SQL
KONFERENZ
2026



OneLake Security for the Power BI Developer



Gabi Muenster
Fabric CAT – Principal Program Manager
(aka Principal Fabric Witch)
Gabi Münster - Microsoft | LinkedIn

OneLake Security Whitepaper

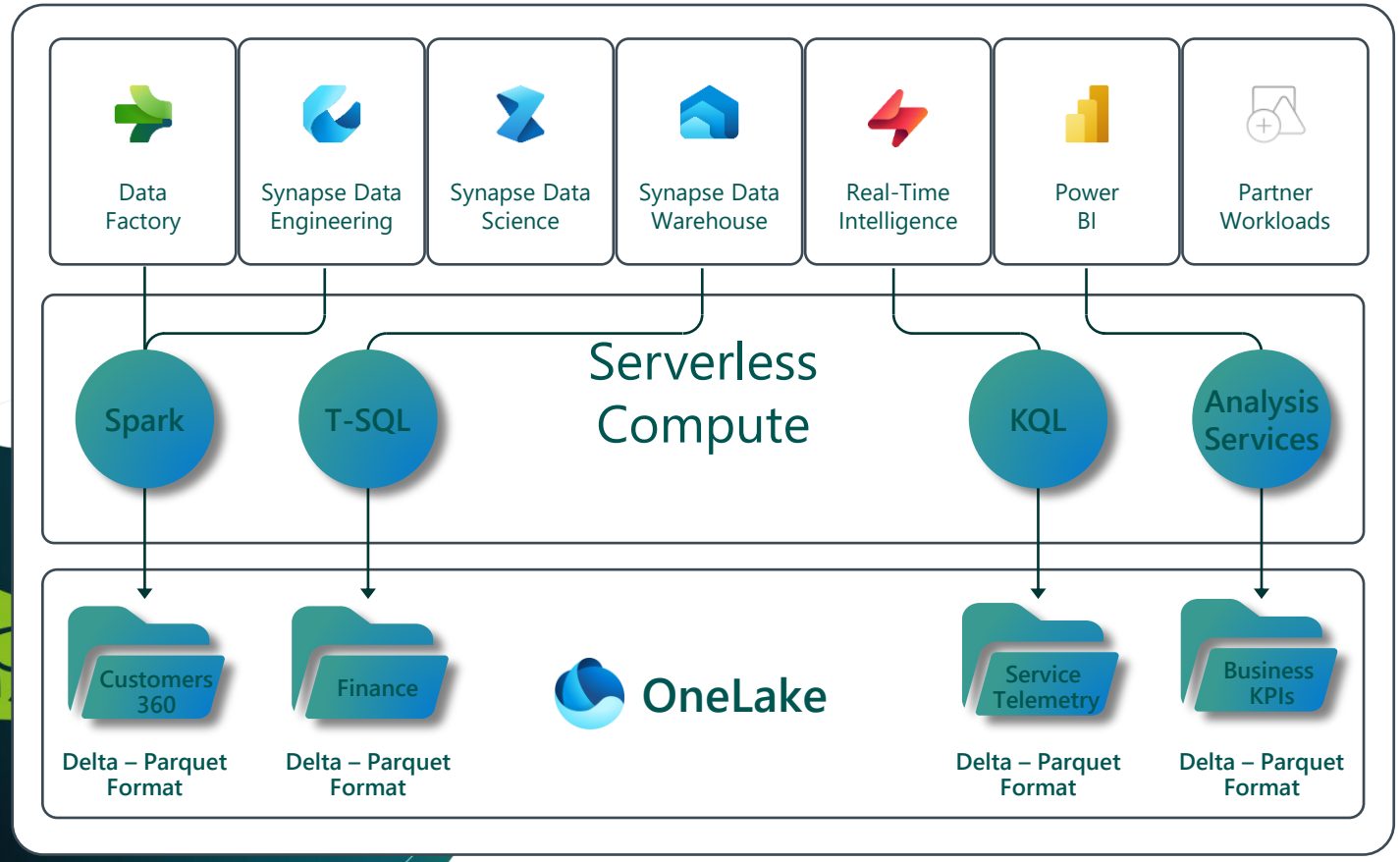
Recent blog post



SQL KONFERENZ 2026

One Copy for all computes

Real separation of compute and storage



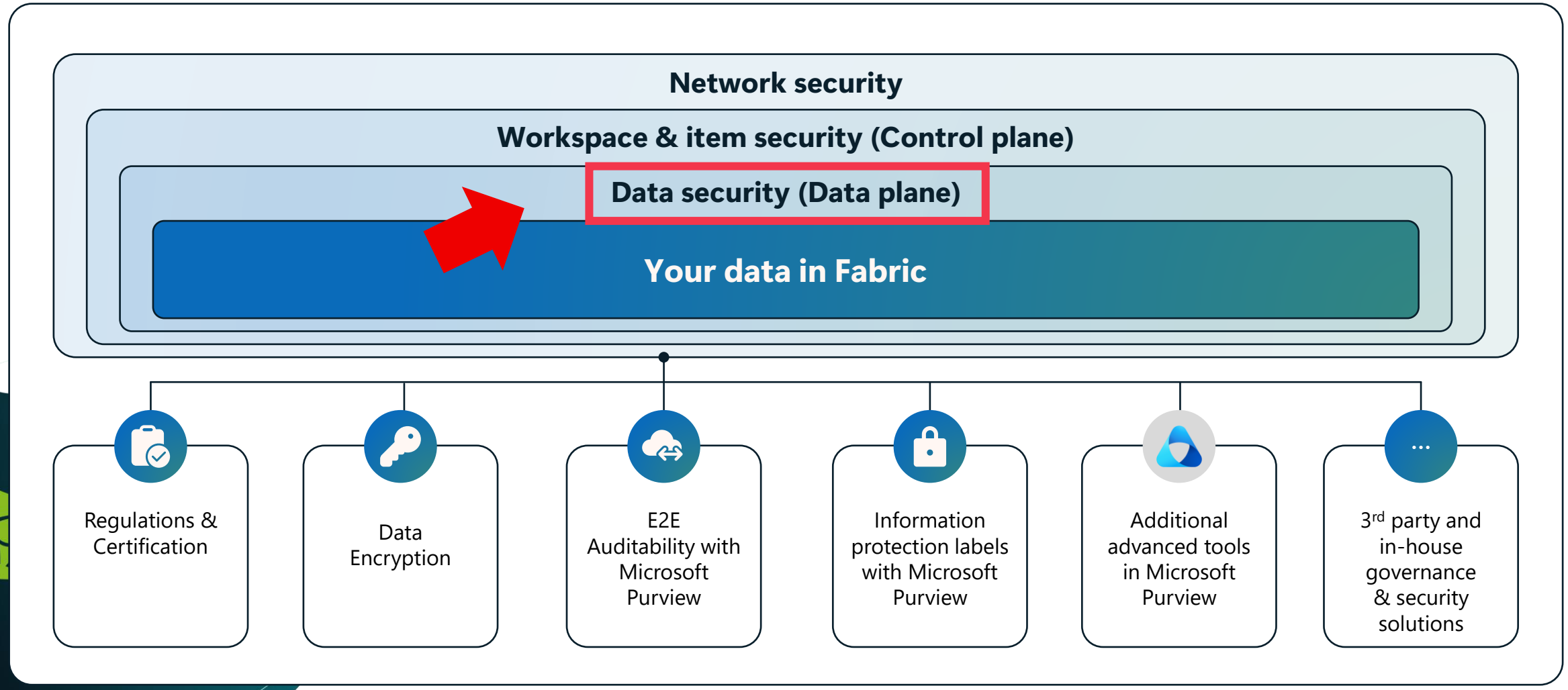
All the compute engines store their data automatically in OneLake as data items.

The data is stored in a single common format.

Delta – Parquet, an open standards format, and it is the storage format for all tabular data in Fabric.

All the compute engines have been fully optimized to work with Delta Parquet as their native format.

Microsoft Fabric – Defense in depth and Principle of Least Privilege



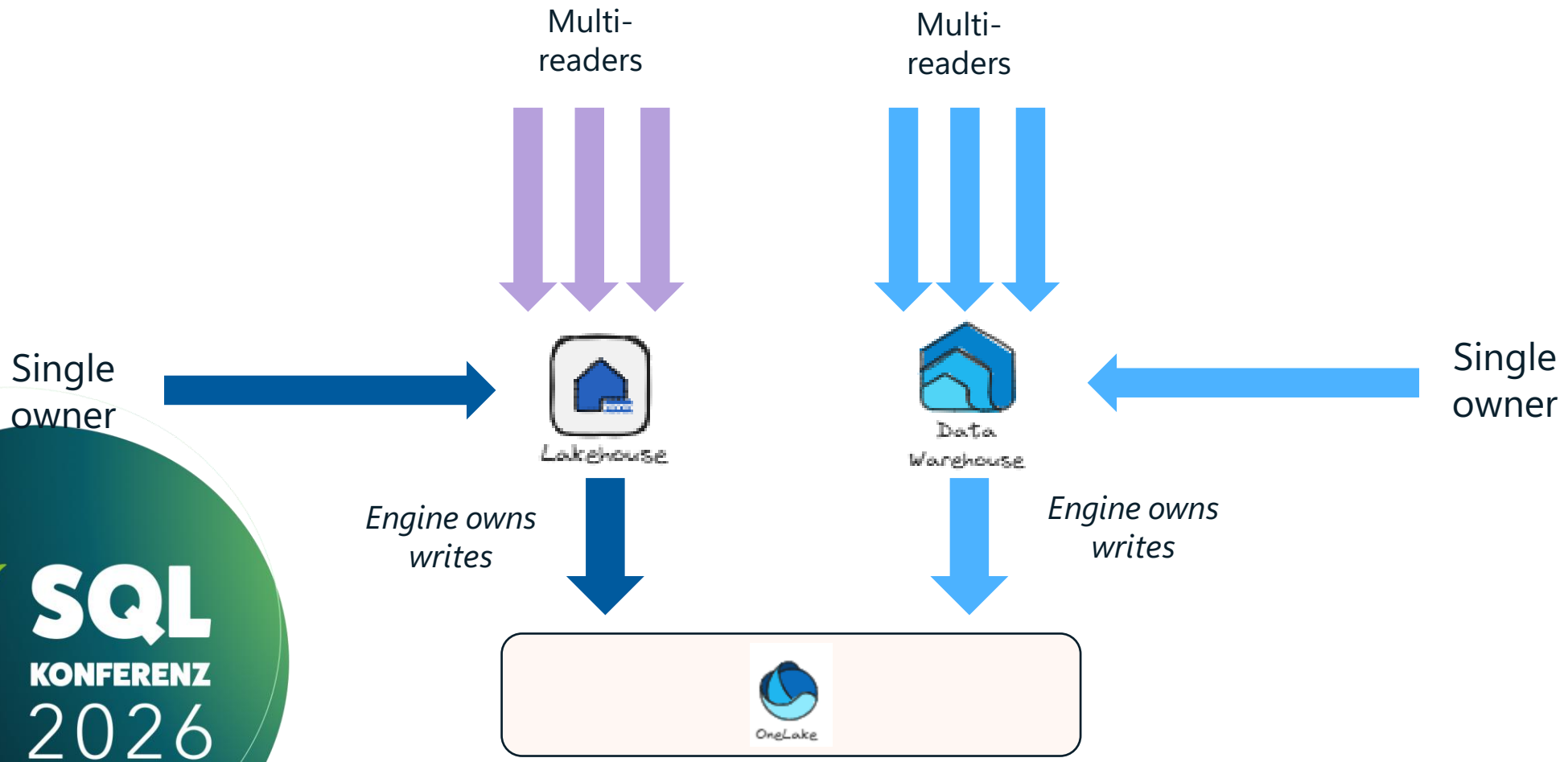


SQL
KONFERENZ
2026

OneLake Security – Overview of concept and current preview functionality

Microsoft Fabric – Owning and Consuming Engines

A table is owned by one engine (CRUD(but can be read by many different engines in Fabric (1P) and 3P engines.



SQL KONFERENZ 2026

Anatomy of a OneLake security role

A role in OneLake security has 3 parts:

- **Members –** user identity, SPNs
- **Scope –** folder, schema, table
- **Permissions** (*and their characteristics)*
  - Grant – Table-Level, RLS, CLS
  - Deny* – supersedes a *grant (work in progress)*



SQL KONFERENZ 2026

Folder level security

Previously known as Data Access Roles

Grant access to folders in OneLake

Access inherits to all subfolders and files

Listing access on parent folders is maintained



SQL KONFERENZ 2026

Table level security

Grant access to tables in OneLake

Access inherits to all subfolders

Listing access on parent schemas is maintained



SQL KONFERENZ 2026

Row level security

Restrict access to specific rows for a table

Set row conditions by writing SQL

Currently only single-table statements are supported

Requires compute to calculate bitmap per role
This will appear as a line item in capacity metrics app



SQL KONFERENZ 2026

Column level security

Restrict access to specific columns in a table

Removes access to both the column metadata and data

Note

Spark SQL can translate SELECT * … into columns where CLS allowlist columns. As a result, it works in notebooks.
SQL analytics endpoint requires users to explicitly mention columns;
SELECT * FROM <table-name> will fail (at least for now);



SQL KONFERENZ 2026

Classified as Microsoft Confidential

Shortcut Types Access Modes

Shortcut type / Authentication mode	User's identity / Passthrough	Delegated
Internal	X	(future plan)
External	-	X



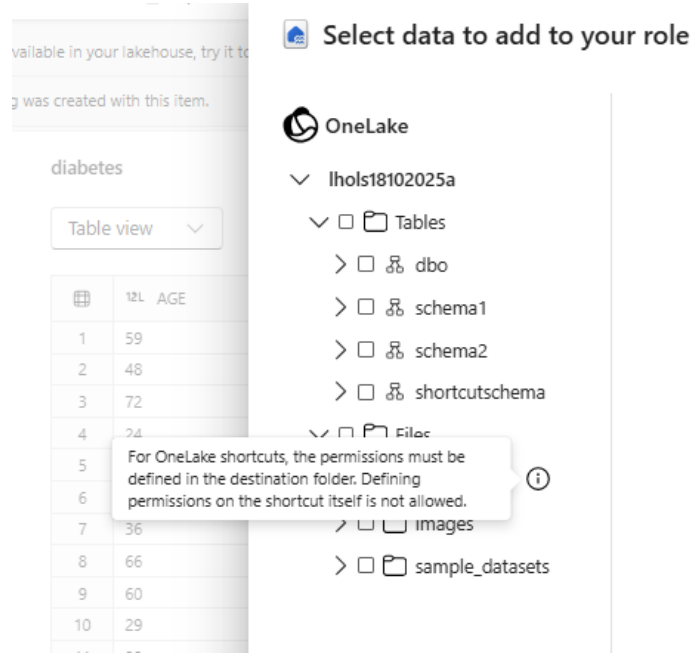
SQL KONFERENZ 2026

Classified as Microsoft Confidential

Internal shortcuts and OneLake security

Internal shortcut uses User's identity / passthrough mode.

Internal shortcuts are pointers to physical objects in OneLake. Hence, security must be applied on the physical location and CANNOT be applied on the shortcut.

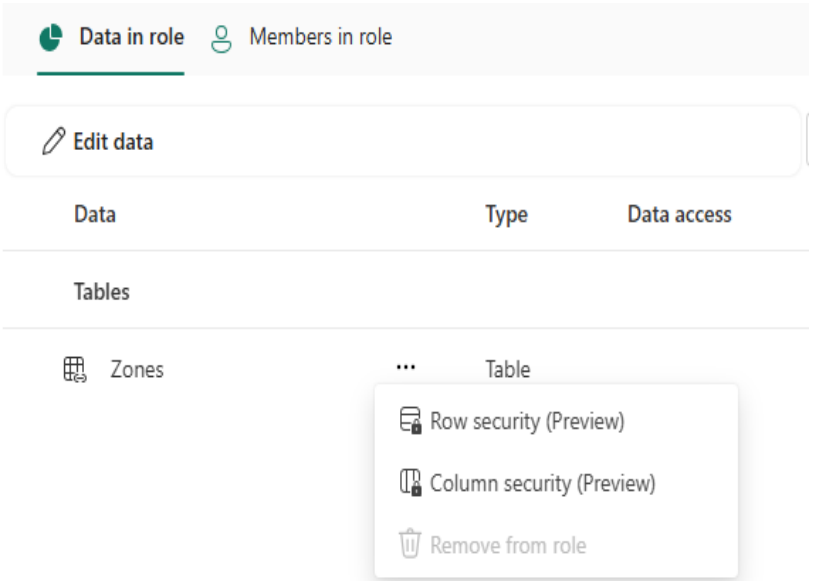


Classified as Microsoft Confidential

External Shortcuts and OneLake security

External shortcuts use delegated mode.

External shortcuts are pointers to physical objects in external storage accounts. For OneLake to be able to evaluate security it must be applied on the shortcut.



Classified as Microsoft Confidential

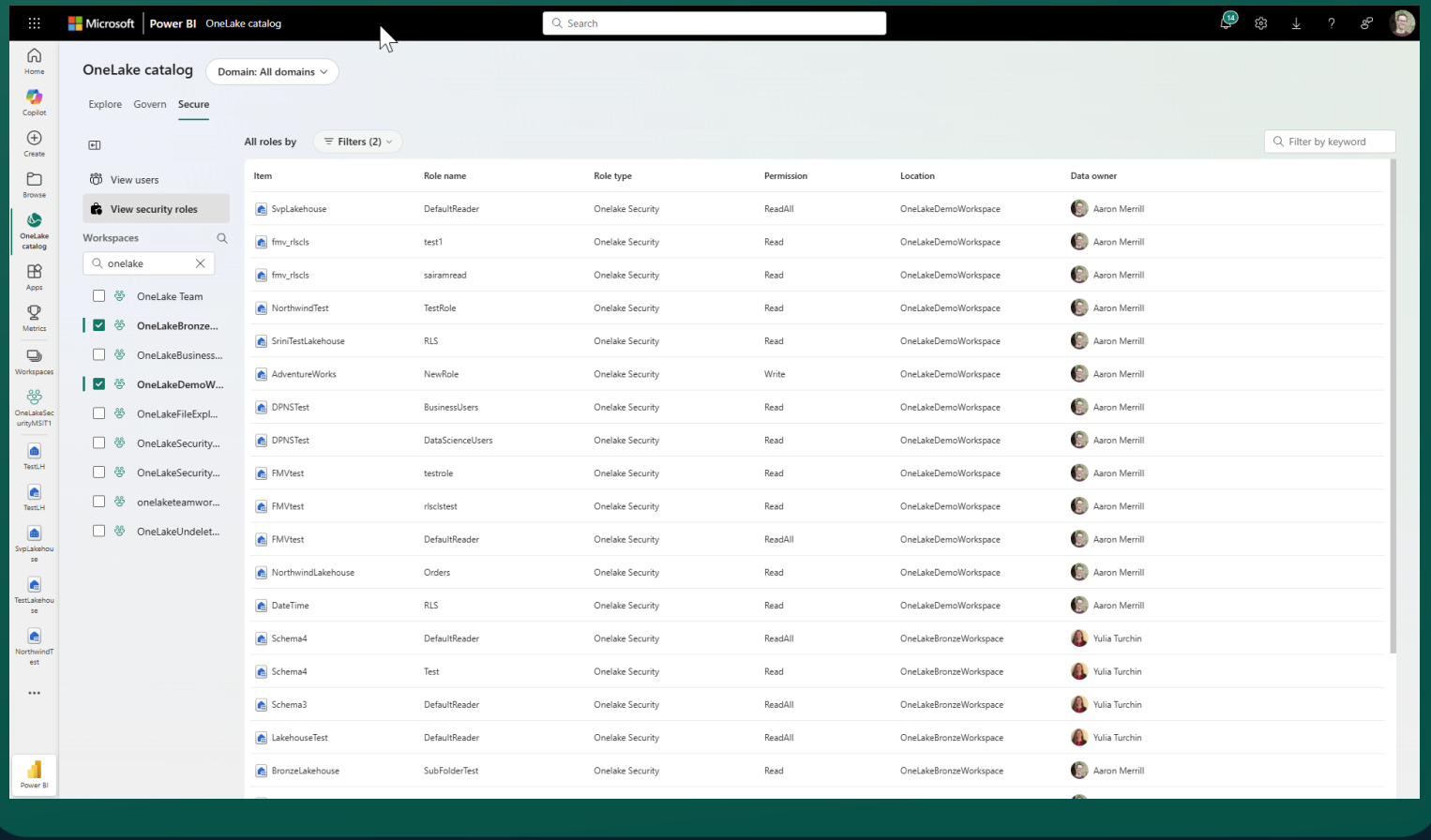


SQL
KONFERENZ
2026

What's there and what's coming?

Secure tab in OneLake catalog

Public Preview



View user access across workspaces and items from a single location.

Search and manage OneLake security roles for all item types.

Create, delete or duplicate OneLake security roles, and configure RLS and CLS.

Classified as Microsoft Confidential

OneLake security functionality – now

OneLake security features:

- Table and Folder security
- Column-level security
- Row-level security
- ReadWrite for lakehouse

Define OneLake security on:

- Lakehouse
- Mirrored databases

OneLake security filtering:

- Lakehouse
- Spark notebooks
- SQL Analytics Endpoint
- Semantic Models

Classified as Microsoft Confidential

OneLake security functionality – planned for next 6 months

OneLake security features:

- Table and Folder security
- Column-level security
- Row-level security
- ReadWrite for lakehouse

+ Strong deny
+ Multi-table RLS
+ Dynamic RLS

Define OneLake security on:

- Lakehouse
- Mirrored databases

+ Azure Mirrored Databrick Catalog
+ All Fabric items
+ Secure tab improvements

OneLake security filtering:

- Lakehouse
- Spark notebooks
- SQL Analytics Endpoint
- Semantic Models

+ Eventhouse
+ 3rd party support

Classified as Microsoft Confidential



SQL
KONFERENZ
2026

Demo:
OneLake Security & Semantic models

The scenario – Import mode model as baseline

- Import mode model with three Power BI roles as baseline

Rolename	RLS policies	CLS policies
GermanyRLS	Store[Country] = 'Germany'	No CLS defined
ItalyRLSCLS	Store[Country] = 'Italy'	Sales[Ordernumber] + Sales [Linenumber] removed

- Several test users to evaluate roles and combinations

Username	GermanyRLS	ItalyRLSCSL
Gabi Trial User	X	
Gabi Muenster (MSFT)		X
Gabi Muenster (GMPBICAT)	X	X

The scenario – OneLake Security

- Contoso Lakehouse as data source with three OLS roles
- Direct Lake on OneLake/SQL Endpoint (Falling back to DirectQuery) mode model

Rolename	RLS policies	CLS policies
GermanyRLS	Store[Country] = 'Germany' Sales[StoreKey] IN (…)	No CLS defined
ItalyRLSCLS	Sales[StoreKey] IN (…)	Sales[Ordernumber] + Sales [Linenumber] removed

- Several test users to evaluate roles and combinations

Username	GermanyRLS	ItalyRLSCSL
Gabi Trial User	X	
Gabi Muenster (MSFT)		X
Gabi Muenster (GMPBICAT)	X	X

Summary

What stays the same?

Combination of RLS and CLS in different roles is not possible in general

Policies in the same role work as Intersection, Policies in different roles work additive (UNION)

What is different?

Security is not distributed through relationships

RLS needs to be defined on FACT table (and ideally on dimension table to keep the same user experience)



SQL KONFERENZ 2026

Classified as Microsoft Confidential



SQL
KONFERENZ
2026

Questions

Your feedback matters!



Classified as Microsoft Confidential