Microsoft Fabric
What's the fuzz about?

17-10-2024 | Webinar | S. van den Beemt

Classifcation: Training (R5)

Algemene informatie en 'huisregels'

WEBINAR

MS Fabric – **What's the fuzz about**

- De webinar wordt opgenomen

- Slides en opname worden achteraf gedeeld via de mail

- Q&A bewaren we tot het eind

- Inzoomen?

- Graag je microfoon uitgeschakeld houden

- Camera's aan: optioneel, liefst wel tijdens Q&A

- Eet smakelijk!

ICT GROUP

Hello world!

Steven van den Beemt

Cloud Architect | ISO MCT
@ICT Group

Agenda

- Introduction

- MS Fabric / OneLake architecture

- MS Fabric security

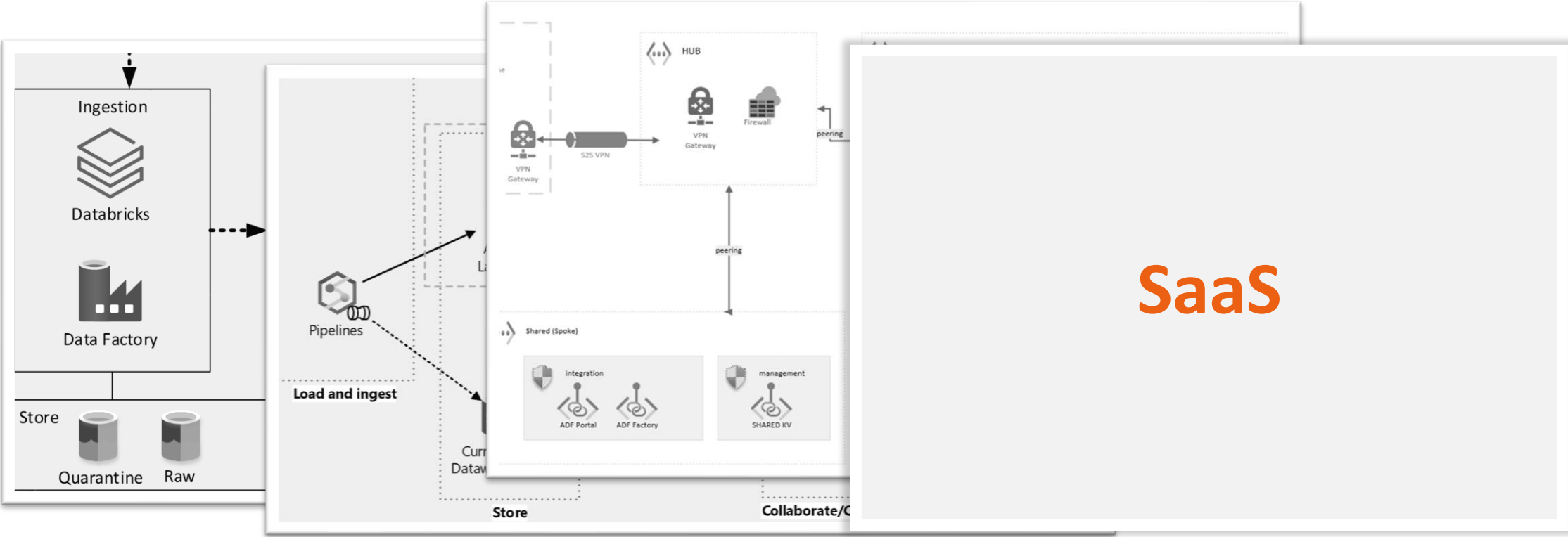- Direct Lake

ICT GROUP

Introduction

Introduction

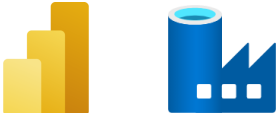2014   2015   2020   2023
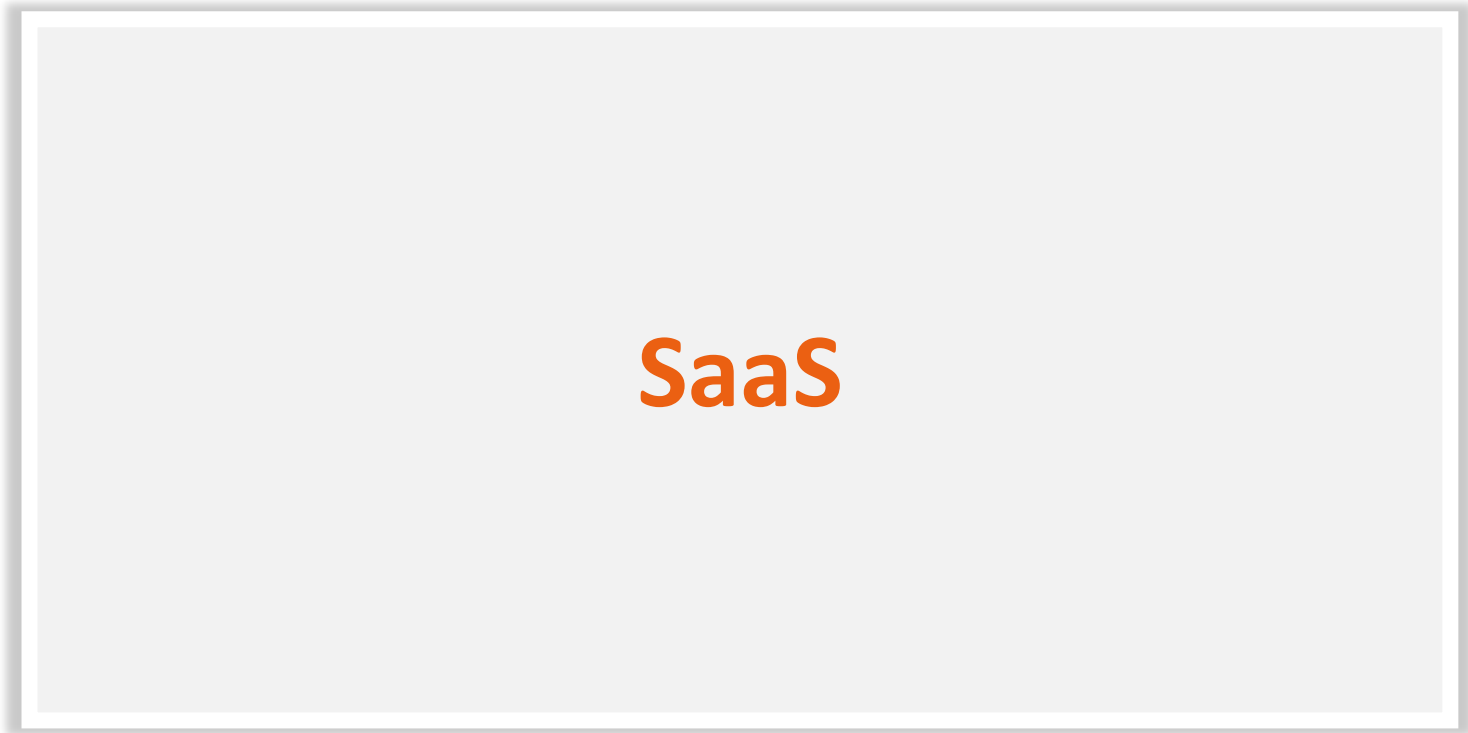

SaaS

ICT GROUP

Introduction

2014　　　　2015　　　　　　　　　　　　　2020　　　　　　　　　　　2023

SaaS

ICT GROUP
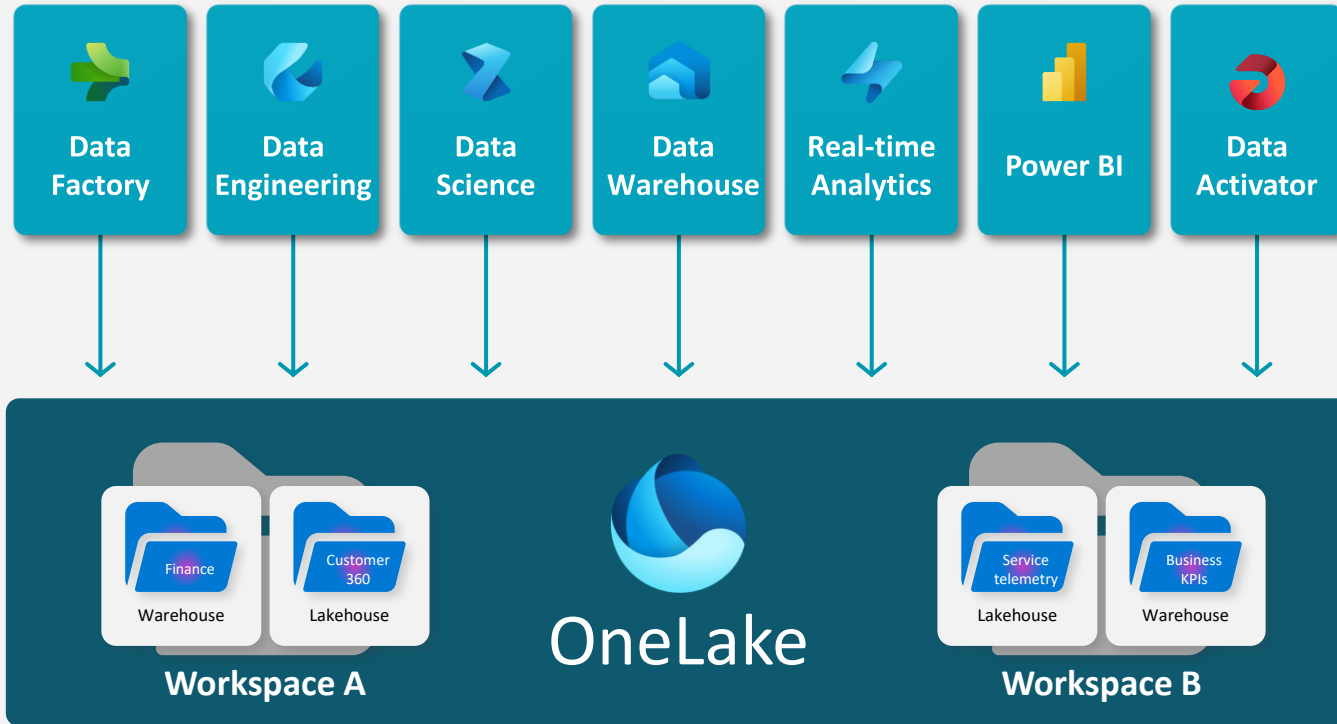
MS Fabric Architecture

Understand Fabric architecture

Single SaaS lake

Provisioned automatically with the tenant.

All workloads automatically store data in OneLake workspace folders.

All data is organized in a hierarchical namespace.

Data in OneLake is automatically indexed for discovery, MIP labels, lineage, PII scans, sharing, governance and compliance.

Diagram labels:
Data Factory · Data Engineering · Data Science · Data Warehouse · Real-time Analytics · Power BI · Data Activator

Finance — Warehouse · Customer 360 — Lakehouse · **Workspace A**

OneLake

Service telemetry — Lakehouse · Business KPIs — Warehouse · **Workspace B**

Intelligent data foundation

ICT GROUP

T-SQL
Spark
KQL
Analysis Services

Lakehouse 1
- Files
- Tables

Warehouse 1
- Compute
- Storage

domain
Workspace 1

Workspace 2

Workspace 3

Capacity

Capacity

OneLake

Delta Log (meta data)
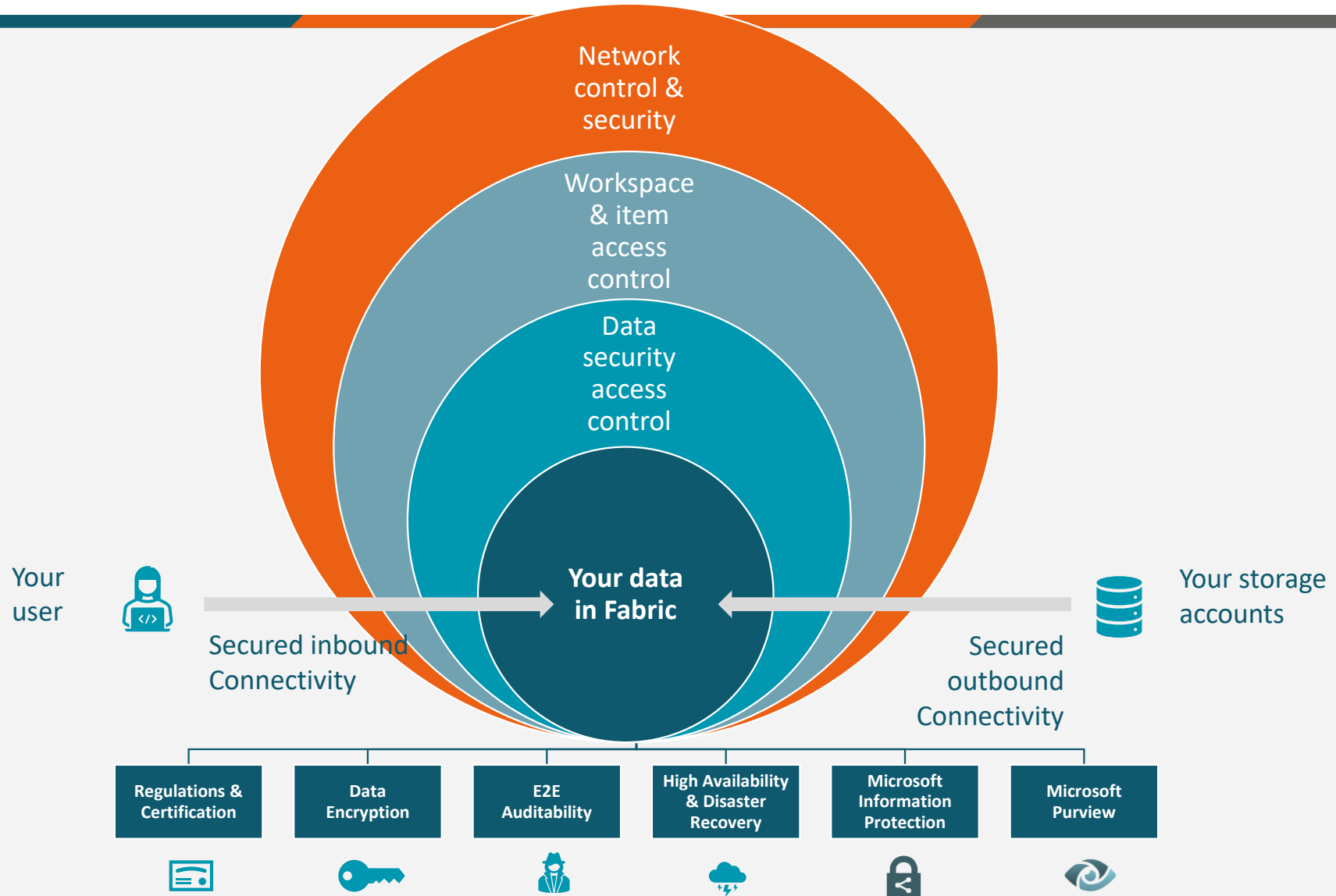
Delta Parquet files

ADLS2

A P I

1 : 1

Demo

ICT GROUP

Security in MS Fabric

Manage Fabric security

Network control & security

Workspace & item access control

Data security access control

Your data in Fabric

Your user

Secured inbound Connectivity

Your storage accounts

Secured outbound Connectivity

| **Regulations & Certification** | **Data Encryption** | **E2E Auditability** | **High Availability & Disaster Recovery** | **Microsoft Information Protection** | **Microsoft Purview** |

Network Control - Inbound

Option 1

1 `<‹·›>` **Customer VNet**

🔒 ─────────

User

↓

`<‹·›>` Private endpoint
(tenant level)

Requires > F64 license

`<‹·›>` Azure Private Link

Option 2

2 User
attempts authentication to Microsoft Fabric

│

Microsoft Entra Conditional Access Policies

Users and groups   Application type

Network location   Device type

Inbound

↓

3 **Microsoft Fabric**

OneLake shortcuts
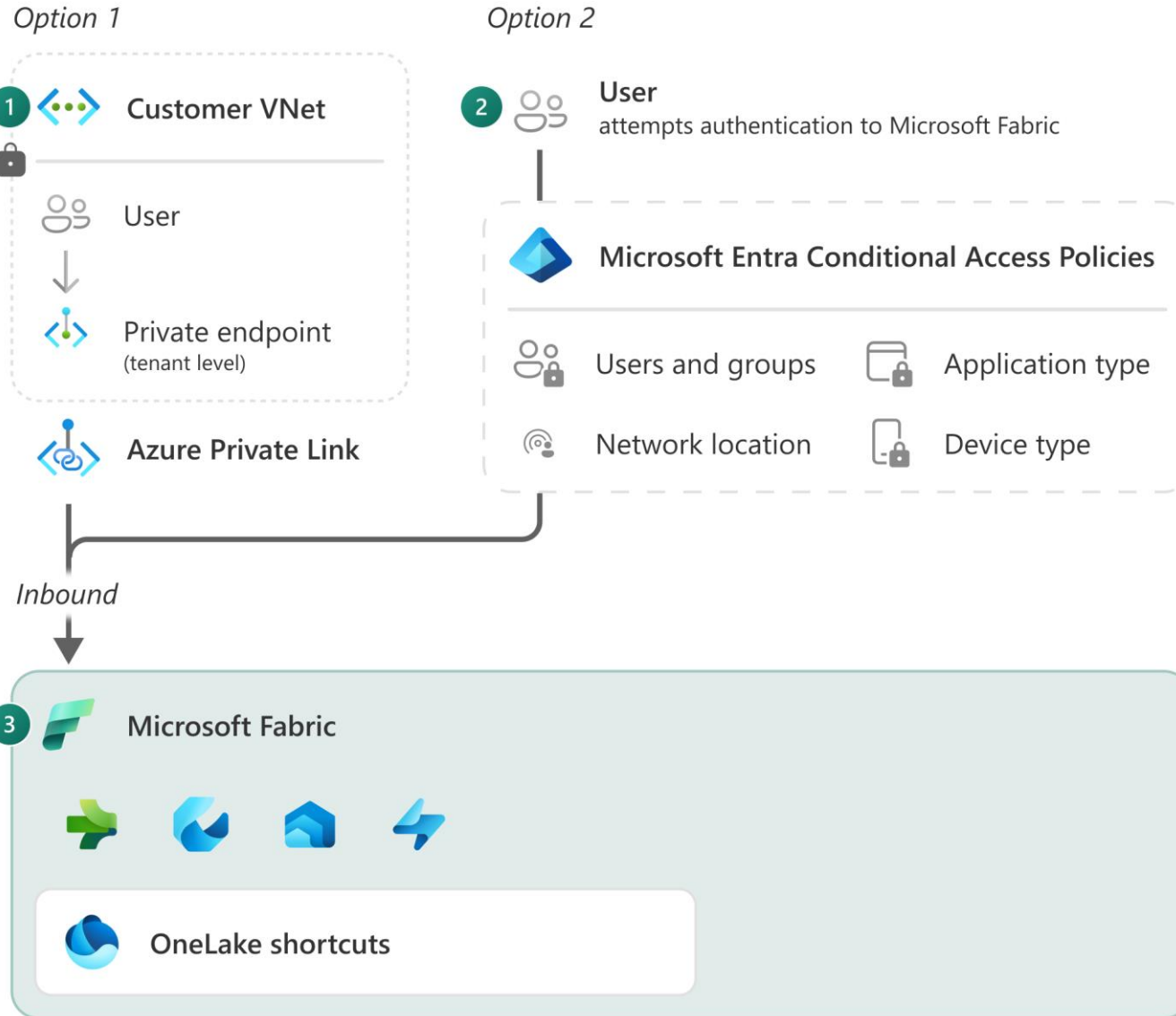
Network Control - Outbound

Customer VNet

Anonymous access from public internet traffic

Managed VNet

External Storages behind secured networks

Microsoft Fabric

Managed Private Endpoints

Spark Clusters
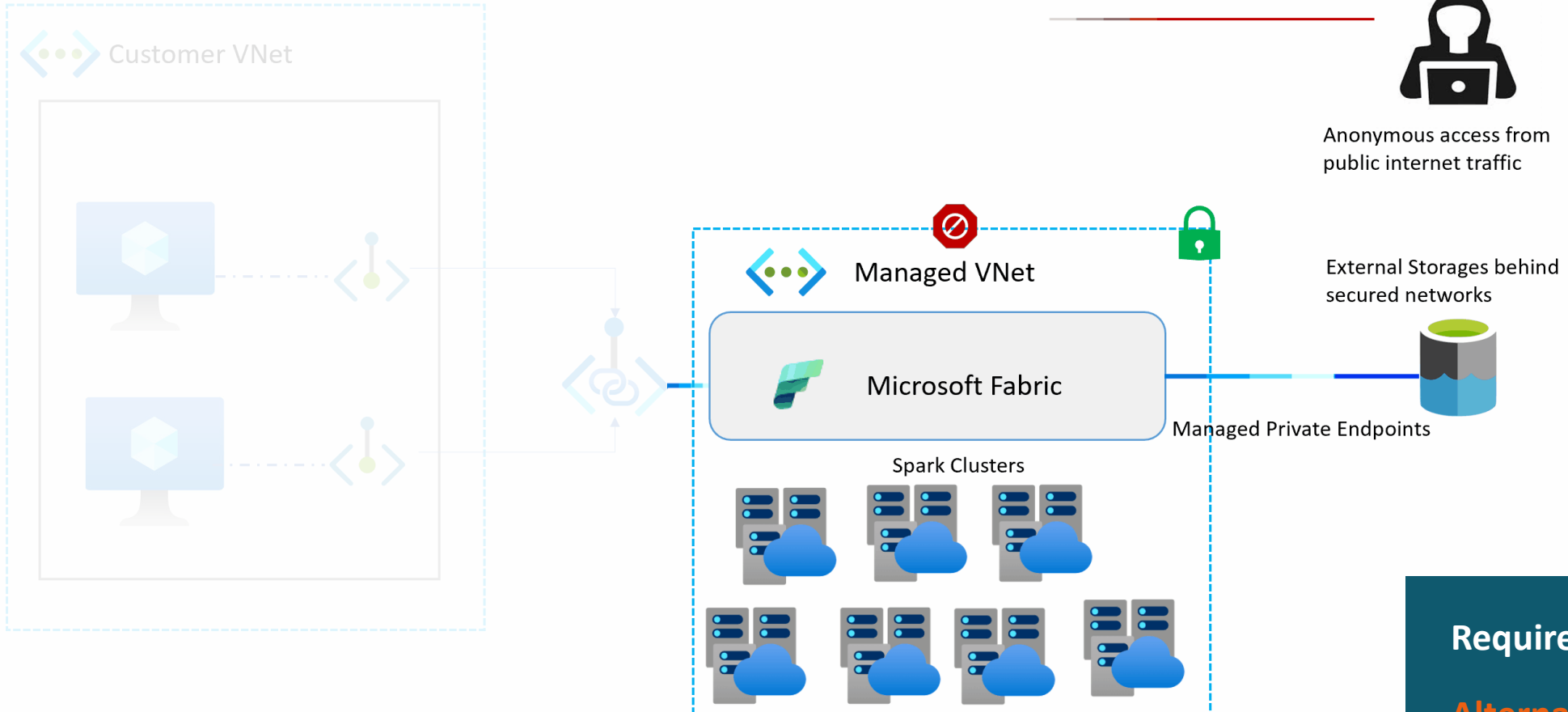
Requires > F64 license

Alternative to PE: Trusted workspace access

Workspace-, Item- & Data item security

Microsoft Fabric: Multiple layers of security and access control

Microsoft Fabric (SaaS at tenant-level)

Domain

Workspace

| Artifact | Artifact | Artifact | Artifact |

OneLake

| Files | Shortcuts | Tables | Tables |

Platform-level access. Fabric relies on Microsoft Entra ID to authenticate users (or service principals). Features can be used, such as MFA, conditional access, restriction from locations and IP ranges.

Domain-specific configuration by domain admins

Workspace-level access. Boundary for managing artifacts, for example within development, test or production. Or for self-service or read-only access.

Item-level access. For example, read all only via Spark. Or only access to certain reports.

SQL Policies, for example Warehouse access through GRANT/DENY SQL commands

OneSecurity (roadmap). Fine-grained access on tables and folders.

Workspace-, Item- & Data item security

Tenant Level

Capacity Level
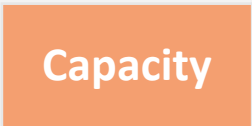
Workspace Level

Item Level

Object Level

Tenant

Capacity

Workspace

Workspace

Warehouse

Lakehouse

Semantic model

Schema

View

ICT GROUP

Workspace roles

Workspace-, Item- & Data item security

Tenant Level

Tenant

Capacity Level

Capacity

Workspace Level

Workspace Workspace

Item Level

Warehouse Lakehouse Semantic model

Object Level

Schema

View

Data Level ?

OneLake

ICT GROUP

What about the data in OneLake?

OneLake security model

Estimated release timeline: Q1 2025
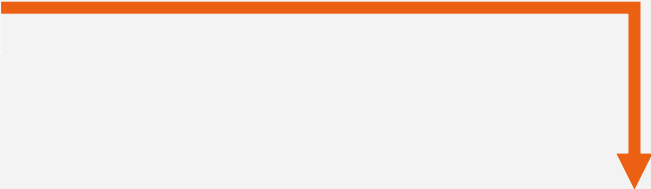
Release Type: Public preview

Managing data security across multiple analytical engines and copies of data is challenging. OneLake and Fabric simplify this by enabling the use of a single data copy across multiple analytical engines without any data movement or duplication. Taking the "one copy" concept further, OneLake is also enhancing security with a finer-grain model, allowing for table and folder access in addition to row and column level security. These security definitions live with the data and travel across shortcuts to wherever the data is used. Security defined at OneLake is universally enforced no matter which analytical engine is used to access the data.

OneLake Data Access Roles

Manage OneLake data access (preview)

Turn on data access roles (preview)

You are about to turn on OneLake data access roles (preview) for this lakehouse. Using this capability, workspace admins, members, and contributors are permitted to change Onelake data access permissions at the folder level. Learn more

ⓘ After OneLake data access roles is applied to GoldLakeHouse only users with Write permission can share the data in this item using External data sharing (preview). Any existing external data shares may stop working. Learn more

Continue   Cancel

ICT GROUP

How are permissions evaluated?

Request from user1 to read OneLake folder1 in a lakehouse → 1 Evaluate workspace permissions for coarse-grain workspace access → 2 Evaluate lakehouse permissions for coarse-grain item access → 3 Evaluate OneLake RBAC permissions for fine-grain folder access
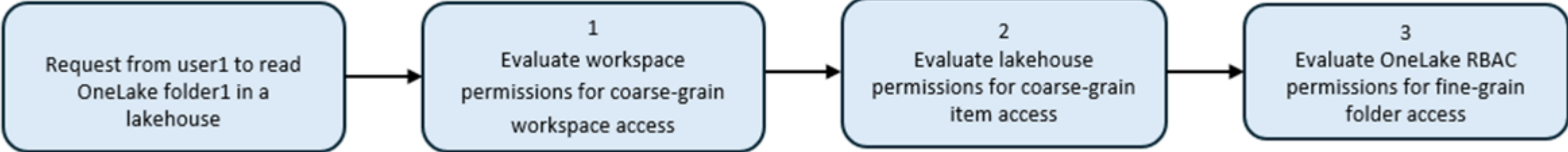
ⓘ Note

*Since Workspace Admin, Member and Contributor Roles automatically grant Write permissions to OneLake, it overrides any OneLake RBAC Read permissions.

◌ Expand table

Workspace Role	Does OneLake apply RBAC Read permissions?
Admin, Contributor, Member	No, OneLake Security will ignore any OneLake RBC Read permissions
Viewer	Yes, if defined, OneLake RBAC Read permissions will be applied

Demo

Direct Lake

Direct Lake

DirectQuery

Translate DAX -> SQL

Send DAX query

Pulls data in
real time (T-SQL)

SQL Server

Data

ICT GROUP

Import

Send DAX query

Scheduled import

Copy of data

SQL Server

Data

ICT GROUP

DirectLake

Send DAX query

Auto refresh (framing)

keep data in memory

Delta Tables

ICT GROUP
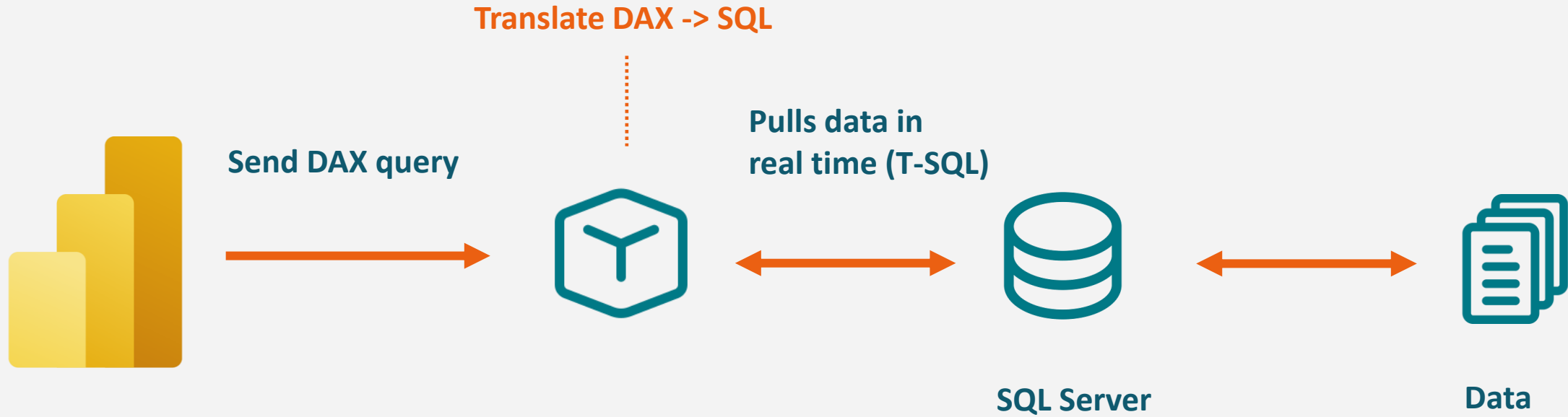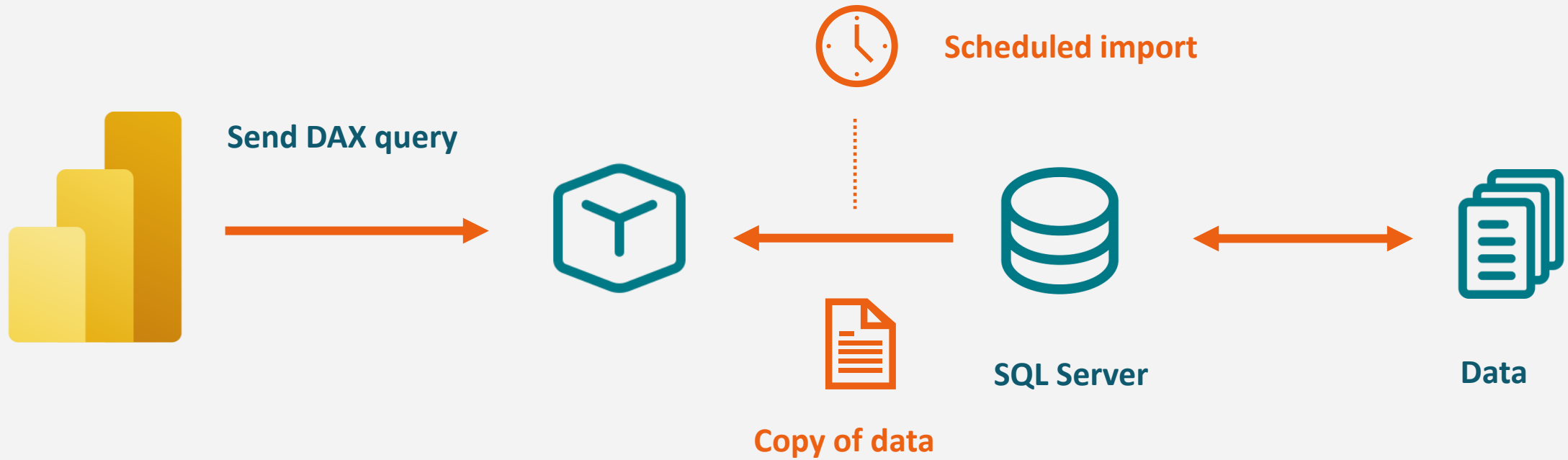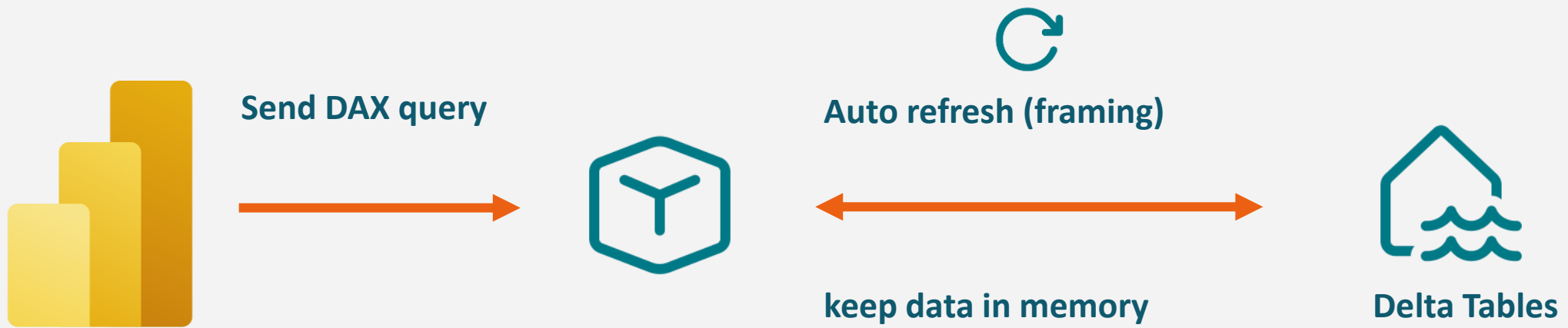
Direct Lake semantic model

Demo

Direct Lake

- **What makes it fast?**
  - PowerBi queries Parquet files stored in OneLake directly
  - Loaded in memory using the VertiPaq engine
  - Data will be transcoded on-the-fly in VertiPaq format
  - V-order storage

- **Fallback to DirectQuery mode**

Wrap-up

Key takeaways

- Outthink your workspace design upfront

- Make sure your capacity is deployed in Europe

- Authorization within MS Fabric is still a challenge
    - Hopefully, this will improve in Q1 - 2025

- DirectLake speeds up your reports when using large datasets

ICT GROUP

Q&A