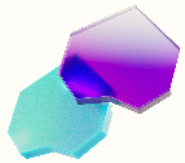
Microsoft | Microsoft Fabric

Fabric security: everything you need to know!

For all the latest security related information please visit: https://aka.ms/MSFabricSecurity

Agenda

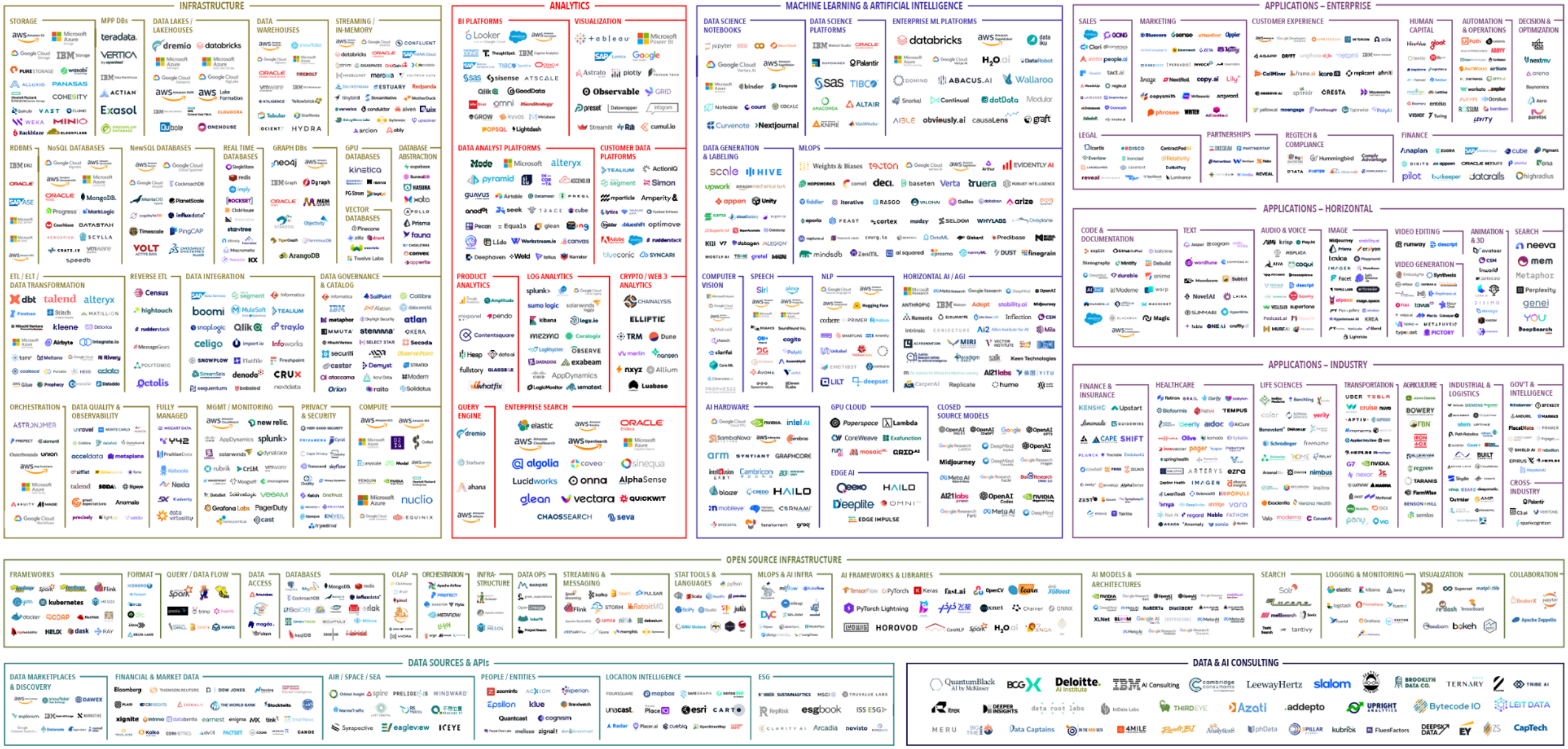
- Intro to Fabric as a SaaS platform
- Authentication to Fabric
- Network protection (Entra & Private Link)
- Connecting to secure data
- Data encryption
- Item level security
- Data residency
- Data Governance and compliance



A world awash with data...

How do you translate data into competitive advantage?

The 2023 ML, AI, and Data Landscape



Version 1.0 - Feb 2023

Blog post: mattturck.com/MAD2023

Interactive version: MAD.firstmarkcap.com

Comments? Email MAD2023@firstmarkcap.com

FIRSTMARK
EARLY STAGE VENTURE CAPITAL

> **Simplify,**
> I am the Chief Data Officer
> and don’t want to be the
> Chief Integration Officer.”
>
> Every CDO, Every Enterprise

Microsoft Fabric

Data analytics for the era of AI

Complete Analytics Platform

Unified product, experience, and architecture

Delivered as **SaaS**

Microsoft Fabric

Data analytics for the era of AI

Complete Analytics Platform

Unified product, experience, and architecture

Delivered as SaaS

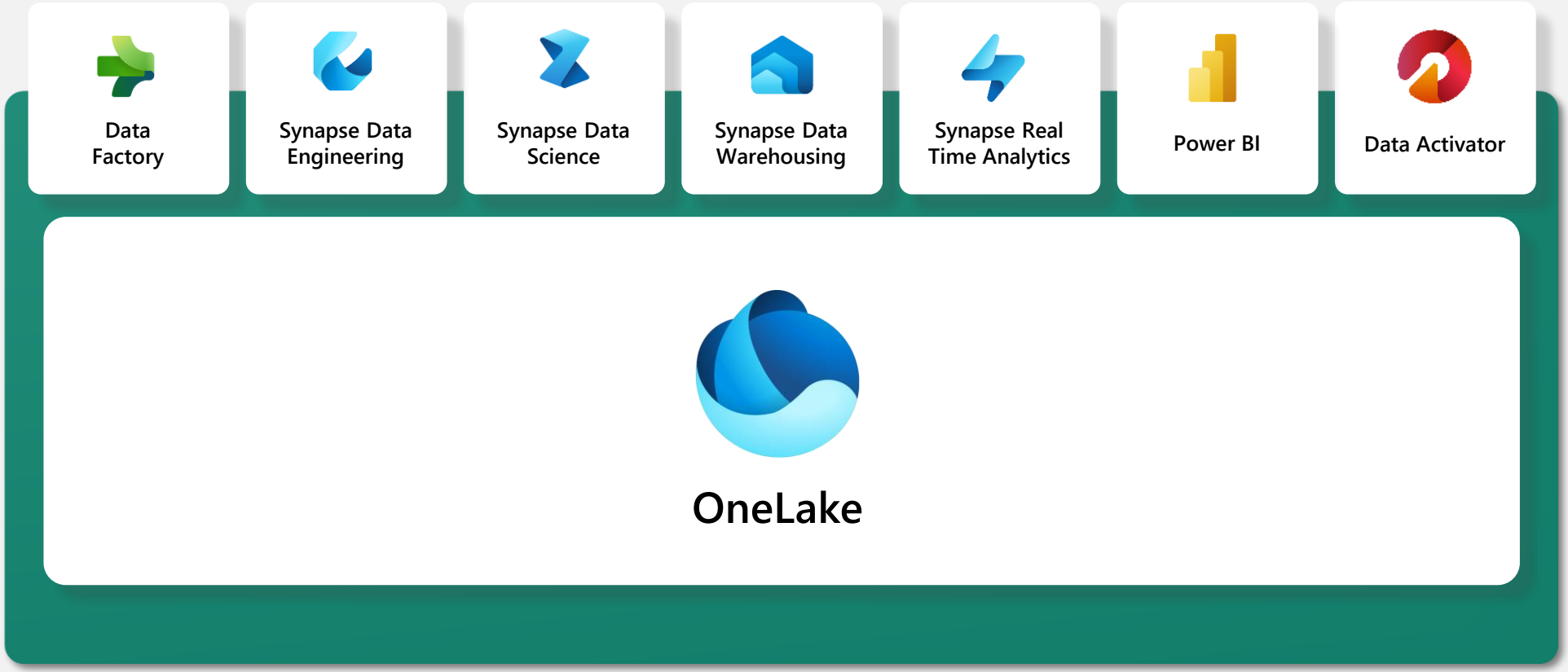
Lake Centric and Open

Common SaaS data lake shared by all compute engines

Deep commitment for open formats and APIs

Microsoft Fabric

The unified data platform for the era of AI



Microsoft Fabric

End-to-end analytics data fabric
From the data lake to the business user

Complete Analytics Platform

- Everything, Best of Breed
- Unified
- Azure OpenAI Copilots

Lake centric and open

- OneLake
- One Copy
- Always Synced

Empower Every Office User

- Familiar and intuitive
- Built into Office
- Insight to action

Pervasive security and governance

- End to end visibility
- Always governed
- Secure by default

Microsoft Fabric

Pervasive Security and Governance for the cloud world

Complete Analytics Platform

Best of Breed

SaaS-ification

Low Code Plus Pro Dev

Lake Centric and Open

One Lake

One Copy

Always Synced

Empower Every Office User

Familiar and Intuitive

Built into Office

Insight to Action

Pervasive Security and Governance

Secure by Default

End to End Visibility

Always Governed

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

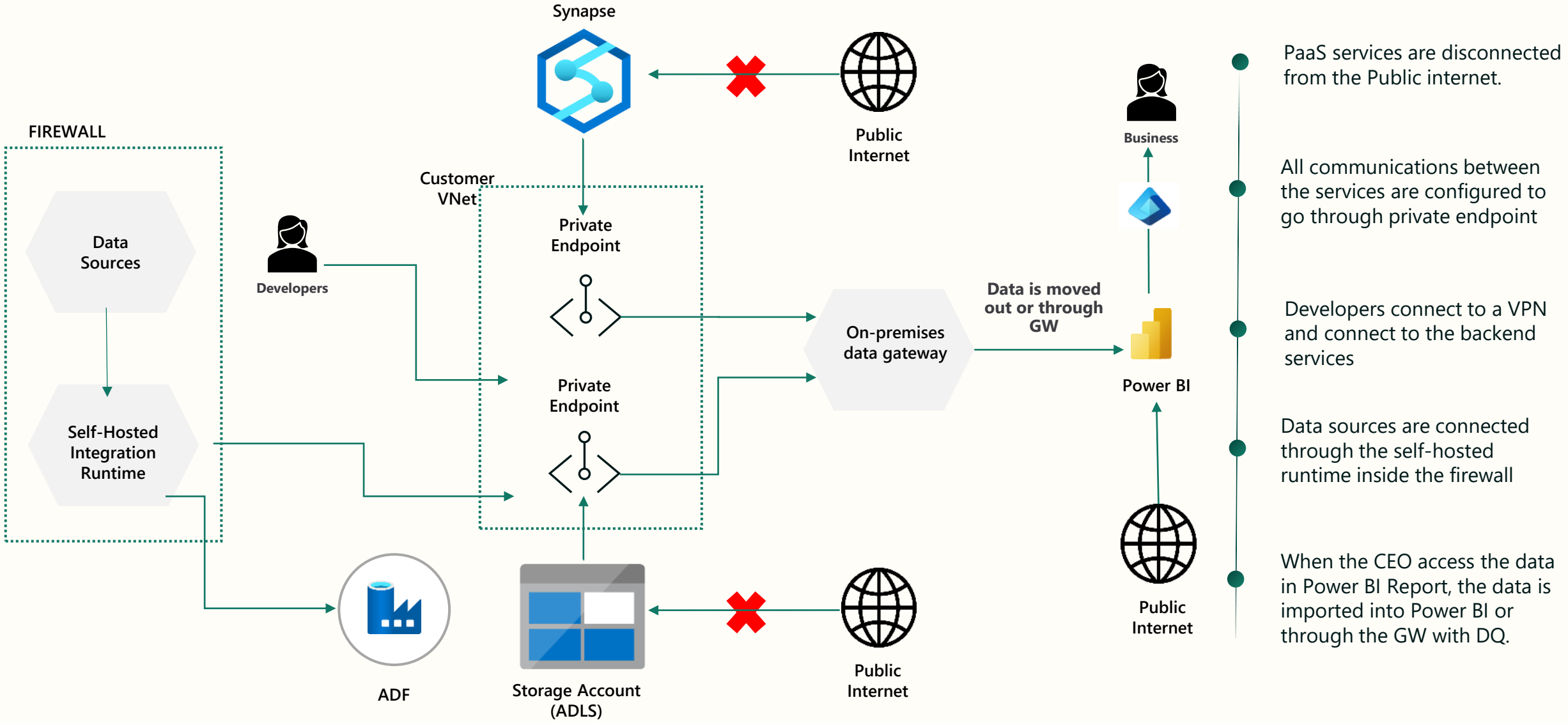
- At the same time, you need to secure, govern and audit your data to protect customers and the company
- SaaS platforms are designed with these challenges in mind.
- Shift from siloed PaaS to integrated SaaS

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.

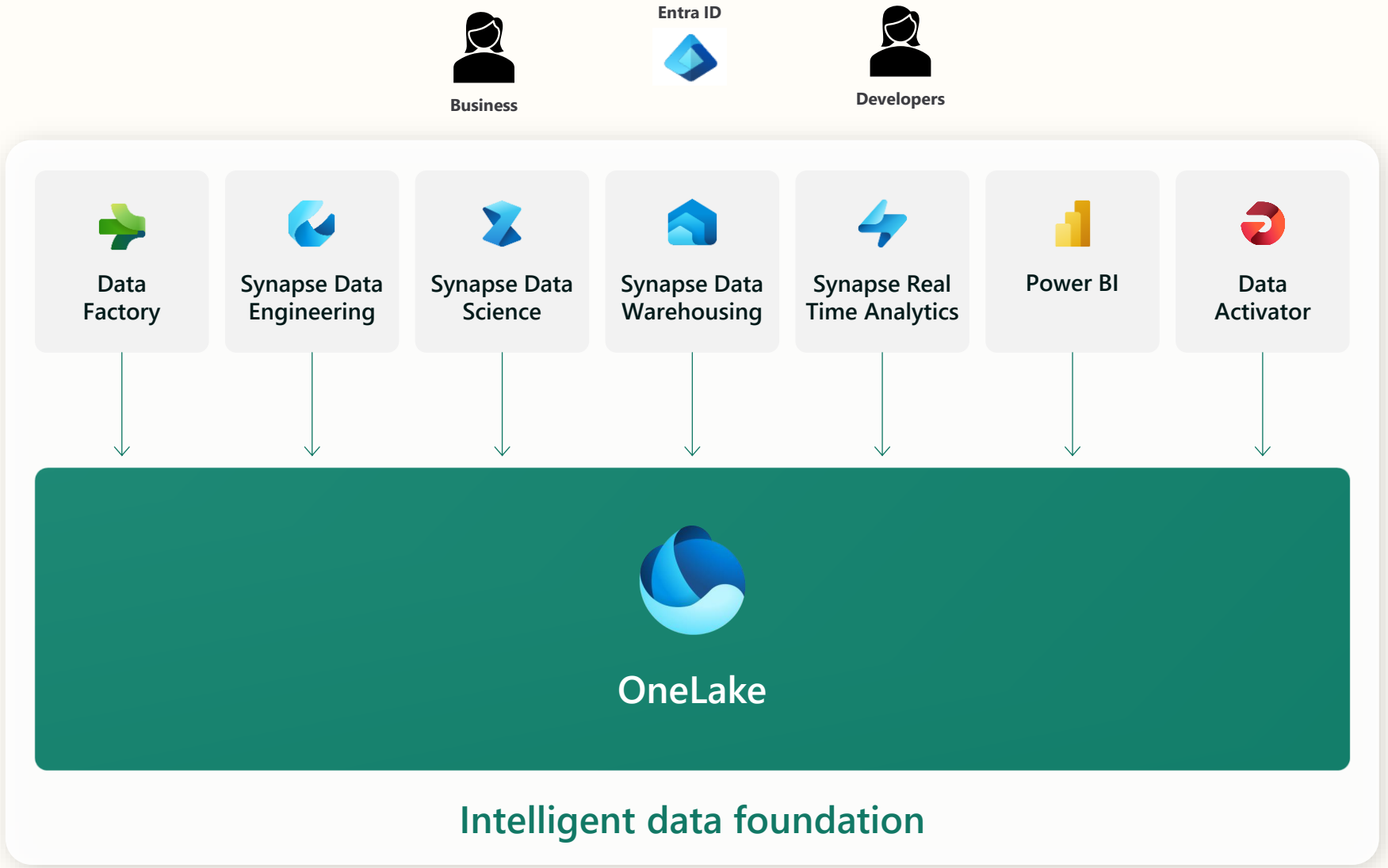
All communications between the services are configured to go through private endpoint

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.

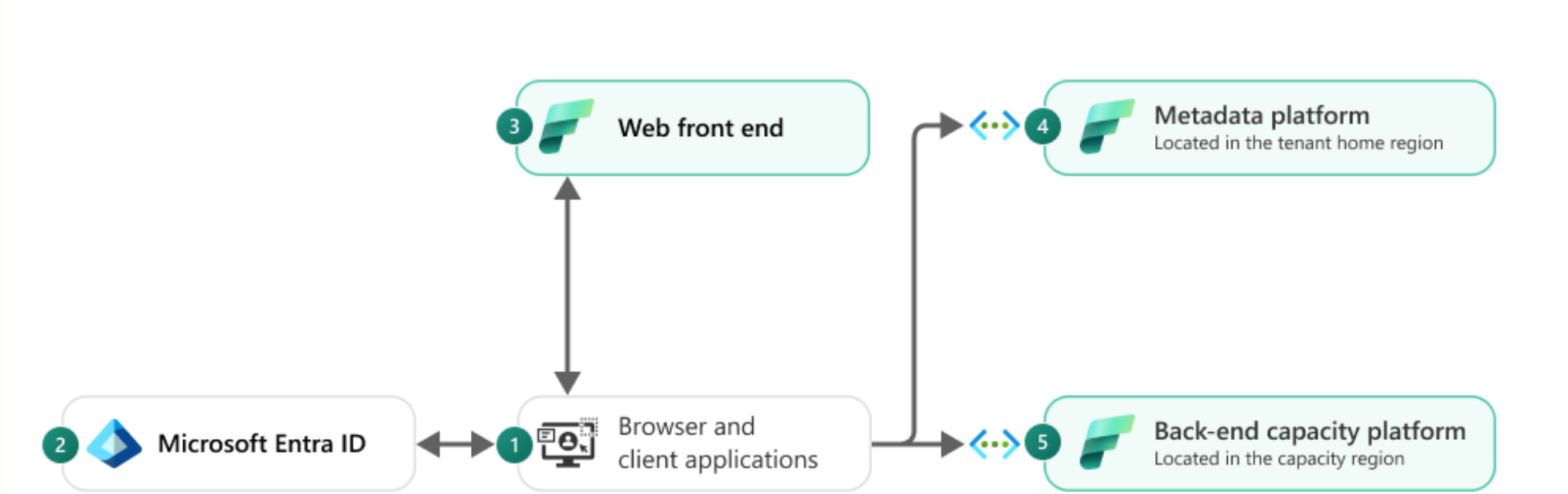
Microsoft Fabric – SaaS World



- 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

Microsoft Fabric Architecture

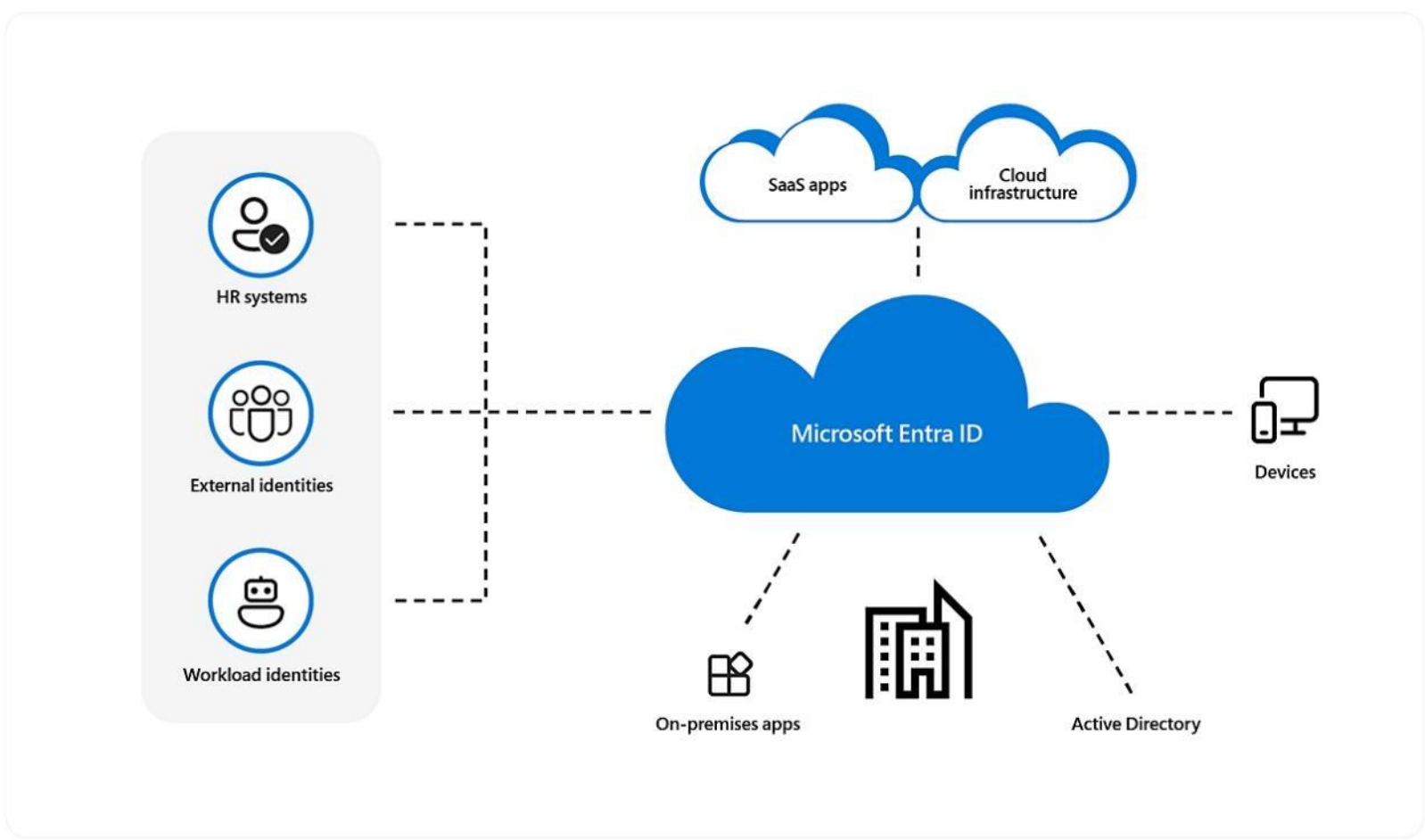
Fabrics is built as a SaaS product.



- Users connect only to “Front End Services” and we are using “Entra ID” to authenticate and **trust all requests**.
- All the clusters **are protected behind “back-end services” and v-nets.**
- Traffic between experiences is **going over MS backend network**
- Traffic to Fabric will be using at **least TLS 1.2**

Authentication

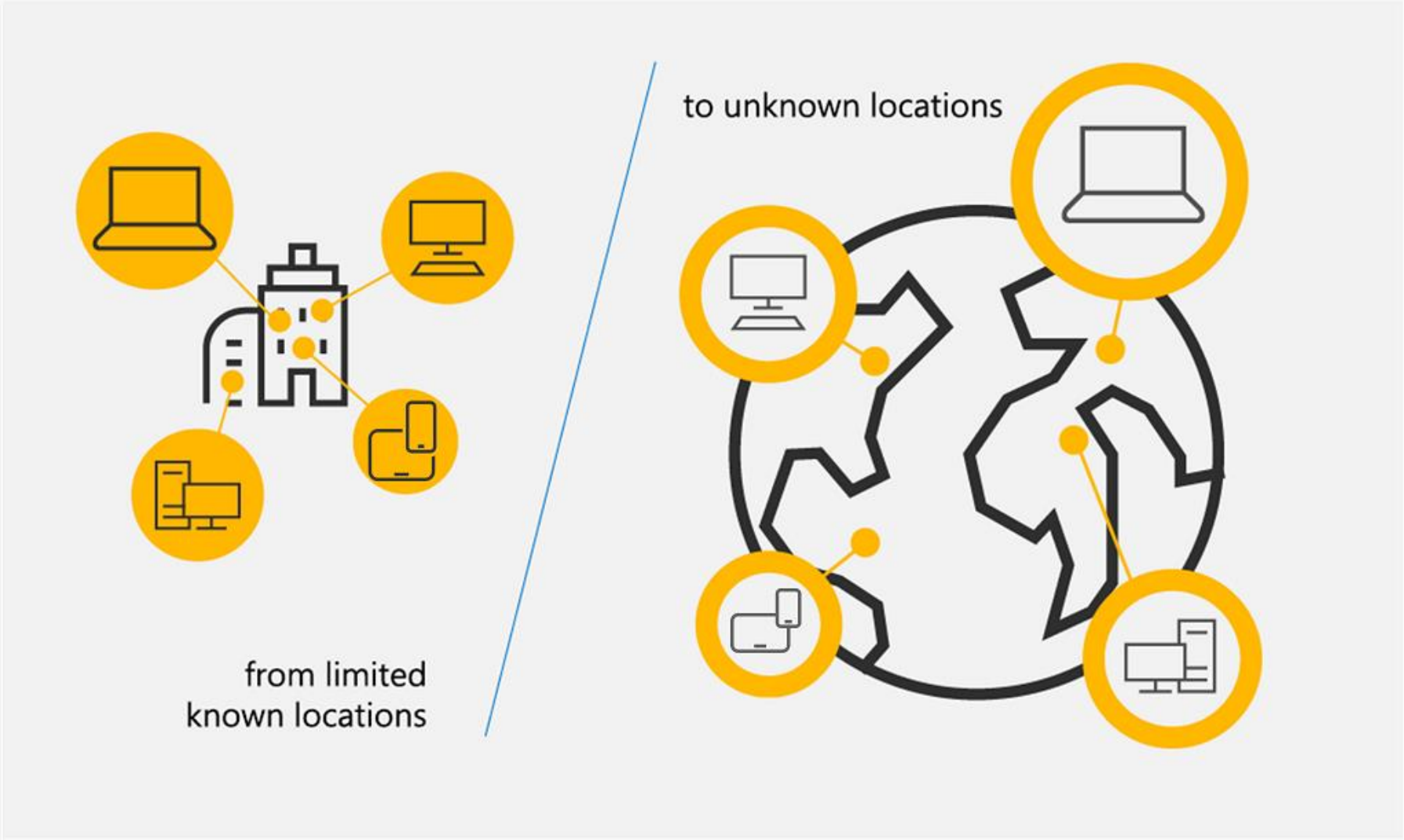
Microsoft Entra ID at the hearth of your security

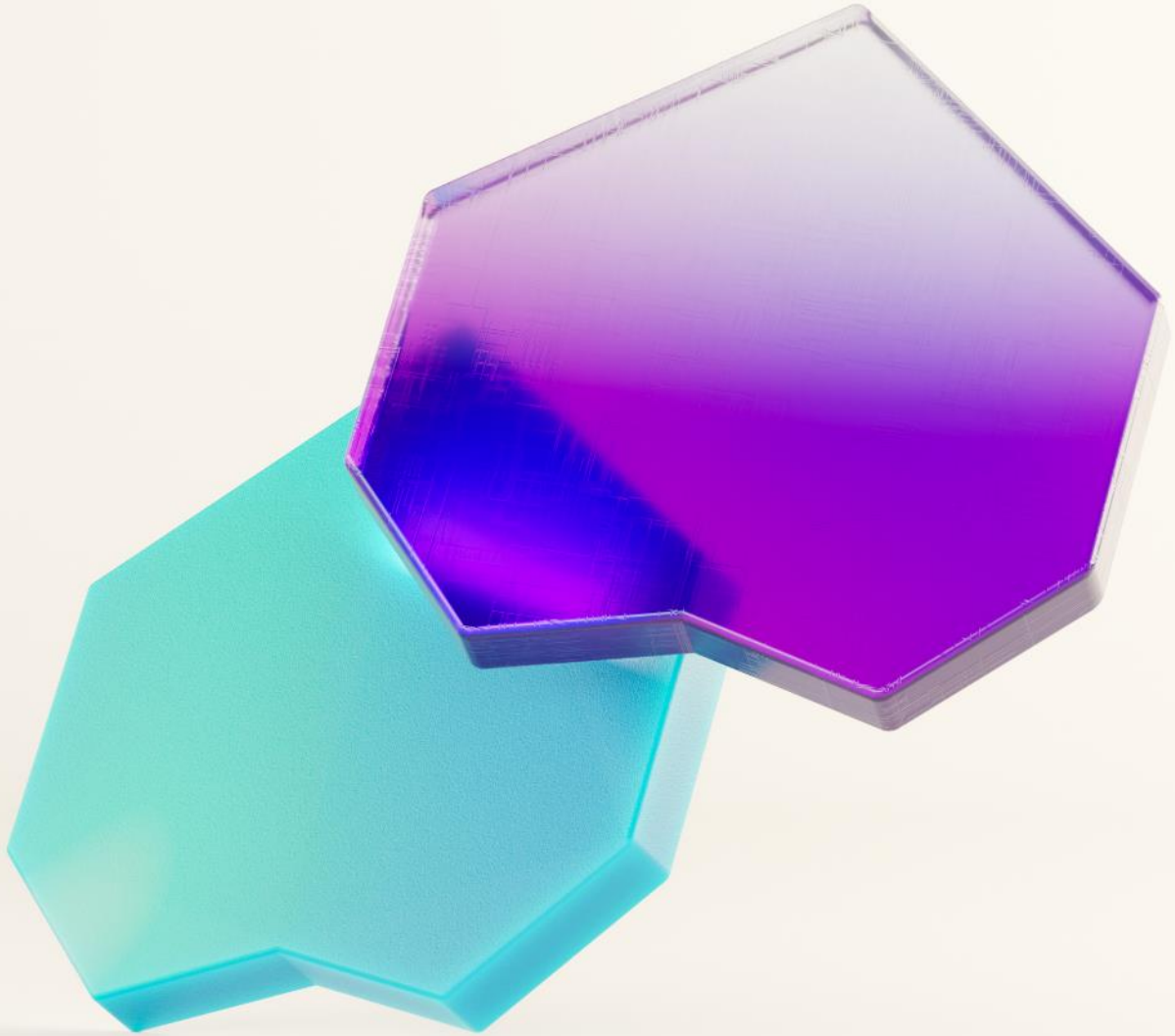


Inbound protection options

Perimeter Network Security

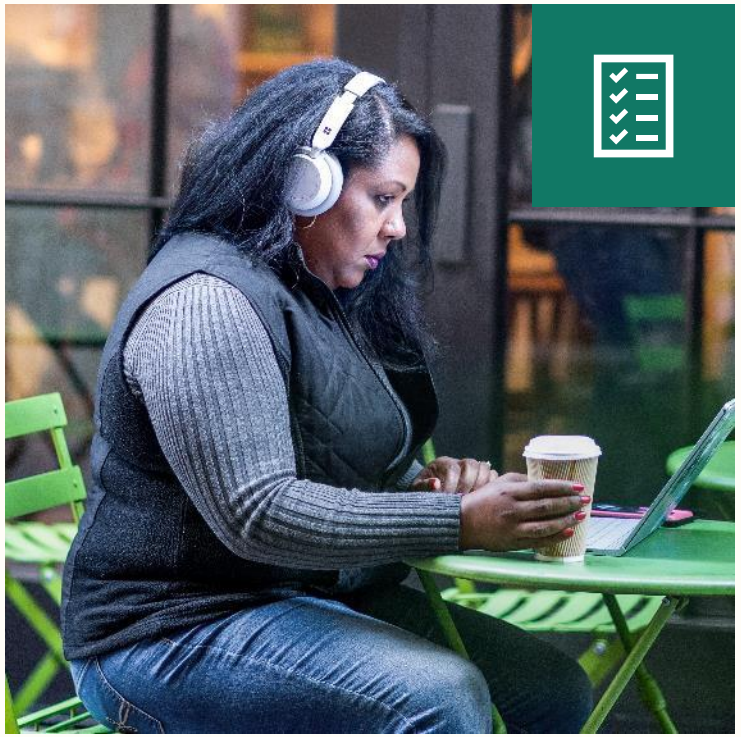
Zero Trust Approach



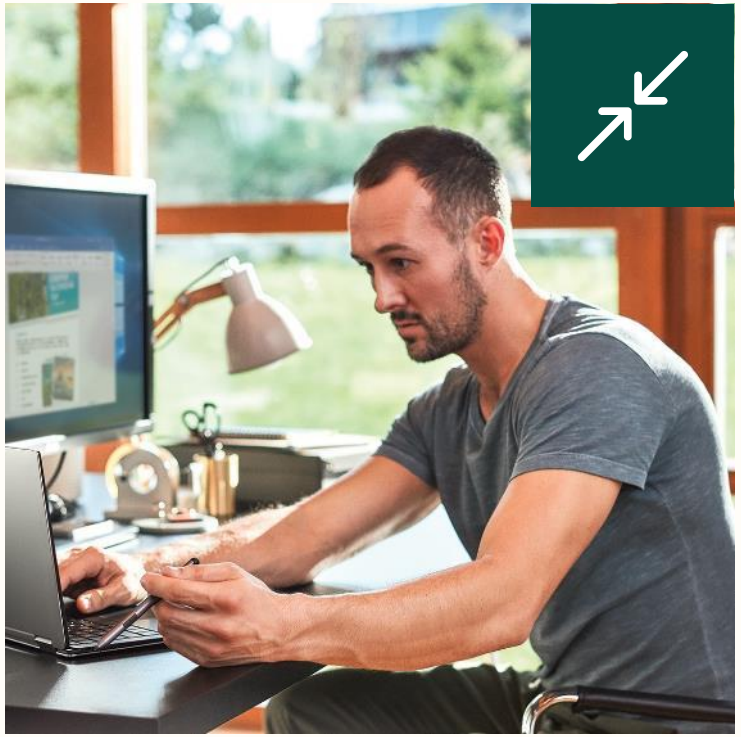


Securing inbound connections Using Zero Trust with Entra CA

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

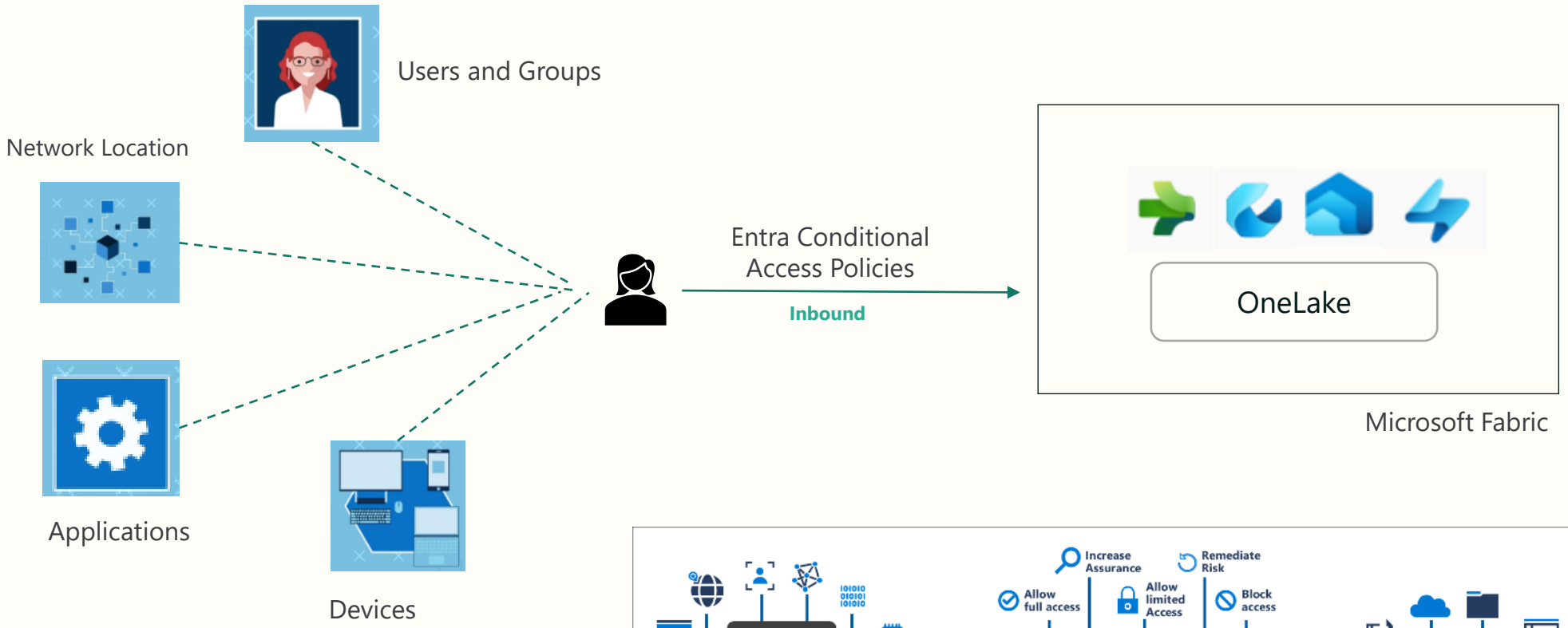
Configurable Conditional Access policies based on context and risk assessment [1]

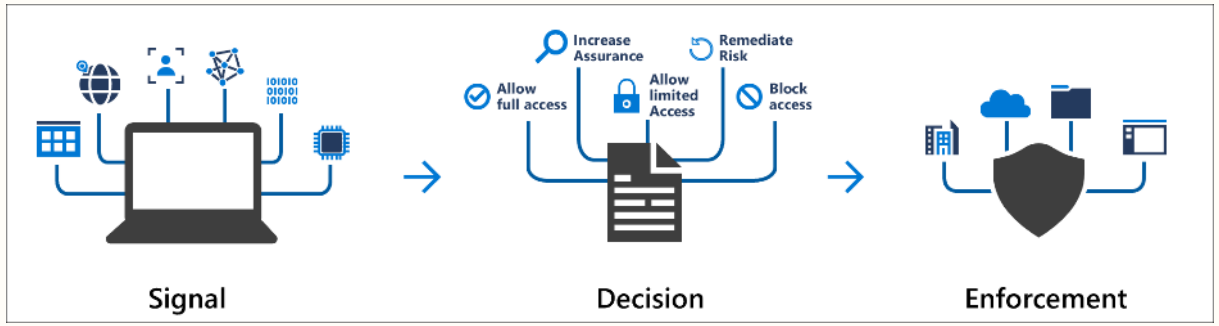
User and entity behavior analytics (UEBA) to automatically protect against identity compromise [2]

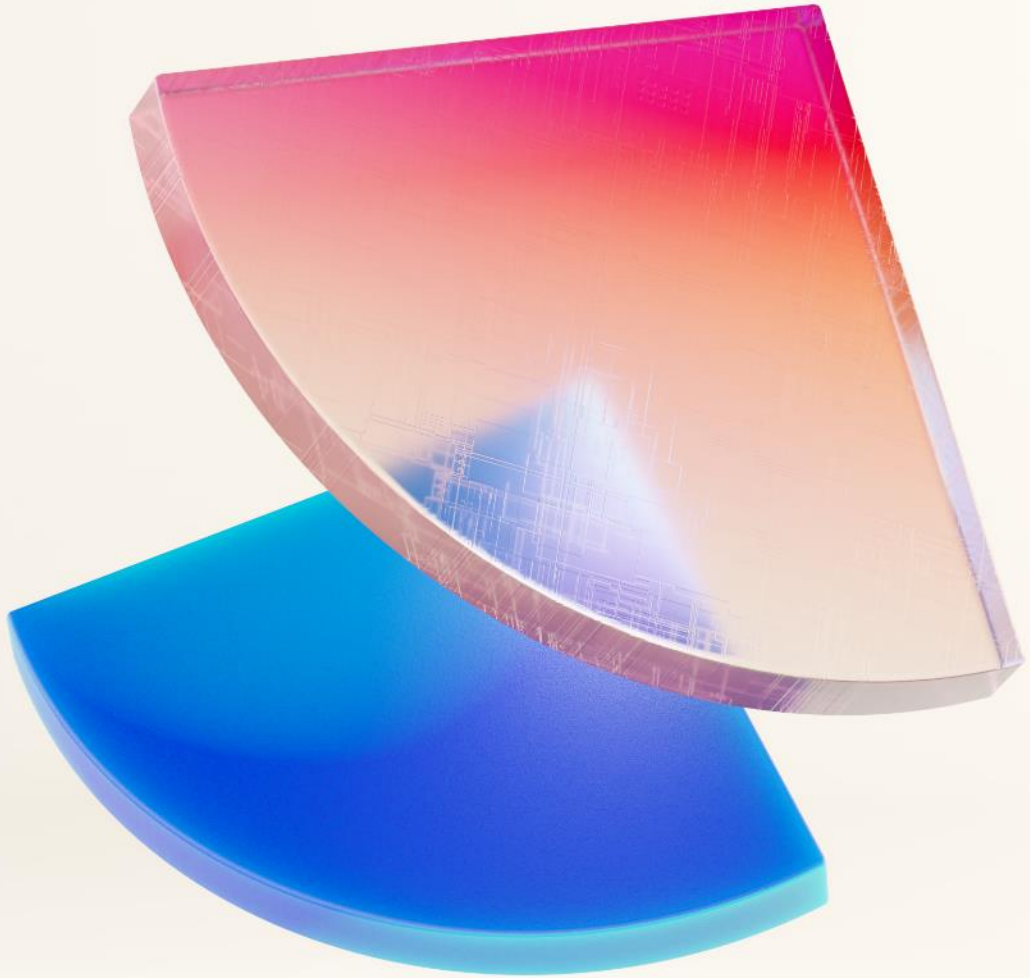
[1]Microsoft Entra ID P1 \ E3 license required *[2]Microsoft Entra ID P2 \ E5 license required*

Conditional Access Policies

Common Decisions – Block, Grant, Require MFA



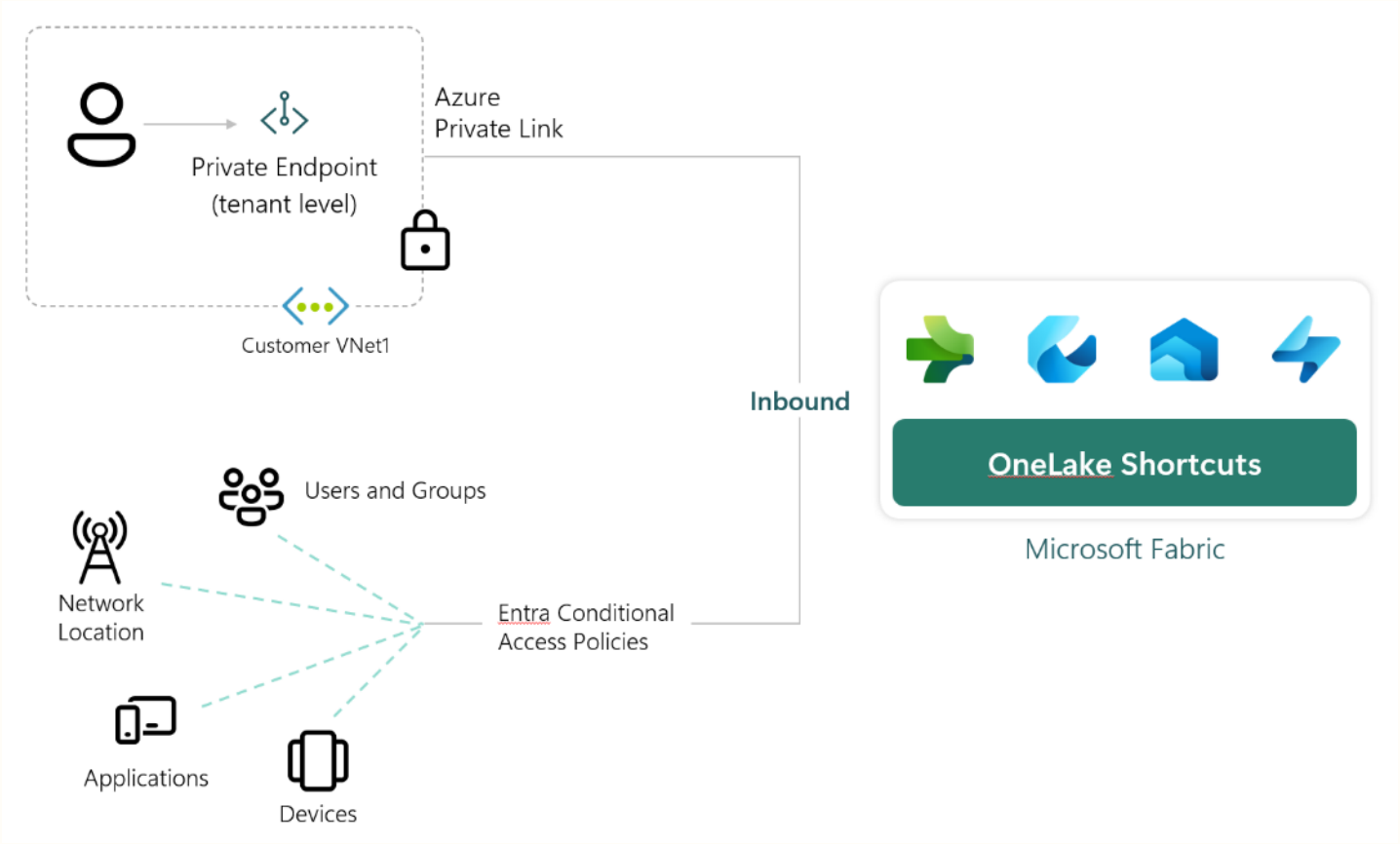




Securing inbound connections using Private Links

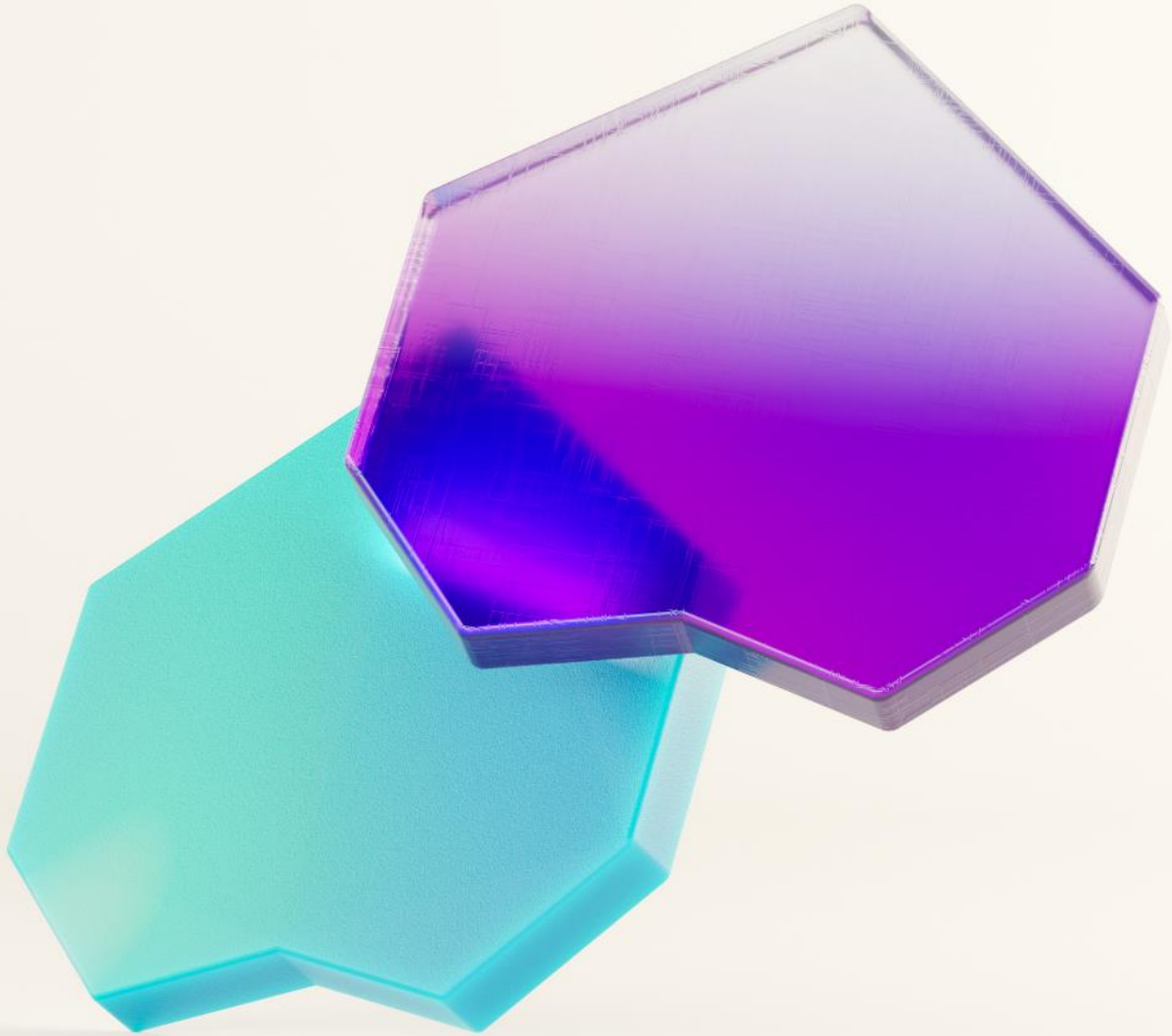
Private Link for Fabric

Perimeter Network Security for your tenant



What it means:

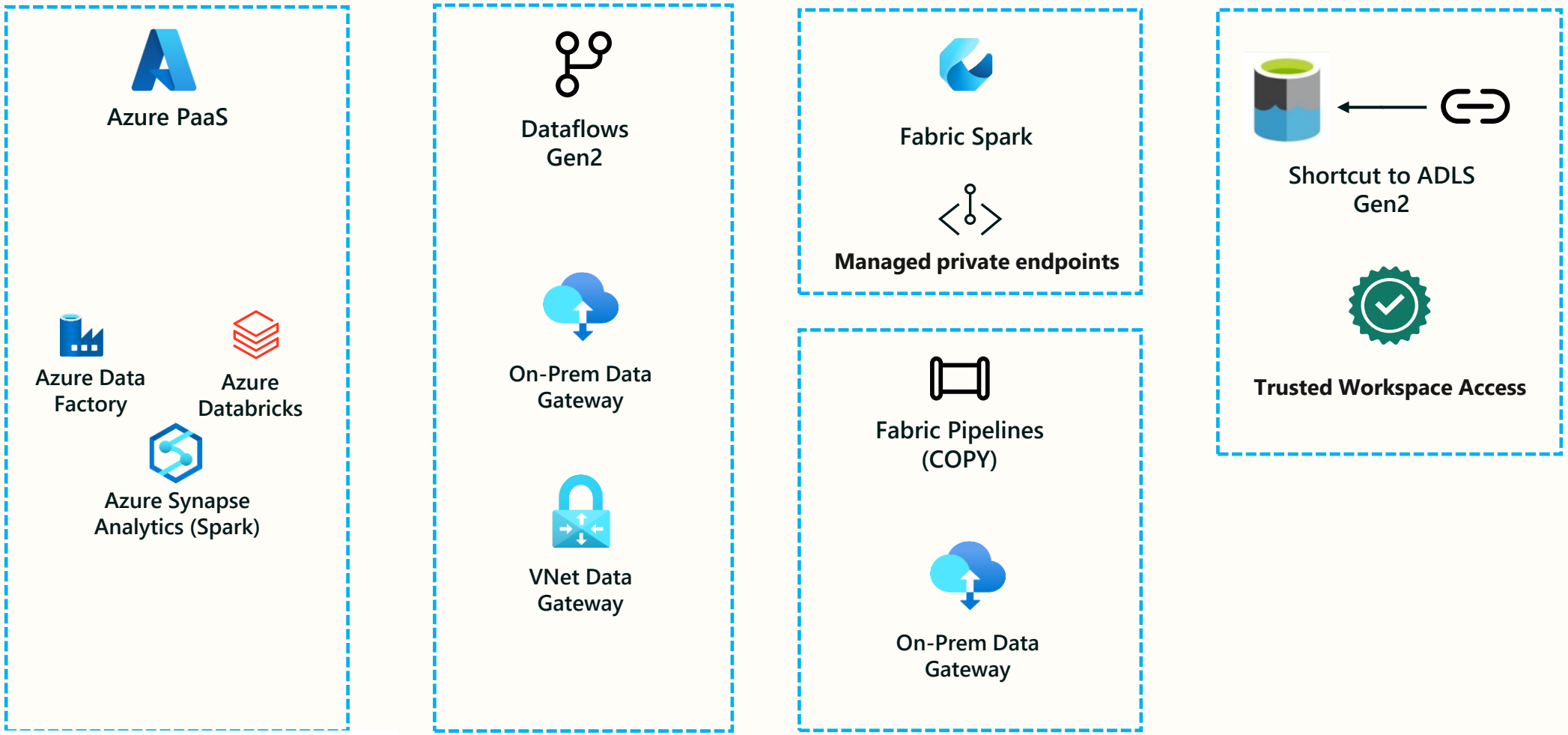
1. Fabric is disconnected from the public internet
2. Every users needs to connect to the private network to get access on every device
3. No longer able to load resources locally (slower reports)
4. Increases ExpressRoute bandwidth and added costs for Private Links
5. Several product limitations (like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

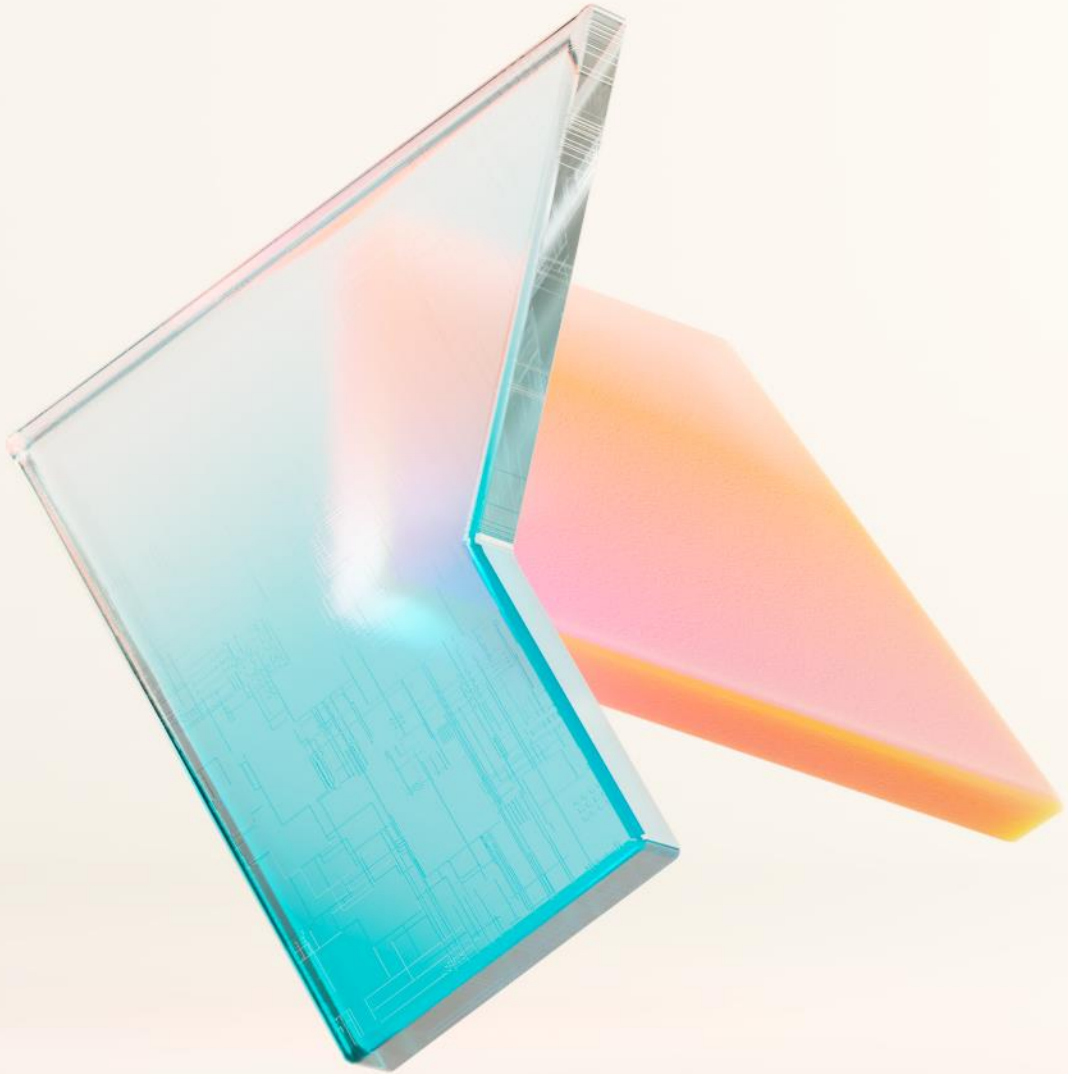


Getting secured data into Fabric

Getting data into Fabric

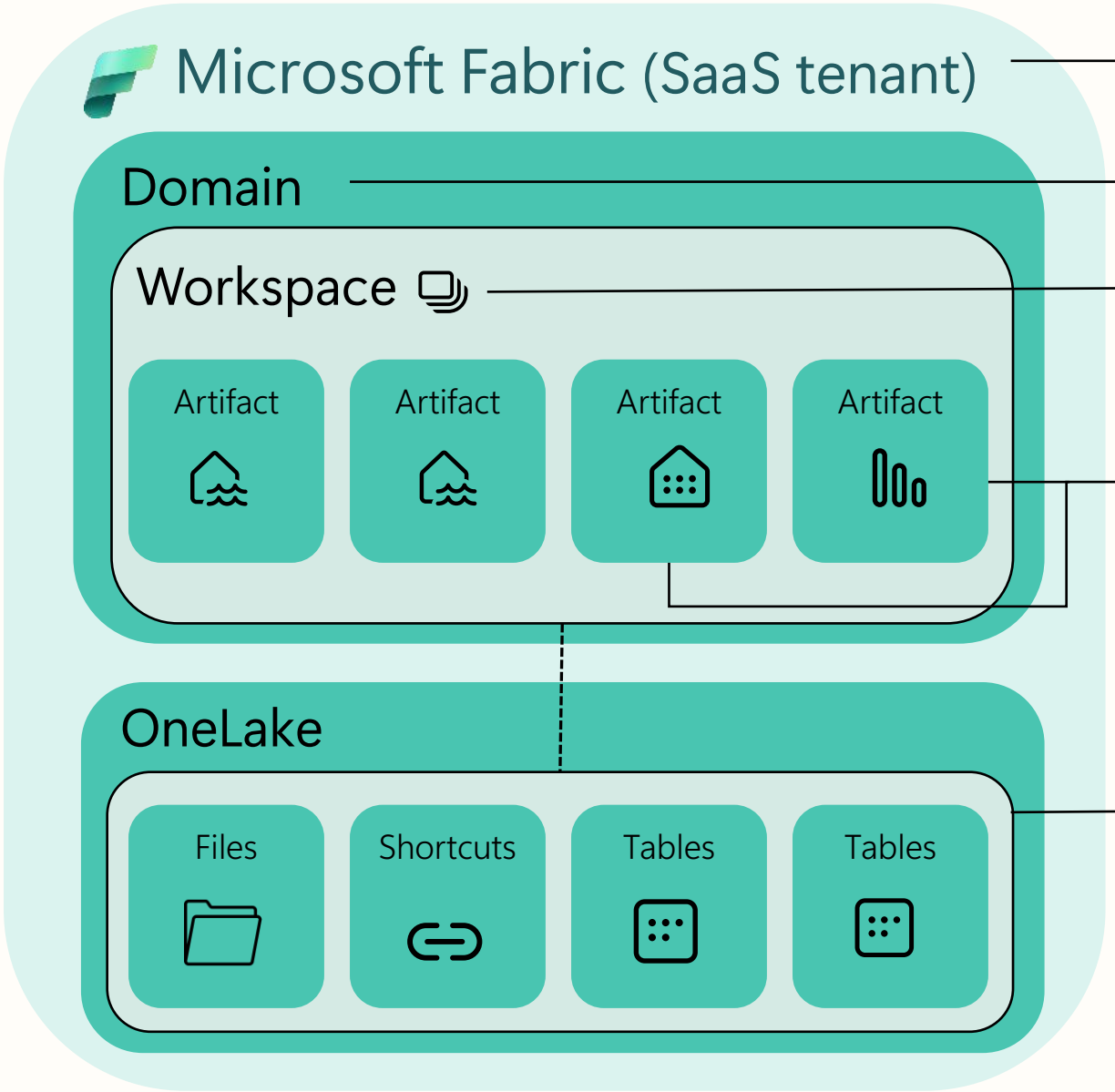
How to connect/load data in the VNET from Fabric





Fine-grained security and access controls in Fabric

Multiple layers of security and access control



Platform level access. Authentication through Entra ID. Inbound through Private Link or Conditional access

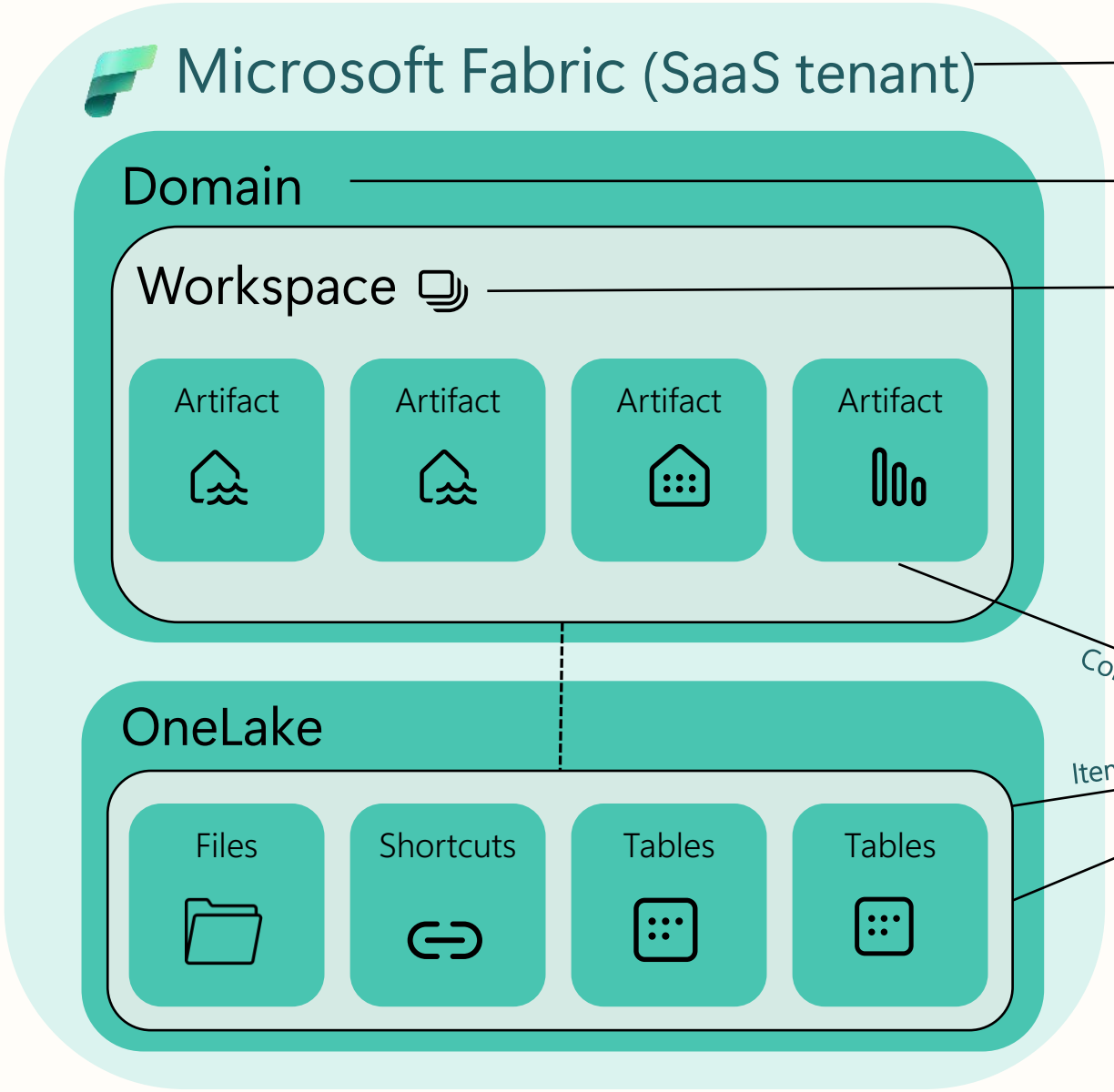
Domain specific configuration. by domain admins

Workspace level access. Boundary for managing artifacts. E.g. admin, contributor and viewers.

Compute security. e.g. Warehouse access through GRANT/DENY or Semantic Models & Warehouse RLS \ OLS.

Item level access. e.g. read all only via OneLake or read access to only subset of data.
More granular roles for files and folders.

Universal security coming later



Platform level access. Authentication through Entra ID. Inbound through Private Link or Conditional access

Domain specific configuration. by domain admins

Workspace level access. Boundary for managing artifacts. E.g. admin, contributor and viewers.

Universal security: Define security once and propagated to OneLake and every compute engine for access and OLS \ RLS

Data Encryption in Fabric

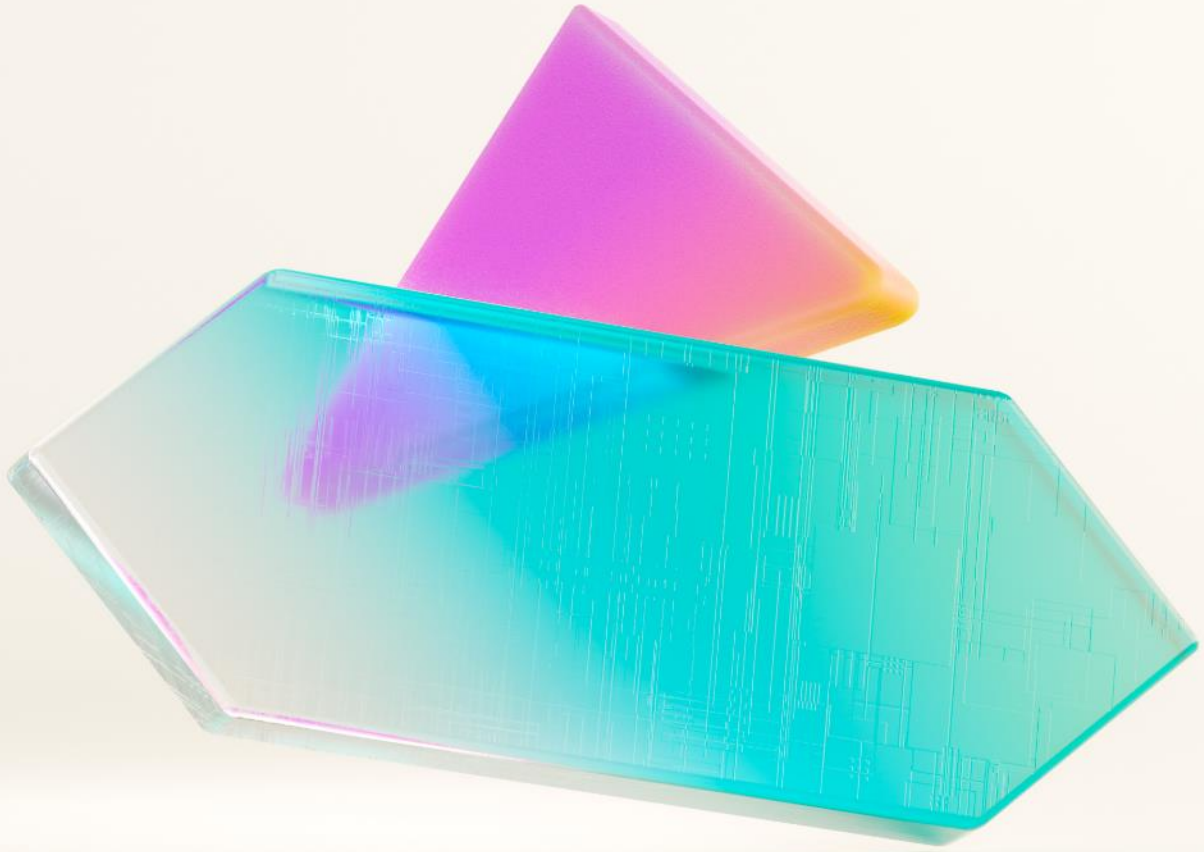
Encryption in Fabric

Encryption in-transit:

- ❑ Transport Layer Security (TLS 1.2) enforced
- ❑ All endpoints
  - ❑ TDS (SQL) (TLS 1.2)
  - ❑ XMLA (HTTPS)
  - ❑ OneLake (ABFSS)
  - ❑ APIs (HTTPS)
- ❑ All internal communications are encrypted in transit

Encryption at-rest:

- ❑ All data encrypted at rest
- ❑ Customer data, metadata, caches
- ❑ Platform managed keys – secure, convenient and low overhead
- ❑ BitLocker encryption wherever applicable



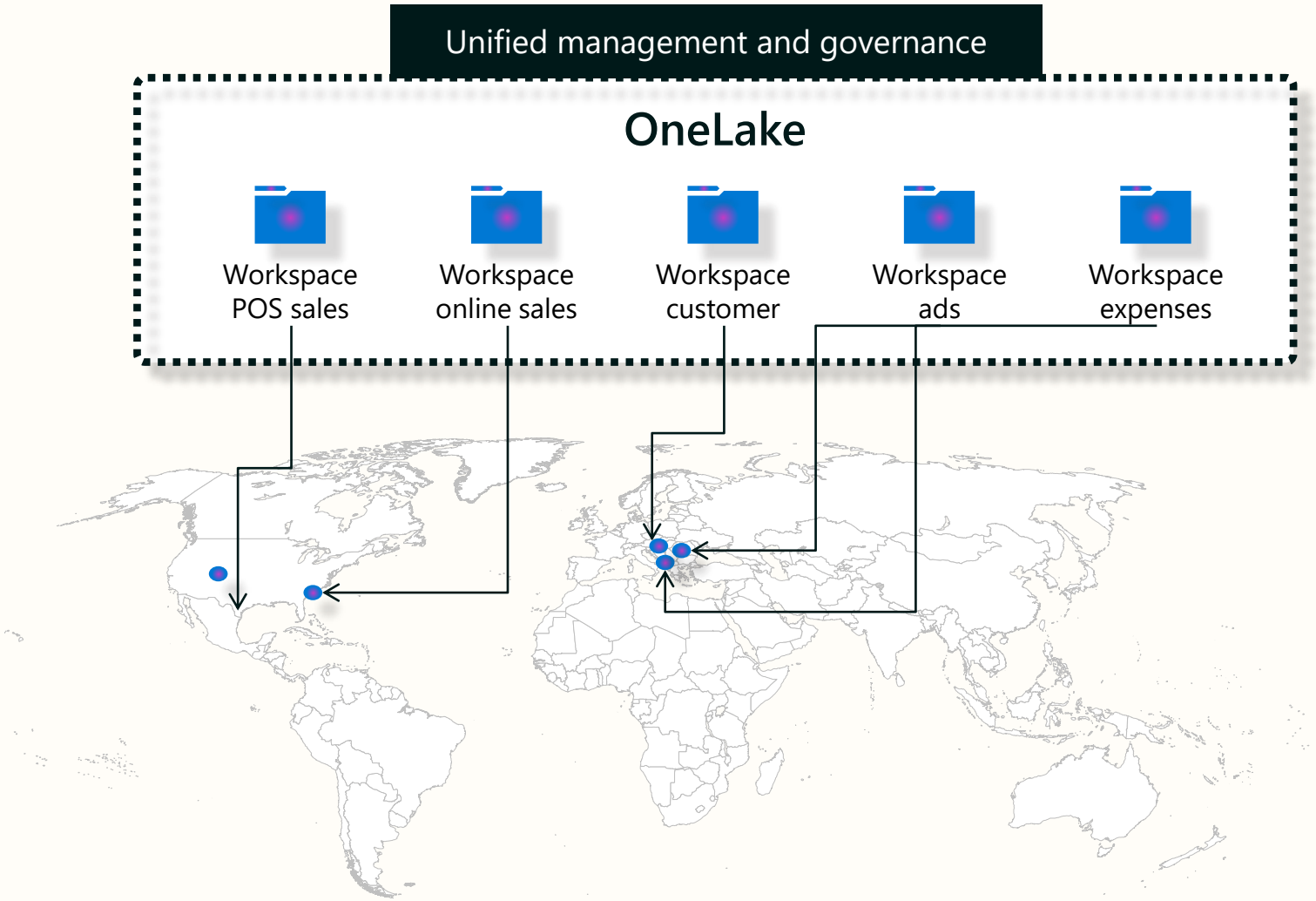
Data Residency and Compliance.

Data Residency

With the largest global footprint, Fabric multi-geo capacities allows control over content storage location in one of 54 data centers world-wide

OneLake which logically spans the world

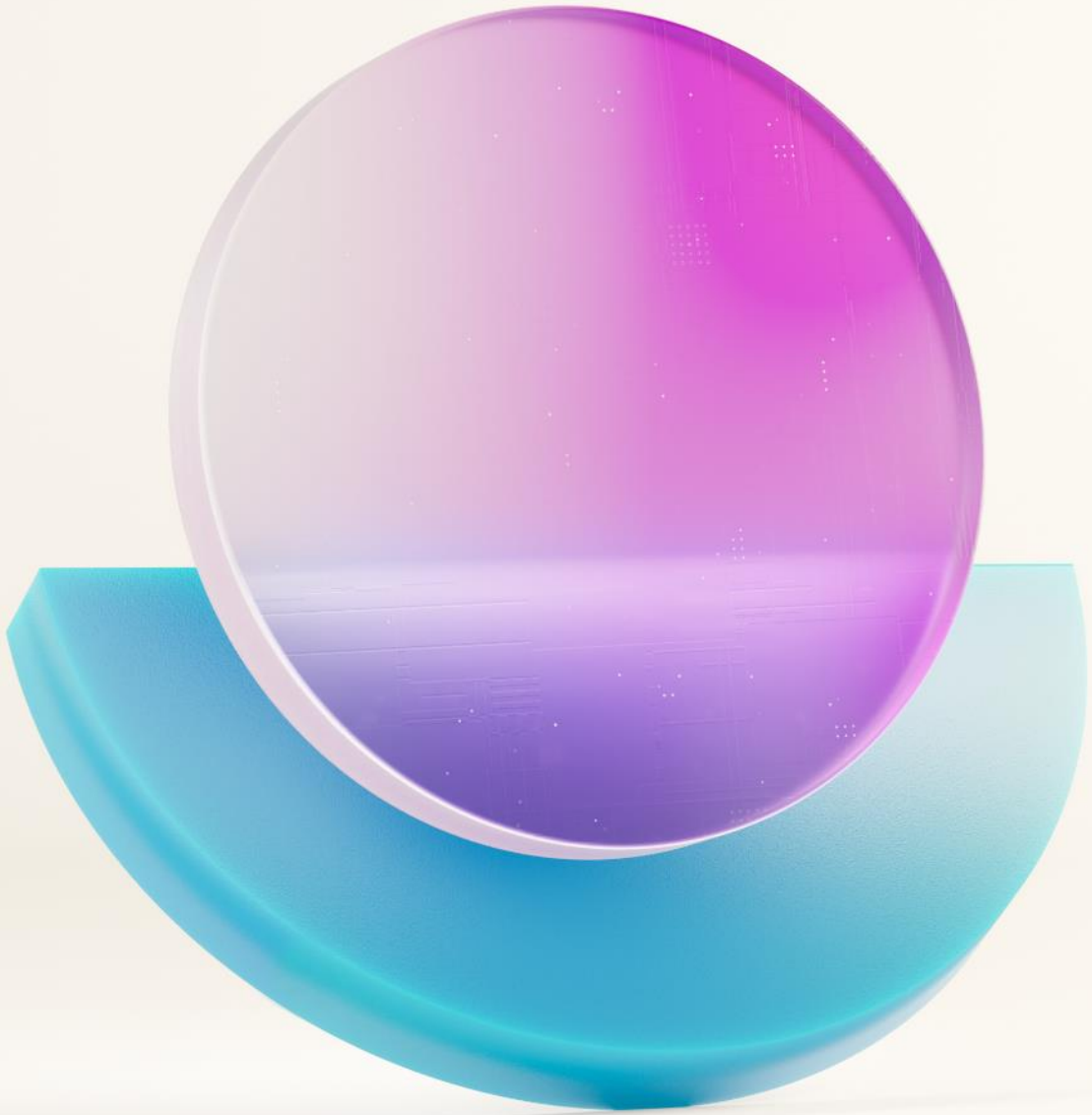
Workspaces can reside in different regions around the world while still being part of the same data lake.



Compliance with Microsoft Fabric

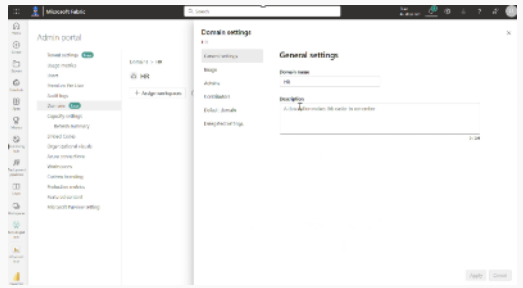
Microsoft Fabric is a core Microsoft online service and supports a wide range of compliance standards including:

- GDPR
- EUDB
- ISO certifications including ISO 27001, 27701, 27017, 27018
- HIPAA compliance
- Other certifications will continue to be available…



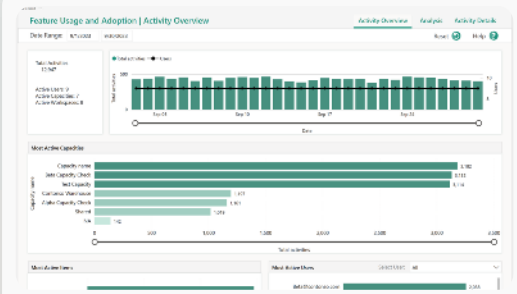
Administration and governance

Admin and Monitor activity across your tenant



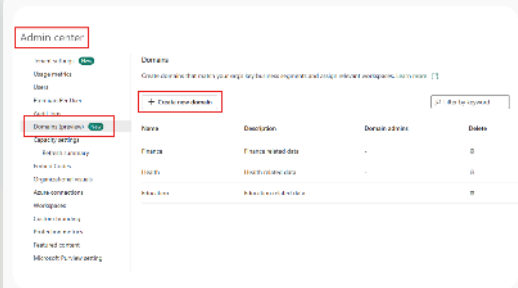
Delegated admin permission

Provide delegated admin permissions per Domain and Capacity



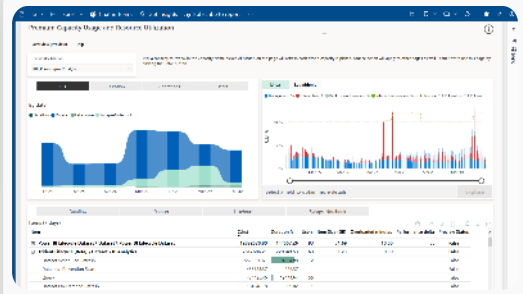
Admin monitoring & auditing

Uncover insights for effective governance with reports and datasets built for admins. Log, view and export user activities from Microsoft Fabric to support auditing



Monitoring hub

Monitor Fabric activities, such as semantic model refresh and Spark Job runs and many others, from a central location

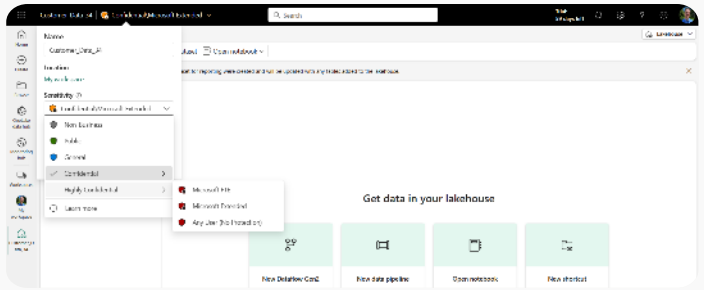


Capacity metrics

Gain visibility into capacity utilization and usage trends with daily aggregation so you can plan and scale your capacity accordingly

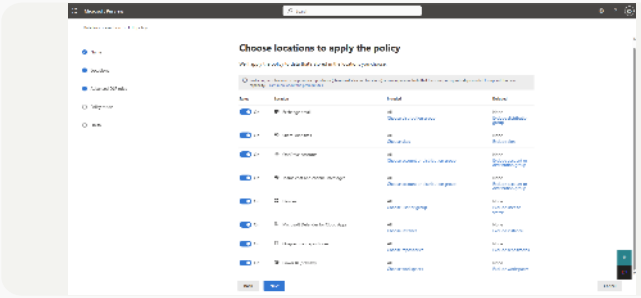
Security and compliance features

Secure and protect data across your organization



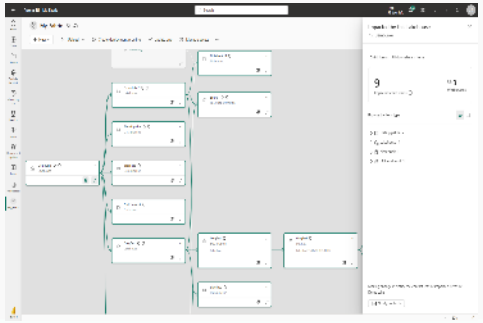
Information Protection labels*

Classify sensitive Fabric data using the same sensitivity labels that are used in Microsoft 365—enforced even when the data is exported



Data Loss Prevention policies*

Automatically detect the upload of sensitive data such as PII and trigger automatic risk remediation actions such as alerts



Metadata & Lineage

See lineage view of analytical projects to see how data flows through items and perform impact analysis to assess impact of changes. Can be extended with Purview Data Map and Scanner API's

*Additional Microsoft Purview purchase required

Microsoft | Microsoft Fabric

Thank you