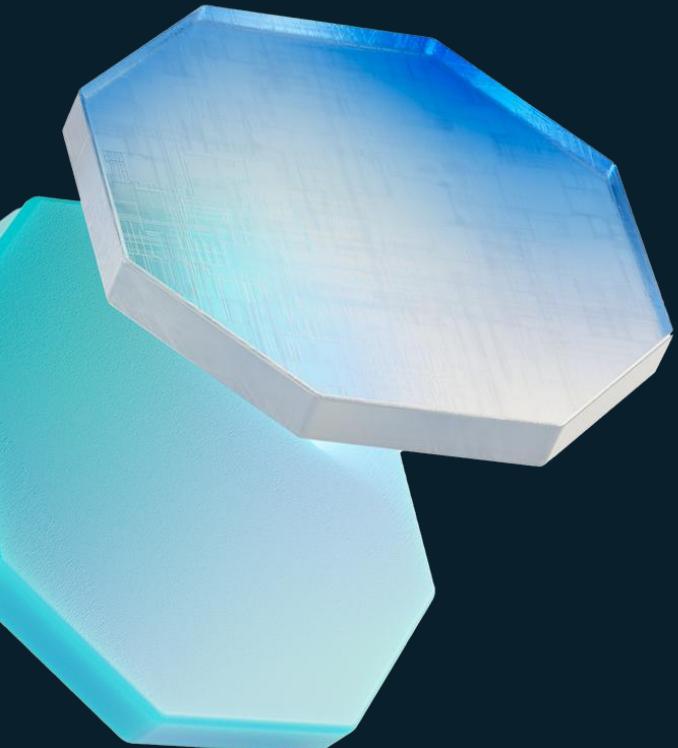


Building a Fortress of Your Fabric Environment: **Security** Best Practices for Data Engineers



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





Winner

Partner of the
Year Awards

Country Award Data & AI
Global Award Identity







Cybercriminals are
getting more
creative just like us

IT Security Challenges

- Increased Attack Surface
- Digital transformation accelerated the adoption of new interconnected technologies

- Compliance & Regulatory requirements



4M
A white briefcase icon inside a white circle, positioned above the number "4M".

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

- 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.

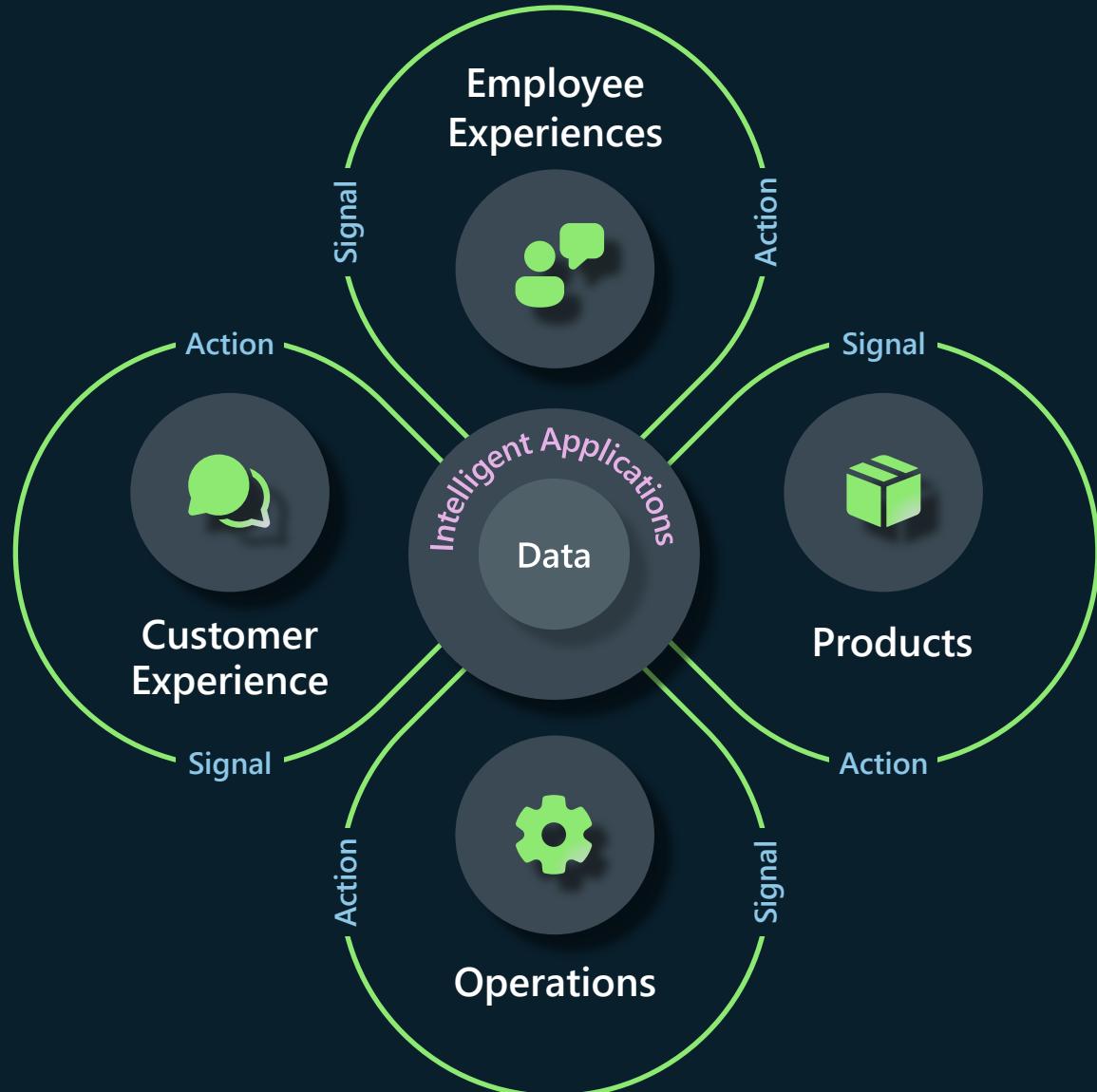
AI is changing the world

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"

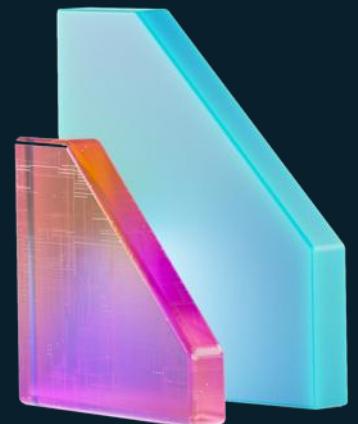
Forrester Analytics Business Technographics Global Data & Analytics Survey



Security : The Cornerstone of Microsoft Fabric

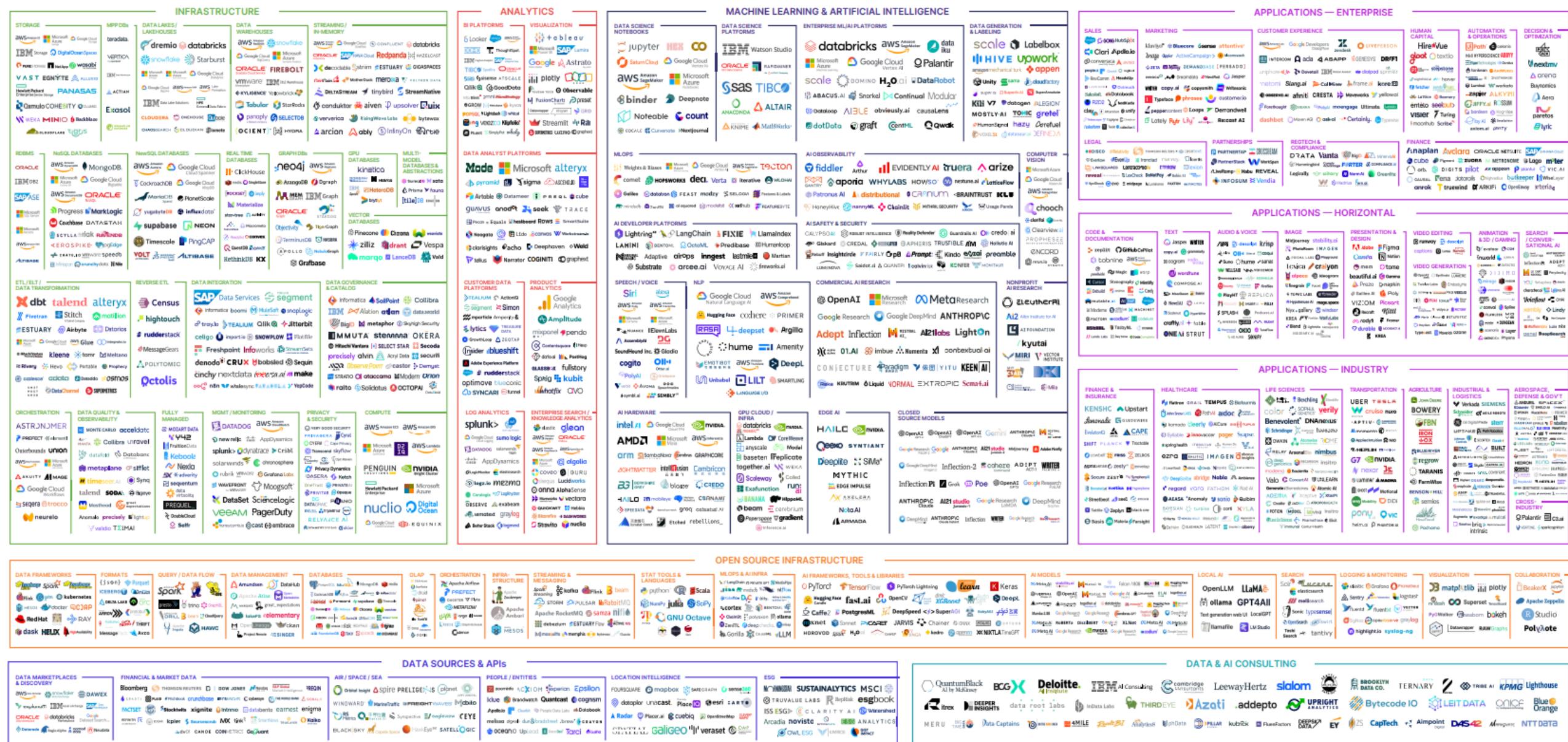
Security is paramount in the digital age, and Microsoft Fabric ensures your data is protected at every stage. By using Fabric, organizations can trust that their data is secure, allowing them to focus on innovation and growth.

How do you translate data into
competitive advantage



The 2024 ML, AI, and Data Landscape

THE 2024 MAD (MACHINE LEARNING, ARTIFICIAL INTELLIGENCE & 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



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.

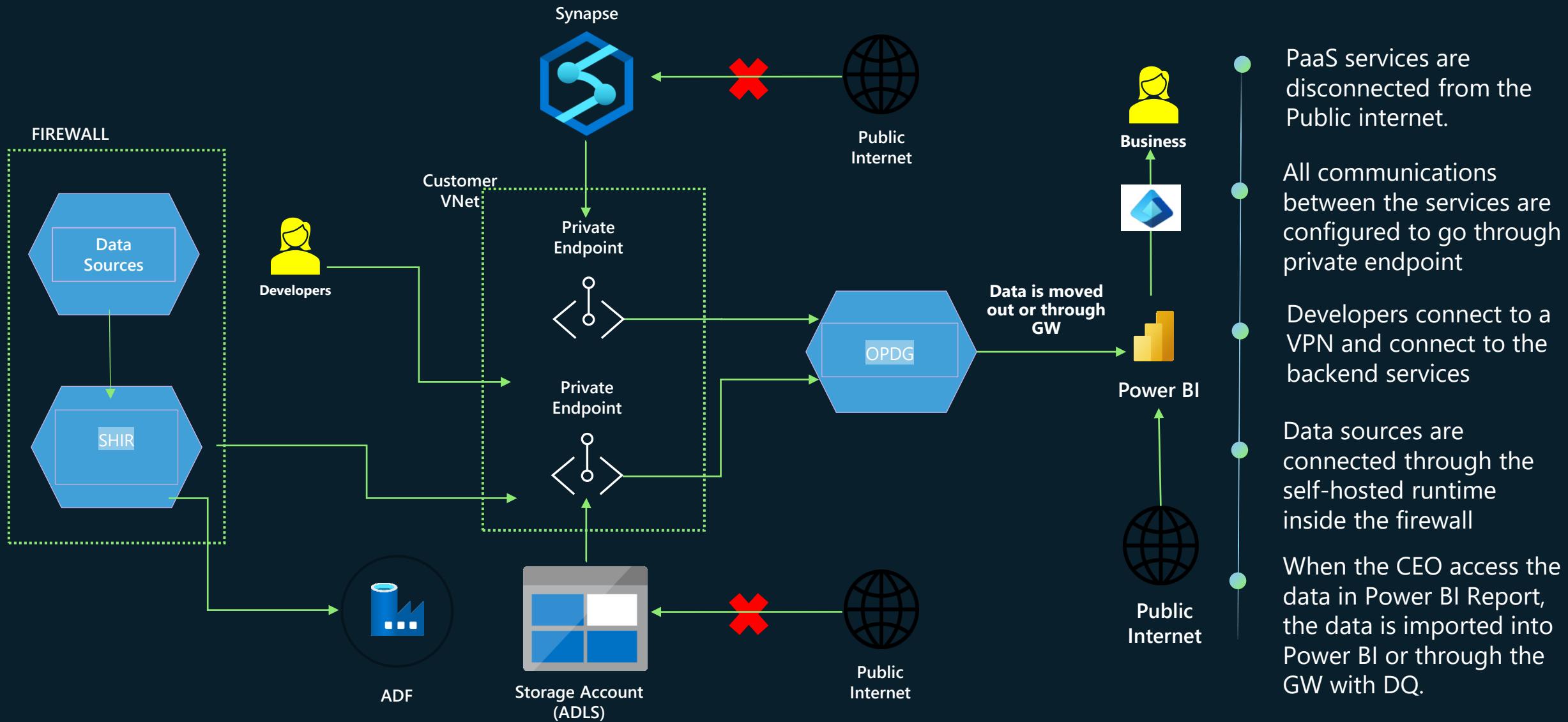


Common network security requirements

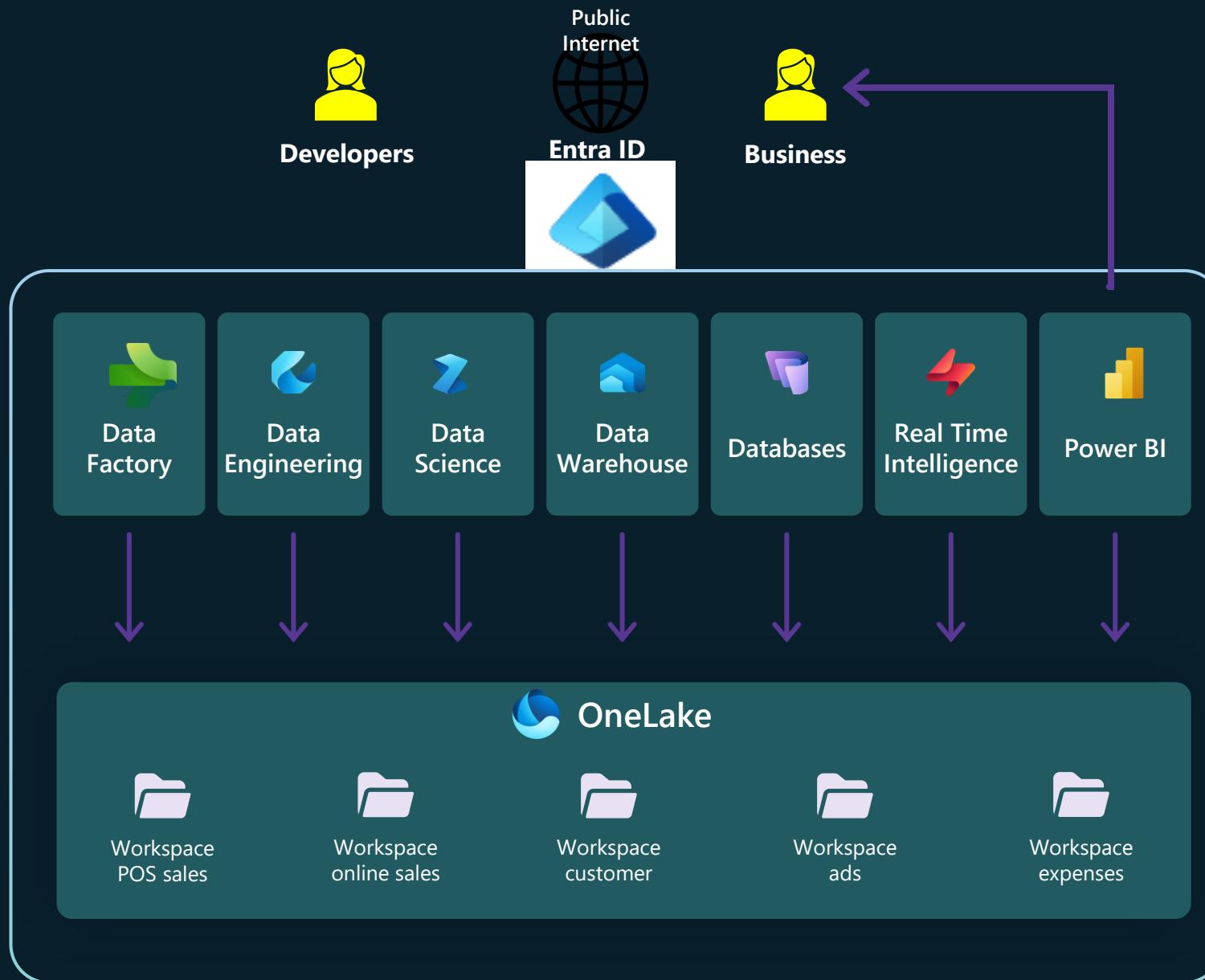
- Need to be able to connect to data inside a firewall\private link from Fabric (outbound).
- Inbound protection (restrict inbound by network location).
- More stringent customers (FSI\HLS):
 - Traffic needs to be private (not via public internet)
 - Endpoints should not be open to the public internet



Existing PaaS World



Microsoft Fabric – SaaS World



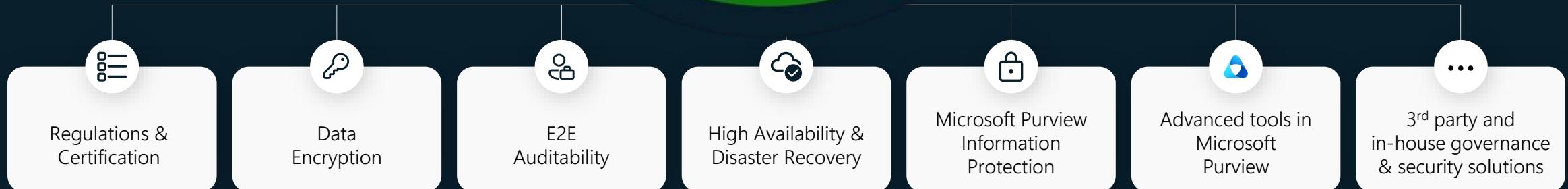
Users connect to the SaaS service from global network

Endpoints and access are protected using Entra ID

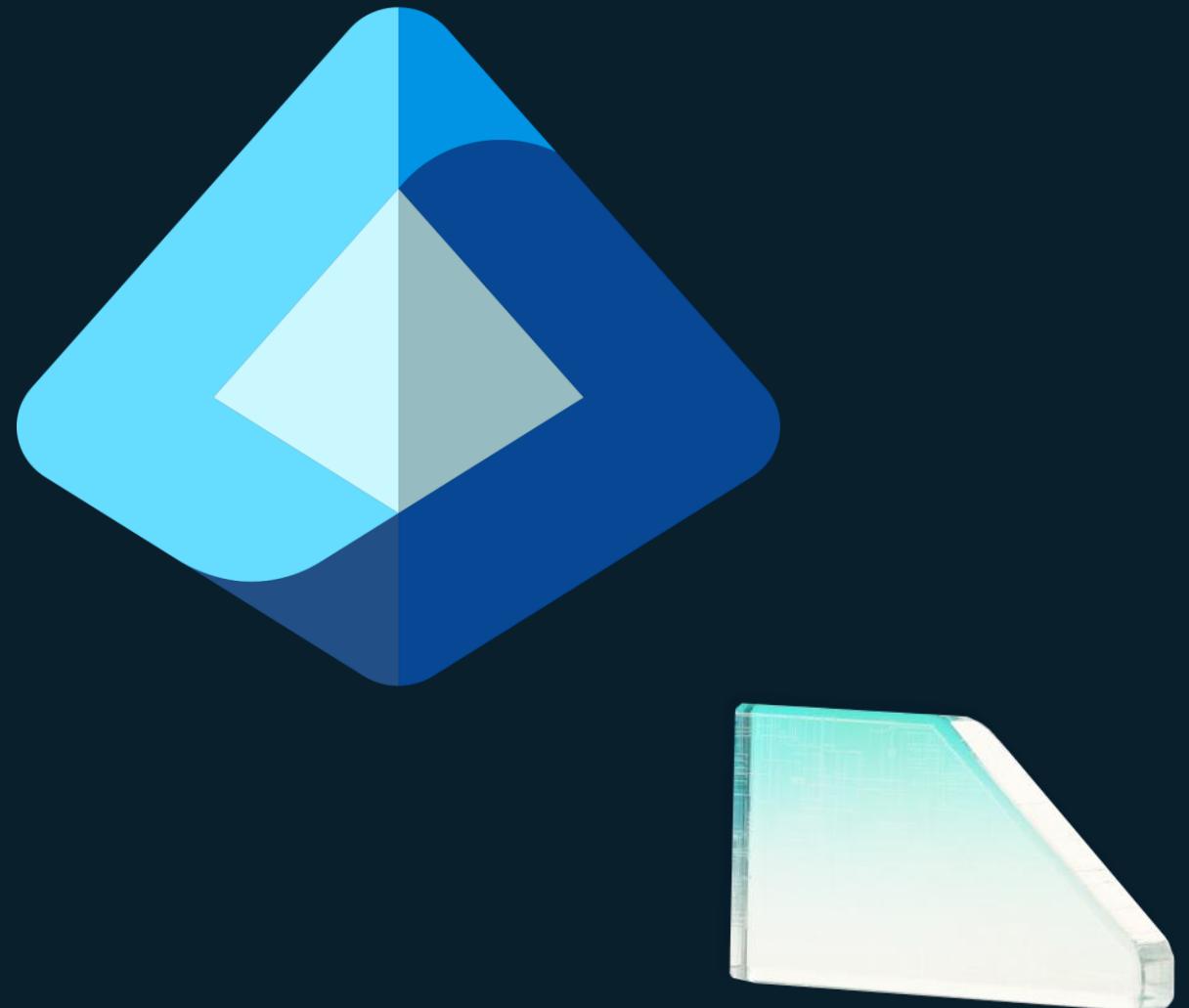
All internal communications between the experiences happens through MS backbone network

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

Security layers in Microsoft Fabric

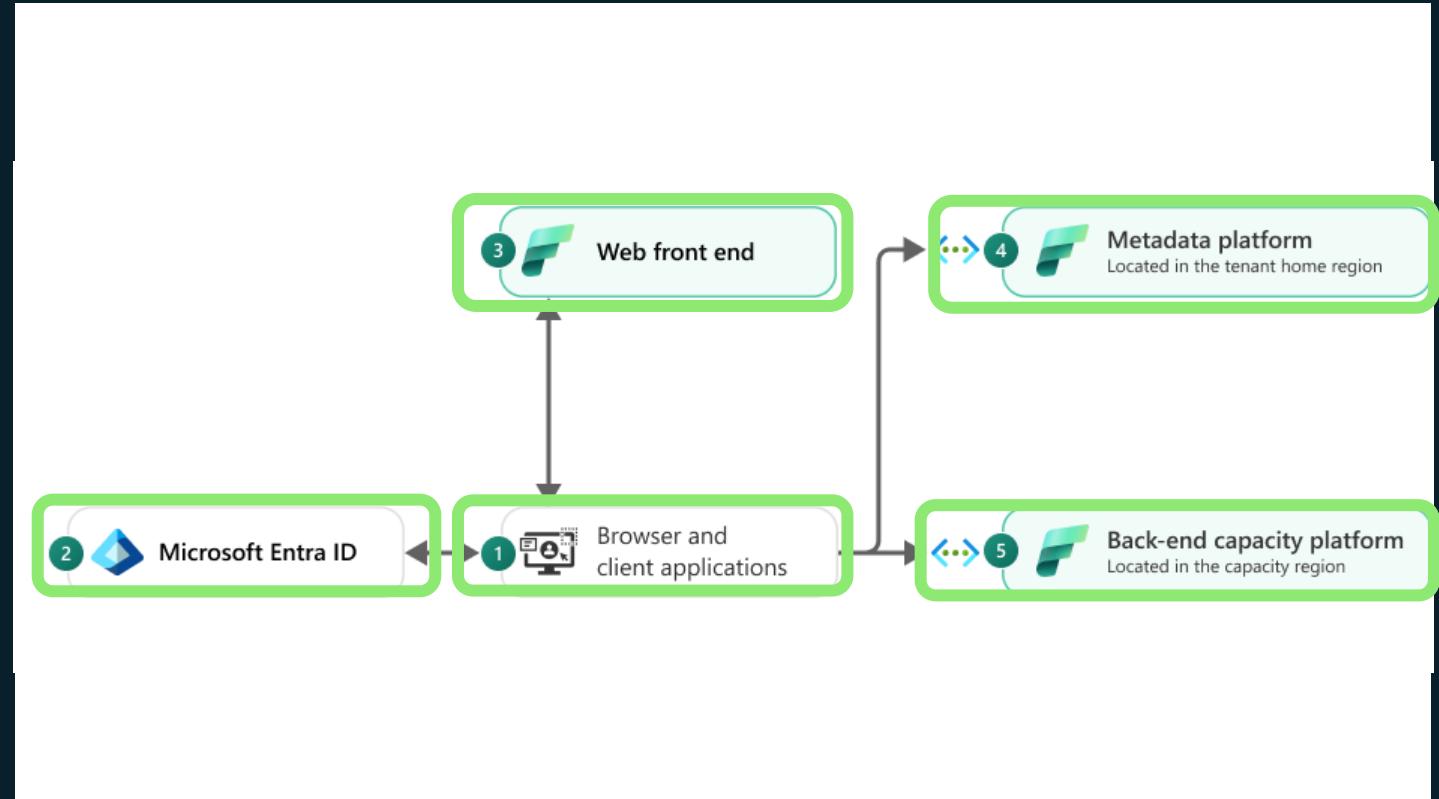


Entra ID



Microsoft Fabric Architecture

1. A user uses a browser or a client application, like Power BI Desktop, to connect to the Fabric service.
2. Authentication is handled by Microsoft Entra ID
3. The web front end receives user requests and facilitates sign-in.
4. The metadata platform stores tenant metadata, which can include customer data. Fabric services query this platform on demand in order to retrieve authorization information and to authorize and validate user requests. It's located in the tenant home region.
5. The back-end capacity platform is responsible for compute operations and for storing customer data, and it's located in the capacity region.



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

Granular access policies

Global scale and resilience

ML, AI, automation

Unified experience

Every identity.
Every resource.
Everywhere.

Any data, apps or resources



IaaS, PaaS, Datacenter



Microsoft 365



Microsoft Fabric



SaaS, websites



On-premises

Secure Access for a connected world



Microsoft Entra

Unify conditional access



Ensure least privilege access



Improve the user experience



Reduce on-premises footprint



Zero Trust Principles

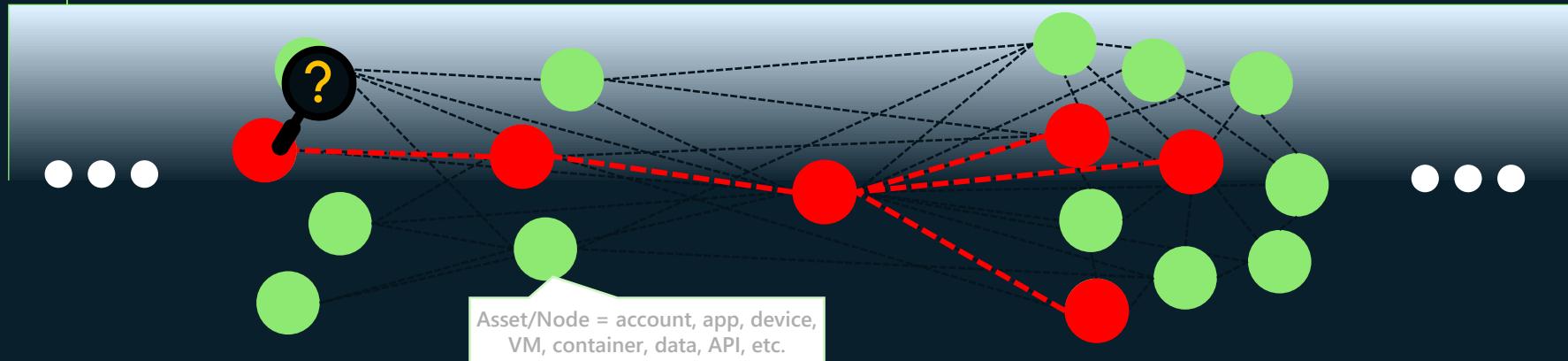
Business Enablement

Align security to the organization's mission, priorities, risks, and processes

Assume Breach (Assume Compromise)

Assume attackers can and will successfully attack anything (identity, network, device, app, infrastructure, etc.) and plan accordingly

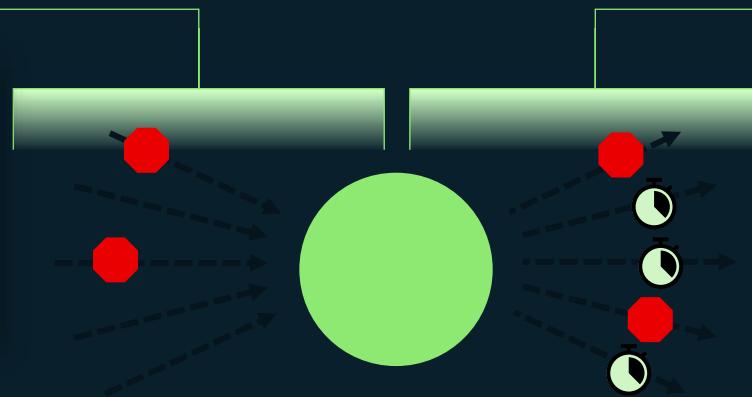
→ *Transforms from "defend the network"-to "enable secure productivity on any network"*



Verify explicitly

Protect assets against attacker control by explicitly validating that all trust and security decisions use all relevant available information and telemetry.

→ Reduces "attack surface" of each asset



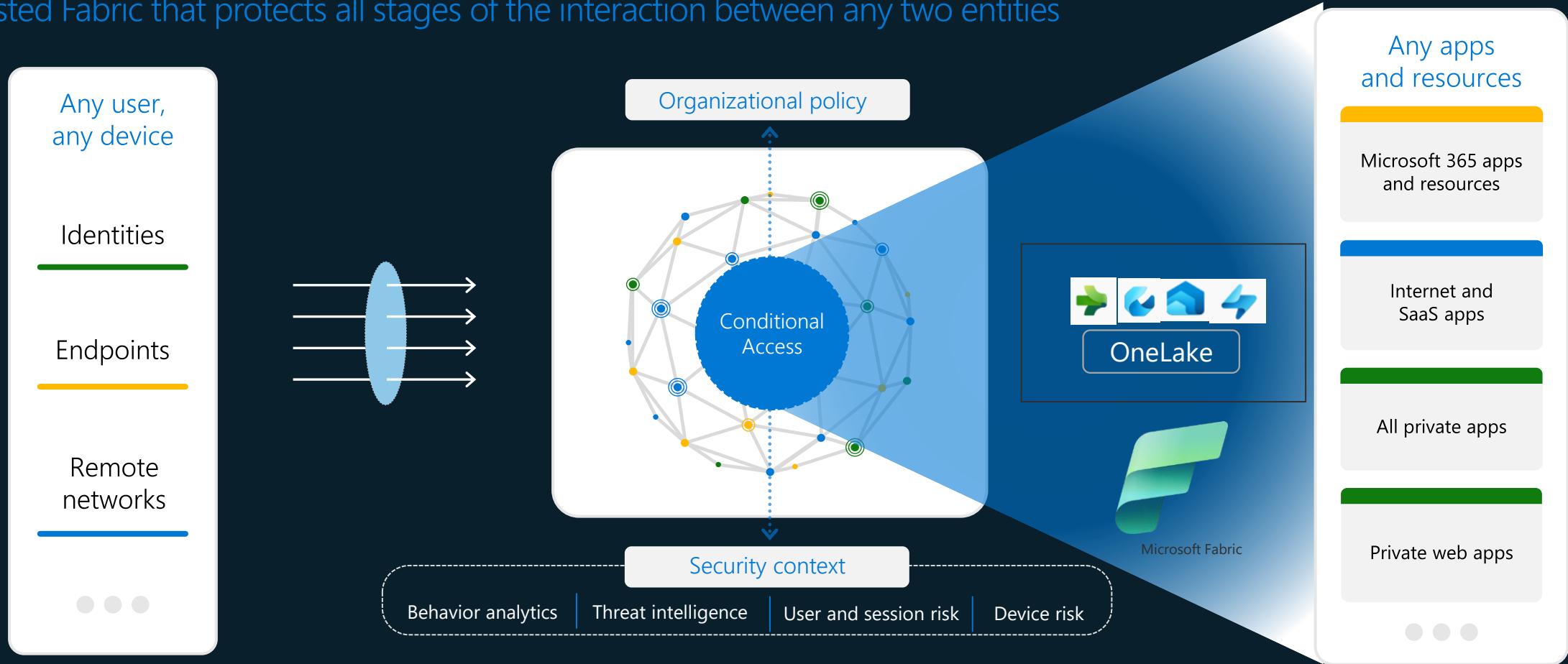
Use least privilege access

Limit access of a potentially compromised asset, typically with just-in-time and just-enough-access (JIT/JEA) and risk-based policies like adaptive access control.

→ Reduce "blast radius" of compromises

Conditional Access - Microsoft's Adaptive Access Vision

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



Centralized control

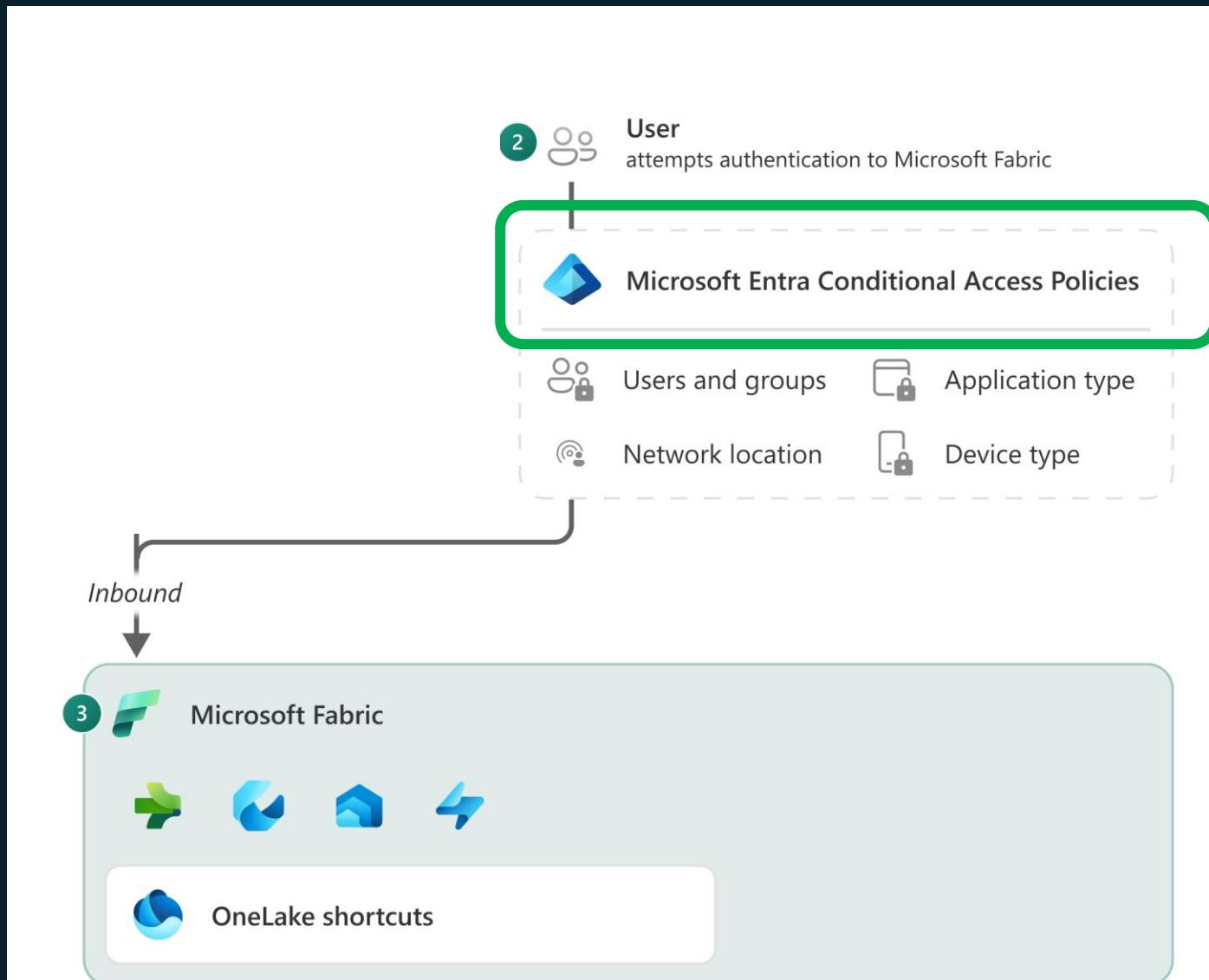
Unified Zero Trust architecture and policy engine simplifies management of access controls and technologies (Directory, SSO, Federation, RBAC, proxy, and more)

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.





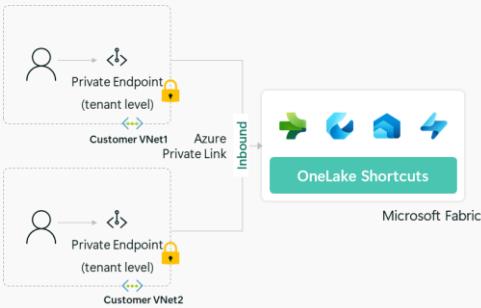
DEMO

Inbound and Outbound



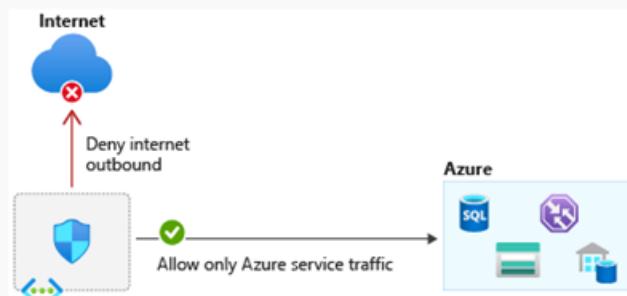
Secure inbound and outbound network connections

Secure and protect data across your organization



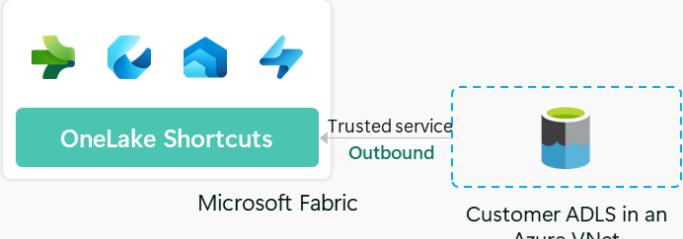
Fabric inbound security

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

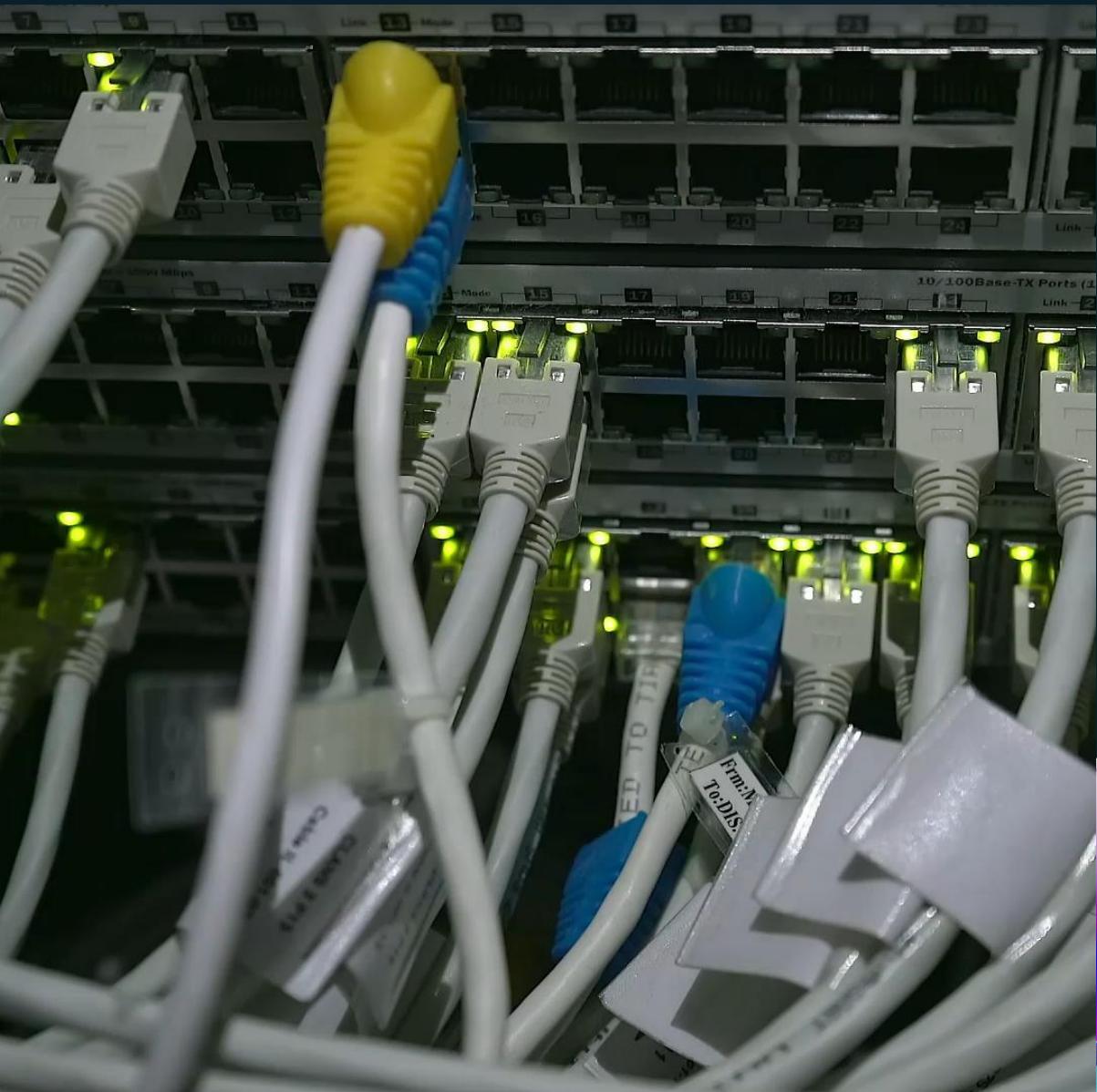


Fabric outbound security

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



Fabric Inbound Security

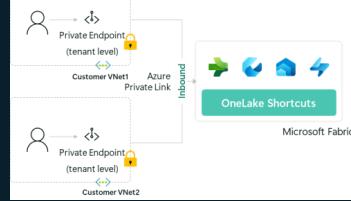


Inbound protection options

Perimeter Network Security

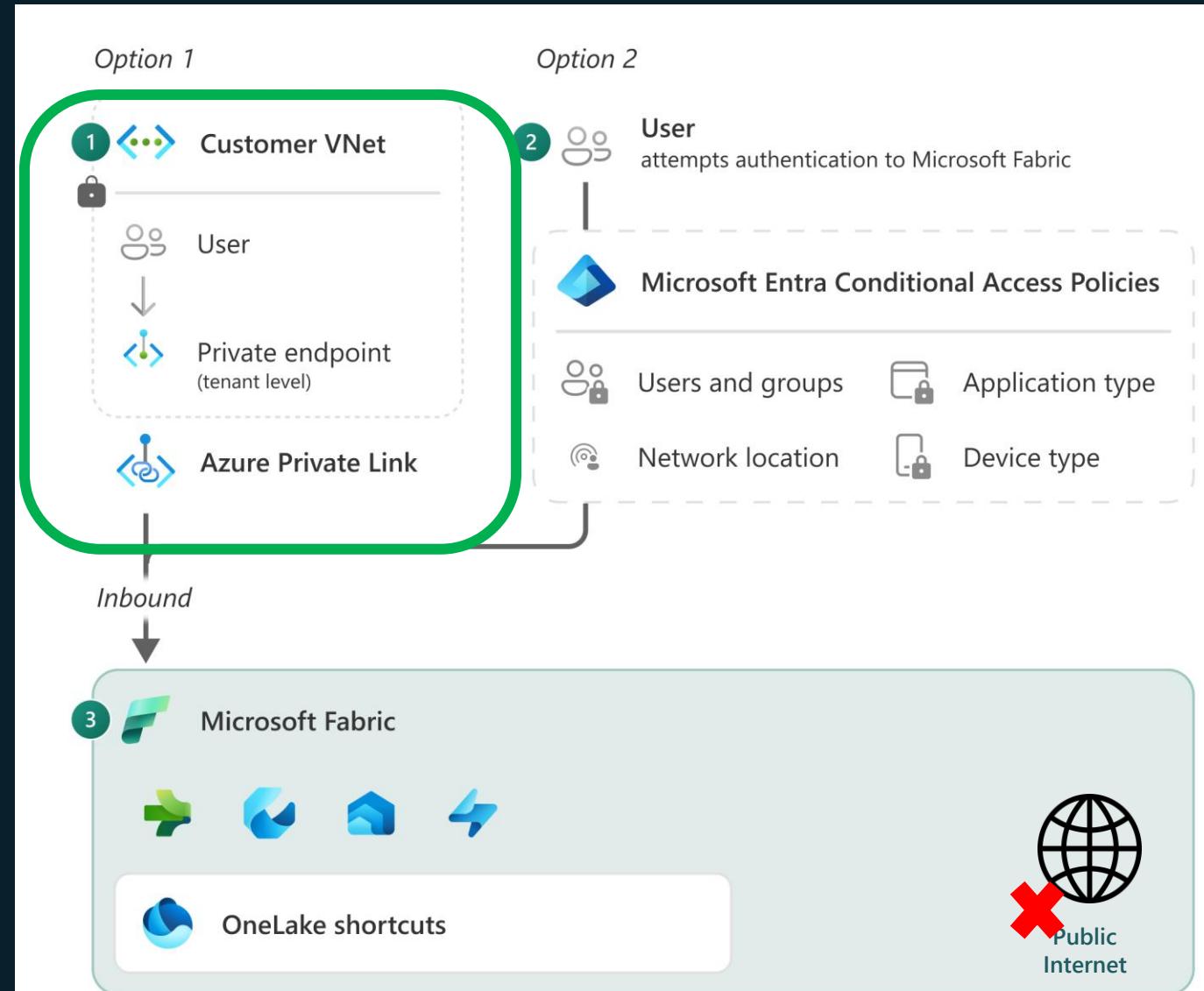


Zero Trust Approach (Conditional Access)



Private Link for Fabric

- What it means:
 1. Fabric is disconnected from the public internet
 2. Every 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)
 6. Only available on tenant level (workspace roadmap)



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**.

Disabled

🛡️ 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](#)

Disabled

🛡️ This setting applies to the entire organization

Apply **Cancel**



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

 Add inbound security rule
nsg-mz-labs-xgnmz-p-euw-01

Source ⓘ
Any

Source port ranges * ⓘ
*

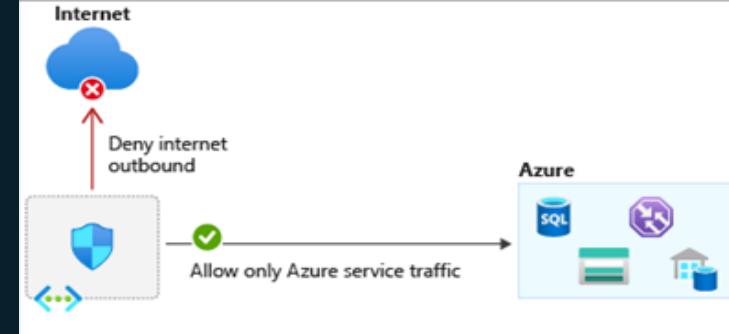
Destination ⓘ
Service Tag

Destination service tag ⓘ
Internet

Service ⓘ
Custom

Destination port ranges * ⓘ
8080

Service Tags



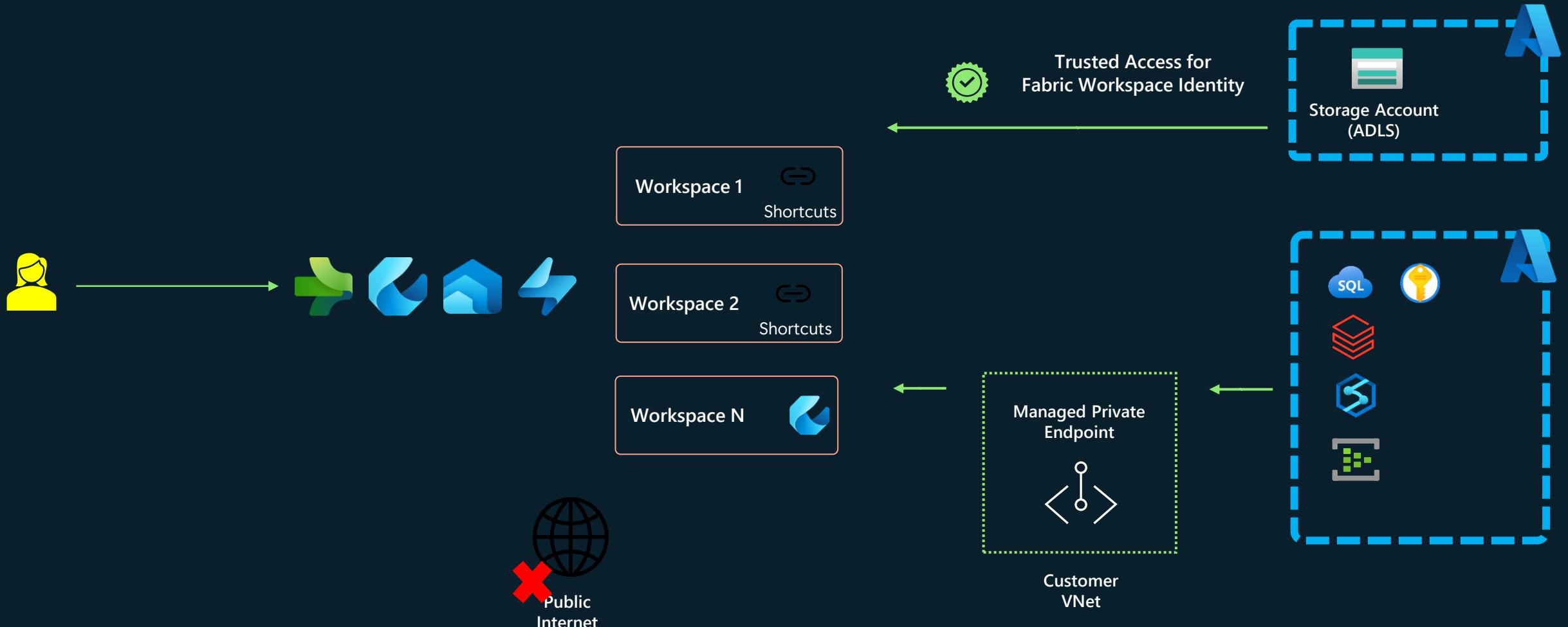
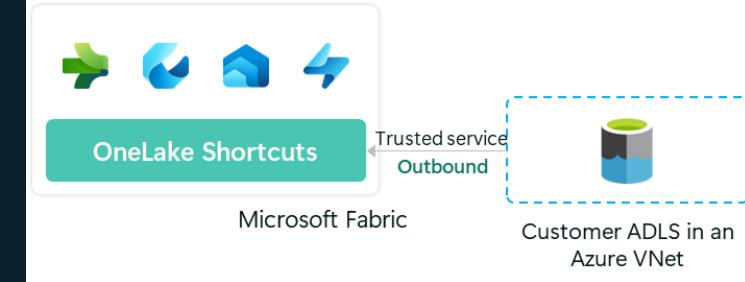
- You can use Azure service tags to enable connections to and from Microsoft Fabric.
- A service tag is a defined group of IP addresses that is automatically managed, as a group, to minimize the complexity of updates or changes to network security rules
- You can use the service tags to define network 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	Yes
SQL	Fabric SQL database	Both	Yes	Yes

Fabric Outbound Security



Getting data into Fabric



A photograph of a person's hands holding a black smartphone. The person is wearing a blue denim jacket over a grey and white striped shirt. The background shows a dark wooden desk with a silver laptop, a white tablet, and a light green textured mug. A white callout box with a five-pointed star icon above the word "DEMO" is overlaid on the image.

DEMO



Home



Create



Browse



OneLake



Apps



Metrics



Monitor



Learn



Real-Time



Workspaces



Fabcon Demo



LH_Data_Landingzone



Power BI



Get data

New semantic model

Open notebook

Manage OneLake data access (preview)

Lakehouse

Share

Home

A SQL analytics endpoint for SQL querying and a default Power BI semantic model for reporting were created with this item.

Explorer



LH_Data_Landingzone

Tables

Files

Search tables

Get data in your lakehouse



Upload files

Upload data from your local machine.



Start with sample data

Automatically import tables filled with sample data.



New shortcut

Access data that resides in an external lake.



New Dataflow Gen2

Prep, clean, transform, and ingest data.



New data pipeline

Ingest data at scale and schedule data workflows.

Fabcon_Demo

 Create deployment pipeline  Create app  Manage access  Workspace settings

[+ New item](#)[New folder](#) [Import](#)[Filter by keyword](#)[Filter](#)[More](#)

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

WS_ManagedPrivateEndpoint

+ New Upload Create deployment pipeline Create app ...

Filter by keyword Filter

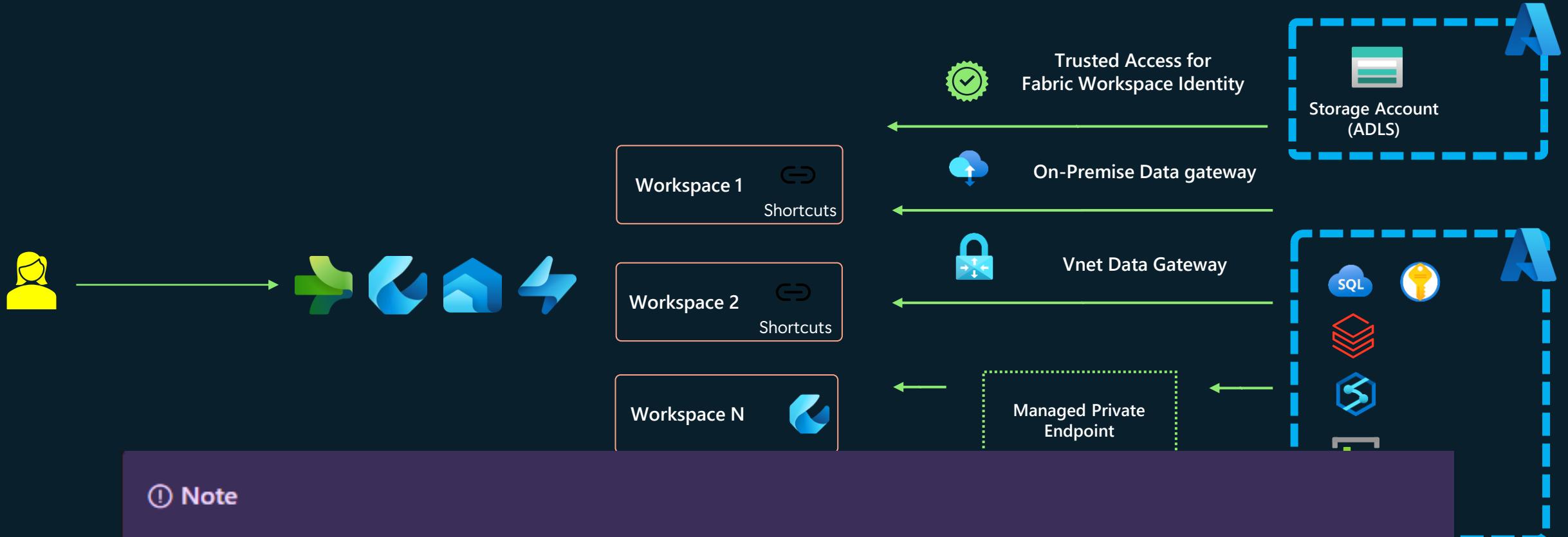
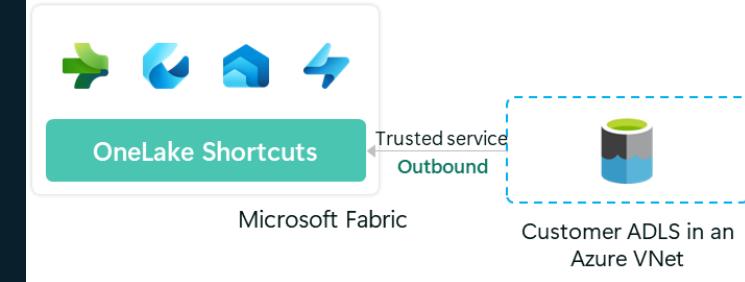
Name	Type	Workspace settings	Next refresh	Endorsement	Sensitivity
ENV	Environment	Ishwarya	—	—	—
NB	Notebook	Ishwarya	—	—	—
outboundLH	Lakehouse	Ishwarya	—	—	—
outboundLH	Semantic model (...	WS_ManagedPriv...	2/26/24, 7:51:12 AM	N/A	—
outboundLH	SQL analytics end...	WS_ManagedPriv...	—	N/A	—
SJD	Spark Job Definiti...	Ishwarya	—	—	—
SJDHelloWorld	Spark Job Definiti...	Ishwarya	—	—	—

Manage access

WS_ManagedPrivateEndpoint

Power BI

Getting data into Fabric



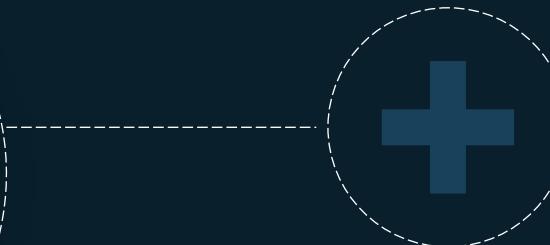
① Note

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**

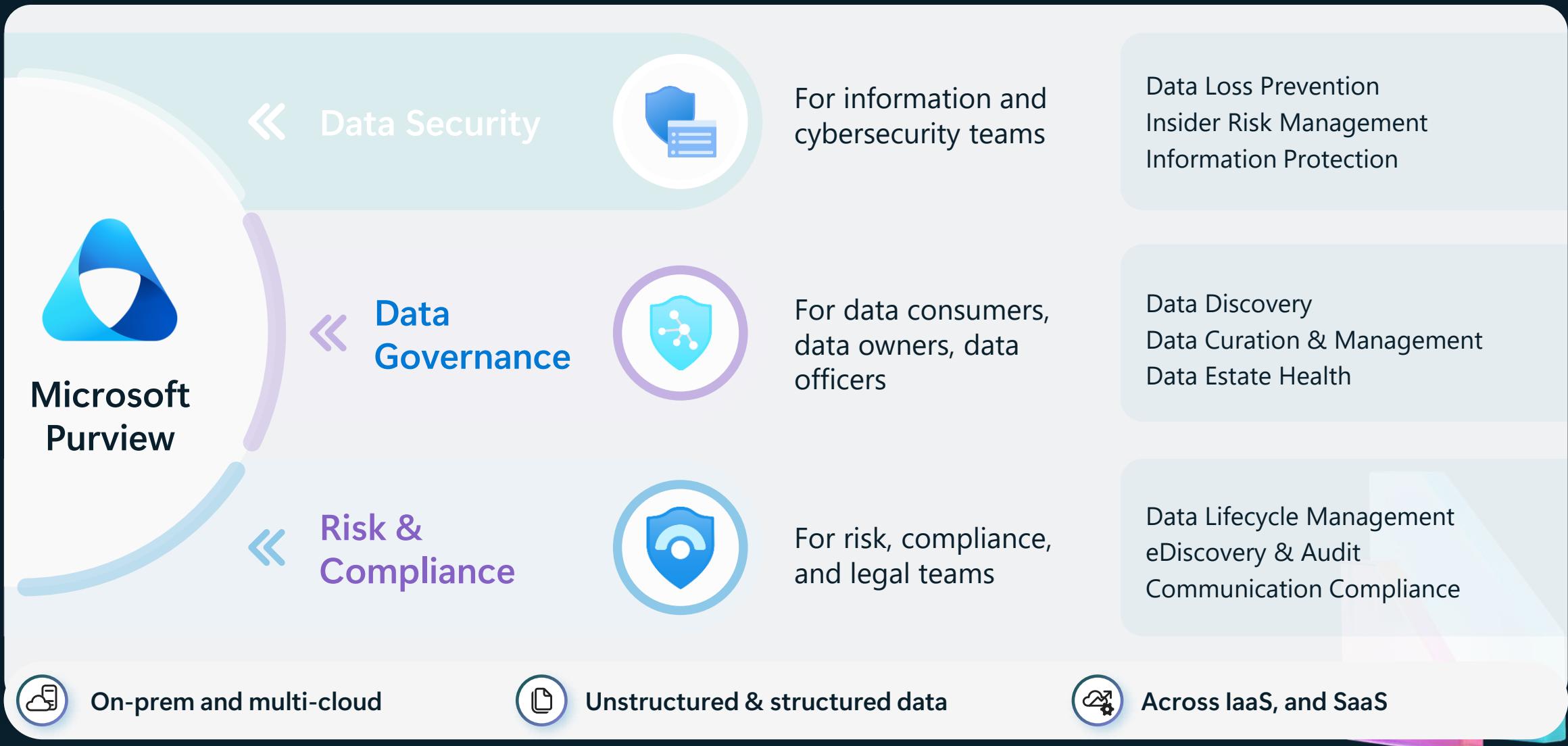
Reshape how you access, manage, and act on data and insights by connecting every data source and analytics service together in Fabric

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

Data ownership

Unmatched security & compliance

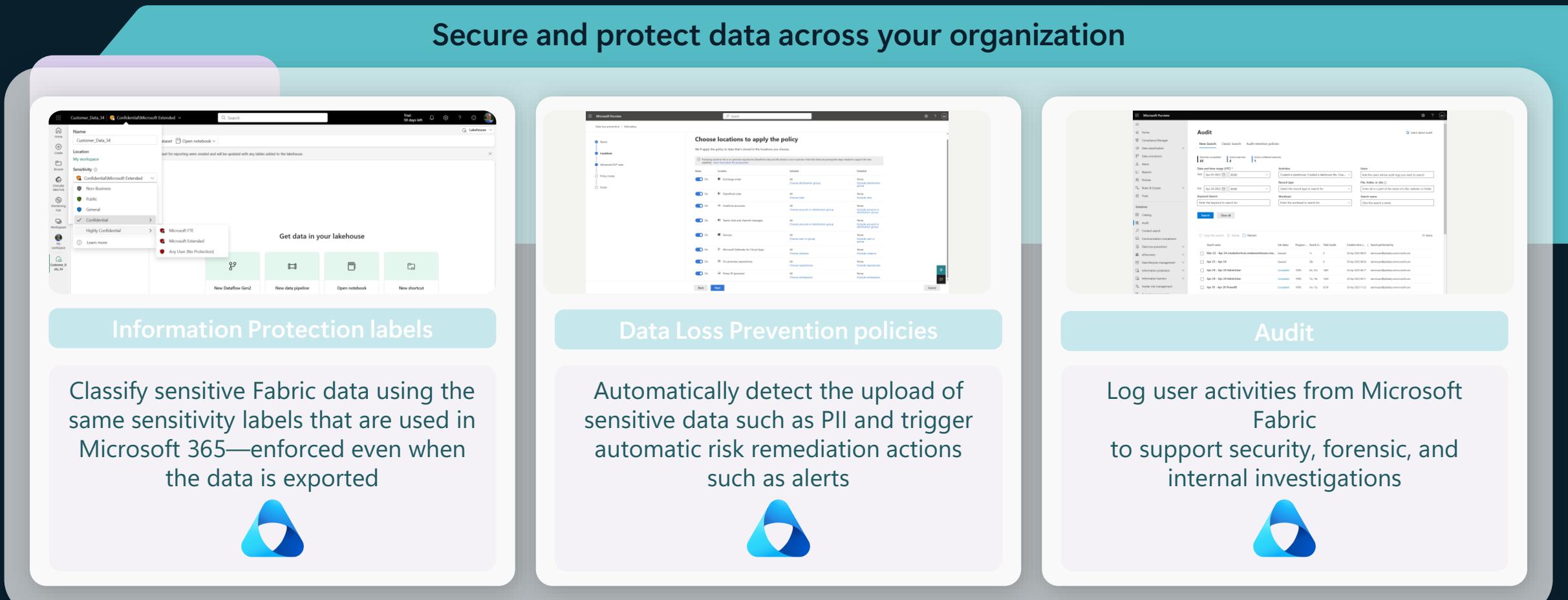
Unified governance



Microsoft Purview

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

*(*Additional Microsoft Purview purchase required)*



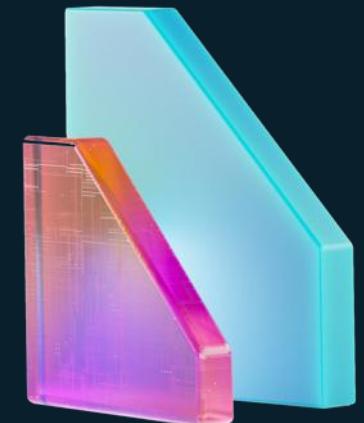
Microsoft Fabric Compliancy

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



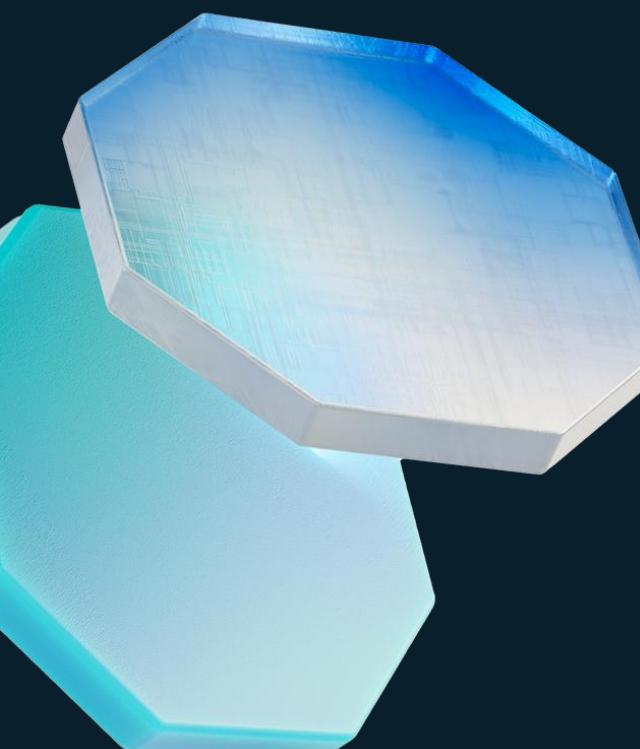
Roadmap

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



More sessions

- **Building a Metadata-Driven Framework with SQL database in Fabric and Data Factory**
 - Grand Ballroom 120
 - Wednesday 14:00 – 15:00
 - Erwin de Kreuk
- **Securing Your Fabric Workloads - Best Practices from the Fabric Security Team**
 - **Wednesday 9:15 AM - 10:15 AM Boulevard Ballroom 162**
- **Deep Dive on OneLake Data Security**
 - **Wednesday 10:00 AM - 11:00 AM Premier Ballroom 313 Aaron Merrill and Cristian Petculescu**
- **Network Security for SaaS Platform**
 - **Tuesday 3:15 PM - 4:15 PM Grand Ballroom 119 Rick Xu and Arthi Ramasubramanian Iyer**
- **Microsoft Purview Data Security in the Era of AI**
 - **Wednesday 10:00 AM - 11:00 AM Grand Ballroom 120 Maithili Dandige and Joanne Marone**



Let's connect



Erwin de Kreuk

- Principal Consultant
- Lead Data & AI InSpark

 @erwindekreuk.bsky.social

 linkedin.com/in/erwindekreuk

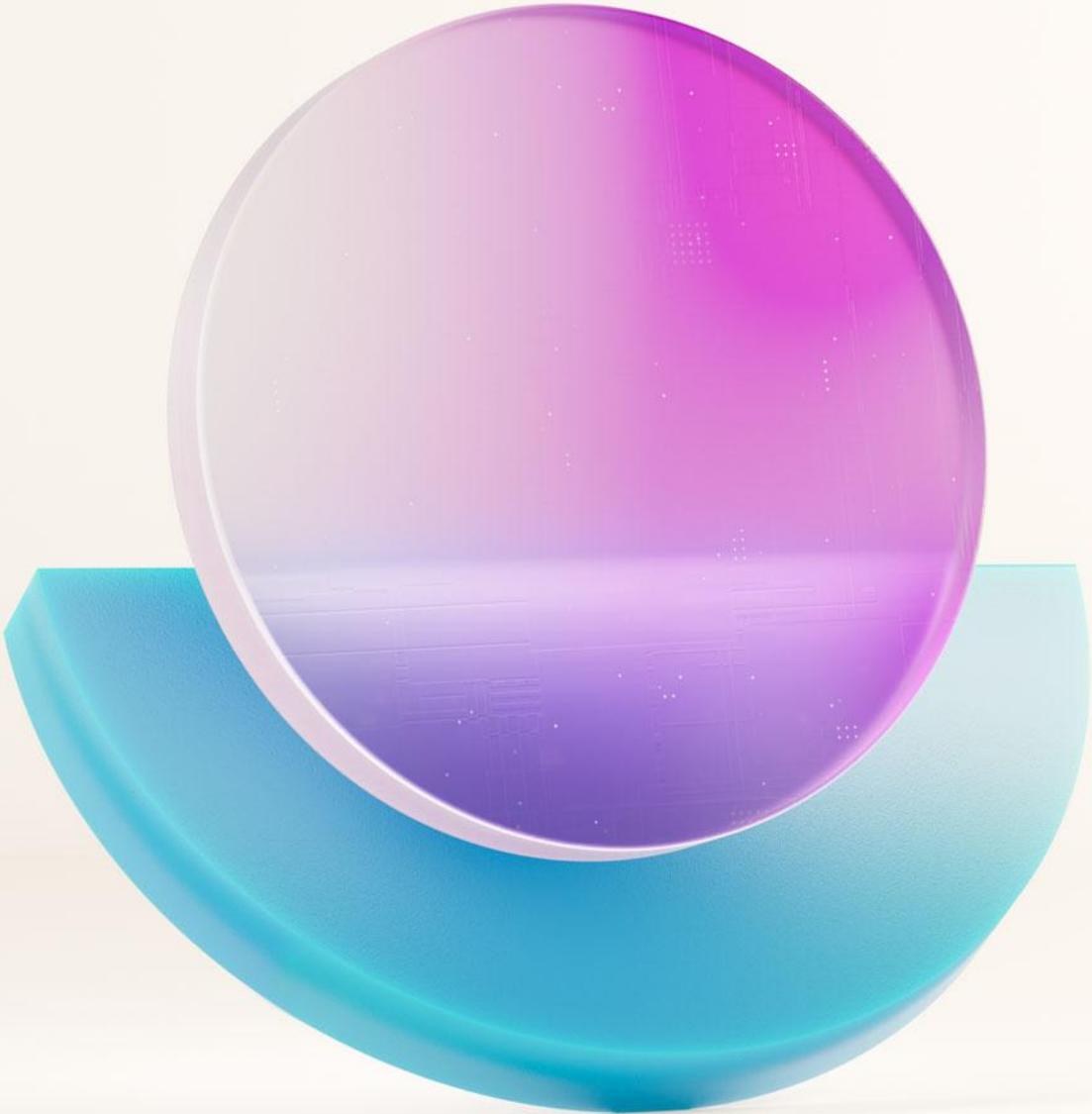
 erwindekreuk.com

 github.com/edkreuk

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

 Dutchfabricusergroup.com





Fast-track your career in data and AI

Become a Microsoft Certified Fabric Data Engineer Associate – take Exam DP-700 for free!

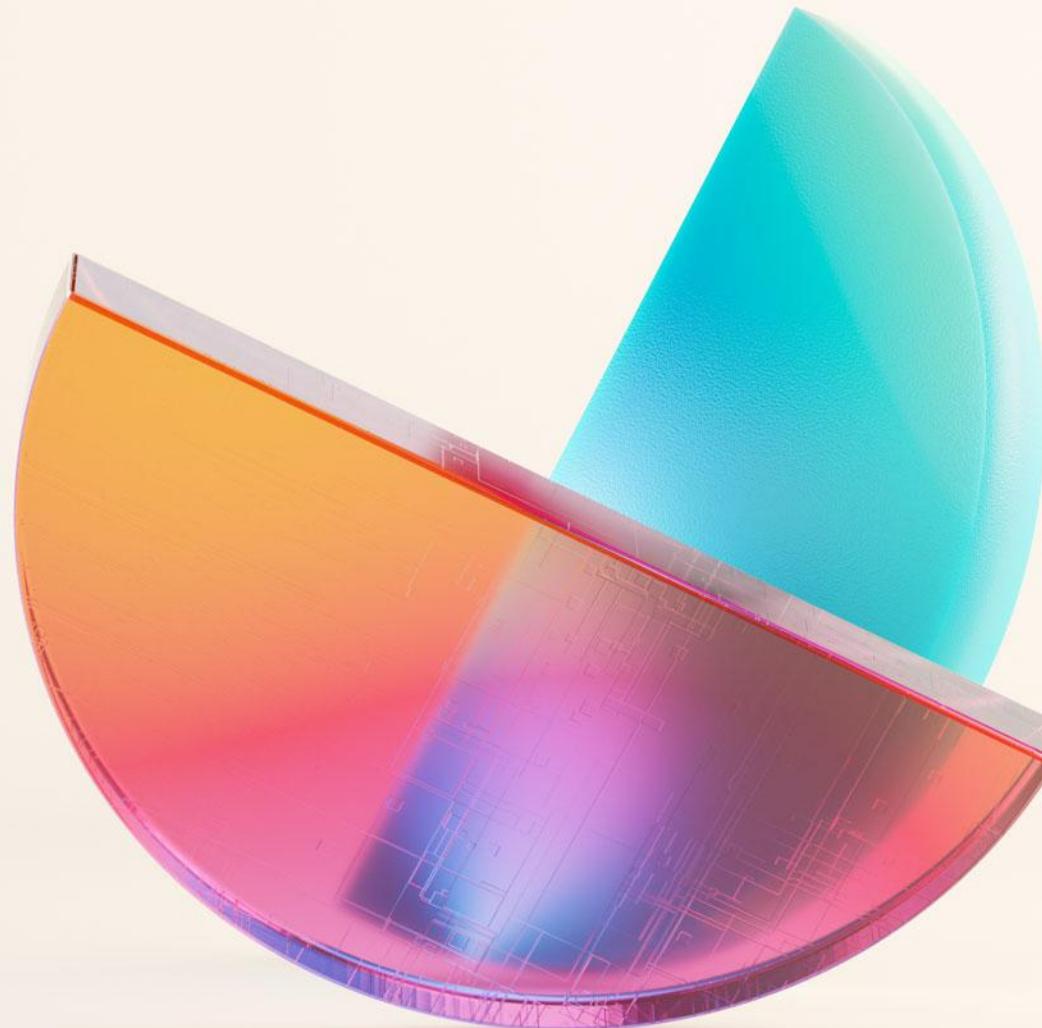
Visit the Fabric Community Lounge to learn more about this *limited-time offer*.



aka.ms/fabcon/dp700



Microsoft Fabric
Community Conference



Learn more about
Microsoft Fabric



Power your AI transformation with a
complete data platform



Get Involved in the Fabric Community



aka.ms/FabricCommunity

Connect with community members, ask questions, and learn more about Fabric



aka.ms/FabricUserGroups

Find a user group that matches your interests in your area or online



aka.ms/SuperUsers

Spread your Fabric knowledge, insights, and best practices with others



aka.ms/MVP

Technology experts that share their knowledge and passion with the community