

Bridging on-premises data with Microsoft Fabric and Purview

Guust Franssens Solution Engineer, Microsoft

Florian Boigner Cloud Solution Architect, Microsoft

Protected data source



Cloud analytics plane



The challenge: analytics at scale, without losing control



- Sovereignty is not a single control: residency, access, encryption, governance, operational transparency, portability and evidence.
- The goal is not "move everything", it is to minimise unnecessary movement and govern what is used.



Microsoft Fabric



Data
Factory



Data
Engineering



Data
Warehouse



Data
Science



Real-Time
Intelligence



Power BI



Partner &
Industry
workloads



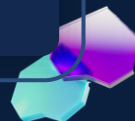
Copilot in Fabric



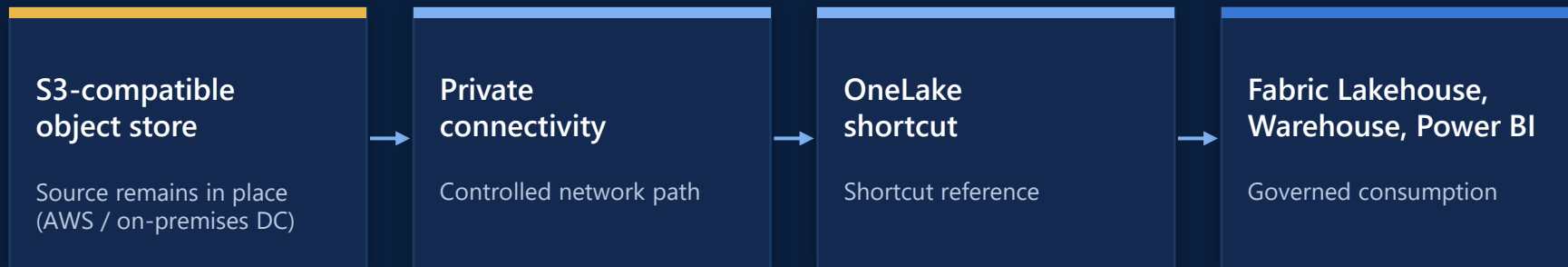
OneLake



Microsoft Purview



A governed access pattern, not a copy-first migration



Governance overlay across the analytics estate with Microsoft Purview

The data store remains the trusted source; Fabric references data in place rather than copying it first.

Analytics without making migration the default

Fabric analytics experiences

Lakehouse, Warehouse, Power BI

Shortcut and controlled access

Reference, not relocation

Trusted source

Remains the system of record

Govern what is derived

Cached, transformed or materialised data becomes part of the Fabric-resident estate and must be governed accordingly.

A practical middle ground between keeping everything local and copying everything to the cloud.

Strengthening control over Fabric-resident data

Private connectivity

Reduces exposure and supports controlled data paths

Customer-managed keys

Customer control for supported persisted Fabric data

Fabric-resident data

Cache, tables, semantic models, reports, derived artifacts

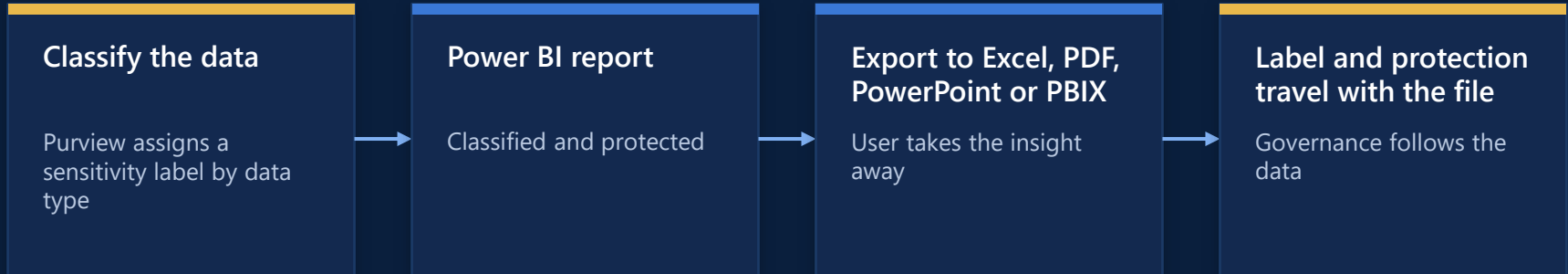
Customer Managed Keys (CMK) are a cryptographic control mechanism

They increase customer control over encryption keys while providing additional security protections for data at rest.

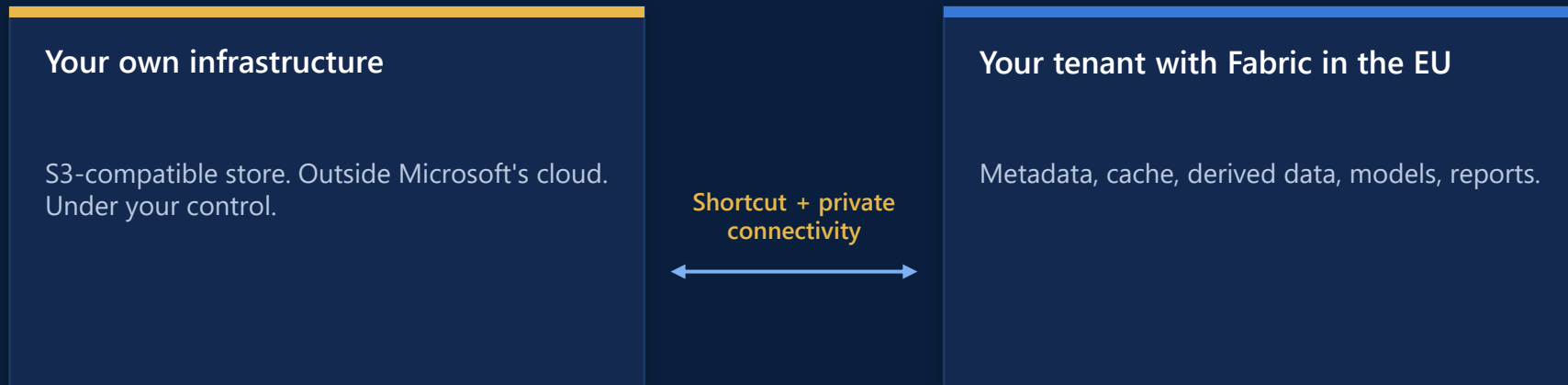
We combine source control, private connectivity, customer-managed encryption, governance and transparency.

Governance does not stop at the analytics platform

Microsoft Purview -> classify sensitive data, then apply sensitivity labels and DLP across the analytics estate

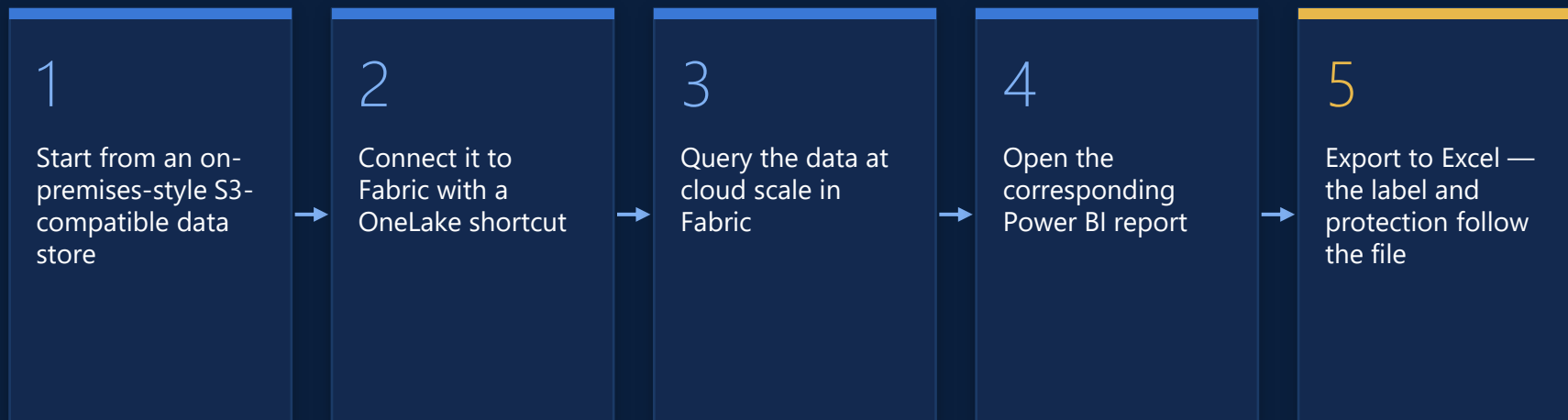


What sits where?



EU Data Boundary: a customer data residency commitment for in-scope services

What we will show in the demo



Start with one governed analytics use case

Confirm tenant home region and Fabric capacity region

Confirm shortcut behaviour and cache implications

Classify data with Purview sensitivity labels

Document residual sovereignty considerations

Validate private connectivity and endpoint topology

Enable CMK where required and document scope

Test DLP and export protection on real user paths

Define portability early using open formats

Validate



Govern



Prove



Scale

Governed analytics does not have to start with wholesale migration. Start with trusted sources, minimise movement, protect what is derived, and make the controls visible.