



Microsoft

Microsoft Fabric

A collection of abstract, semi-transparent 3D geometric shapes, including cubes, hexagons, and circles, in shades of blue, cyan, and yellow, floating against a white background.

Fabric security:  
everything you  
need to know!



<https://www.linkedin.com/in/vengat83>

# Venkatesh Parasuraman

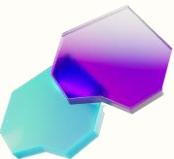
Principal Program Manager, Microsoft Fabric

CAT – Customer Advisory Team



# Agenda

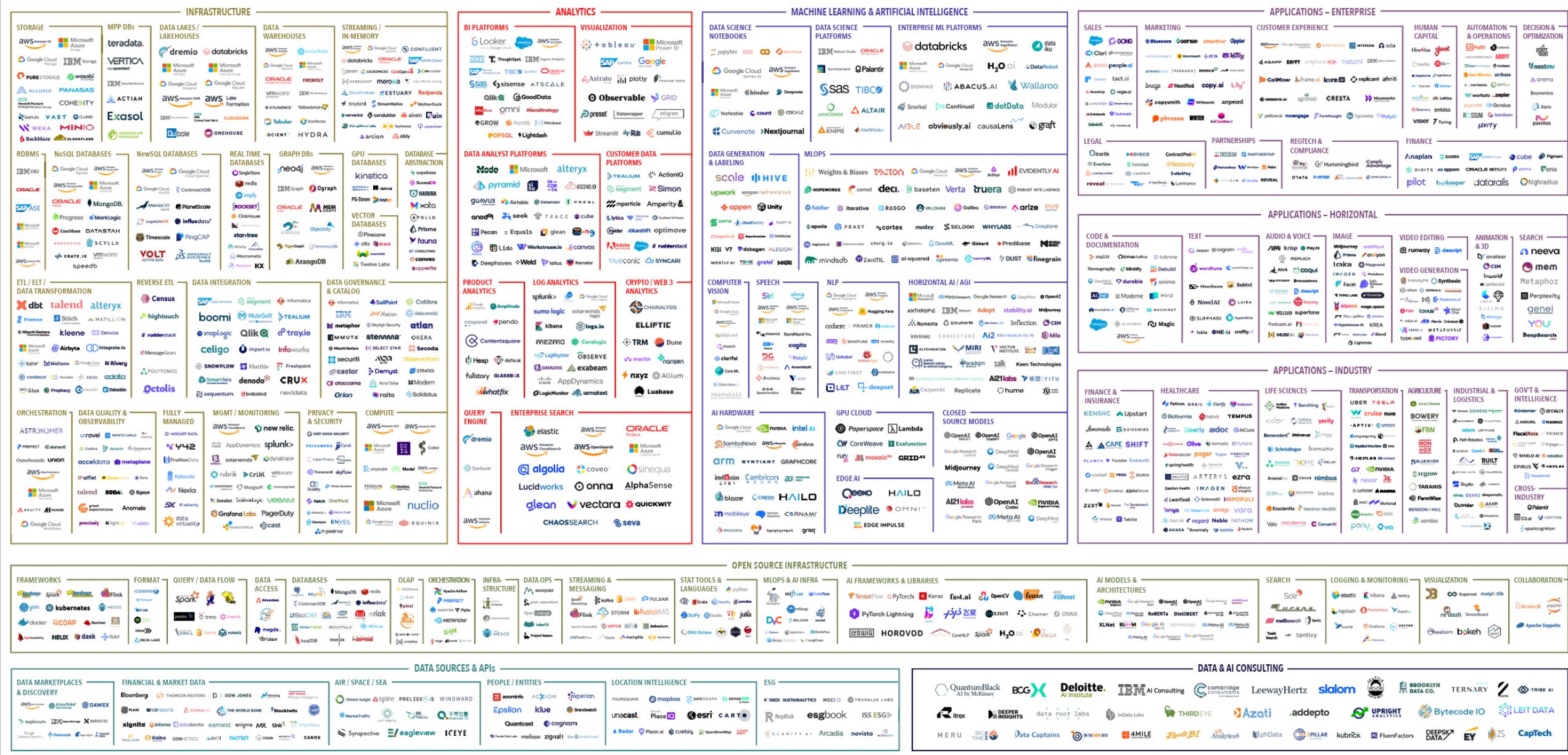
- Intro to Fabric as a SaaS platform
- Authentication to Fabric
- Network protection (Entra & Private Link)
- Connecting to secure data
- Data encryption
- Item level security
- Data residency
- Data Governance and compliance



A world awash with data...

**How do you translate data into  
competitive advantage?**

# The 2023 ML, AI, and Data Landscape



“

Simplify,  
I am the Chief Data Officer  
and don't want to be the  
Chief Integration Officer.”

Every CDO, Every Enterprise



# Microsoft Fabric

The unified data platform for the era of AI



Data  
Factory



Synapse Data  
Engineering



Synapse Data  
Science



Synapse Data  
Warehousing



Synapse Real  
Time Analytics



Power BI



Data Activator



OneLake

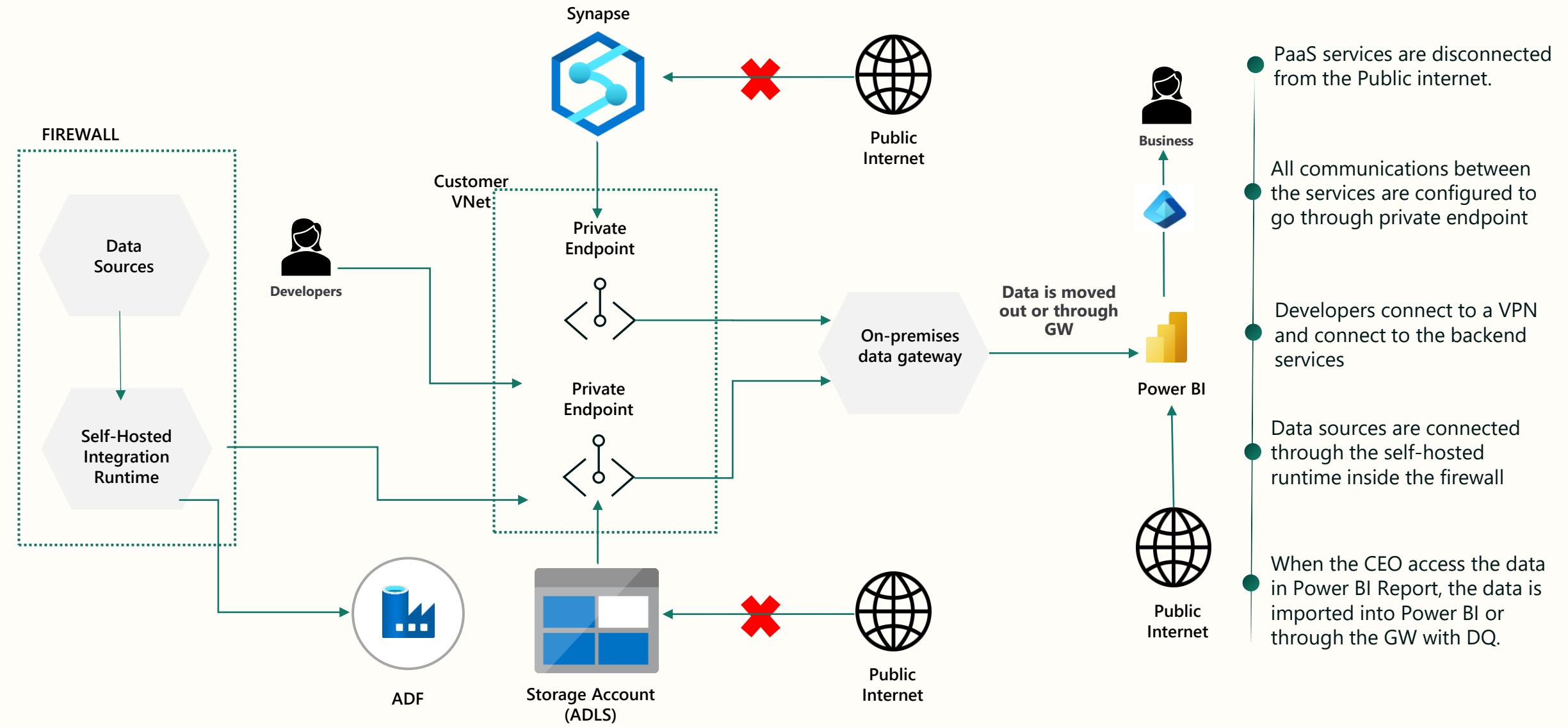
# Modern data challenges

- 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

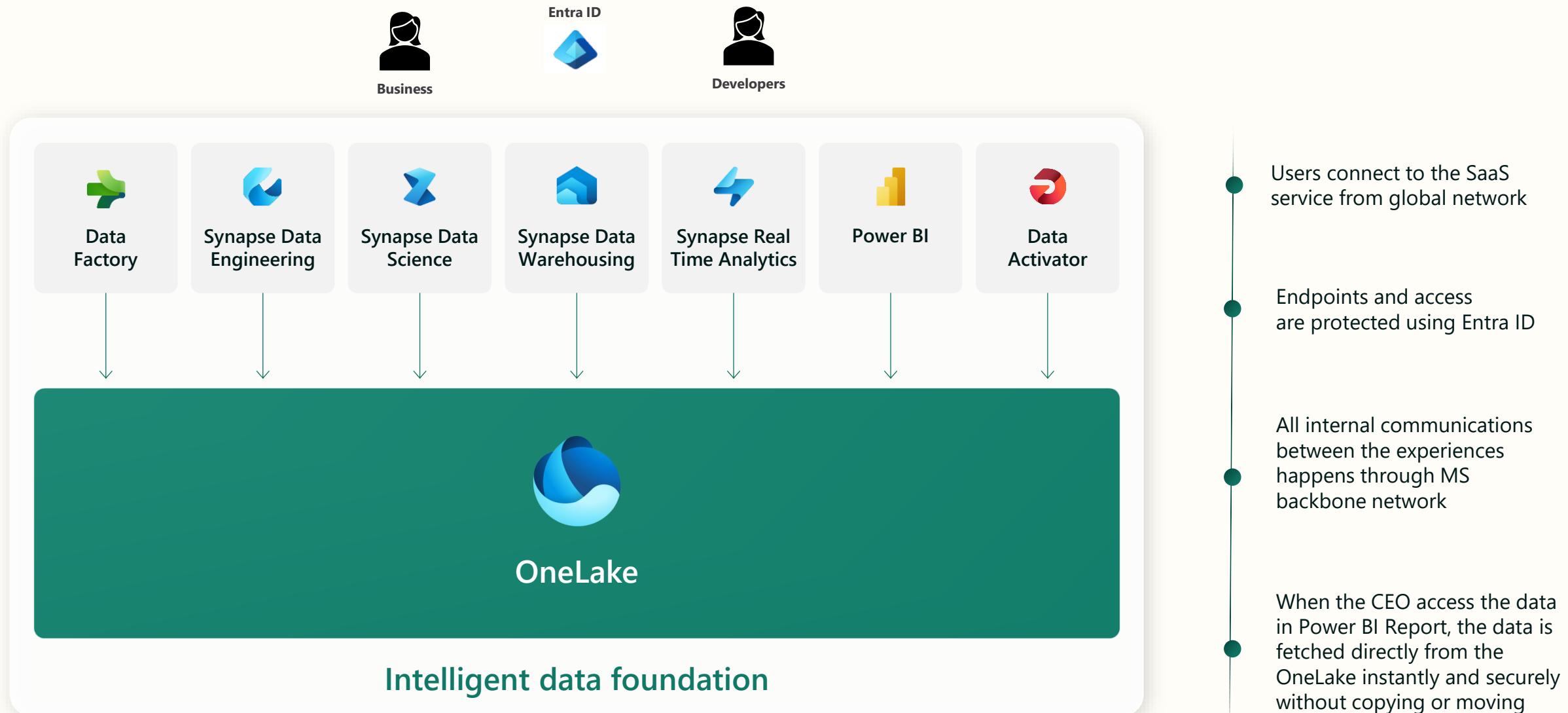
# Common network security requirements

- 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

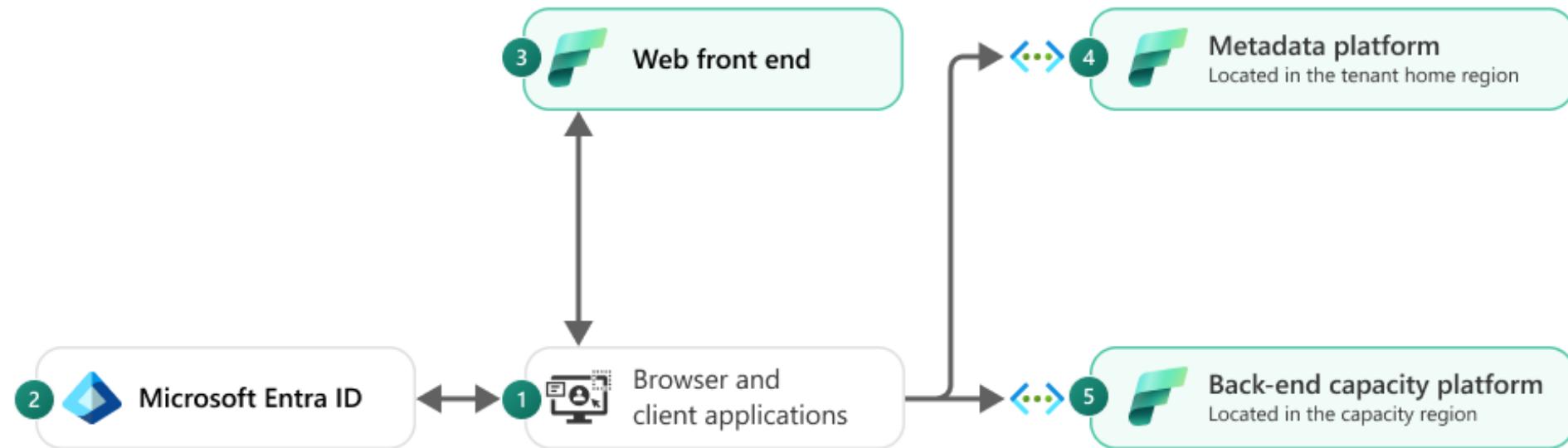


# Microsoft Fabric – SaaS World



# Microsoft Fabric Architecture

Fabrics is built as a SaaS product.

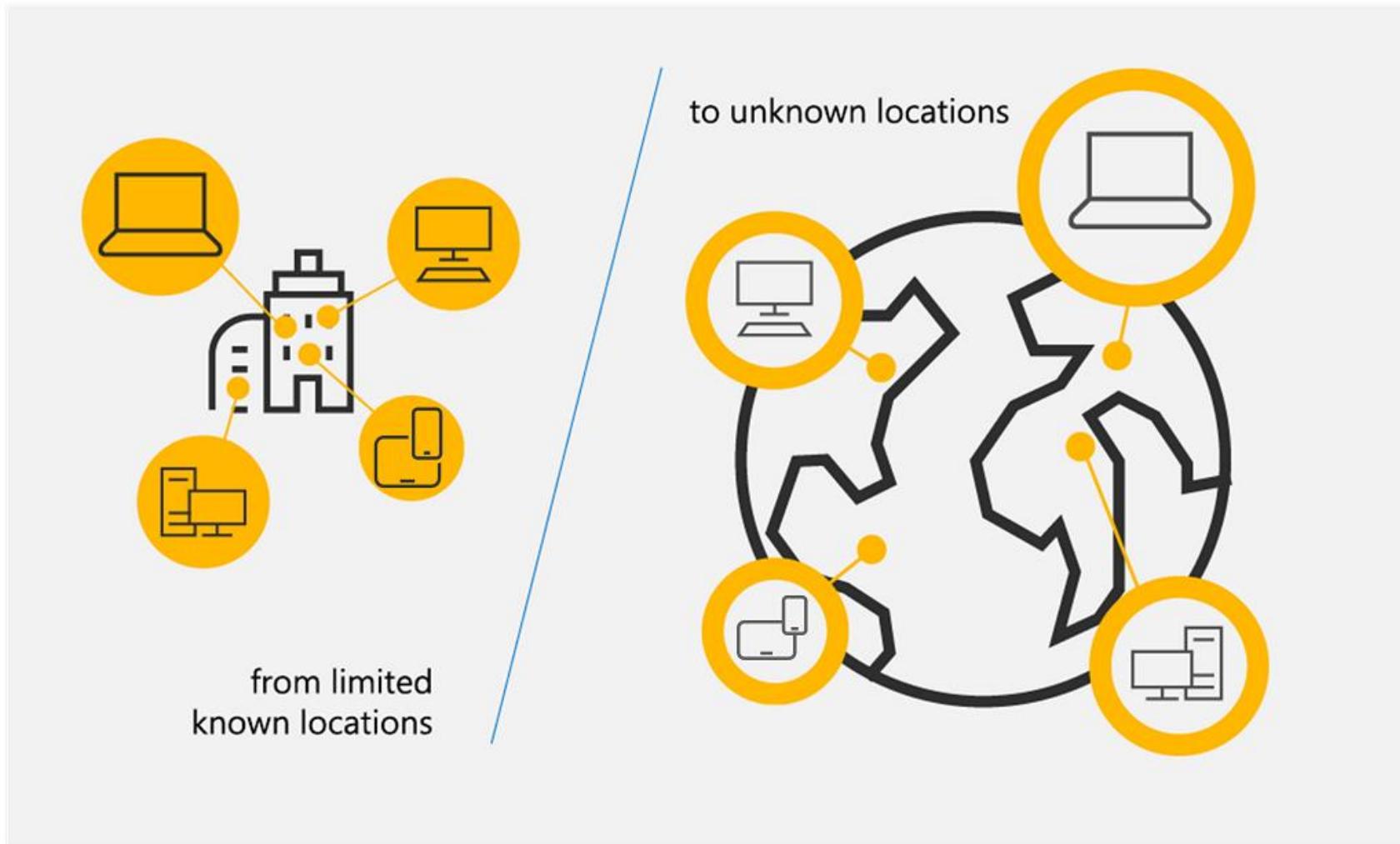


- Users connect only to “Front End Services” and we are using “Entra ID” to authenticate and **trust all requests**.
- All the clusters **are protected behind “back-end services” and v-nets**.
- Traffic between experiences is **going over MS backend network**
- Traffic to Fabric will be using at **least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

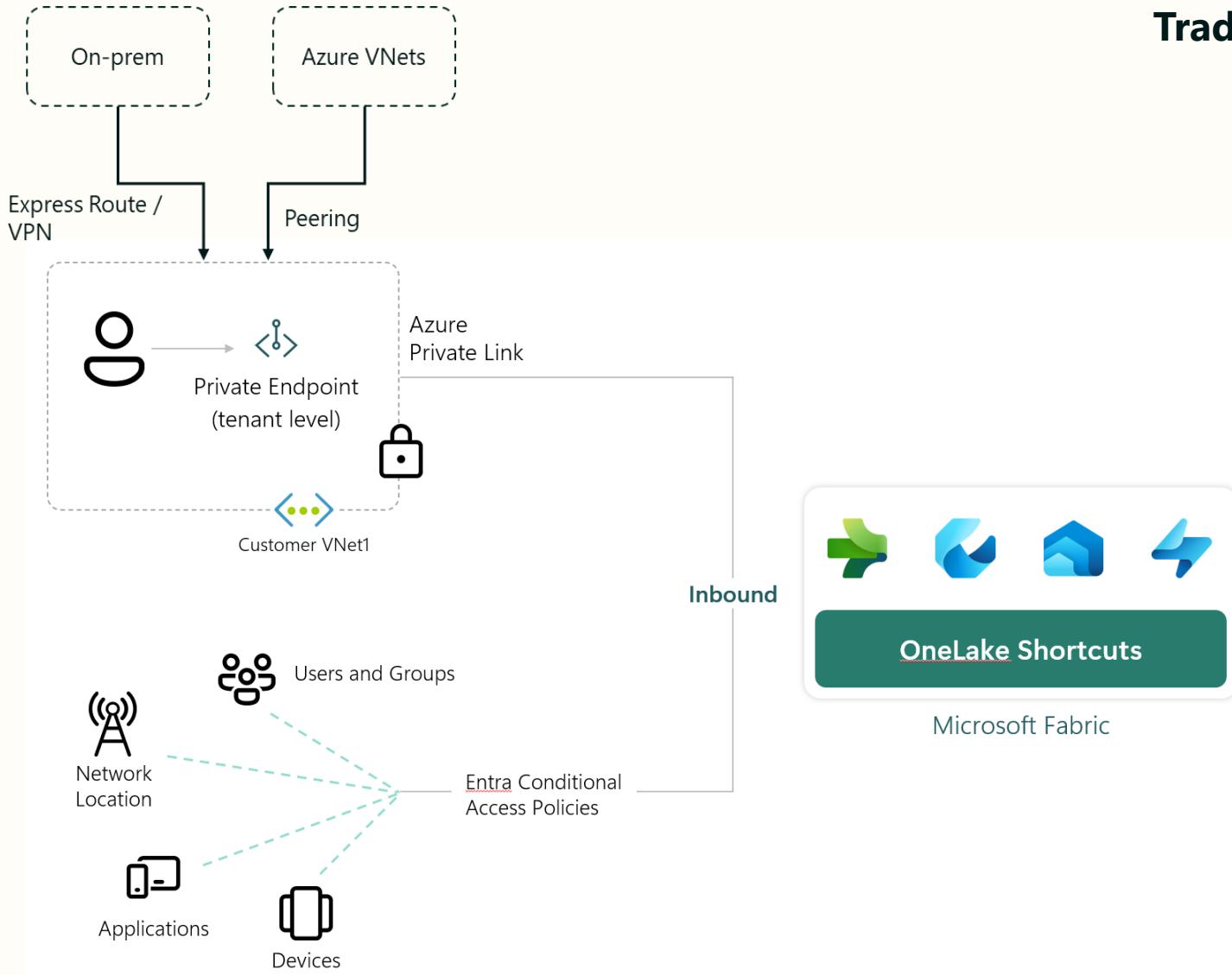
# Inbound protection options

Perimeter Network Security

Zero Trust Approach



# Inbound Protection options for Microsoft Fabric

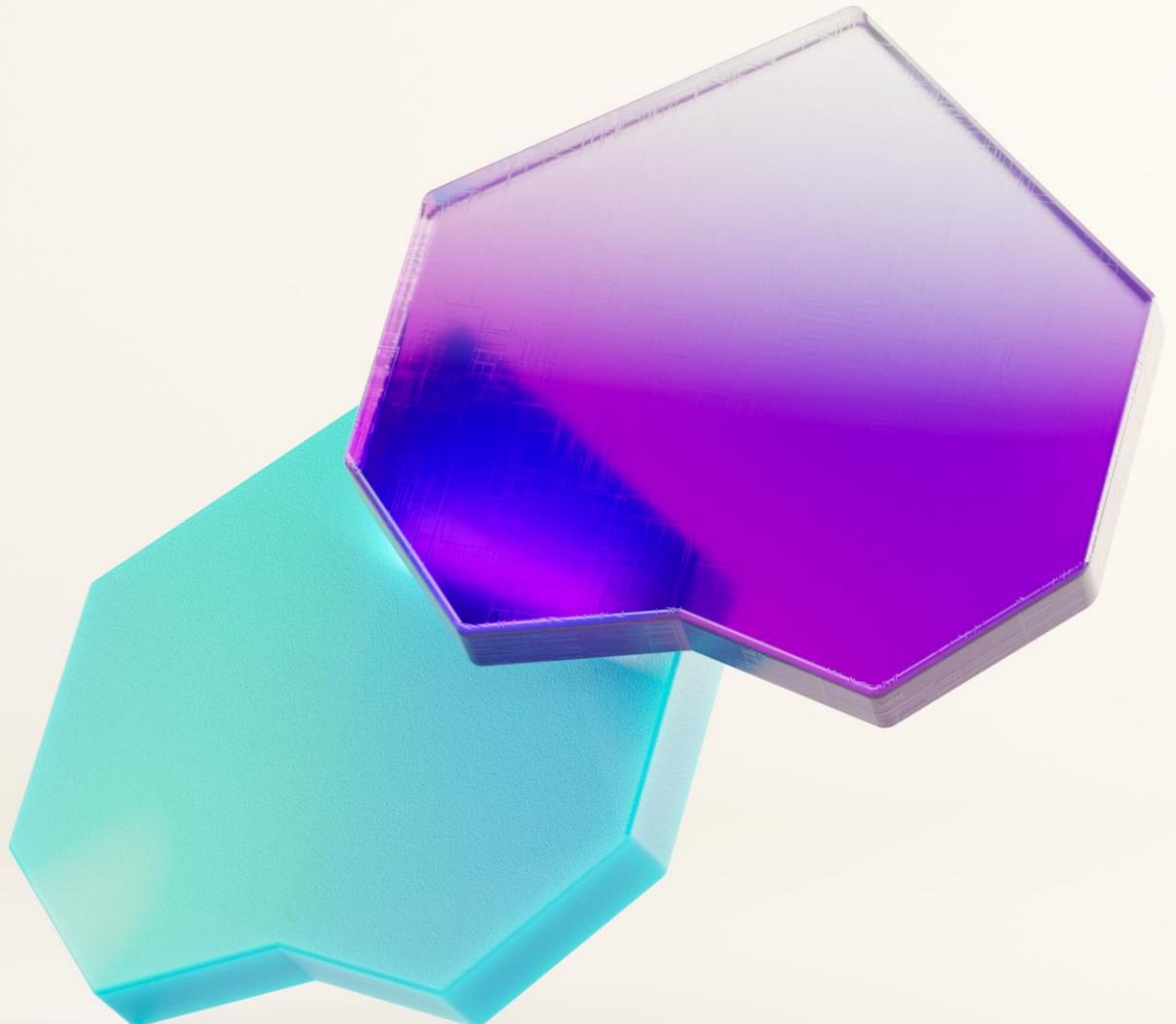


## Traditional Network Security with Private Links:

- Popular/Recommended option for PaaS
- not widely adopted for SaaS

## Zero Trust with Microsoft Entra:

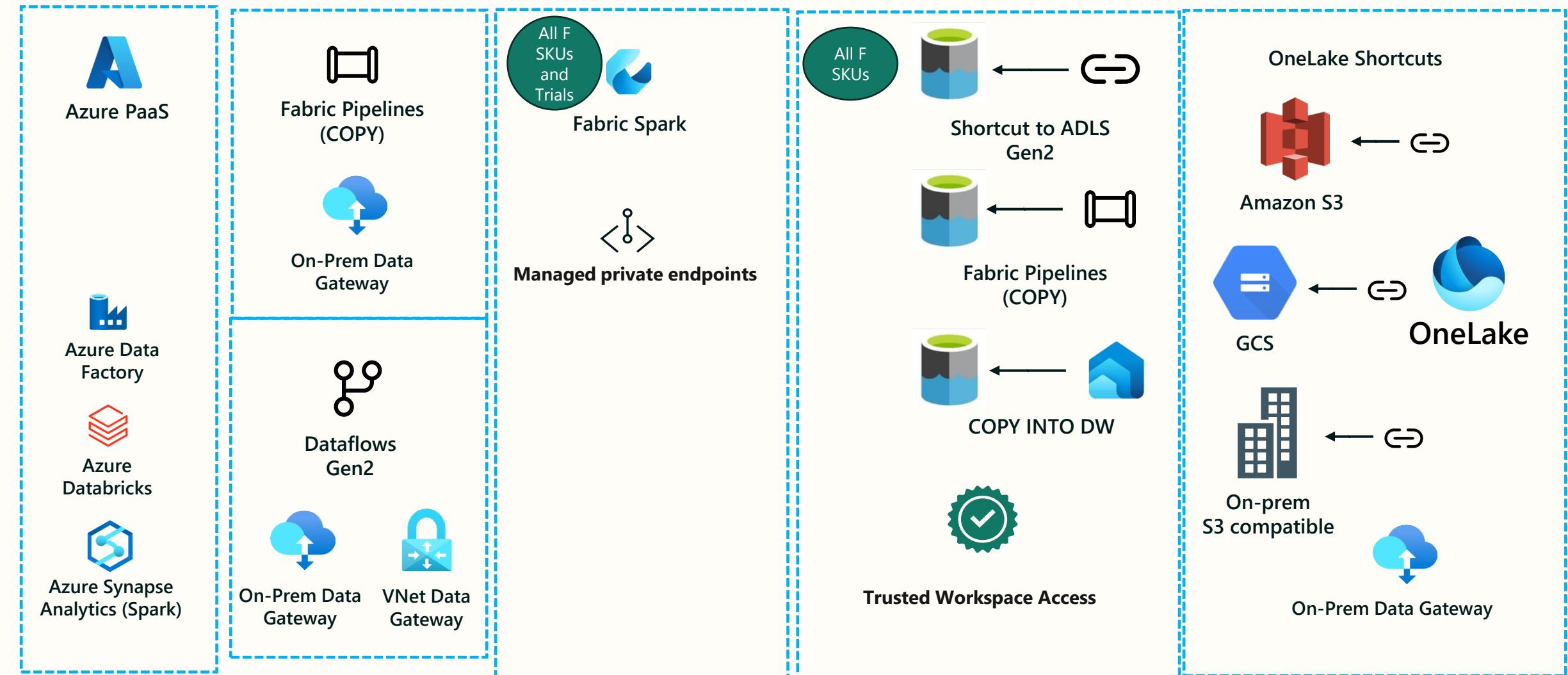
- Conditional Access Policies, MFA, Device Protections
- Widely adopted for SaaS such as M365, SharePoint Online, Teams, OneDrive for Business, OneLake

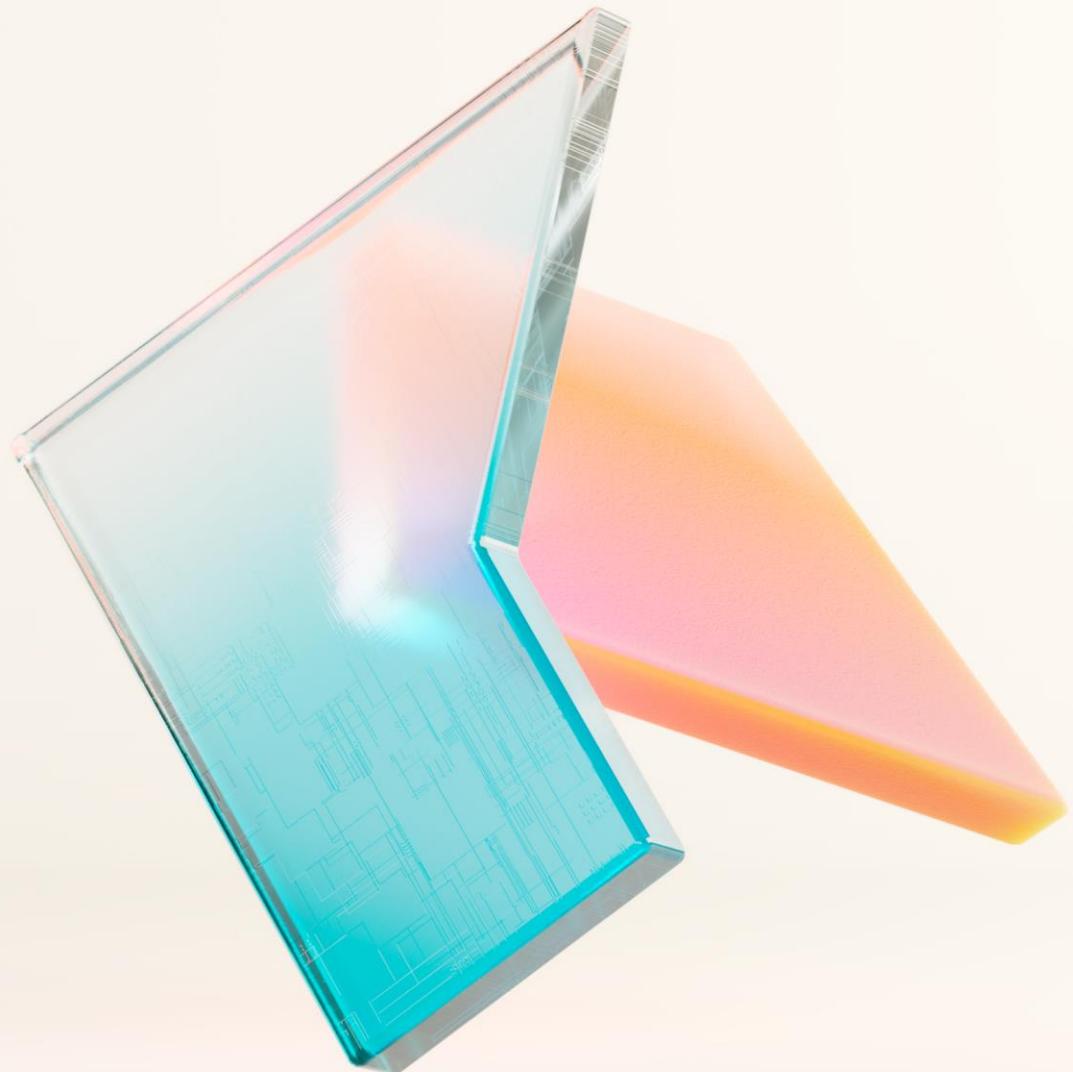


Getting secured data  
into Fabric – Outbound  
Connectivity

# Getting data into Fabric – Outbound Connectivity

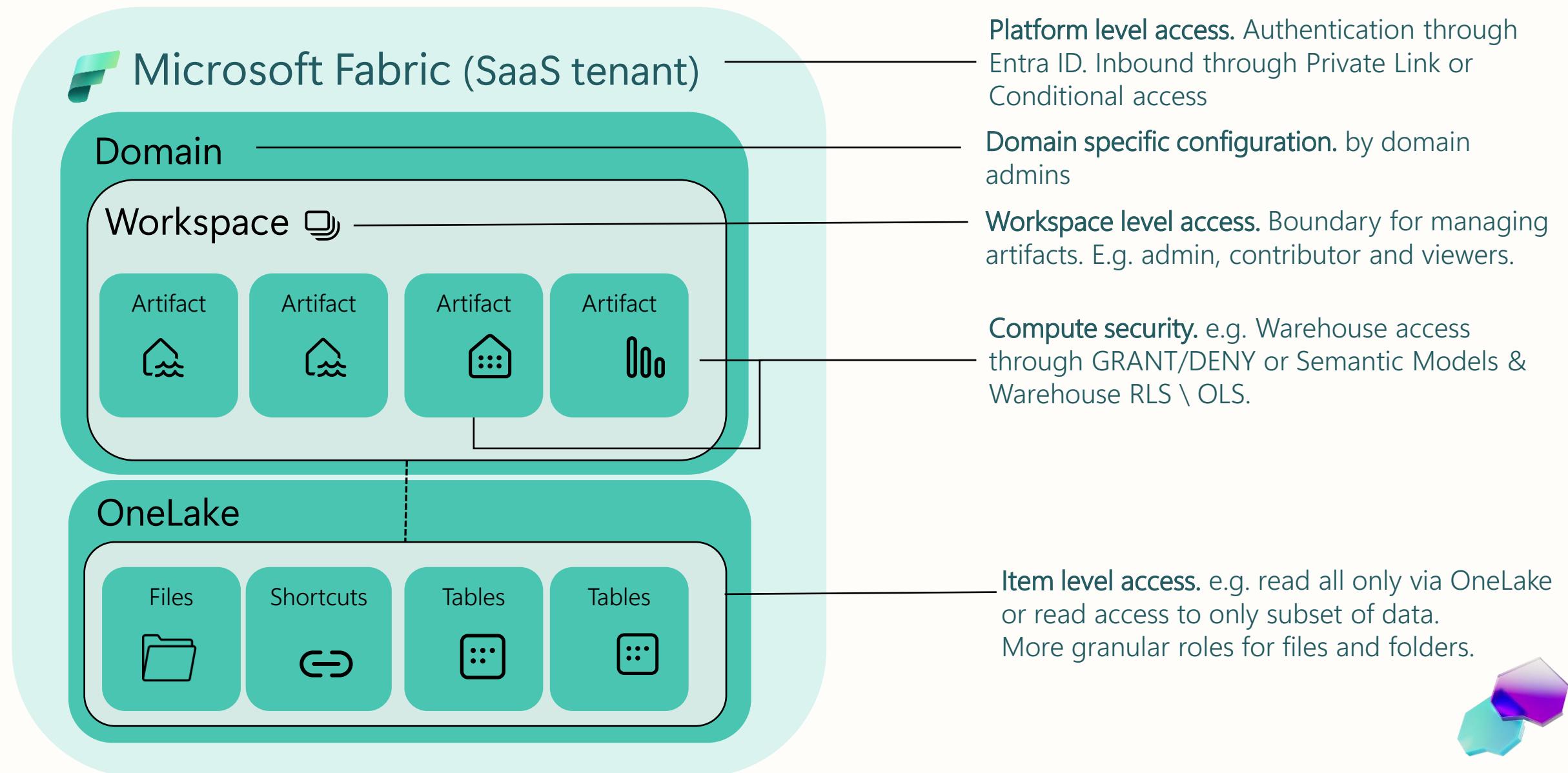
How to connect/load data in the VNET from Fabric





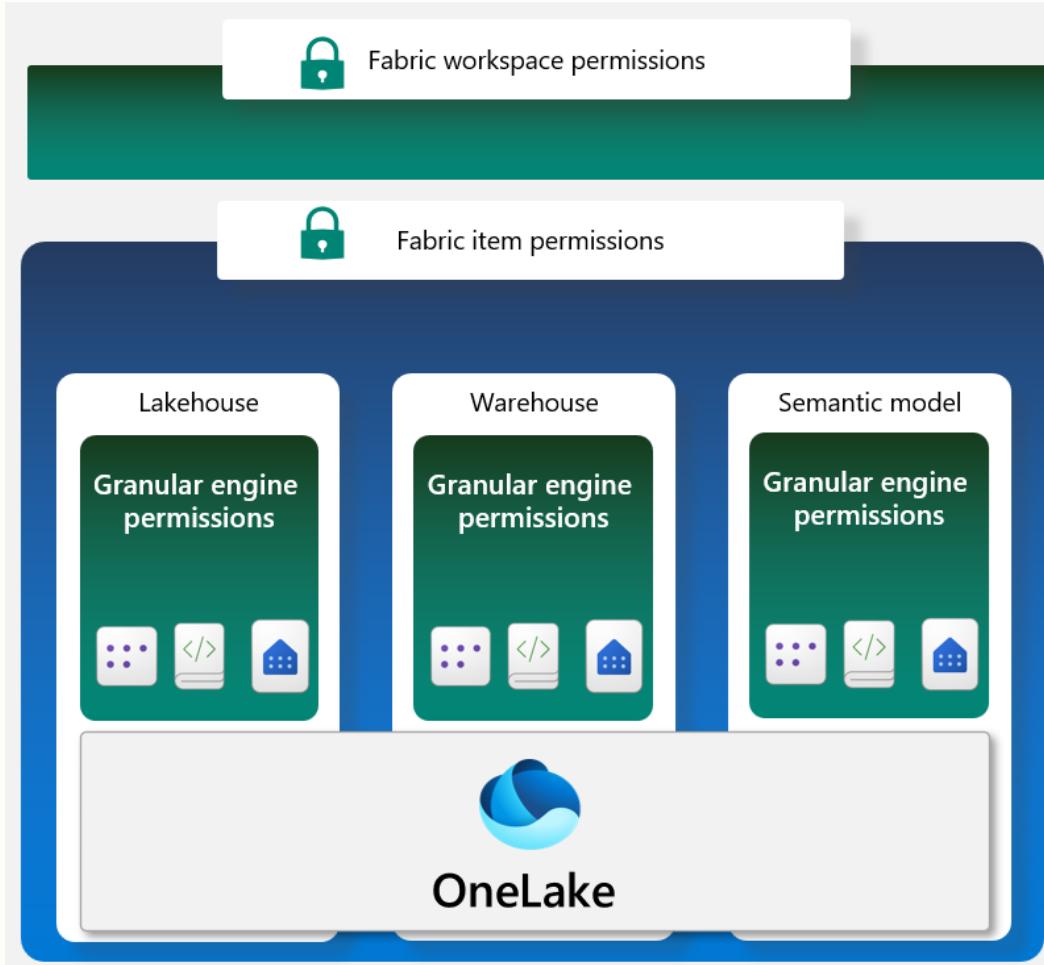
Fine-grained security and  
access controls in Fabric

# Multiple layers of security and access control

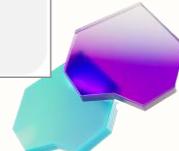
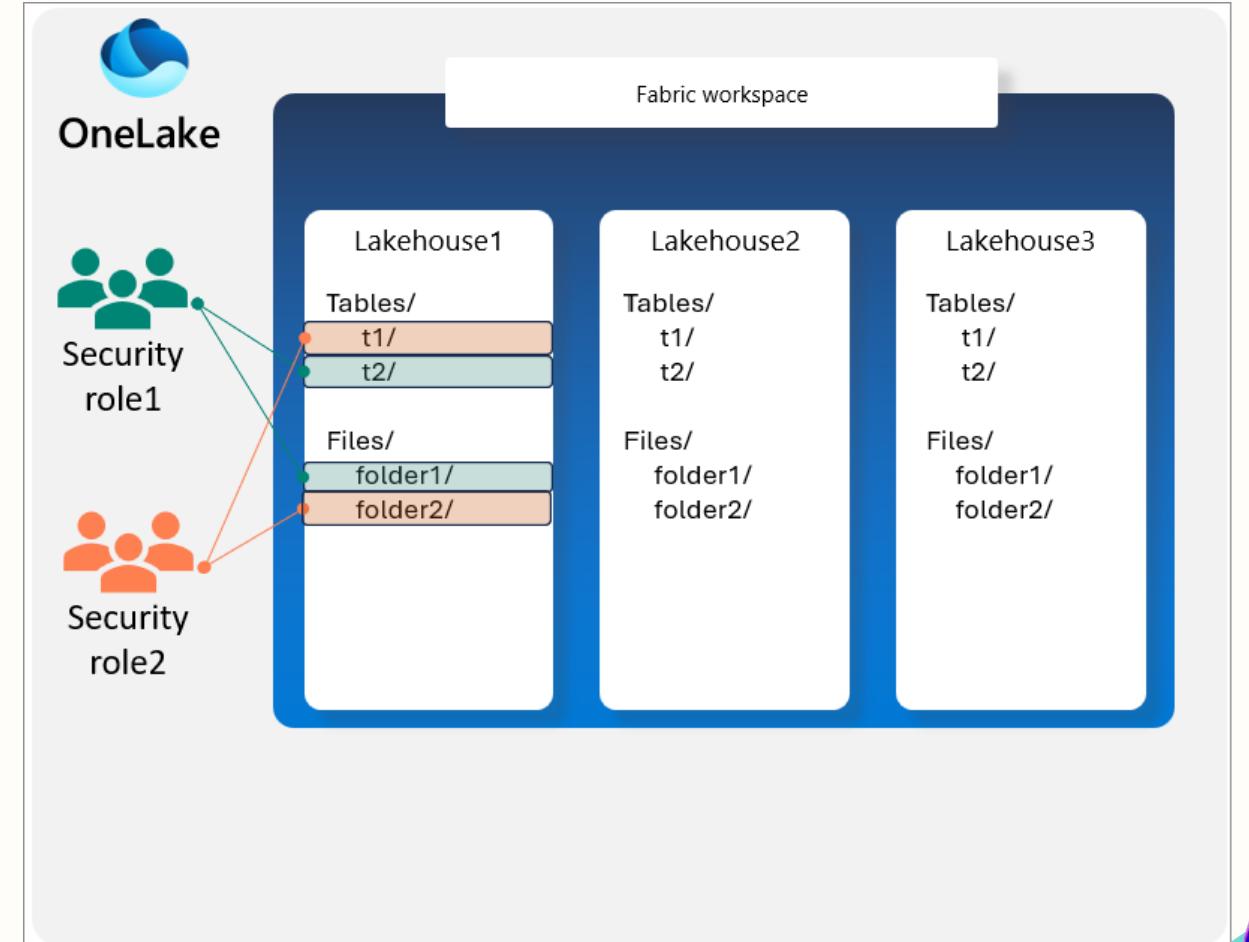


# Data Security – Access Controls

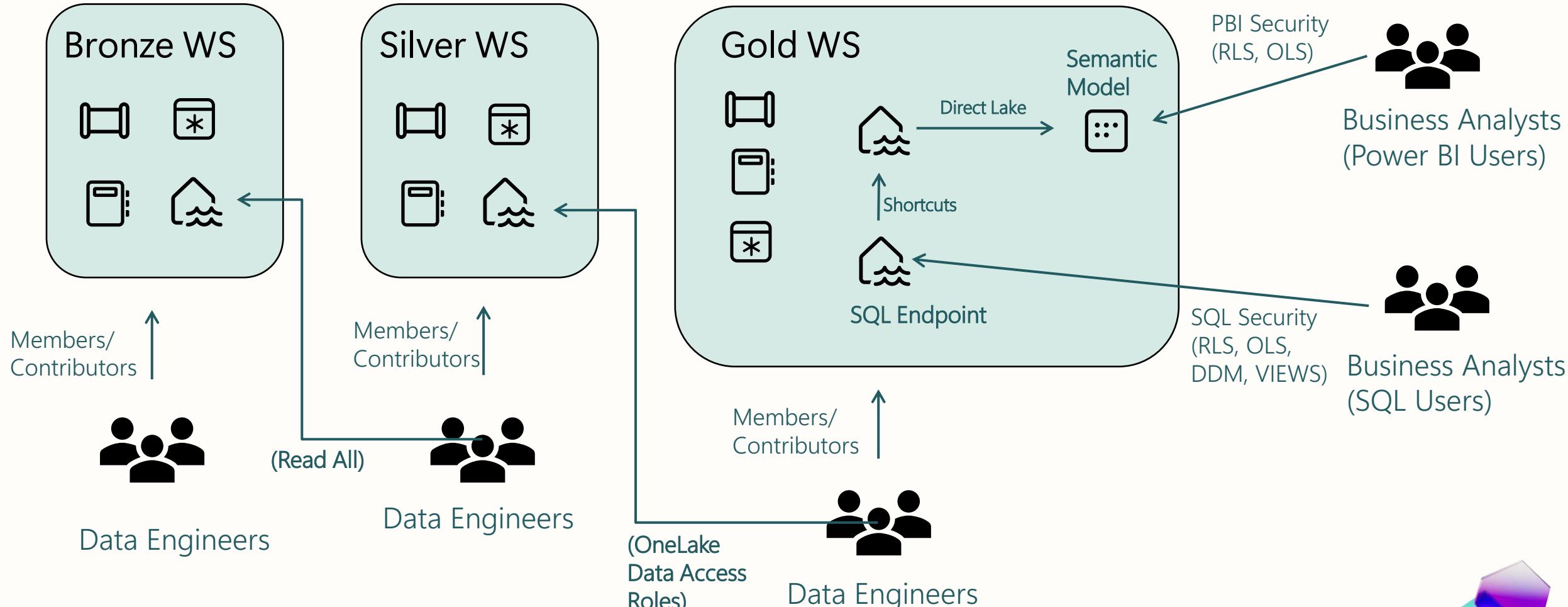
Granular Compute Level Security (SQL, PBI, KQL)



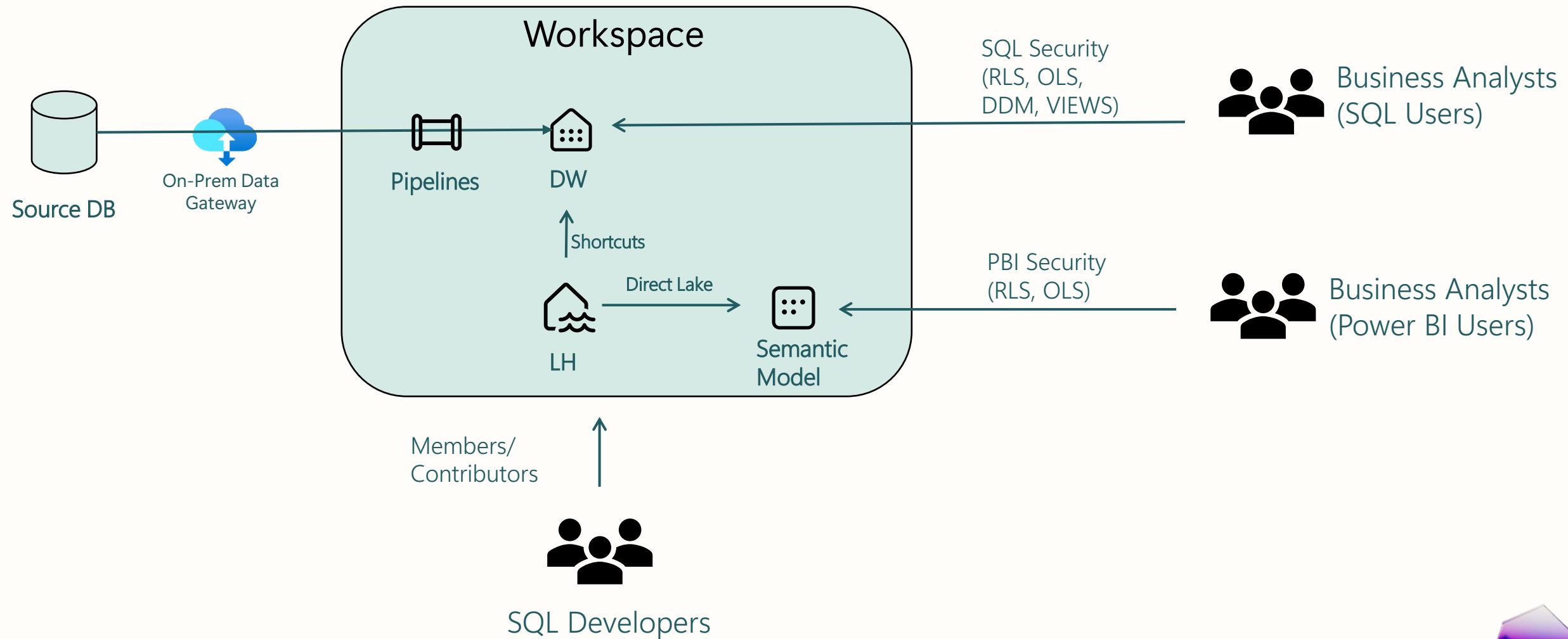
OneLake Security – Data Access Roles (Spark & OneLake APIs for now)



# End to end security scenario – Medallion architecture



# End to end security scenario – Data Warehouse Migration





## Data Encryption in Fabric

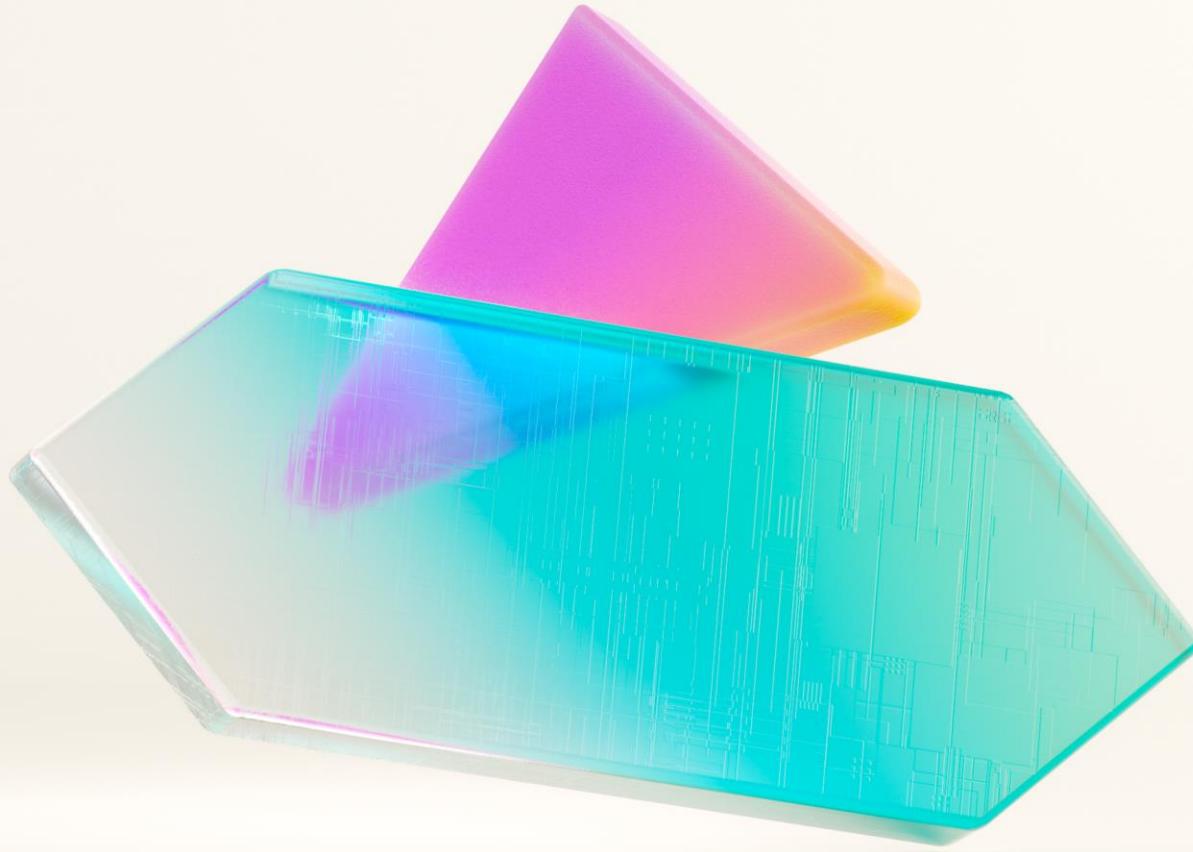
# Encryption in Fabric

## 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.

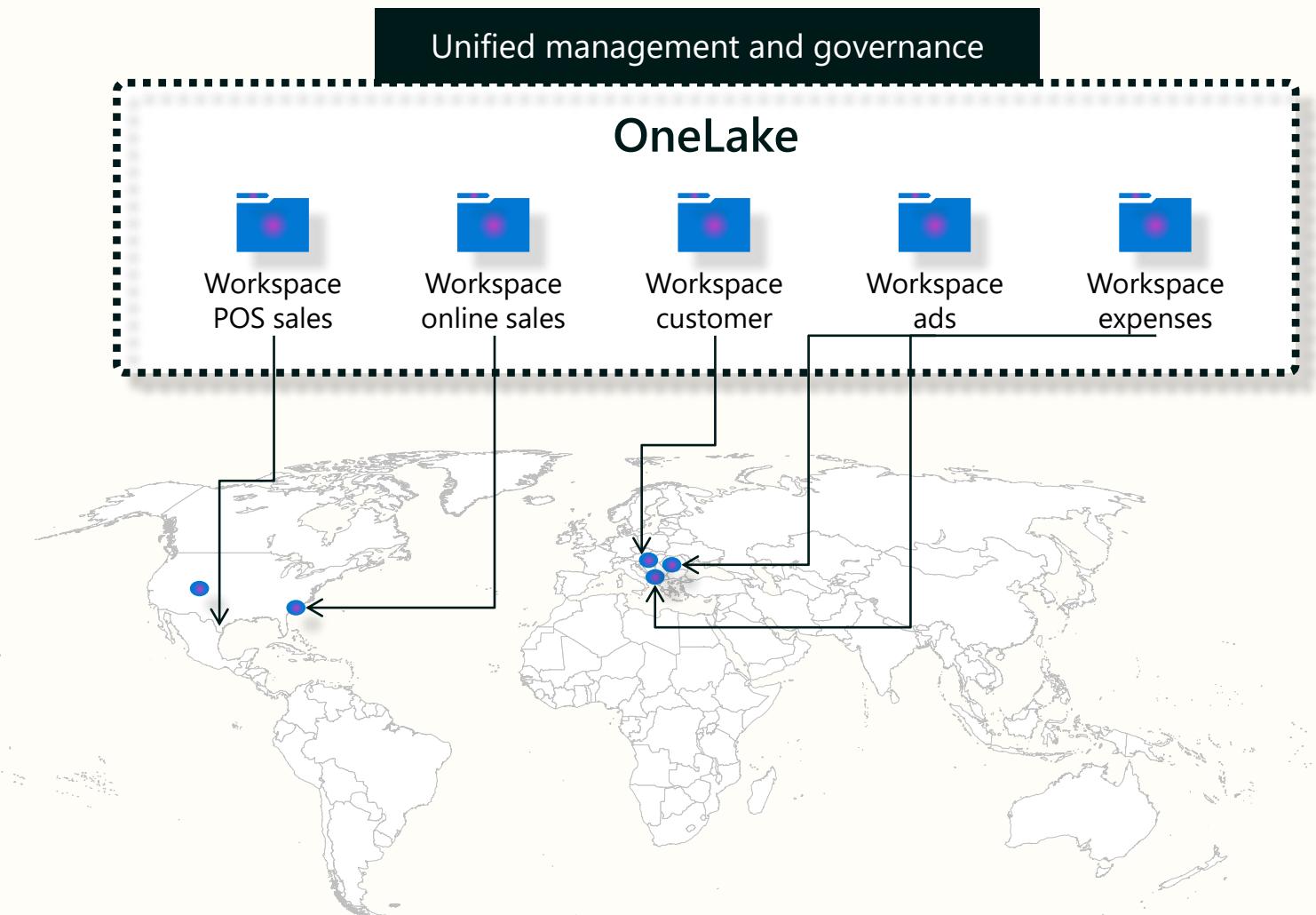
# Data Residency

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.

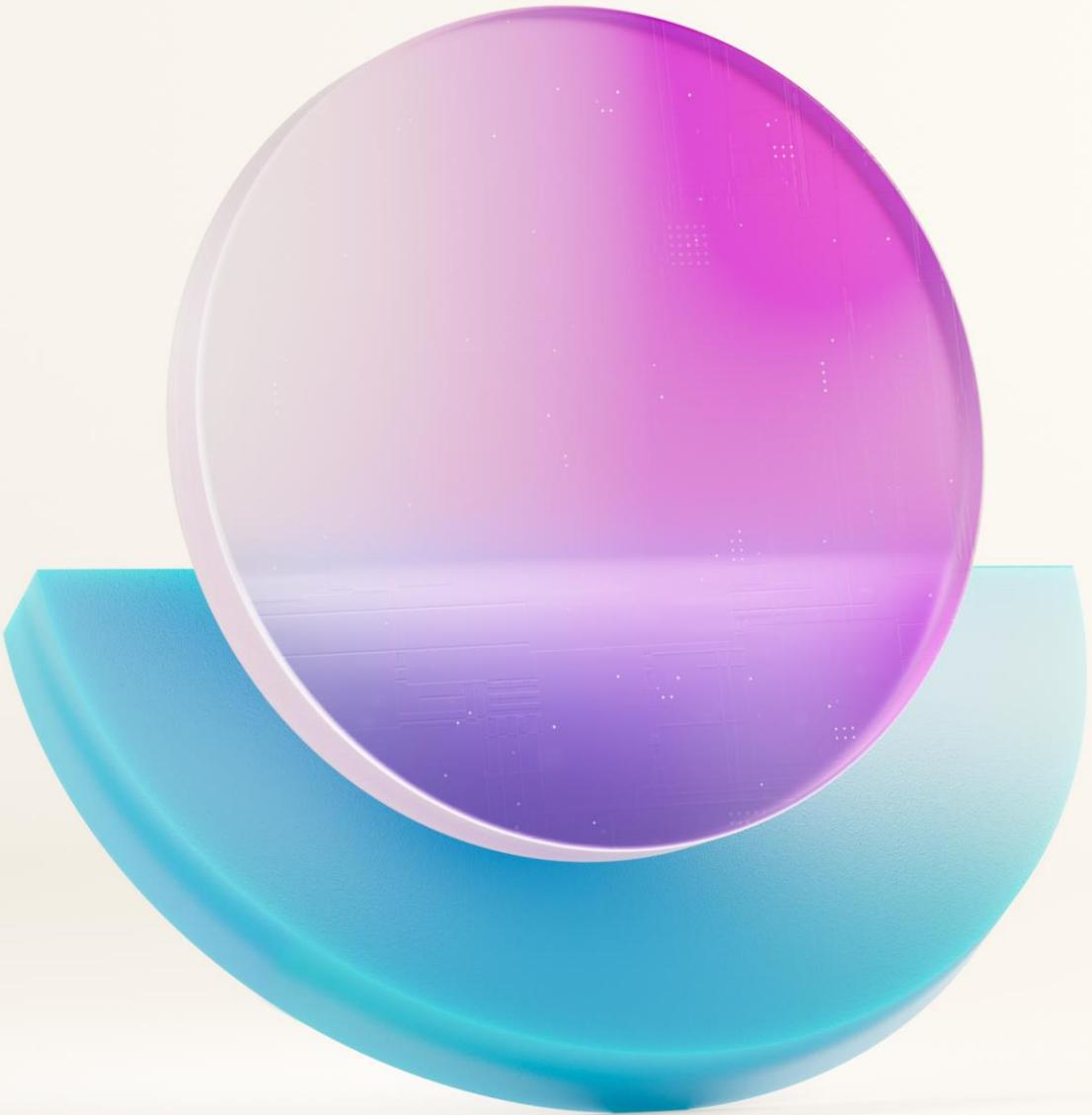


# Compliance with Microsoft Fabric

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

The screenshot shows the 'Domain settings' page for the 'HR' domain. It includes sections for General settings, Administrators, and Delegated settings. A note says: 'A delegator makes this easier to remember.'

## Delegated admin permission

Provide delegated admin permissions per Domain and Capacity



The dashboard displays activity metrics over time, including Total Activities, Active Users, Active Capacities, and Most Active Items. It also shows capacity usage details like Total Capacity, Shared Capacity, and Capacity Name.

## 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



The Admin center interface shows a list of domains: Finance, Health, and Education. Each domain has a 'Domain admins' section where users can manage access.

## Monitoring hub

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



The dashboard provides visibility into capacity utilization and usage trends. It includes a timeline chart showing capacity usage over time and a table of detailed capacity metrics.

## 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

The screenshot shows the Microsoft Data Lake studio interface. On the left, there's a sidebar with icons for Home, Create, Data, Data hub, Monitoring, Workbooks, and Ingestion. The main area has a title bar with 'Customer\_Data\_34' and 'Confidential/Microsoft Extended'. A search bar is at the top right. Below it, a card says 'Total 59 days left' and 'Last updated 1 hour ago'. A 'Lakehouse' button is also present. The main content area shows a table with columns 'Name' (Customer\_Data\_34), 'Location' (My workspace), 'Sensitivity' (Confidential/Microsoft Extended), and a note about reporting. A dropdown menu for 'Confidential' is open, showing options: Microsoft FTE, Microsoft Extended, and Any User (No Protection). At the bottom, there are four buttons: 'New Dataflow Gen2', 'New data pipeline', 'Open notebook', and 'New shortcut'. A banner on the right says 'Get data in your lakehouse'.

## 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



The screenshot shows the 'Choose locations to apply the policy' step in the Microsoft Purview Data Governance wizard. On the left, a sidebar lists navigation options: Home, Locations (selected), Advanced DLP rules, Policy mode, and Help. The main area displays a table titled 'Choose locations to apply the policy' with columns: Item, Location, Inherited, and Enabled. The table lists various locations with checkboxes for enabling or disabling inheritance. A note at the top states: 'We'll apply the policy to data stored in the locations you choose. Select the locations where you want to apply the policy. You can always change this later.' A 'Next Step' button is at the bottom.

Item	Location	Inherited	Enabled
<input checked="" type="checkbox"/>	Exchange mail	All	Choose distribution group
<input checked="" type="checkbox"/>	OneDrive sites	All	Choose site
<input checked="" type="checkbox"/>	OneDrive accounts	All	Choose account or distribution group
<input checked="" type="checkbox"/>	Name chat and channel messages	All	Choose account or distribution group
<input checked="" type="checkbox"/>	Devices	All	Choose user or group
<input checked="" type="checkbox"/>	Microsoft Defender for Cloud Apps	All	Choose instance
<input checked="" type="checkbox"/>	On-premises databases	All	Choose replication
<input checked="" type="checkbox"/>	Power BI (green)	All	Choose workspace

## Data Loss Prevention policies\*

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



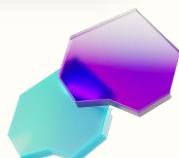
The screenshot shows the Microsoft Power BI Data Flow interface. On the left, there's a sidebar with various icons for file operations like Open, Save, and Share. The main workspace displays a complex data flow diagram with multiple stages. Stage 1 contains three inputs: 'Sales Order' (10 rows), 'Customer' (10 rows), and 'Product' (10 rows). Stage 2 has two parallel paths. The left path processes 'Sales Order' and 'Customer' through a 'Merge' step, resulting in a single output of 10 rows. The right path processes 'Product' through a 'Select' step, also resulting in 10 rows. Stage 3 merges these two outputs into a final stage. Stage 4 contains a 'Select' step followed by a 'Sink' step. A tooltip on the right indicates that 9 rows were processed. The top navigation bar shows 'Power BI Data Flow' and the status 'Data loaded'.

## 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*



 Filter by title

Security documentation

✓ Overview

Security overview

Security fundamentals

Permission model

Governance and compliance  
documentation

Admin documentation

Security white paper 

› Network security

› Data security

› Power BI security

› Reliability

✓ Guidance

End-to-end security scenario 

# Fabric Security Whitepaper

<https://aka.ms/fabricsecuritywhitepaper>

## End-to-end security scenario

<https://learn.microsoft.com/en-us/fabric/security/security-scenario>



<https://www.linkedin.com/in/vengat83>

# Vengatesh Parasuraman

Principal Program Manager, Microsoft Fabric

CAT – Customer Advisory Team





Microsoft

Microsoft Fabric

Thank you

