SQL Day

# BUILDING A FORTRESS OF YOUR FABRIC ENVIRONMENT: SECURITY BEST PRACTICES FOR DATA ENGINEERS

## 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

Microsoft® MVP Most Valuable Professional

Microsoft

INSPARK

# Winner

## Partner of the Year Awards

## Country Award Data & AI

## Global Award Identity

# 17th edition
# SQLDay Conference

**12-14 May 2025, WROCŁAW + ONLINE**

SQL Day

## Platinum sponsors

DATUMO

Woodler

## Gold sponsors

lingaro

VOLVO

TECHNOLOGY INNOVATION DATA KNOWLEDGE tidk

software one

Dataedo

## Silver sponsors

Capgemini

DATA RISE LAB

elitmind

C&F

kursy FABRIC


SQL Day

# Cybercriminals are getting more creative just like us

# AI transformation is happening now

| | |
|---|---|
| 95% | of organizations are implementing or developing an AI strategy[1] |
| 75% | of knowledge workers already using AI at work (doubled in the past 6 months)[2] |
| 1% | of risk leaders are thoroughly prepared for mass GenAI availability risks[3] |

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

# Making data security essential for adoption of AI

## Data security incidents are widespread and increasing in severity

**156**

Incidents in 2024 and severity increased from 20% in 2023 to 27% in 2024[1]

## Insider risk is significant

**20%**

insiders account for 20% of data breaches, adding to costs[2]

## Data leaks and oversharing are top of mind concerns

**80%**

of leaders cited leakage of sensitive data as their main concern around adopting Generative AI[3]

[1,2]Microsoft Data Security Index report
[3]First Annual Generative AI Study: Business Rewards vs. Security Risks, Q3 2023, ISMG, N=400

# 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.**

* The value of data | World Economic Forum (weforum.org)

# Agenda

- Microsoft Fabric
- Challenges
- Entra ID
- Inbound / 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

# A world awash with data...

In today's digital age, data is everywhere. From social media interactions to online transactions, the amount of data generated every second is staggering. This vast ocean of information holds immense potential.

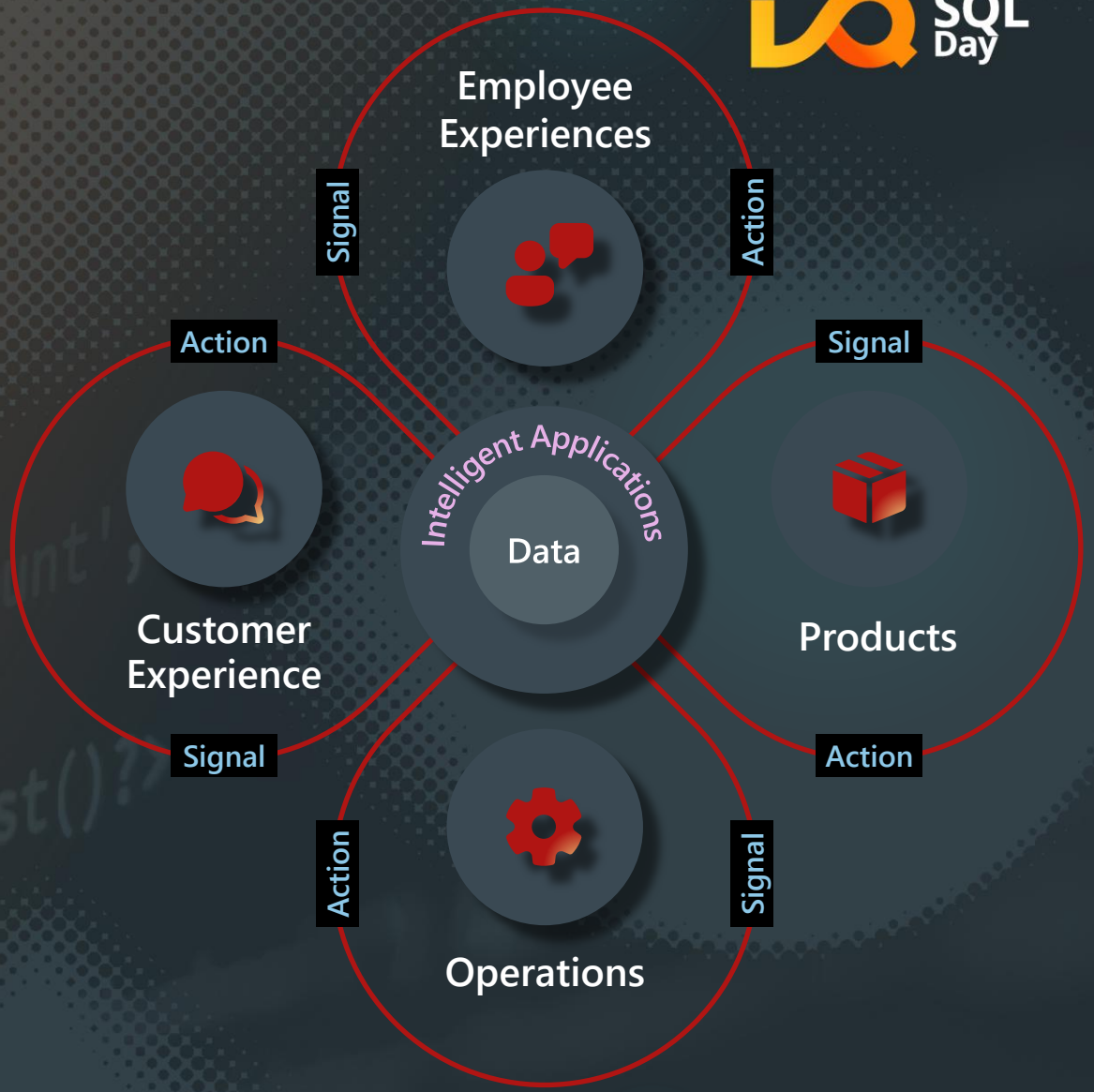
# AI is changing the world

Artificial Intelligence (AI) is at the forefront of this transformation. By leveraging data, AI systems can learn, adapt, and make decisions with unprecedented accuracy and speed. From healthcare to finance, AI is revolutionizing industries, driving innovation, and improving lives.

# 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

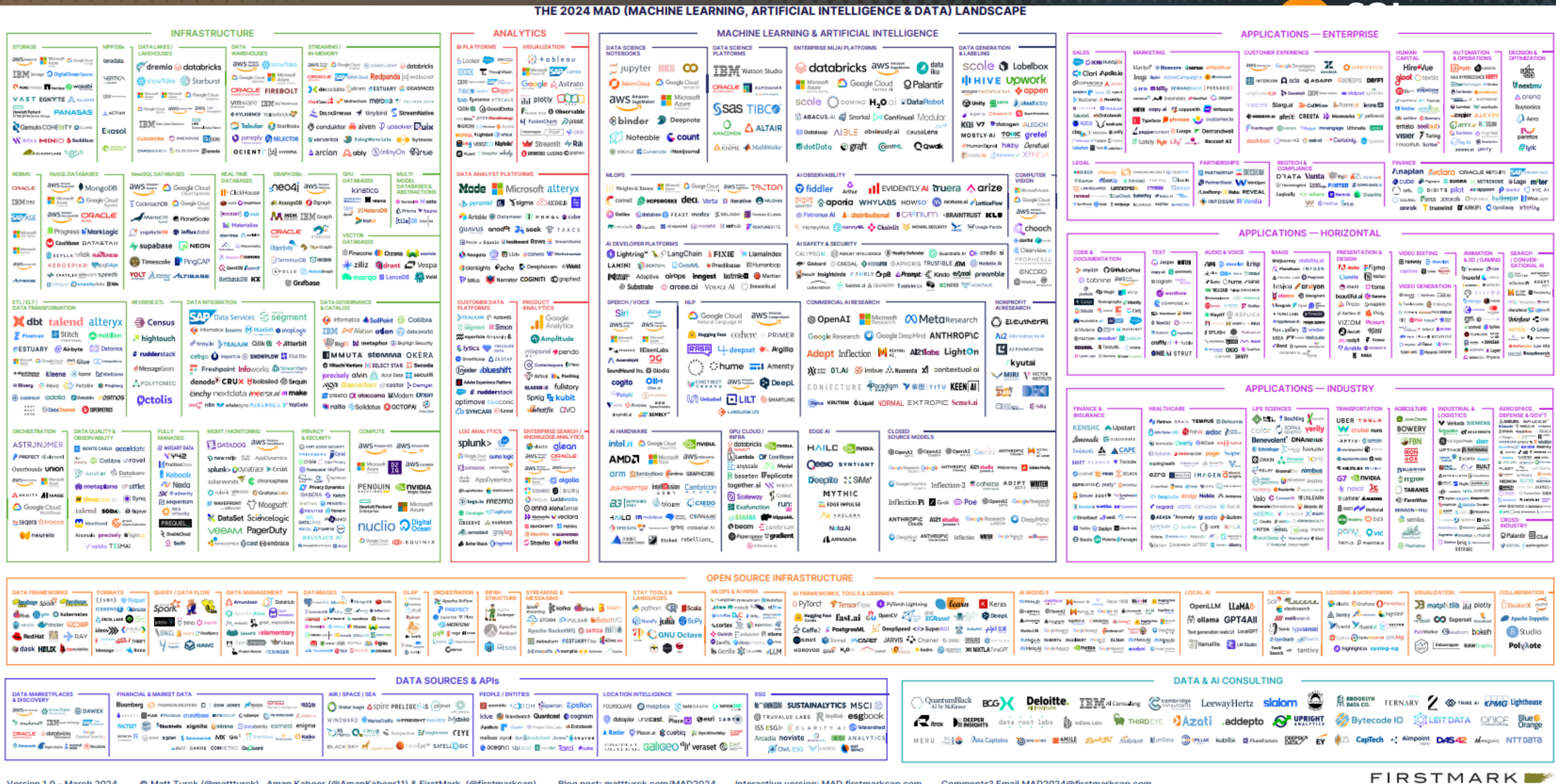


# Security : The Cornerstone of Microsoft Fabric

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



Unify,

I am the Chief Information Officer and don't want to be the Chief Integration Officer.

Help me govern and secure my data estate.

Every CIO, Every Enterprise

# Microsoft Fabric

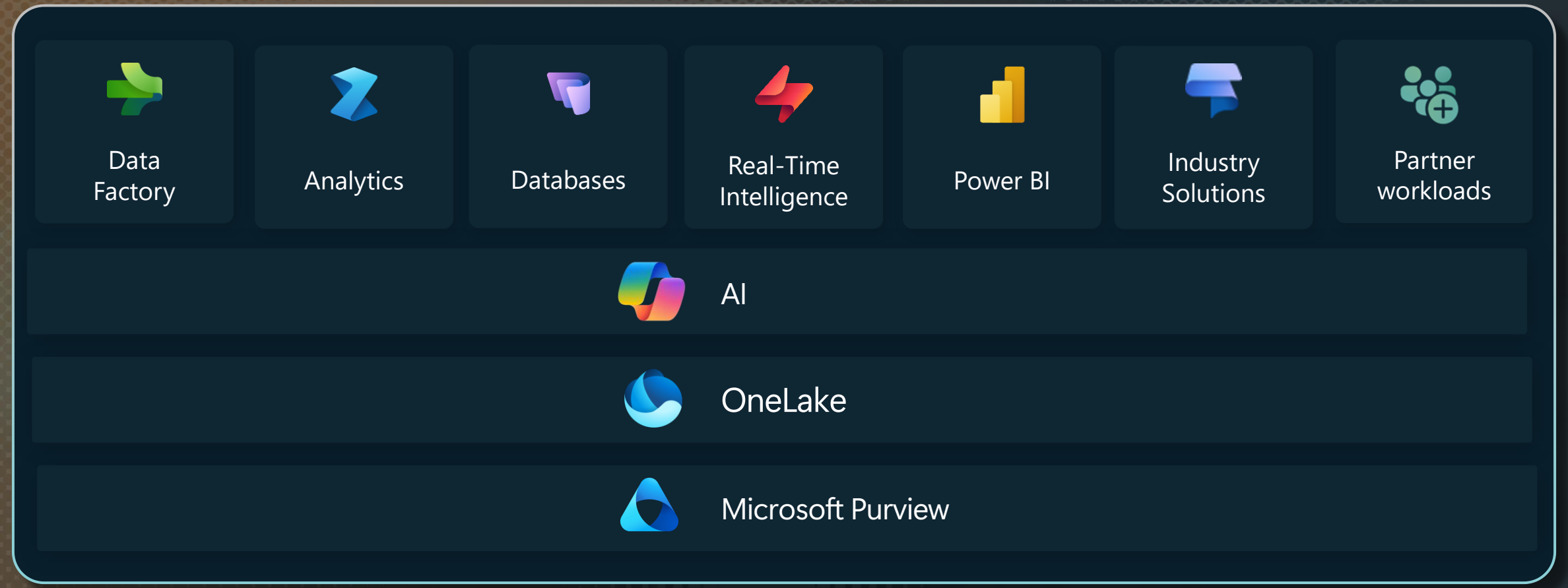
## The unified data platform for AI transformation

SQL Day

| From | | To |
| --- | --- | --- |
| Isolated component | → | Unified stack |
| Single database | → | All the data |
| Gen AI Bolted-in | → | Gen AI built in |

# Microsoft Fabric

## The unified data platform for AI transformation



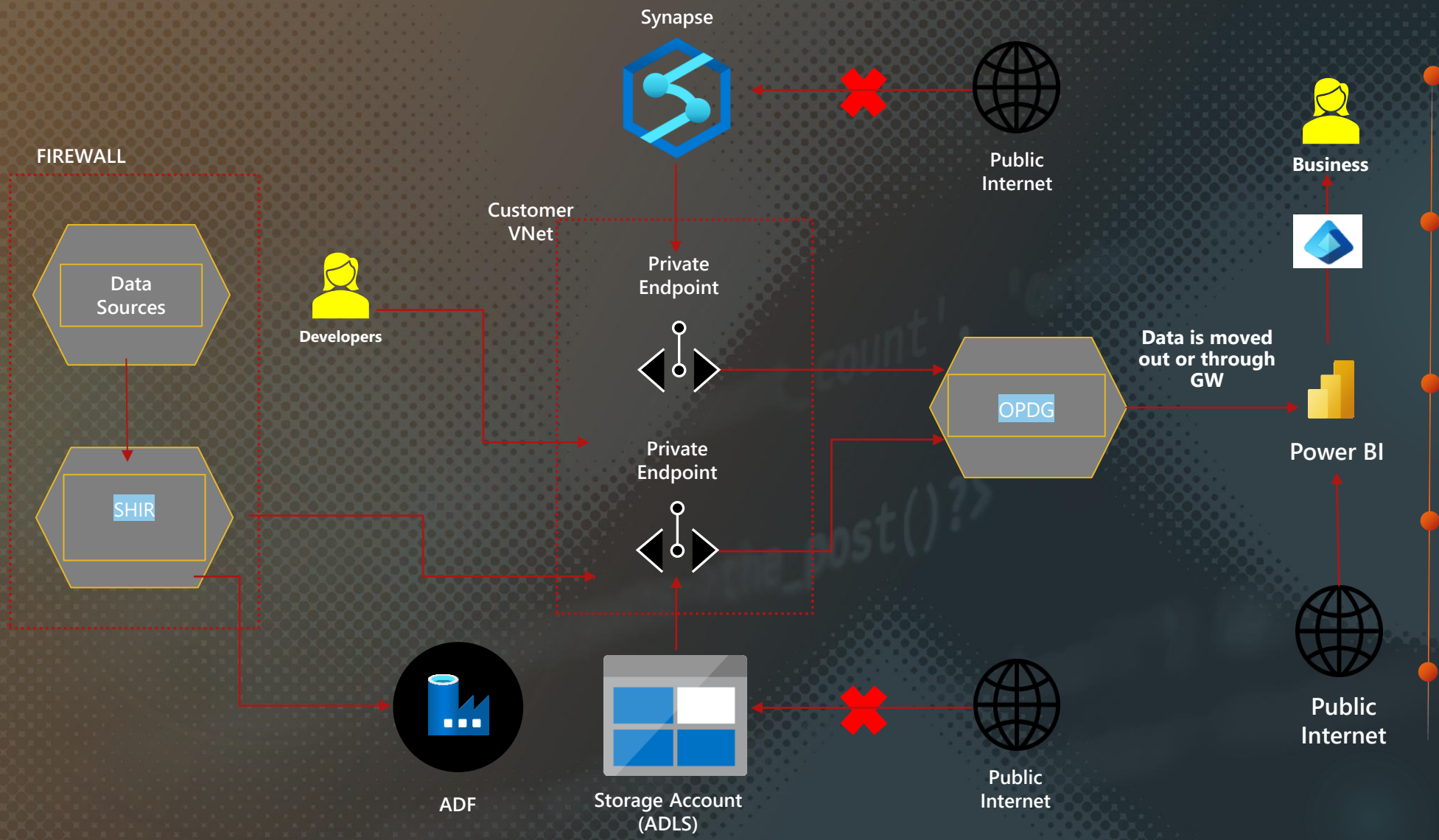
# Modern data challenges

- 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

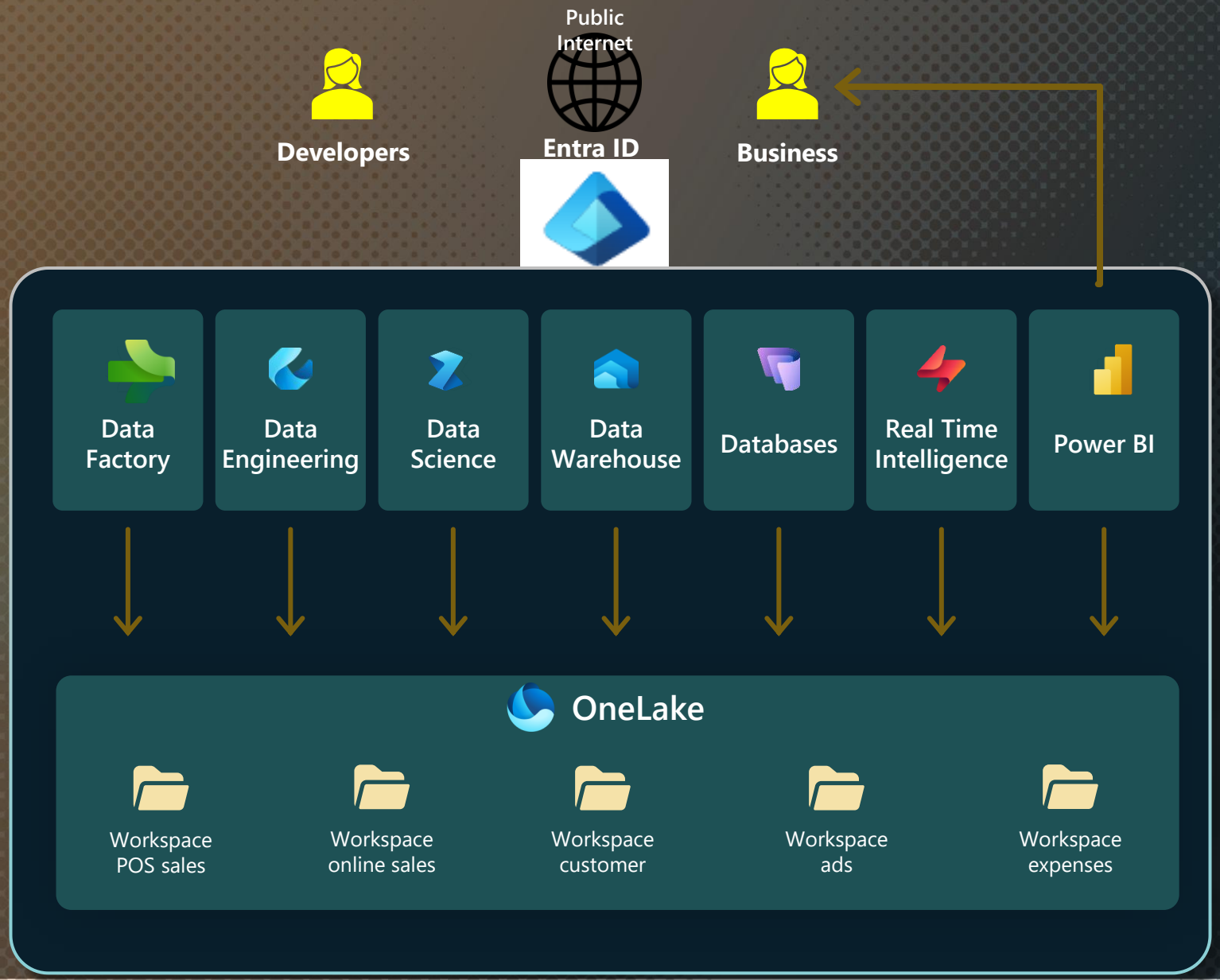
- Need to be able to connect to data inside a firewall\private link from Fabric (outbound).
- Inbound protection (restrict inbound by network location).
- More stringent customers (FSI\HLS):
  - Traffic needs to be private (not via public internet)
  - Endpoints should not be open to the public internet

# 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




Users connect to the SaaS service from global network

Endpoints and access are protected using Entra ID

All internal communications between the experiences happens through MS backbone network

When the CEO access the data in Power BI Report, the data is fetched directly from the OneLake instantly and securely without copying or moving

# Entra ID

# Microsoft Entra

**Any employee**
Cloud-based and on-premises identities, groups and roles

**Any location**
HQ, branch office, home, remote

**Any platform**
Android, iOS, Linux, MacOS, Windows

**Any device**
Corporate and personal


Any data, apps or resources

**IaaS, PaaS, Datacenter**

**Microsoft 365**

**Microsoft Fabric**

**SaaS, websites**

**On-premises**

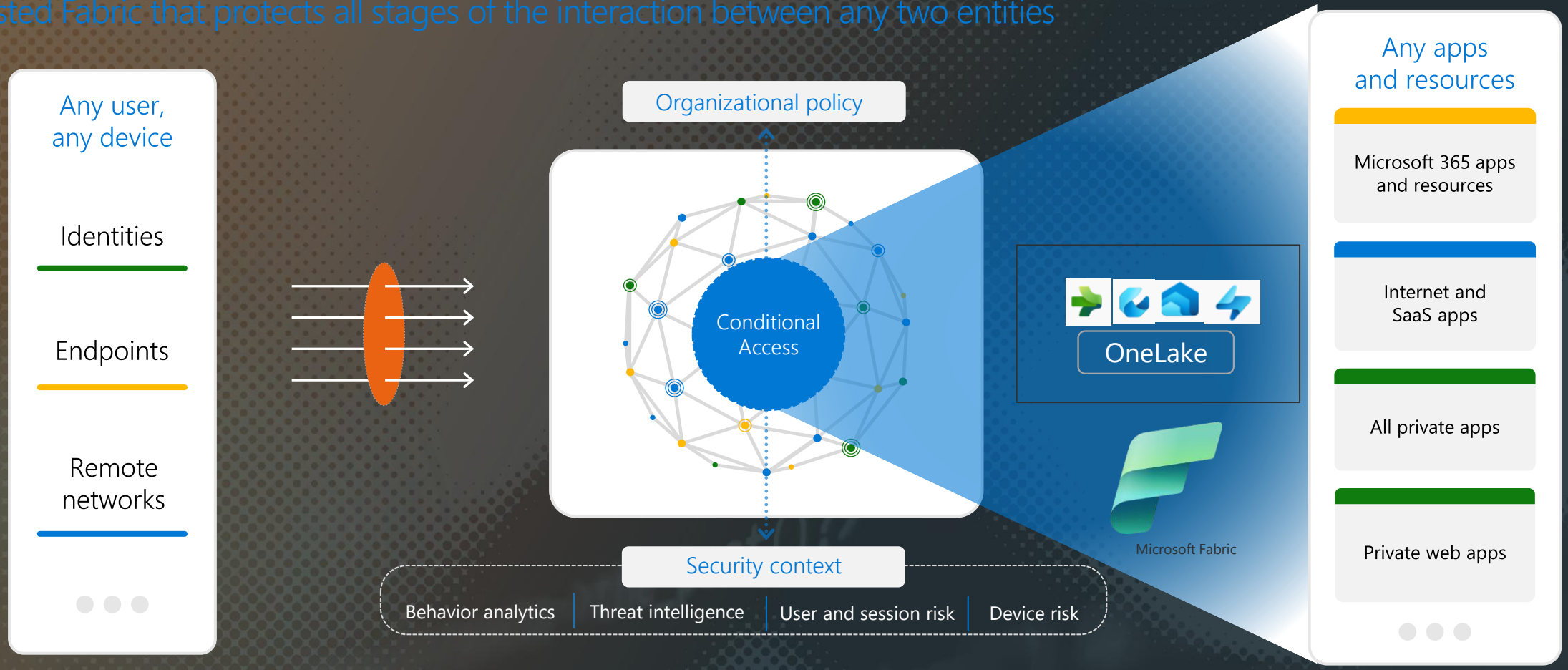
Secure Access for a connected world


SQL Day

- Unify conditional access
- Ensure least privilege access
- Improve the user experience
- Reduce on-premises footprint

# Conditional Access - Microsoft's Adaptive Access Vision

Trusted Fabric that protects all stages of the interaction between any two entities




## Centralized control

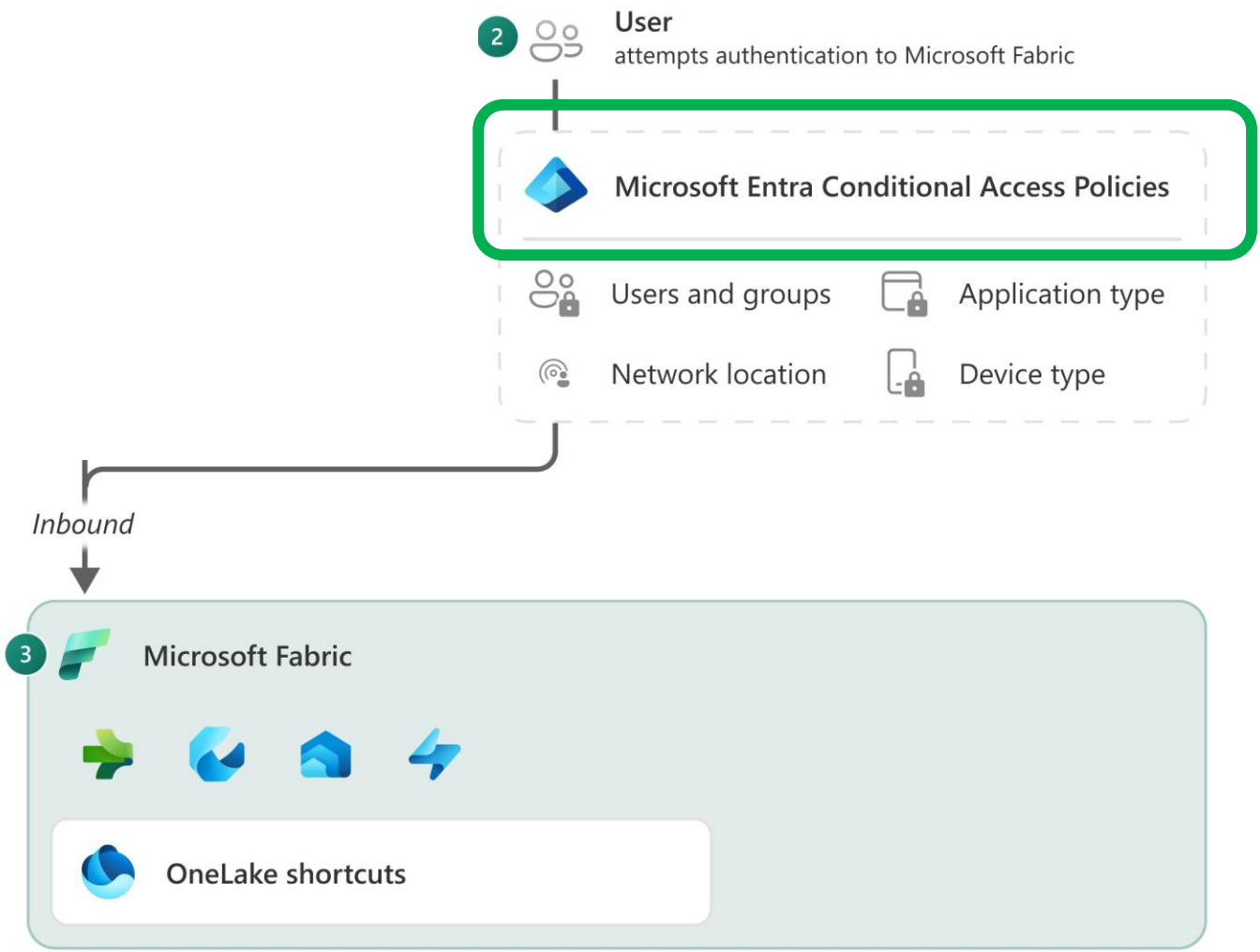
Unified Zero Trust architecture and policy engine simplifies management of access controls and technologies (Directory, SSO, Federation, RBAC, proxy, and more)

## Consistent enforcement

Centralized policy is consistently applied across all resources where the action happens (identity, data, network + infra and apps across cloud, on-premises, IoT, OT, and more)

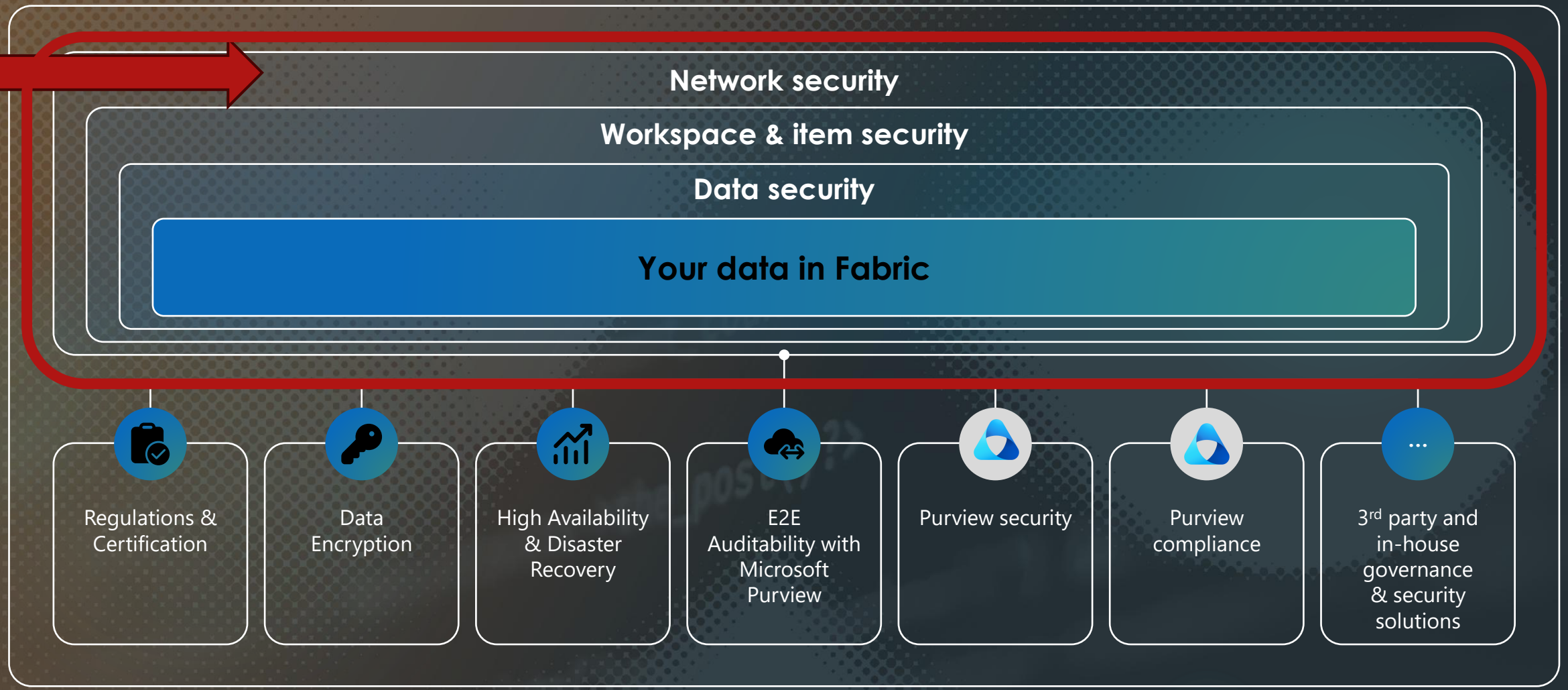
# Microsoft Fabric Conditional Access

- Conditional access requires Microsoft Entra ID P1 licenses.



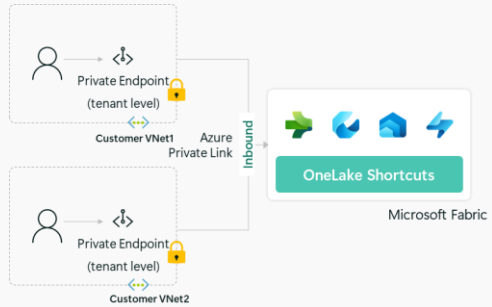

DEMO

# Security layers in Microsoft Fabric



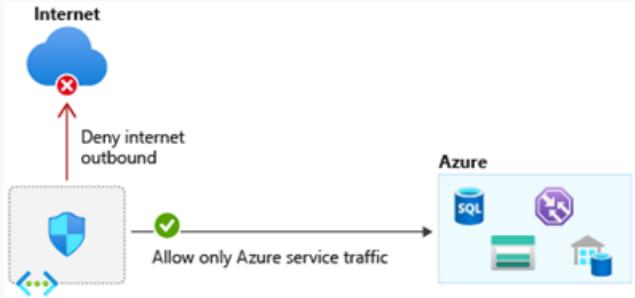
# Secure inbound and outbound network connections

## Secure and protect data across your organization



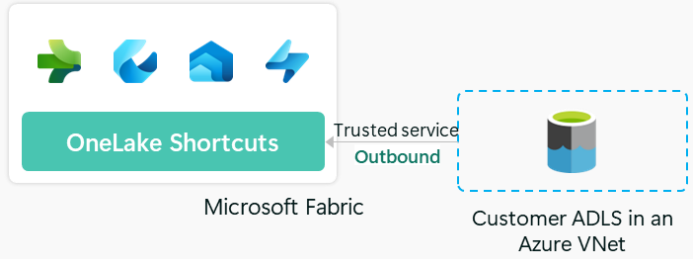

### Fabric inbound security

Seamlessly secure inbound data access scenarios with Fabric's holistic identity and network security




### Service tags

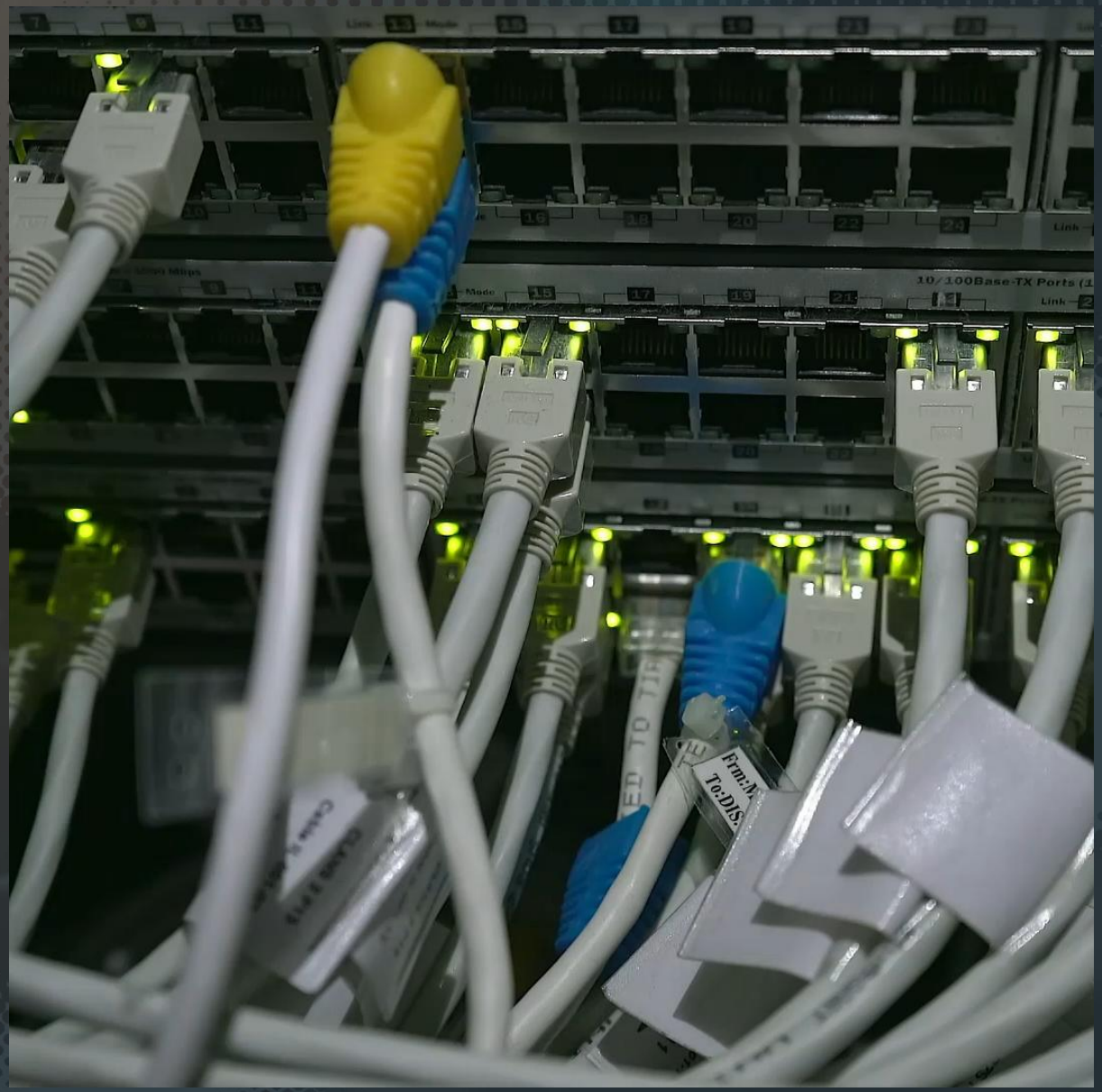
Minimize the complexity of updating network security rules using Azure service tags to group and manage IP addresses for a service




### Fabric outbound security

Securely connect to your protected data sources and/or ingest data into OneLake

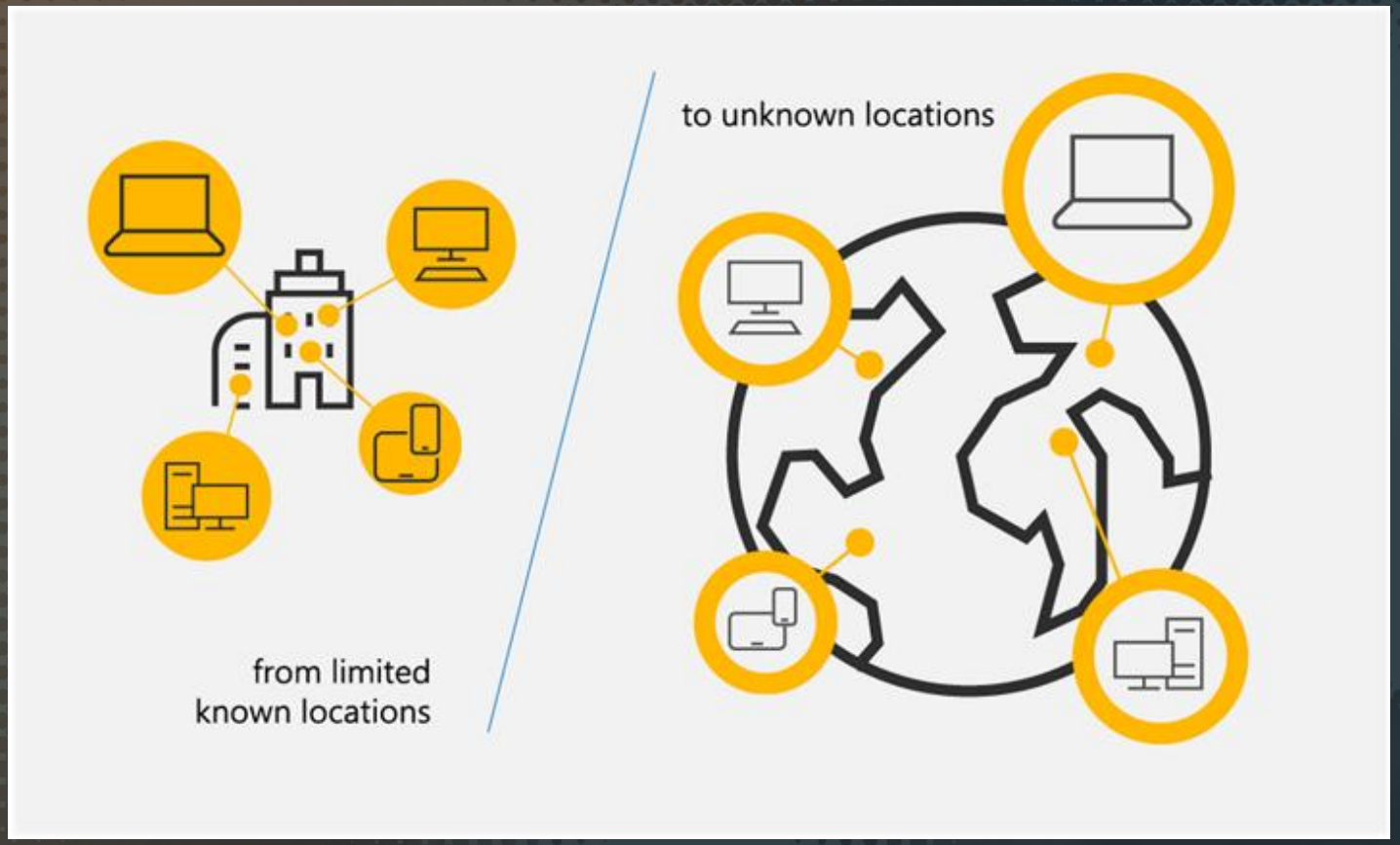
# Fabric Inbound Security



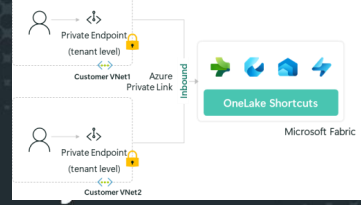
# Inbound protection options

**Perimeter Network Security**

**Zero Trust Approach(Conditional Access)**

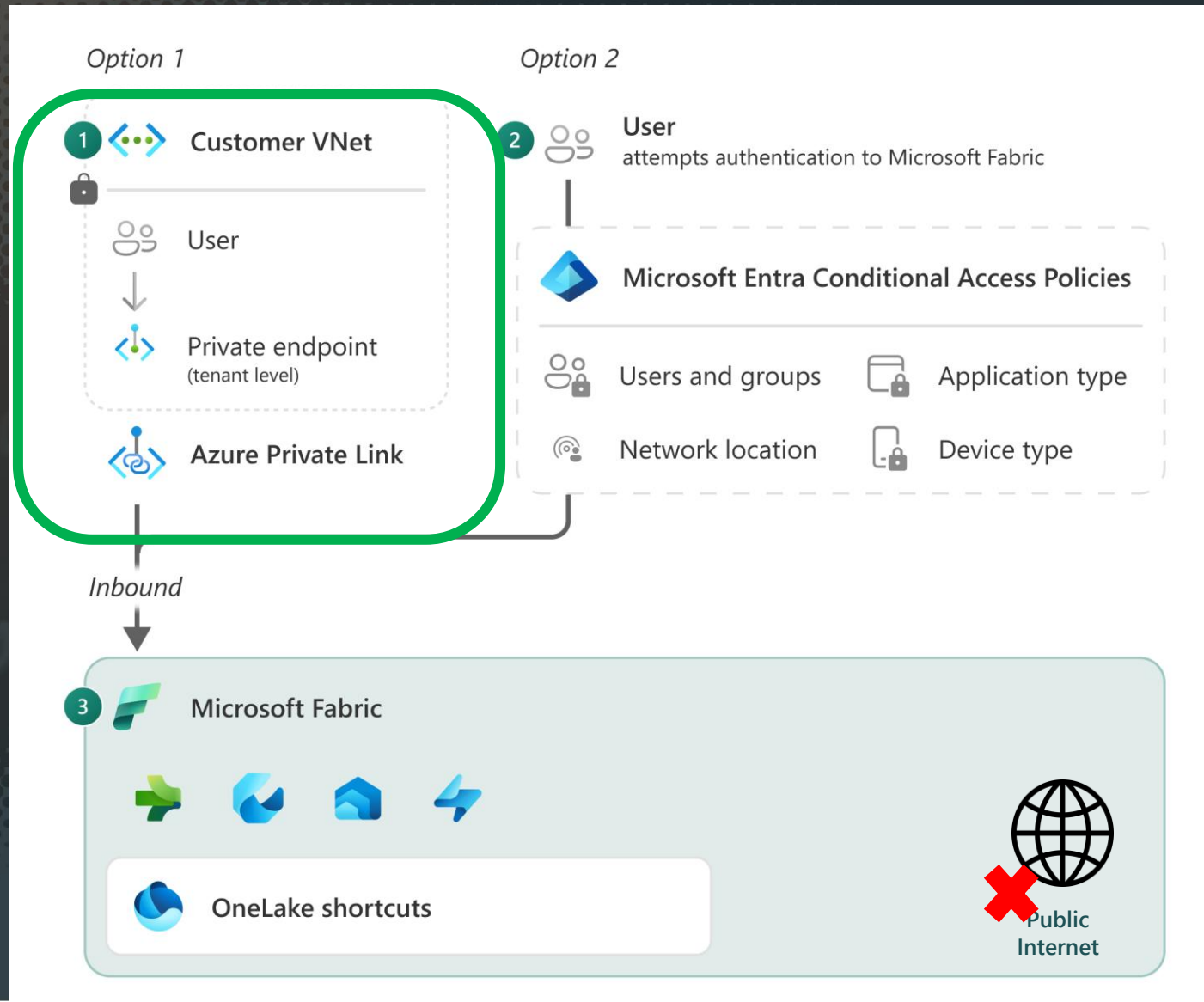


# Private Link for Fabric



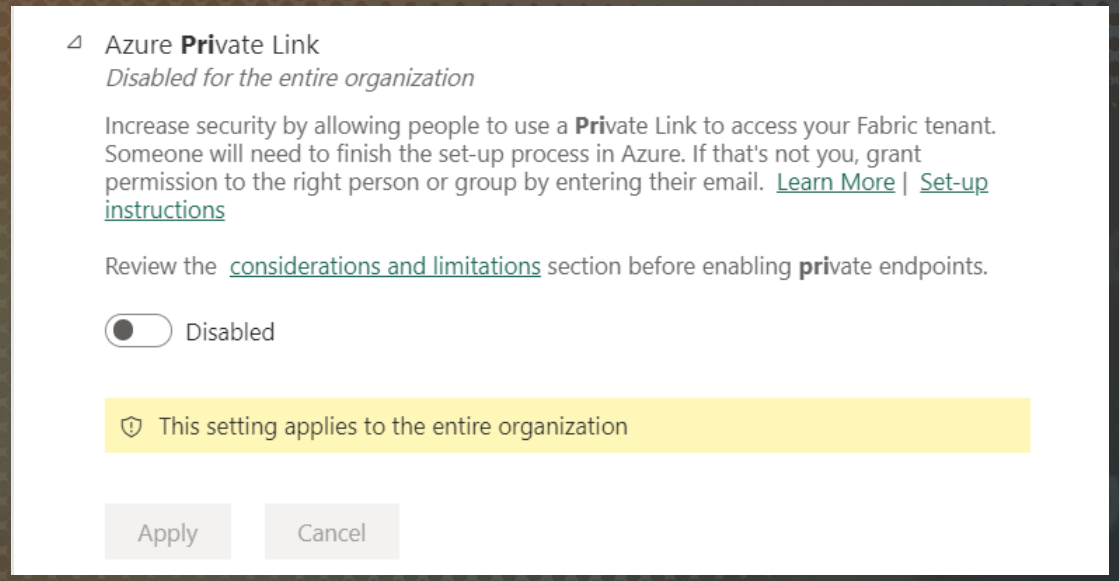

- What it means:

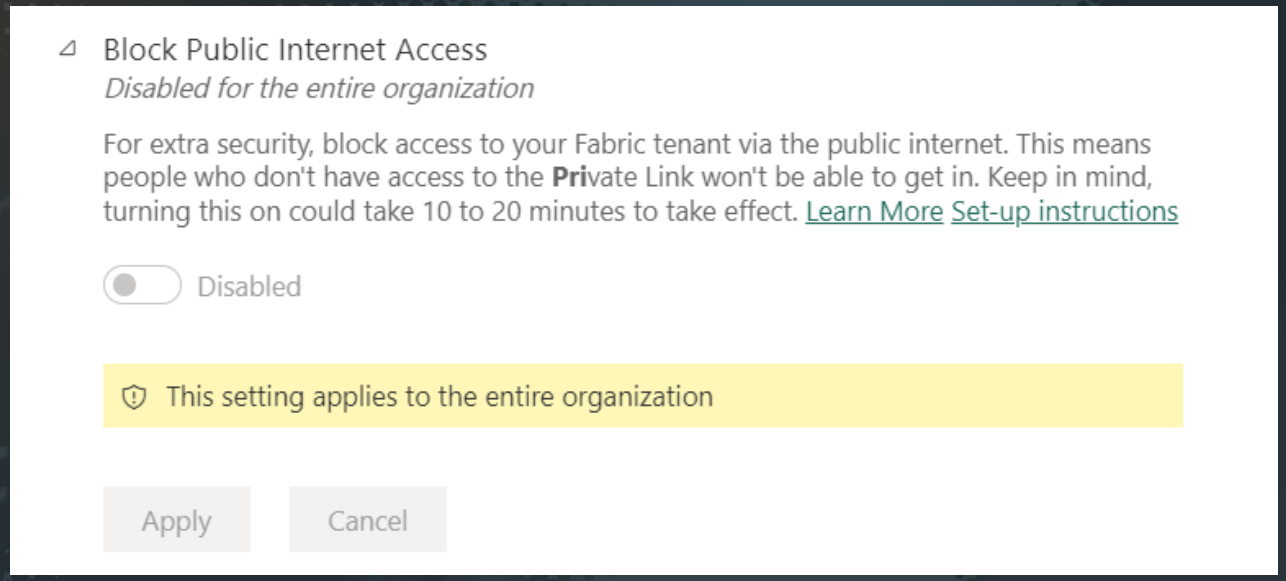
1. Fabric is disconnected from the public internet
2. Every users needs to connect to the private network to get access on every device
3. No longer able to load resources locally (slower reports)
4. Increases ExpressRoute bandwidth and added costs for Private Links
5. Several product limitations (like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



# Private Link for Fabric

- Private Link for Fabric (Admin Portal)
- Admin Portal



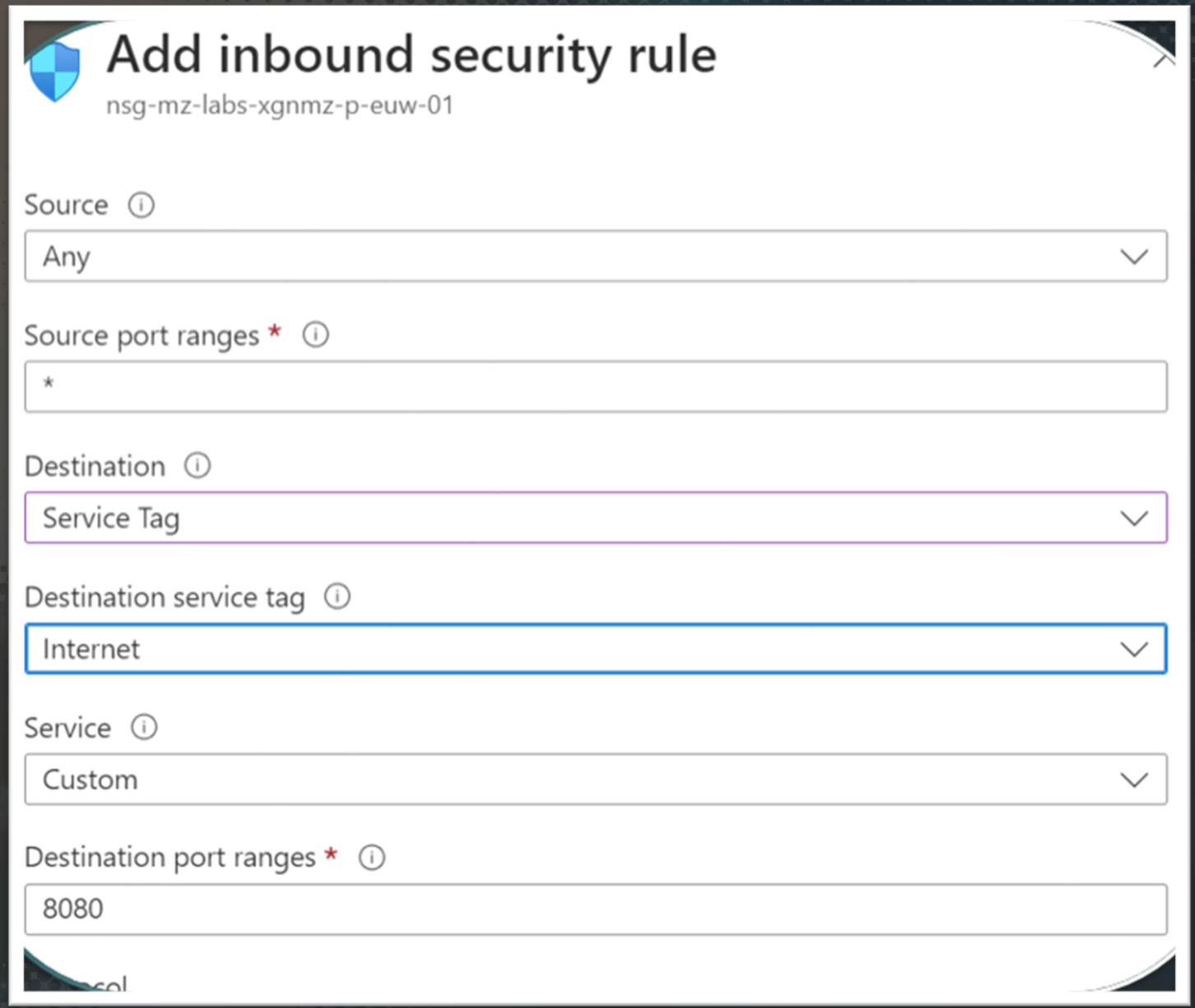



# Private Links

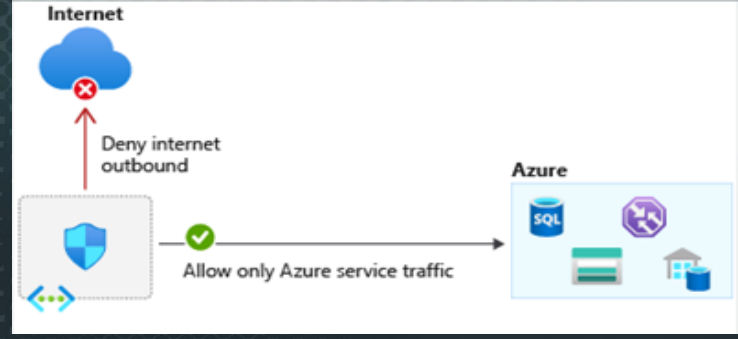
## Limitations

- 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.

# Service Tags



# Service Tags

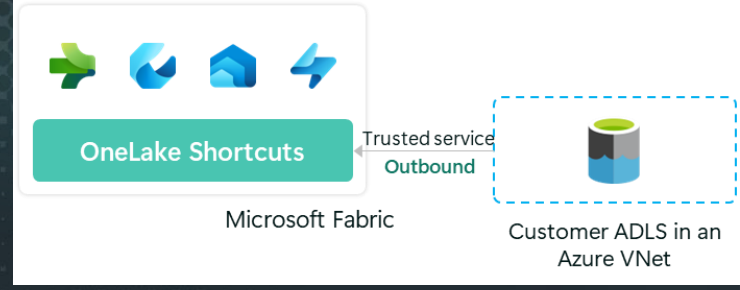



- You can use Azure service tags to enable connections to and from Microsoft Fabric.
- A service tag is a defined group of IP addresses that is automatically managed, as a group, to minimize the complexity of updates or changes to network security rules
- You can use the service tags to define network access controls:
  - Network security groups.
  - Azure Firewall.
  - User-defined routes..

| | | | | |
|---|---|---|---|---|
| DataFactory | Azure Data Factory | Both | No | Yes |
| DataFactoryManagement | On premises data pipeline activity | Outbound | No | Yes |
| EventHub | Azure Event Hubs | Outbound | Yes | Yes |
| Power BI | Power BI and Microsoft Fabric | Both | No | Yes |
| PowerQueryOnline | Power Query Online | Both | No | Yes |
| KustoAnalytics | Real-Time Intelligence | Both | No | No |
| SQL | Fabric SQL | Both | Yes | Yes |

# Fabric Outbound Security

# Getting data into Fabric




Trusted Access for Fabric Workspace Identity

Storage Account (ADLS)

Workspace 1
Shortcuts

Workspace 2
Shortcuts

Workspace N

OneLake

Inbound

Managed Private Endpoint

Customer VNet

Public Internet

Create and use managed private endpoints in Microsoft Fabric - Microsoft Fabric | Microsoft Learn


DEMO

Power BI Fabcon_Demo

Search

Trial: 28 days left

78

Home
Create
Browse
OneLake
Apps
Metrics
Monitor
Learn
Real-Time
Workspaces
Fabcon_Demo
LH_Data_Landingzone
Power BI

# Fabcon_Demo

Create deployment pipeline | Create app | Manage access | Workspace settings

New item | New folder | Import

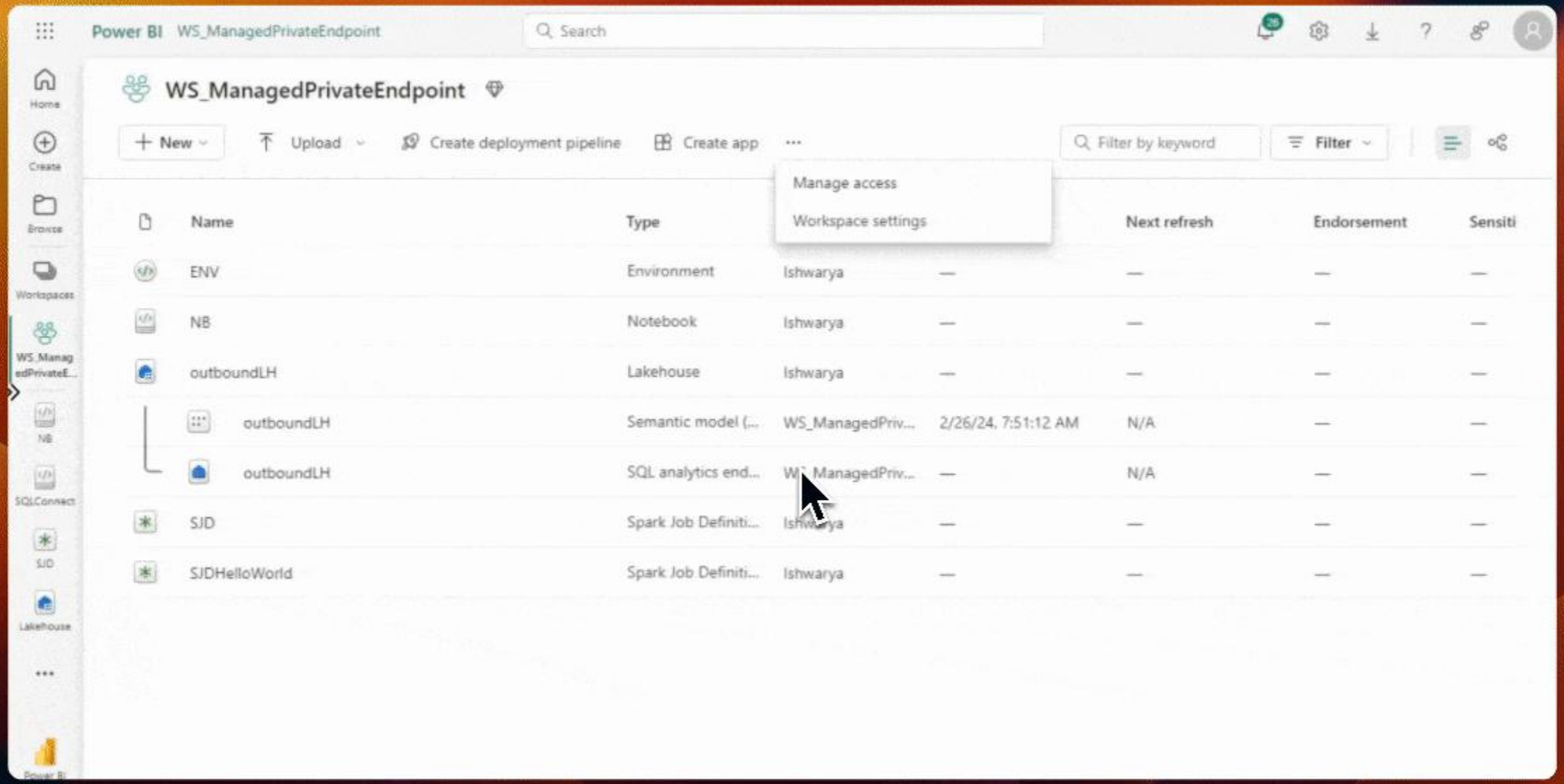
Filter by keyword | Filter

## Choose from predesigned task flows or add a task to build one (preview)

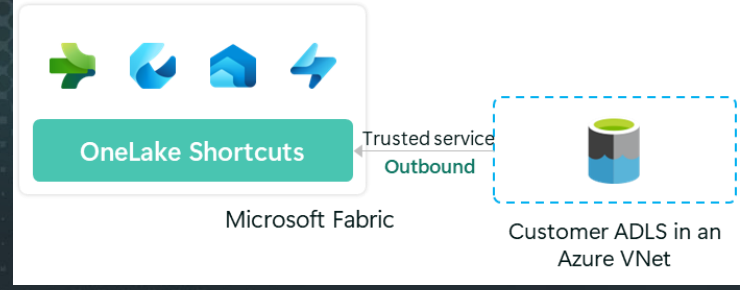
Select from one of Microsoft's predesigned task flows or add a task to start building one yourself.

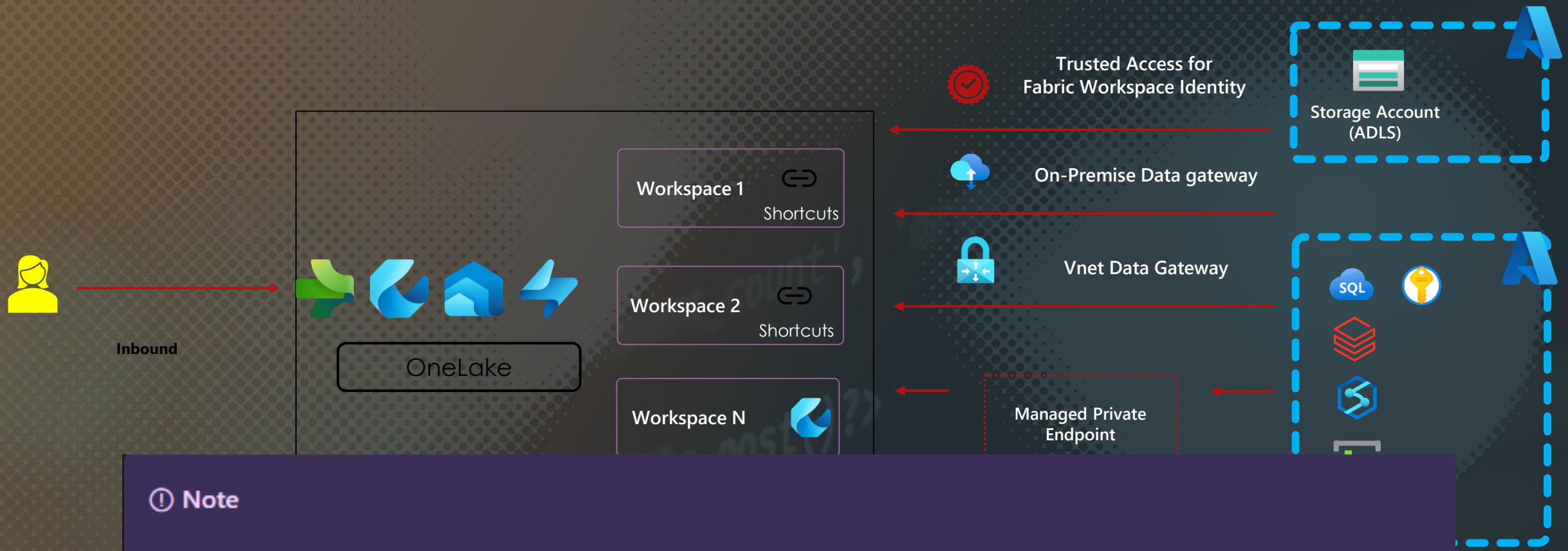
Select a predesigned task flow | Add a task

| Name | Type | Task | Owner | Refreshed | Next refresh | Endorsement | Sensitivity | Included in app |
|---|---|---|---|---|---|---|---|---|
| LH_Data_Landingzone | Lakehouse | — | Erwin de Kreuk | — | — | — | Internal | |
| LH_Data_Landingzone | Semantic mod... | — | Fabcon_Demo | 3/5/2025, 6:48:0... | N/A | — | Internal | |
| LH_Data_Landingzone | SQL analytics ... | — | Erwin de Kreuk | — | — | — | — | |


Power BI
WS_ManagedPrivateEndpoint
Search
Home
Create
Browse
Workspaces
WS_ManagedPrivateE...
NB
SQLConnect
SJD
Lakehouse
Power BI
WS_ManagedPrivateEndpoint
New
Upload
Create deployment pipeline
Create app
Filter by keyword
Filter
Manage access
Workspace settings
Name
Type
Next refresh
Endorsement
Sensiti
ENV
Environment
Ishwarya
NB
Notebook
Ishwarya
outboundLH
Lakehouse
Ishwarya
outboundLH
Semantic model (...
WS_ManagedPriv...
2/26/24, 7:51:12 AM
N/A
outboundLH
SQL analytics end...
N/A
SJD
Spark Job Definiti...
Ishwarya
SJDHelloWorld
Spark Job Definiti...
Ishwarya

# Getting data into Fabric




**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.

Create and use managed private endpoints in Microsoft Fabric - Microsoft Fabric | Microsoft Learn

# 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 |
| --- | --- | --- |

SQL Day

Microsoft Purview

## Data Security

For information and cybersecurity teams

Data Loss Prevention
Insider Risk Management
Information Protection

## Data Governance

For data consumers, data owners, data officers

Data Discovery
Data Curation & Management
Data Estate Health

## Risk & Compliance

For risk, compliance, and legal teams

Data Lifecycle Management
eDiscovery & Audit
Communication Compliance

On-prem and multi-cloud

Unstructured & structured data

Across IaaS, and SaaS

# 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

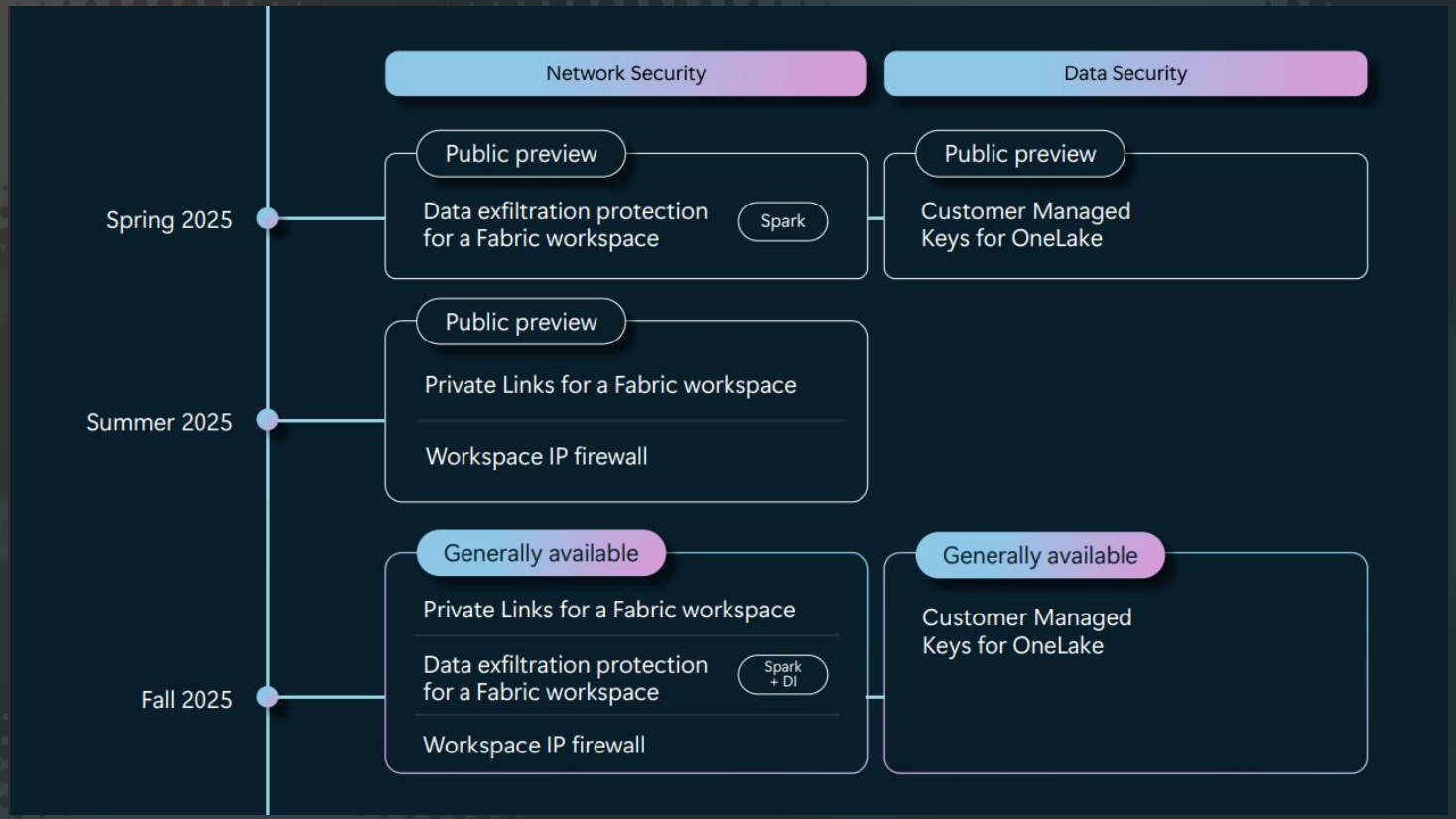
Detect risky usage signals in PowerBI

# Microsoft Fabric Compliancy

- GDPR
- EUDB
- ISO certifications including ISO 27001, 27701, 27017, 27018
- HIPAA, HITRUST compliant
- SOX compliant
- SOC 1, SOC 2, Type 2
- FedRamp

# Roadmap

- Private Link support at a workspace level
- Data exfiltration protection for Spark (Spring)
- Workspace Public IP Firewall
- Customer Managed Keys



Let's connect

# Thank you

# Feedback in the Whova app

@erwindekreuk.bsky.social

linkedin.com/in/erwindekreuk

erwindekreuk.com

github.com/edkreuk

https://sessionize.com/erwin-de-kreuk/

Dutchfabricusergroup.com

Microsoft® MVP Most Valuable Professional