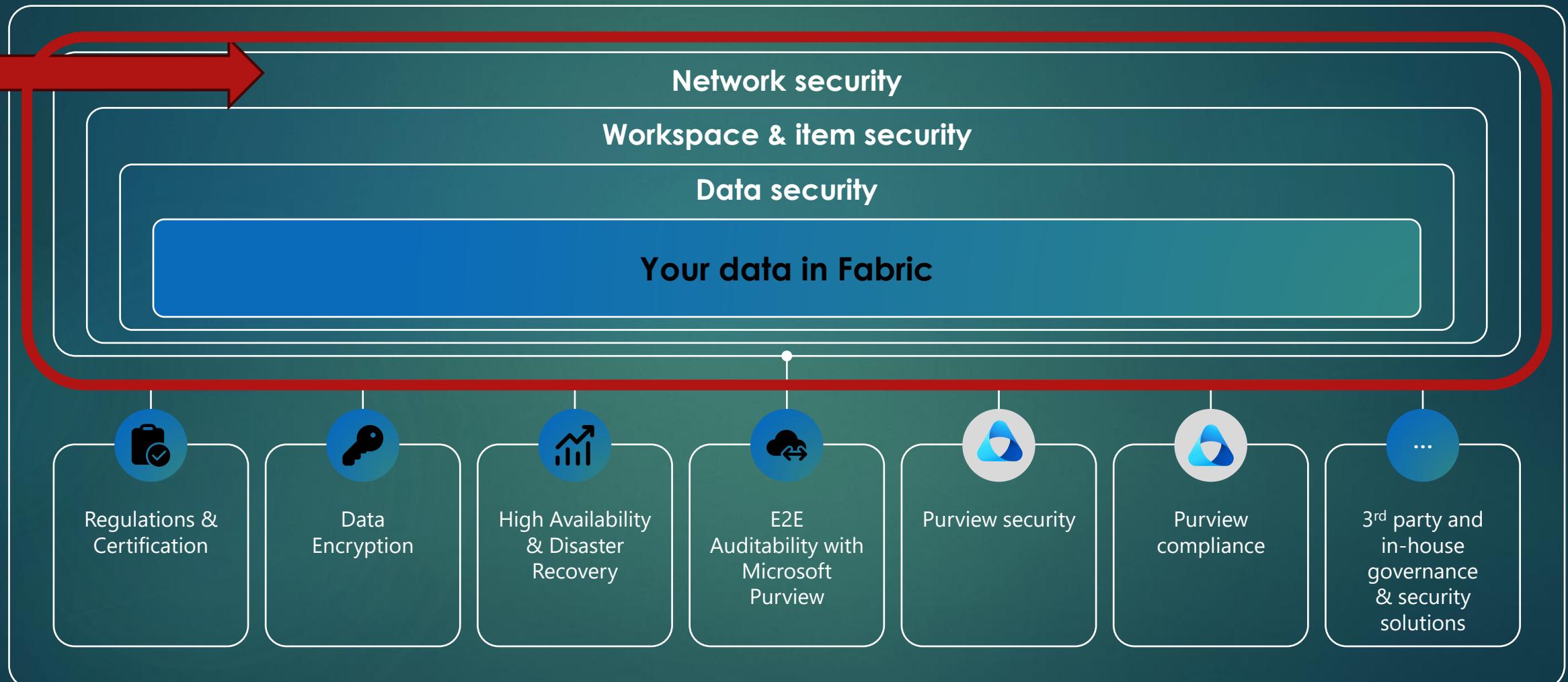
Microsoft Fabric – SaaS World



Security layers in Microsoft Fabric



Security layers in Microsoft Fabric



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

Fabric leverages Entra ID for secure adaptive access

Protect access to resources and data with strong authentication and risk-based access policies



User-friendly multifactor authentication (MFA) and Passwordless authentication support



Configurable Conditional Access policies based on context and risk assessment ¹



User and entity behavior analytics (UEBA) to automatically protect against identity compromise ²

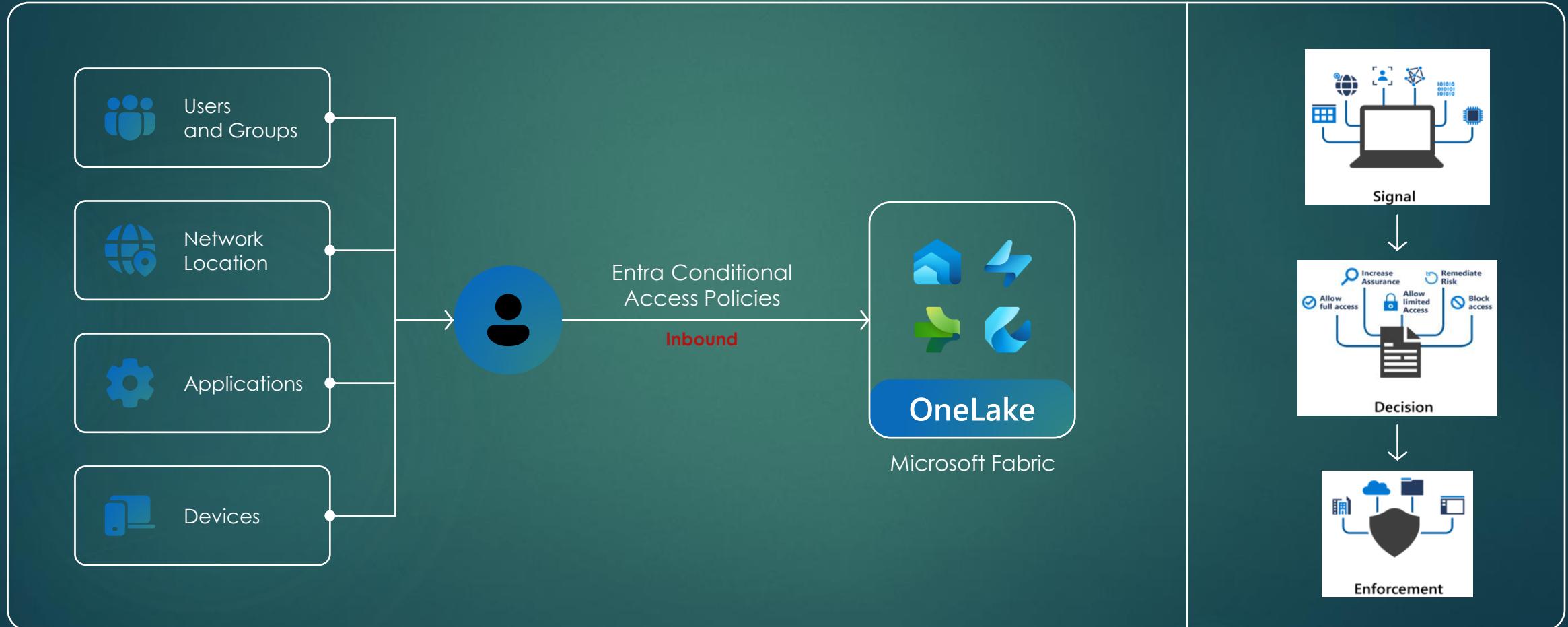
¹Microsoft Entra ID P1 \ E3 license required



²Microsoft Entra ID P2 \ E5 license required

Conditional Access Policies

Common Decisions – Block, Grant, Require MFA



Entra ID Conditional Access



- 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

Microsoft Entra



InSpark Labs
(InSpark B.V.)

Tenant ID cd004ec9-bc4b-4...

Primary domain insparklab...

399

572

239

560

[View devices](#)

[View apps](#)



Erwin de Kreuk
Global Administrator

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

[View user profile](#)

My role assignments



2

- 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](#)



75% in the last 30 days

[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 noise from locations that are marked Trusted or configured in Conditional Access Policies cannot be bypassed.

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 >

i Conditional Access | Overview

Microsoft Entra ID

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

Refresh

Got feedback?

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

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](#)

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](#)

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](#)

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](#)

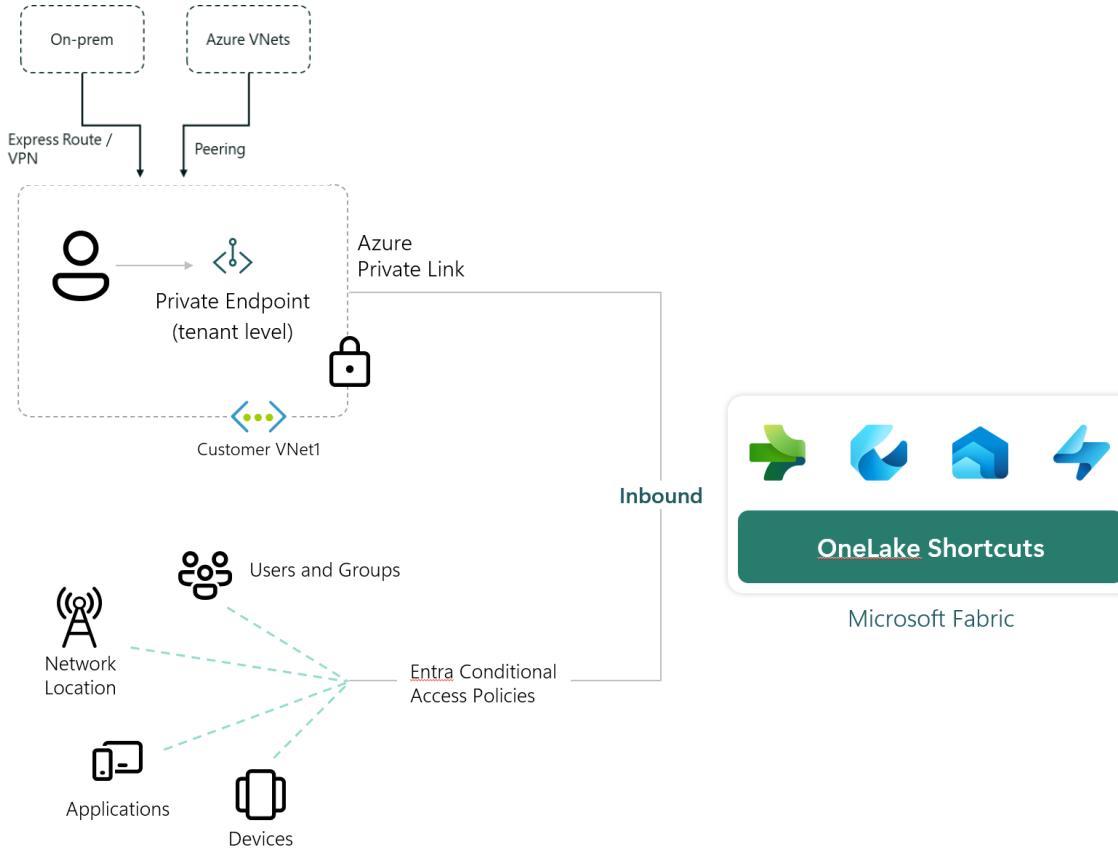
 Block access Grant access Require multifactor authentication Require authentication strength Require device to be marked as compliant Require Microsoft Entra hybrid joined device Require approved client app
[See list of approved client apps](#) Require app protection policy
[See list of policy protected 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

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 (i)

- Quickstart template
 Template spec

Quickstart template (disclaimer) (i)



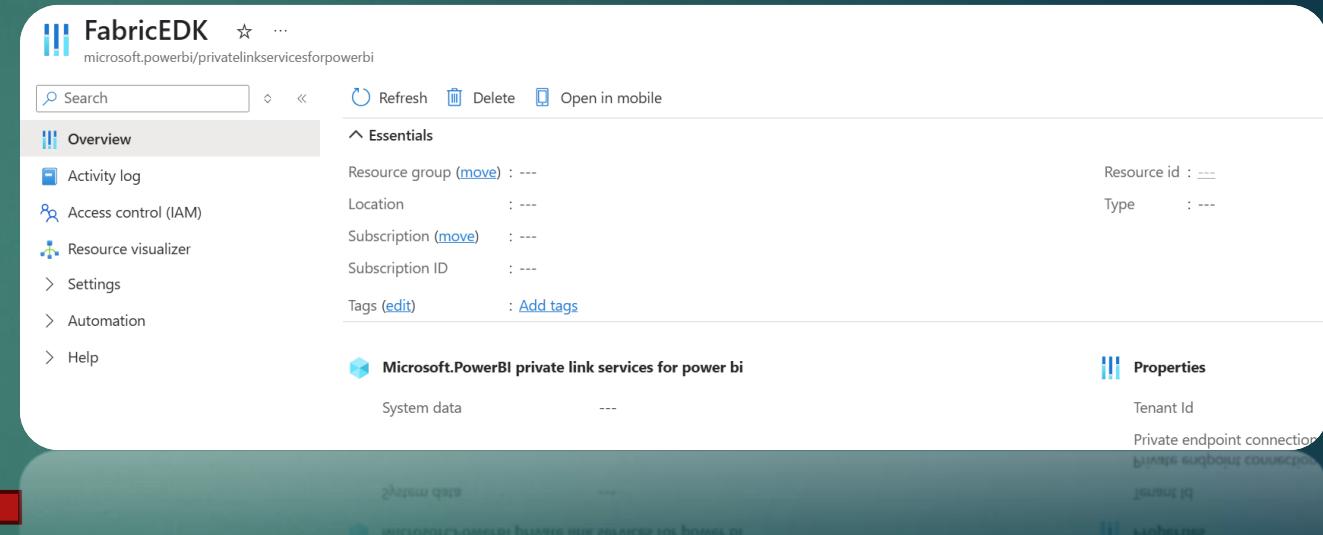
Private Link for Fabric

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/deploymentschema.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 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. ⓘ

Allow read access to storage logging from any network

Allow read access to storage metrics from any network

Allow read access to storage metrics from any network

Allow read access to storage logs from any network

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

Private Link for Fabric

Perimeter Network Security for your tenant

Limitations

Fabric supports up to 450 capacities in a tenant where Private Link is enabled.

When capacity is newly created, it won't support private link until its endpoint is reflected in the private DNS zone. This can take up to 24 hours. Trial capacity is not supported

Tenant migration is blocked when Private Link is turned on in the Fabric admin portal.

Customers can't connect to Fabric resources in multiple tenants from a single virtual network, but rather only the last tenant to set up Private Link.

Each private endpoint can be connected to one tenant only. You can't set up a private link to be used by more than one tenant.

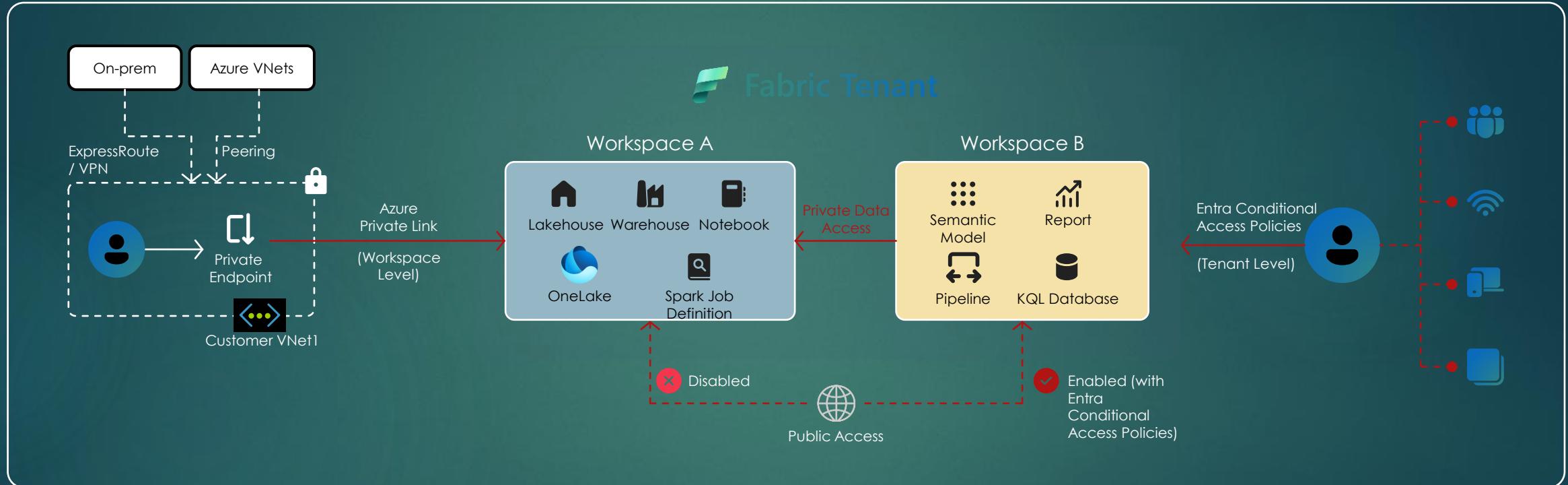
On-premises data gateways aren't supported and fail to register when Private Link is enabled. To run the gateway configurator successfully, Private Link must be disabled. Learn more about this scenario. VNet data gateways will work.



Sneak peak of what's next on the
roadmap...

Workspace level Private Link for Fabric

Perimeter Network Security for your workspace



Selected workspaces can be protected using Private Links and closed from public internet.

Create a secure connection between public and private workspaces using private data access.

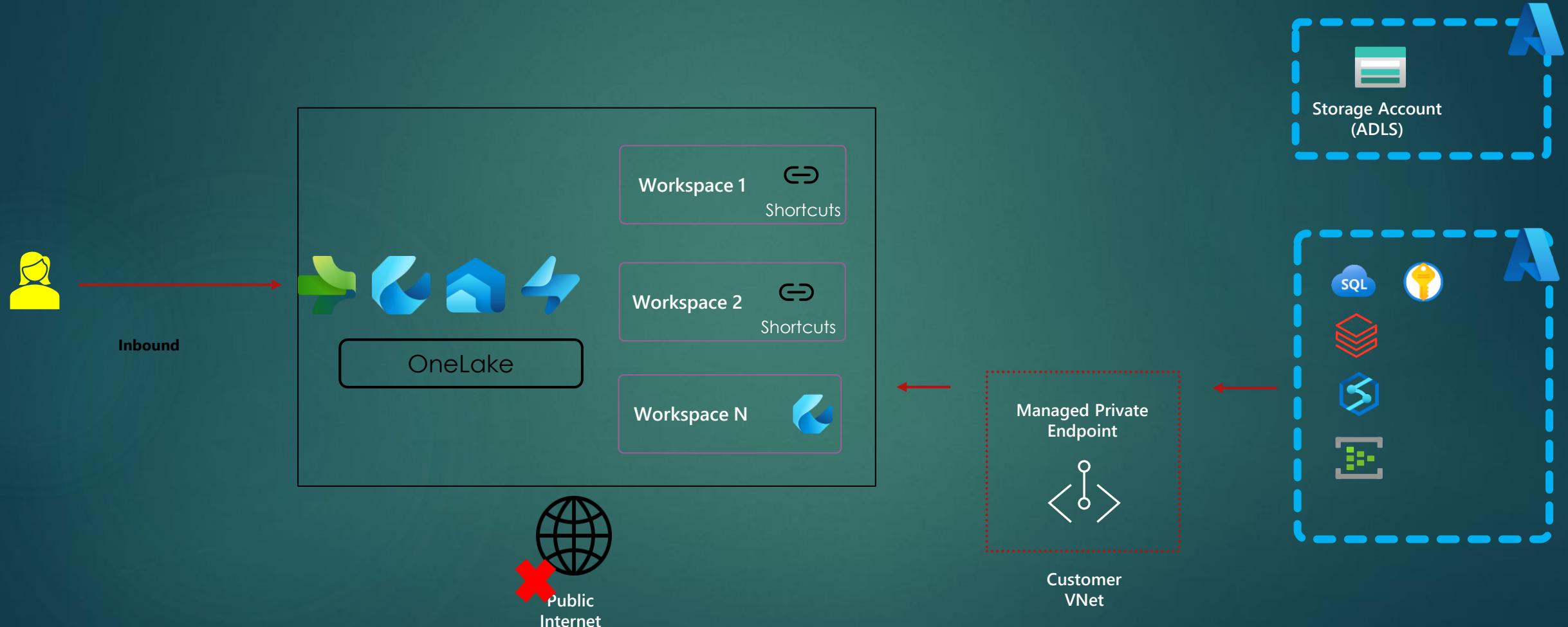
Public workspaces are secured through Entra policies for example to use Power BI.

Limitations of tenant wide PL don't apply !!!

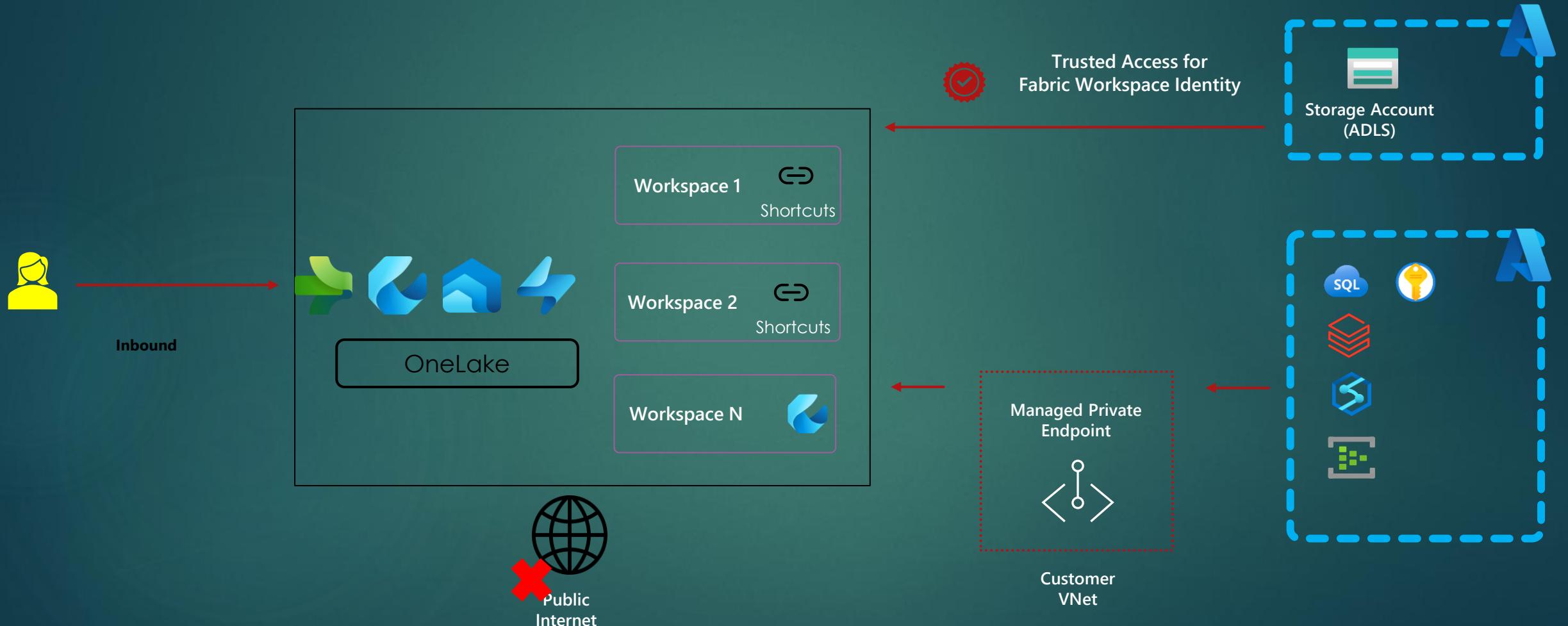
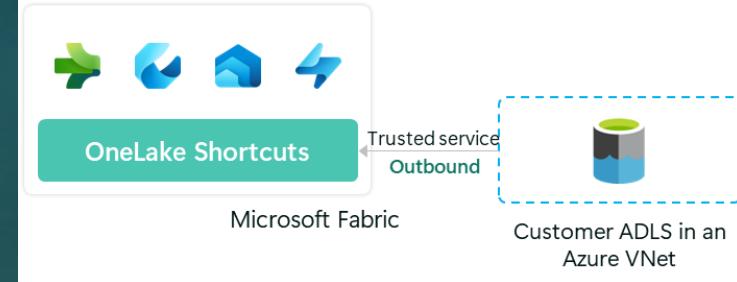
Fabric Outbound Security



Getting data into Fabric



Getting data into Fabric



Getting data into Fabric

Storage account name

Region

TenantID

WorkspaceId

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-  
0000000000/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.

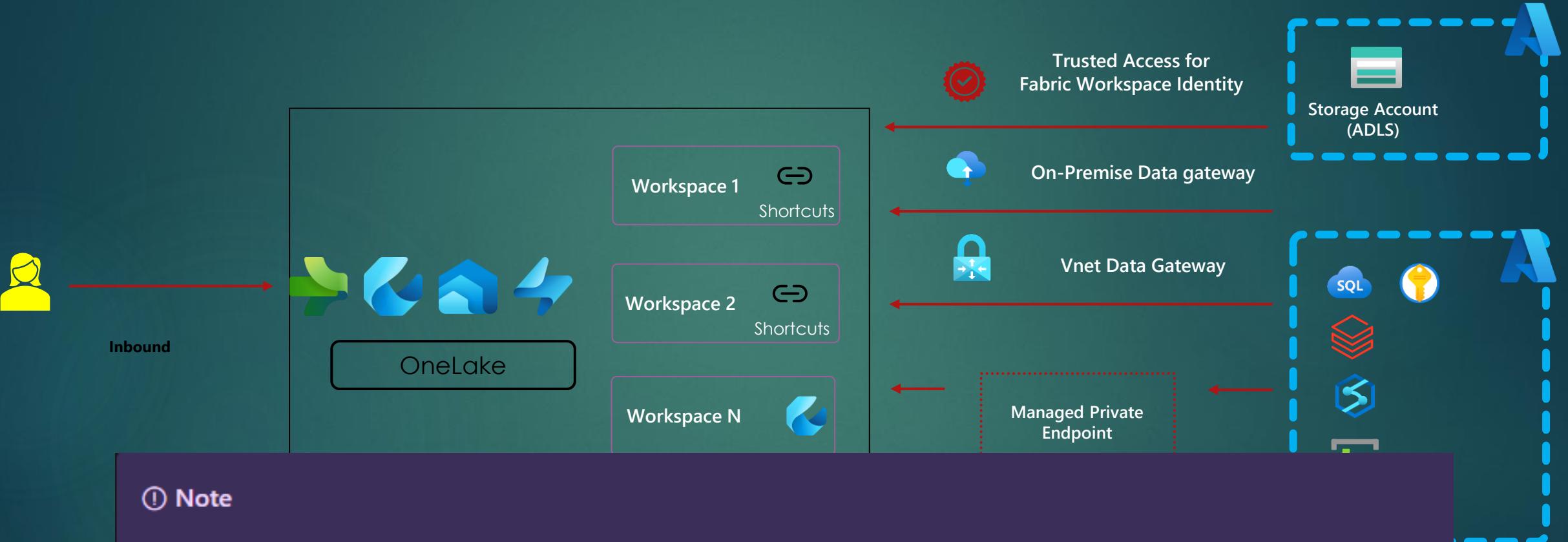
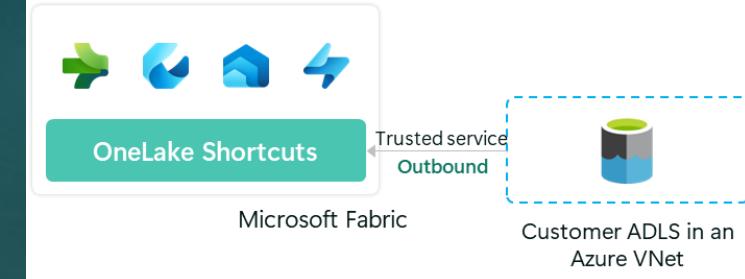
Resource type	Instance name
Microsoft.Fabric/worksaces	05613f19-4fc0-46d0-add8-72cad691880f

Select a resource type: Select one or more instances

A photograph of a person's hands holding a smartphone, set against a background of a desk with a laptop, a tablet, and a coffee cup. A white callout box with a five-star rating icon is overlaid on the image, containing the word "DEMO".

DEMO

Getting data into Fabric



① Note

Trusted workspace access is **generally available**, but can only be used in F SKU capacities. For information about buying a Fabric subscription, see [Buy a Microsoft Fabric subscription](#). Trusted workspace access is not supported in Trial capacities.

Microsoft Purview



**Microsoft
Fabric**



**Microsoft
Purview**

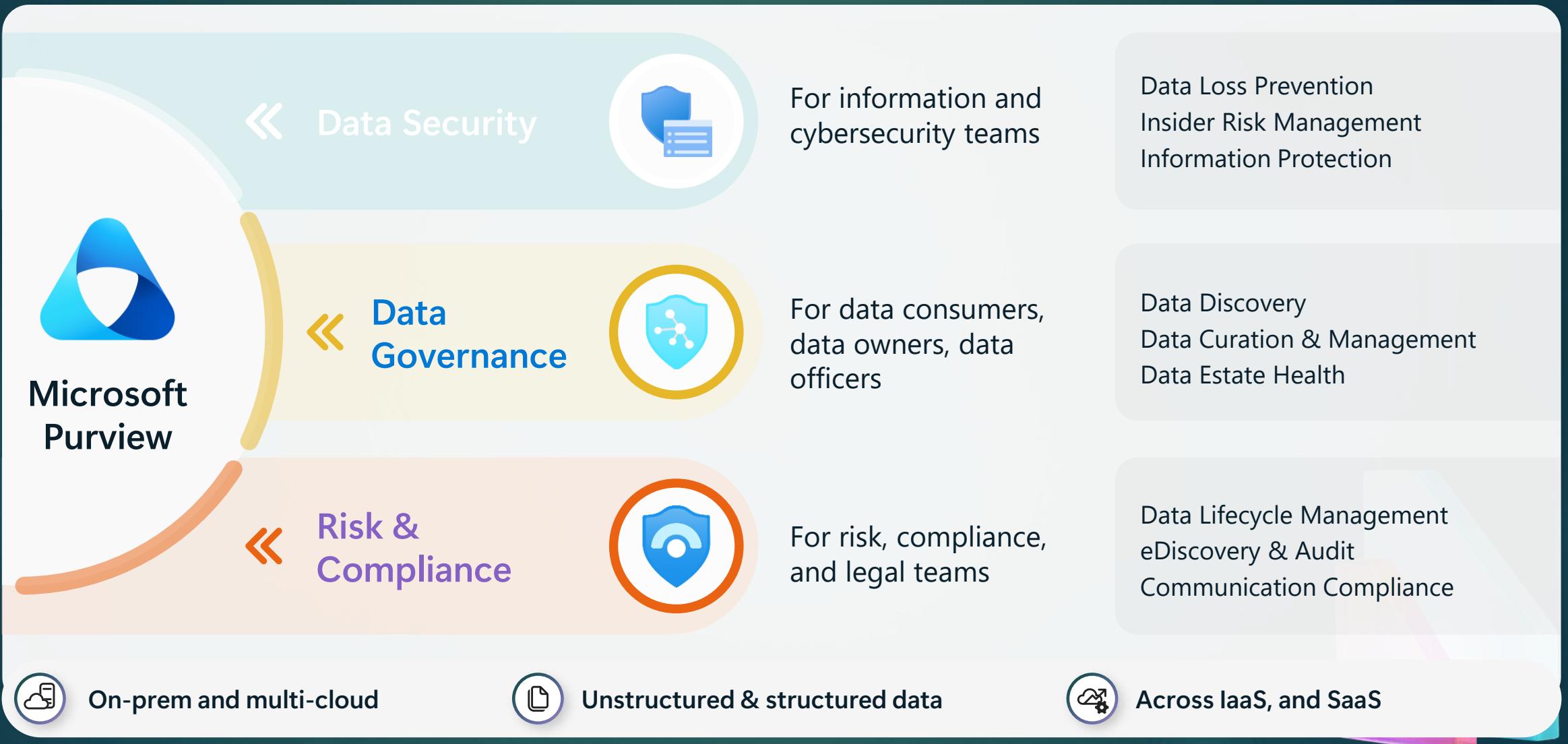
Reshape how you access, manage, and act on data and insights by connecting every data source and analytics service together in Fabric

Keep your data safe and governed with unified data governance, information protection, and risk and compliance solutions

Data ownership

Unmatched security & compliance

Unified governance



Data Security integrations in Fabric

Information Protection

- Manual labeling of Fabric assets
- Label-based access control for specific users and groups
- Downstream inheritance from Lakehouse to other items within a Fabric workspace

Data Loss Prevention

- DLP policies to notify users with policy tips when they interact with sensitive data in semantic models and lakehouse.
- DLP policies to restrict access to users outside of your organization for semantic models

Insider Risk Management

- Detect risky usage signals in PowerBI

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](#)

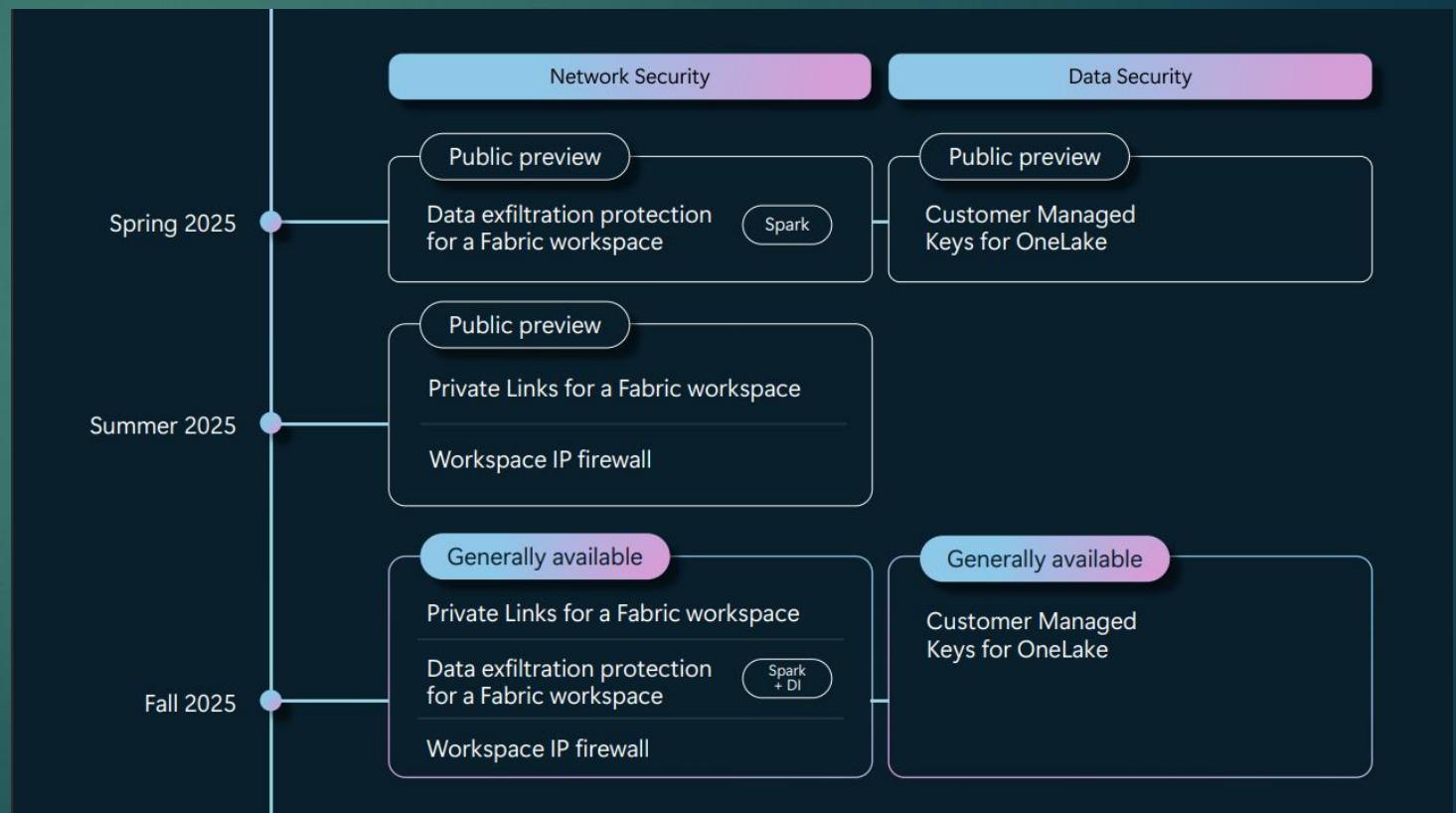
Roadmap

Private Link support at a workspace level

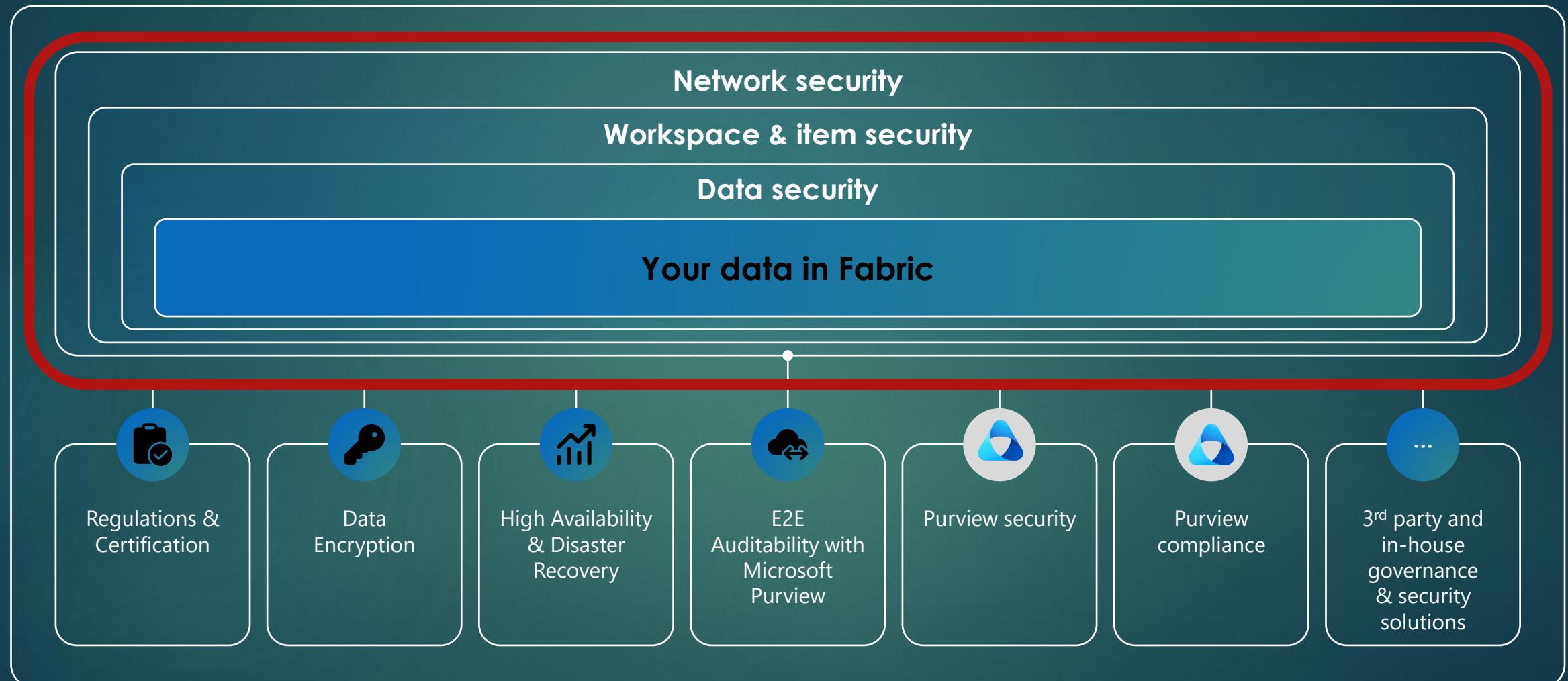
Data exfiltration protection for Spark (Spring)

Workspace Public IP Firewall

Customer Managed Keys(preview)



Recap



Let's connect



Thank you

Feedback in the app

- 🦋 @erwindekreuk.bsky.social
- linkedin linkedin.com/in/erwindekreuk
- 🌐 erwindekreuk.com
- github github.com/edkreuk
- sessionize <https://sessionize.com/erwin-de-kreuk/>
- Dutchfabricusergroup Dutchfabricusergroup.com

