#FABCONSQLCON2026

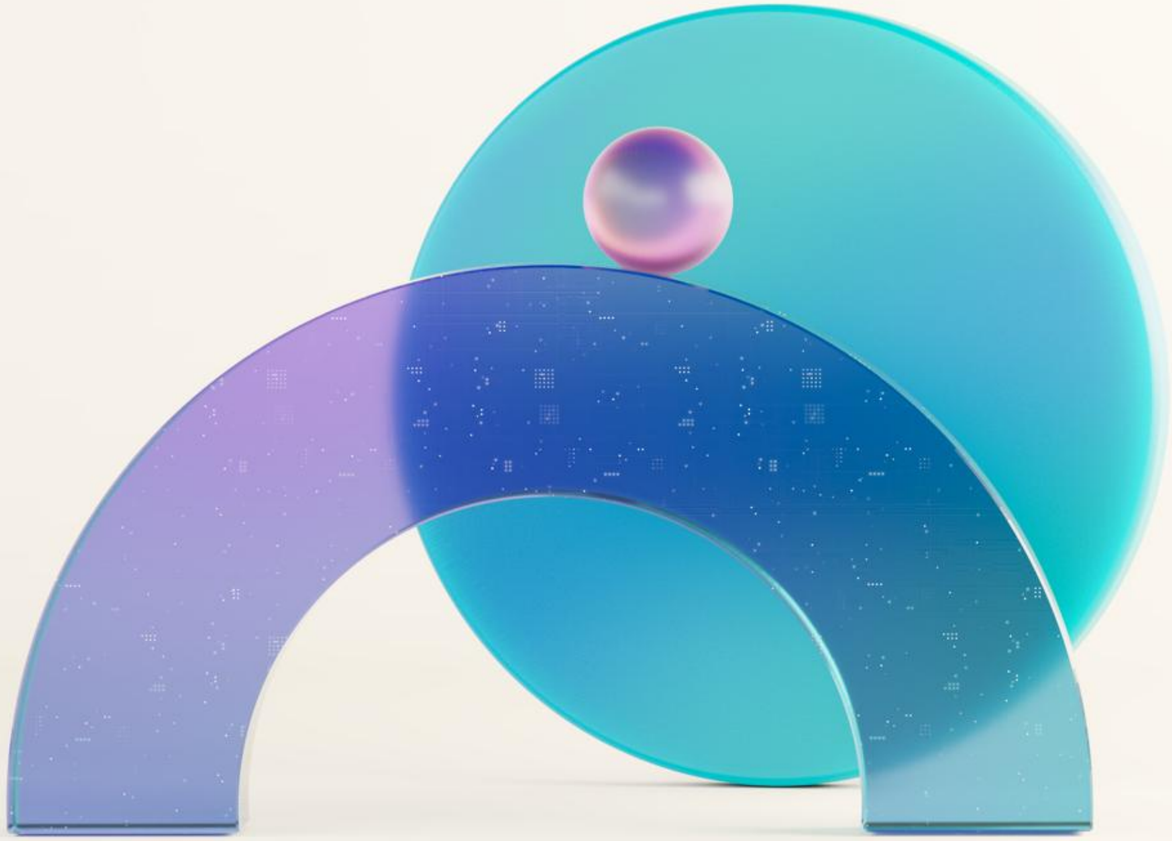
FABCON
Microsoft Fabric
COMMUNITY CONFERENCE

SQLCON
Microsoft SQL
COMMUNITY CONFERENCE

ATLANTA MARCH 16 - 20, 2026

Microsoft

Microsoft Fabric
Community Conference



Hardening Fabric Warehouse Security

Building Layered Defense from Authentication to Governance

About your Speakers

Freddie Santos
Senior Product Manager
Fabric Warehouse

Sam Debruyn
Freelance Data Platform Architect
MVP Microsoft Fabric

*Our mission is to **"make sure you never make the news—for the wrong reasons"***

Session Roadmap

“To build a truly secure and compliant Warehouse; security must be approached in layers”

1

- Cybersecurity Threats, Risks, and Impacts on Fabric Data Warehouse

2

- Layers of Protection

2.1

- Identity is the Foundation

2.2

- Network Restricted: Reducing Attack Surface

2.3

Data Protection: Continuous Encryption

2.4

Policy Enforcement: Limiting Data Exposure

2.5

Fully Observable & Governed

The Stakes Have Never Been Higher

3,322

Data Breaches Tracked in 2025 in the US alone — An All-Time High

About $34 billion dolars In financial loses – US only.

$10.22M*

average cost of a single data breach

230

breaches due to incorrect security configurations of cloud components

246 days

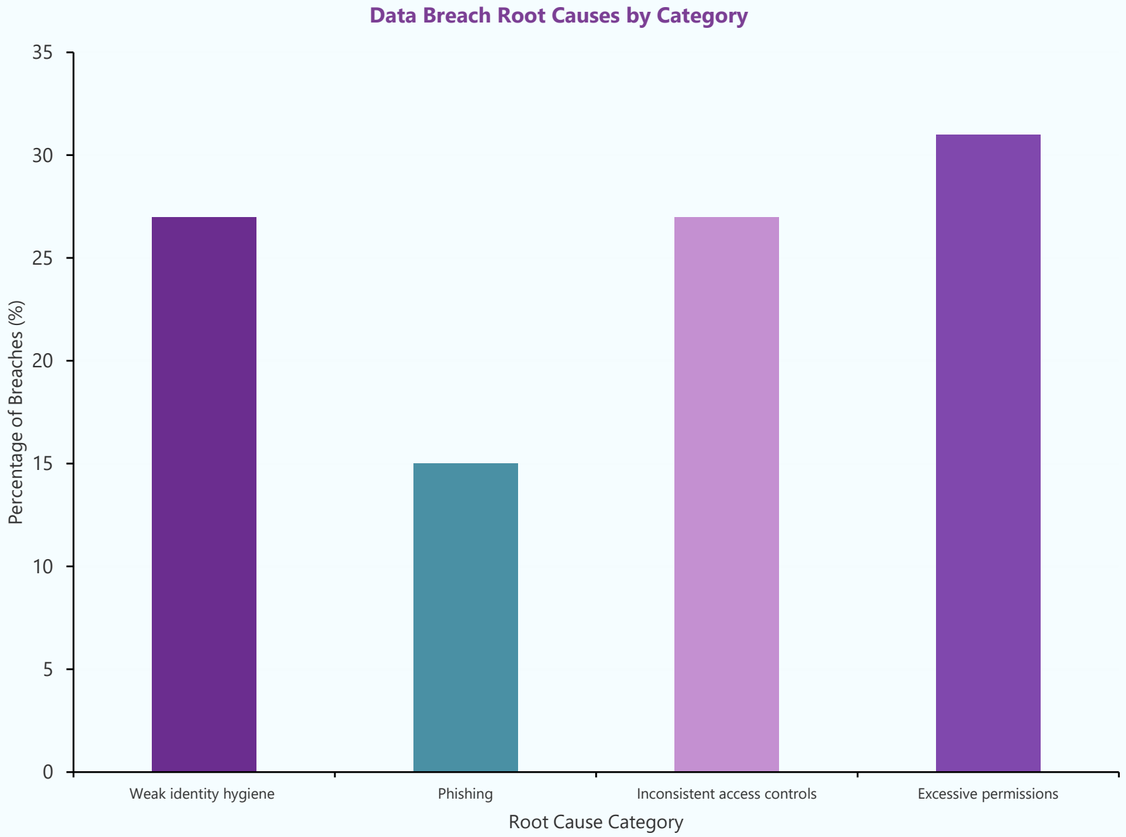
needed on average to identify and contain the breach

*Attackers are no longer **breaking in** —they're simply **logging in** with stolen credentials, making **identity and configuration hardening** your first line of defense*

* IBM Cost of a Data Breach Report 2025

Where Breaches Actually Start

What the Data is Telling us:



- **Weak Identity Hygiene (~27%)**
  - Stale credentials, no MFA, unmanaged service principals, shared accounts. Identity remains the easiest initial entry point.
- **Phishing (~15%)**
  - Users are still the front door. Credential theft and token replay bypass perimeter defenses.
- **Inconsistent Access Controls (~27%)**
  - Roles applied unevenly, no least-privilege model, ad-hoc grants, security policies exist — but are not consistently enforced.
- **Excessive Permissions (~31%)**
  - Overprivileged users and service accounts expand blast radius, breaches escalate because access is broader than necessary.
- **Supply Chain & Indirect Access Risk**
  - Modern attacks don’t always start inside — they propagate through connected systems.

Sources:

50 Identity And Access Security Stats You Should Know...

Identity Security: Cloud’s Weakest Link in 2025 | CSA

Weak Authentication

Target accounts with poor password hygiene or no MFA

↓

Open Network

Exploit public endpoints and unrestricted access paths

↓

Data Ingestion

Inject malicious data through uncontrolled COPY operations

↓

Bypass Policies

Access sensitive data without row or column restrictions

↓

Avoid Detection

Operate below monitoring thresholds to remain invisible

How would attackers break Into Your Warehouse?

Understanding the attack surface helps prioritize our defense layers

- Every security layer creates a barrier attackers must overcome, exponentially increasing difficulty
- Stolen credentials remain the primary entry vector, making authentication the critical first line
- Network restrictions force attackers to build complex infrastructure, raising costs and detection risk
- Data-level policies ensure compromised accounts cannot access all sensitive information
- Comprehensive monitoring provides observability to detect and respond to anomalous behavior patterns

Six Layers of Defense

- Each maturity level builds upon the previous layer, creating defense in depth that prevents single points of failure
- Organizations typically progress through levels sequentially, though some controls can be implemented in parallel based on risk assessment
- Level 1 provides the essential foundation—without strong authentication, all other controls become less effective
- Mature organizations operate at Level 4-5, where policies are enforced automatically and all access is continuously monitored
- The goal is not perfection but continuous improvement, moving up the maturity curve with each implementation

Layer 1: Identity Management

Identity Management -Verify Every Identity

Zero Trust Policy

MFA Support

Fine-Grained Control

- **Microsoft Entra Integration:** Fabric Warehouse leverages Microsoft Entra ID as the primary authentication mechanism, eliminating username-password vulnerabilities and enabling centralized identity management
- **Service Principal Authentication:** Service principals provide application identities with managed secrets and **certificates**, enabling automated processes without storing credentials in code or configuration files
- **Workspace Identity (Coming Soon):** support for workspace-scoped managed identities will allow secure, **keyless authentication for data access scenarios** such as COPY INTO and external integrations — eliminating secret management for automation workflows.

Identity Hardening Best Practices

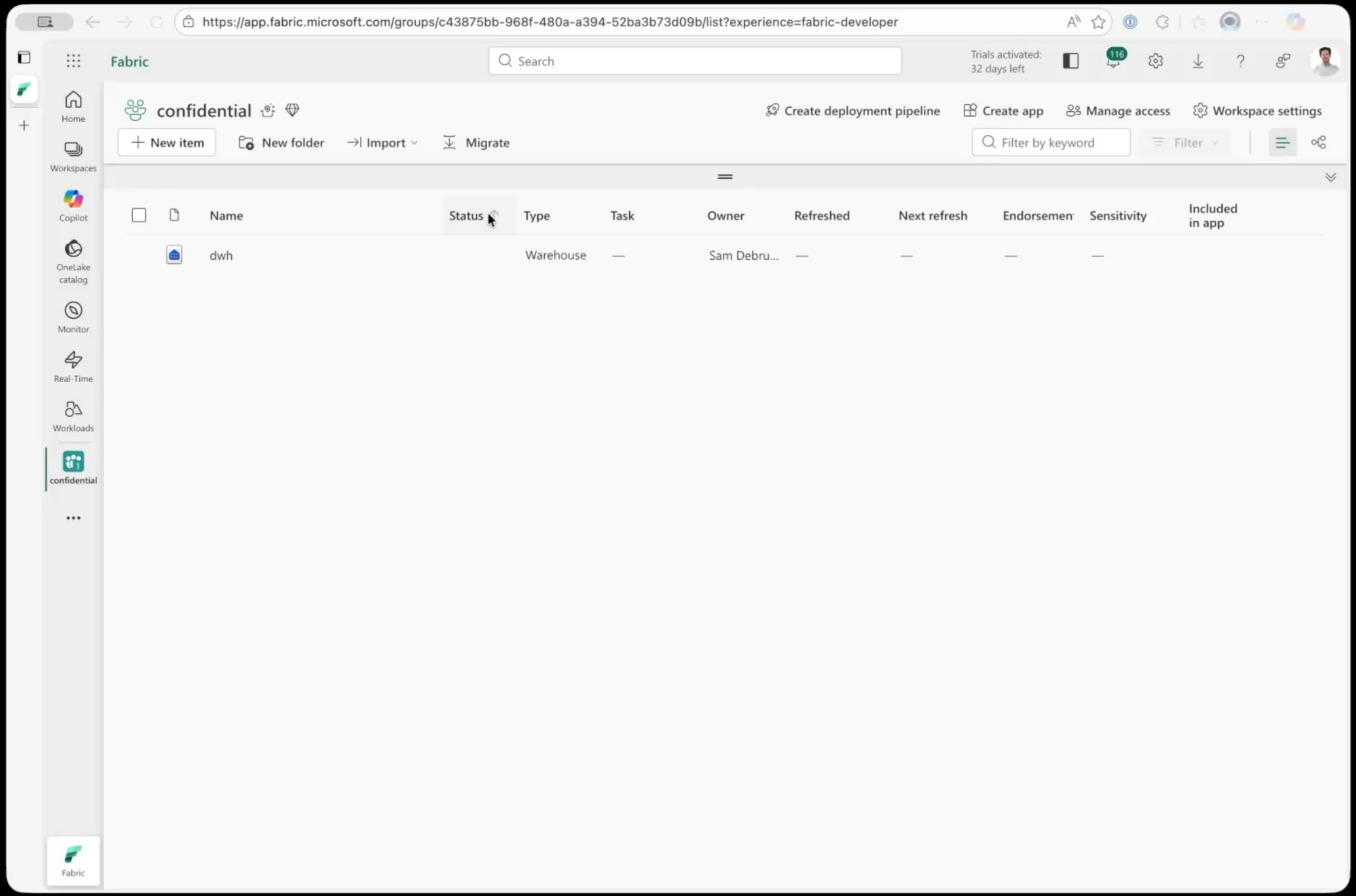
Conditional Access

Proper Housekeeping

- **Enable Service Principal Access:**
  Use application identities for automation and CI/CD instead of user accounts to eliminate shared credentials and reduce lateral risk.
- **Enforce Conditional Access:**
  Require MFA, compliant devices, and location restrictions through Microsoft Entra policies.
- **Rotate Service Principal certificates:**
  Implement proactive certificate rotation to prevent expired credentials and minimize operational disruption.
- **Apply Least Privilege:**
  Grant only required workspace and object-level permissions to service principals and users.
- **Audit Identity Activity:**
  Regularly review identity usage, last sign-in times, and privileged role assignments to detect stale or overprivileged accounts.
- **Leverage Privileged Identity Management:**
  Assign permissions to Entra ID Groups and provide just-in-time and restricted access to data.

Demo

Identity Management

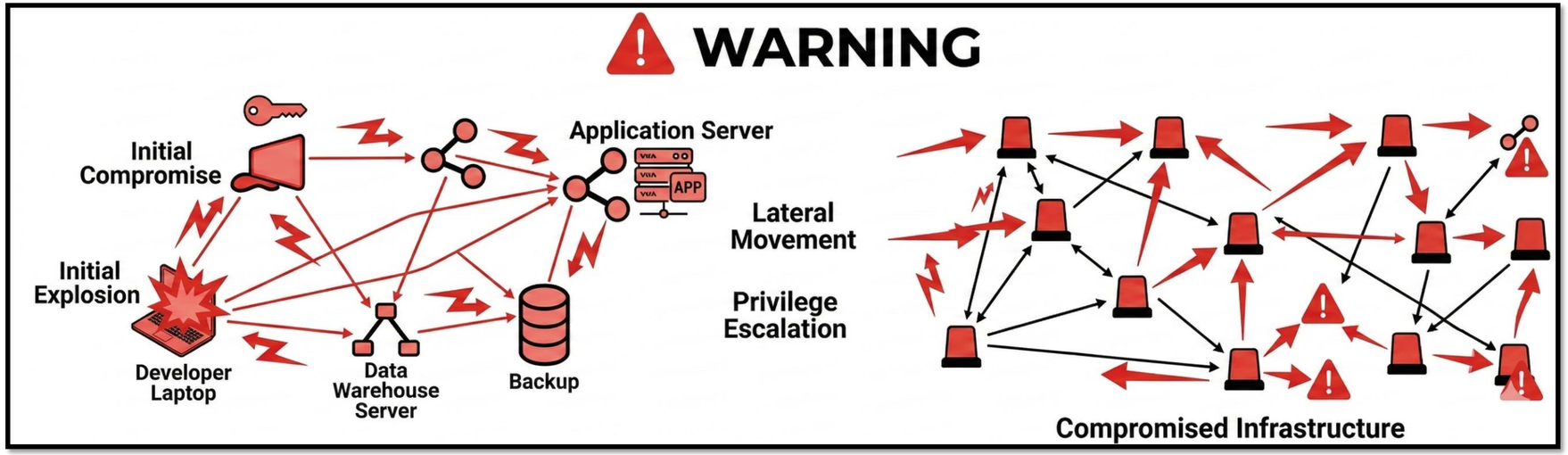

https://app.fabric.microsoft.com/groups/c43875bb-968f-480a-a394-52ba3b73d09b/list?experience=fabric-developer
Fabric
Search
Trials activated:
32 days left
116
Home
Workspaces
Copilot
OneLake catalog
Monitor
Real-Time
Workloads
confidential
Fabric
confidential
Create deployment pipeline
Create app
Manage access
Workspace settings
New item
New folder
Import
Migrate
Filter by keyword
Filter
Name
Status
Type
Task
Owner
Refreshed
Next refresh
Endorsemen
Sensitivity
Included in app
dwh
Warehouse
—
Sam Debru...
—
—
—
—

Layer 2: Network Isolation and Controls

The Blast Radius: Why We Need "Internal Locks"

There are risks in a flat network architecture

- **Risk of a Flat Network Architecture:** Without internal segmentation, a single compromised entry point grants an attacker unrestricted lateral movement across the entire data estate.
- **The 62-Minute* Window:** In non-isolated environments, attackers can move from an initial breach and perform a lateral move (e.g., your Production Warehouse) in an average of just 62 minutes.
- **Containment via Micro-segmentation:** Implementing internal "locks" ensures that security failures are localized, protecting the core Data Warehouse from the broader impact and costs of a breach.



*CrowdStrike 2024 Global Threat Report

Network Isolation

Defining the right boundaries ensures data traffic never traverses the imposed limits

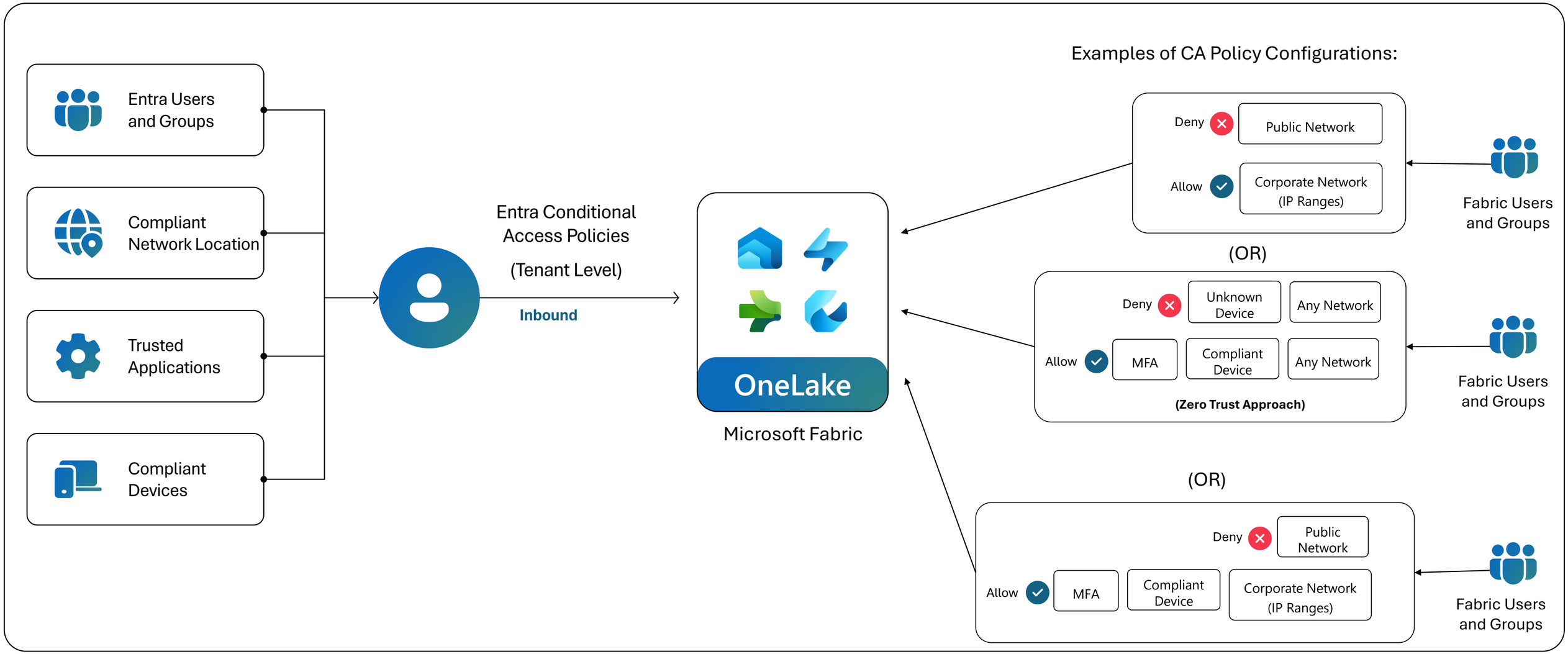
Protect Inbound Connections

Protect Outbound Connections

- **Inbound Protection:** Use Private Links and Workspace Firewalls to block the public internet and define strict access boundaries.
- **Outbound Protection:** Data Warehouse exfiltration vectors are minimal, leveraging on Outbound Access Protection will prevent exfiltration techniques on Warehouse.
- **Identity Integration:** Apply Entra ID Conditional Access to add AI-driven, context-aware validation to every connection.

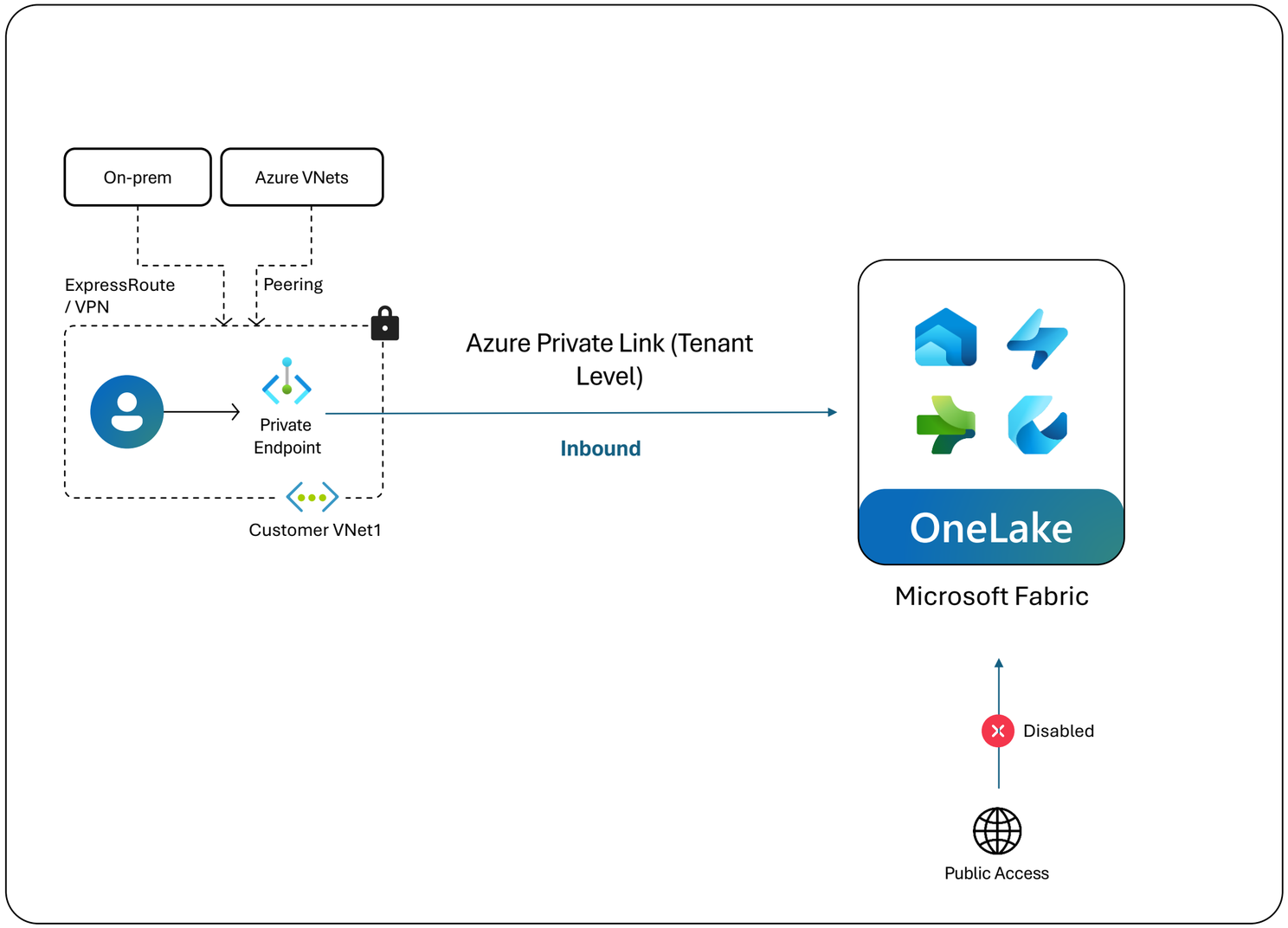
Entra ID - Conditional Access Policies

Restrict all inbound access to Fabric to compliant networks, devices, etc.



Tenant level Private Link (TPL) for Fabric

Perimeter Network Security for your tenant

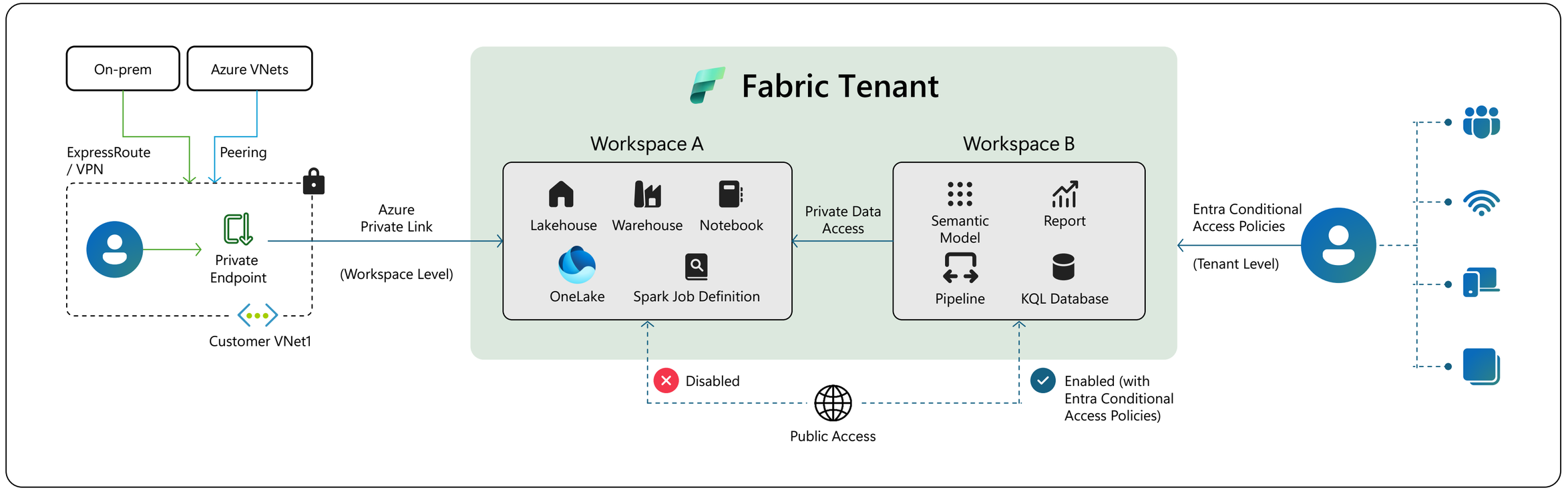


What it means:

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)

Workspace level Private Link for Fabric

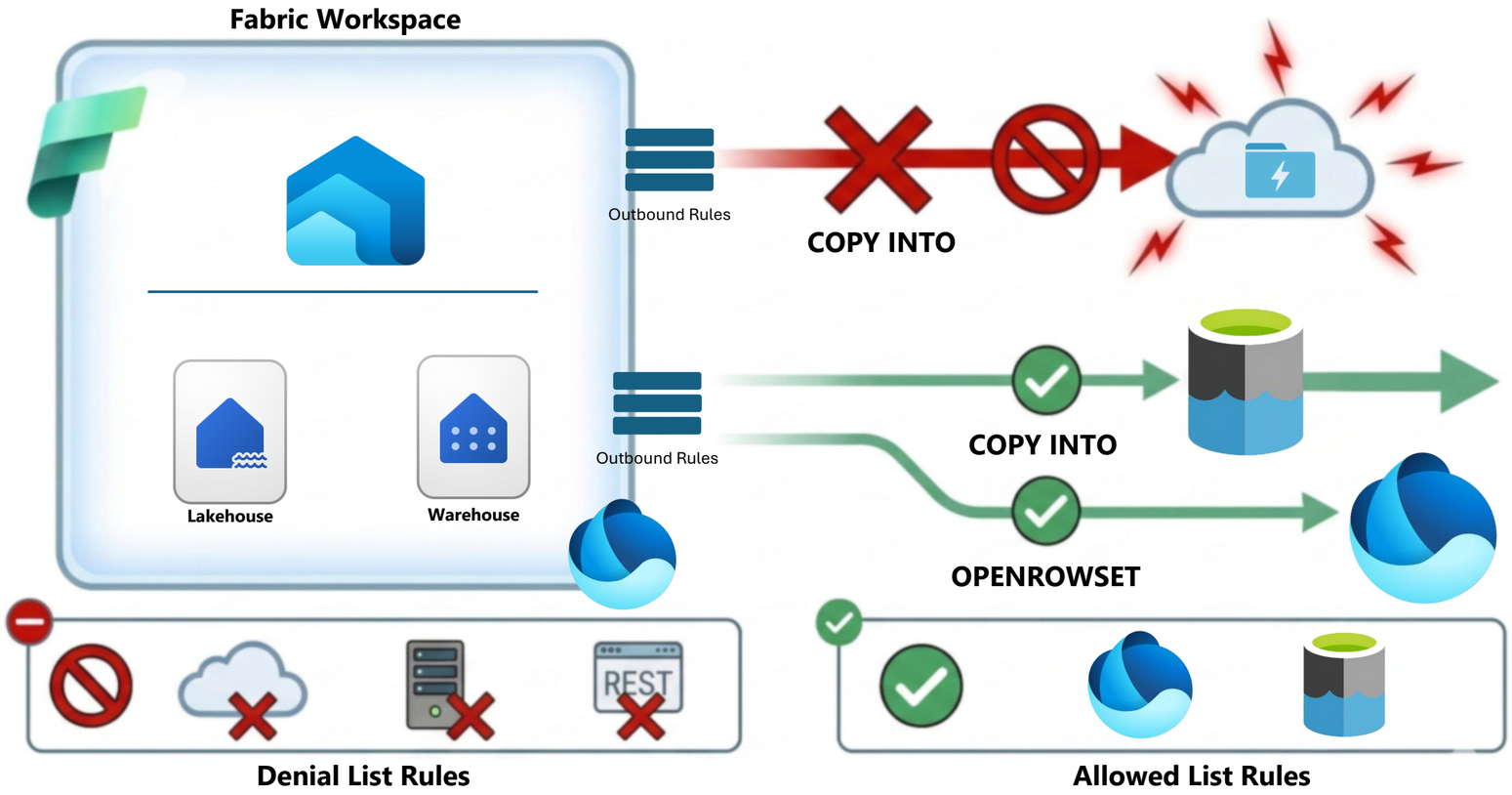
Perimeter Network Security for your workspace



Outbound Access Protection

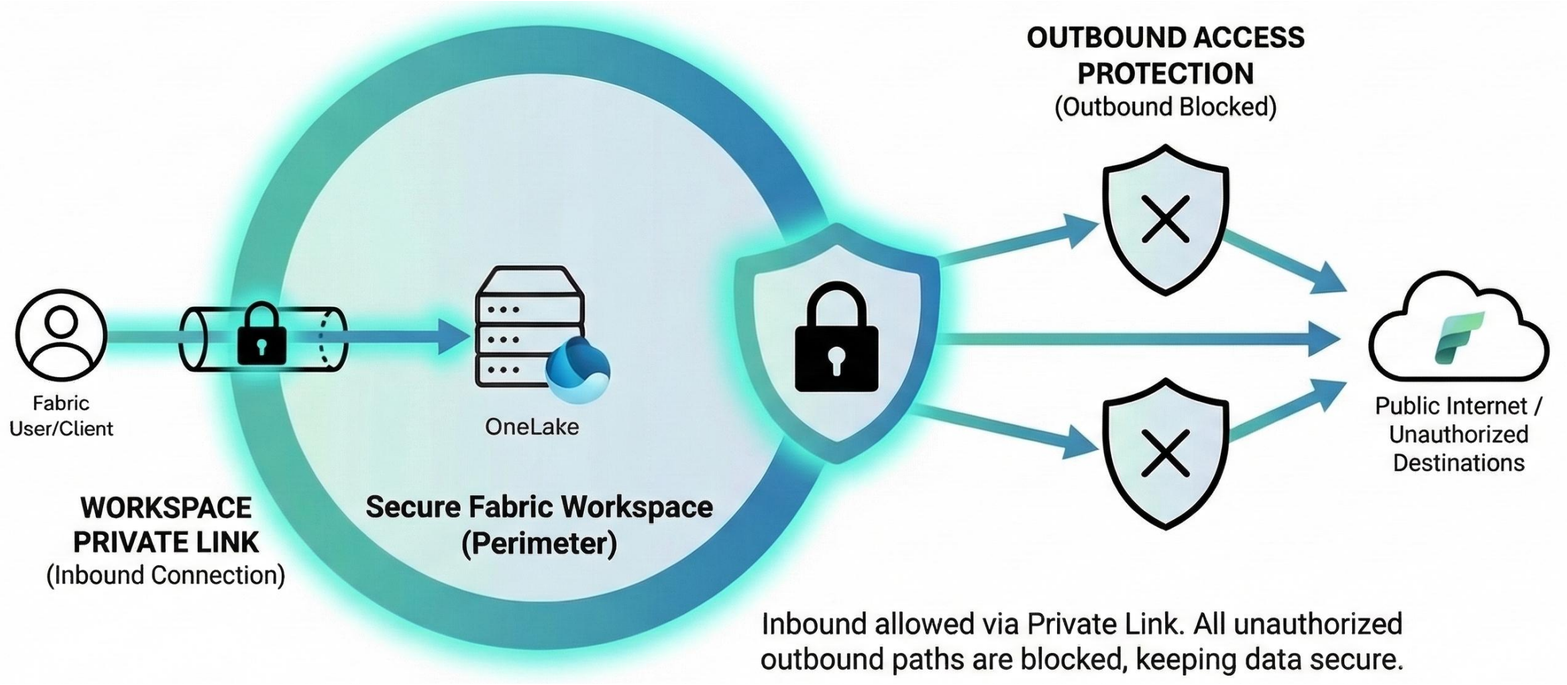
Sealing the Vault

- **Complete Exfiltration Prevention:** OAP ensures that even if a system is compromised, data cannot be leaked to unauthorized public endpoints or non-whitelisted external tenants.
- **Granular Trusted Routing:** You maintain strict control by explicitly allowing connections only to validated resources, such as trusted Fabric Workspaces or specific ADLS Gen2 paths.
- **Operational Integrity:** By blocking unauthorized COPY INTO or OPENROWSET attempts by default, you ensure that data movement only occurs between pre-approved, secure environments.



Extreme Network Protection

🛡️ Outbound Access Protection + 🔒 Workspace Private Link



Outbound Access Protection (OAP): Blocks unauthorized data export from the Data Warehouse.

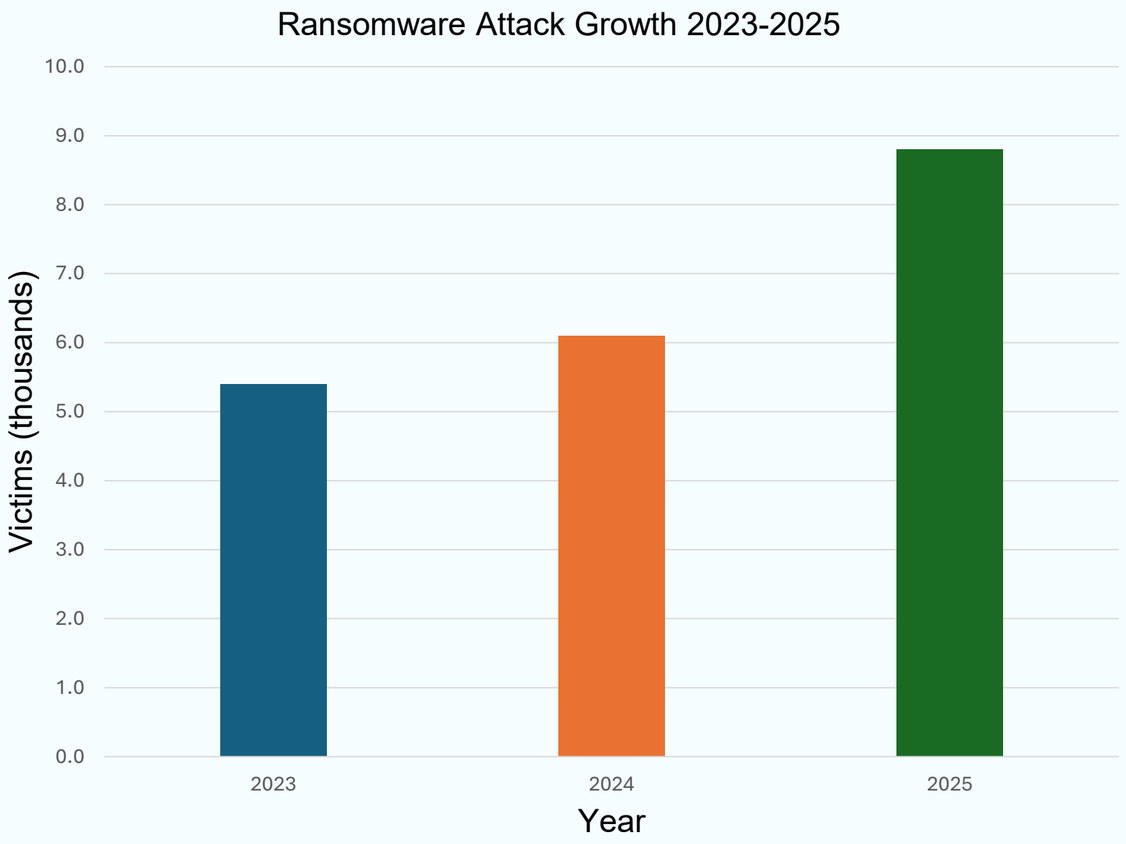
Workspace Private Link: Ensures inbound access is limited to private, secure network boundaries.

Together: They create a **zero-trust boundary** around your workspace, preventing sensitive data from leaking *in or out*.

⚠️ Whether you use TPL or WS PL or use Firewall Rules to access Fabric over public endpoint**, Entra Conditional Access** is a must ! ⚠️

Layer 3: Encryption

The Ransomware Crisis - Network Protection as Foundation



Source: The State of Ransomware in the U.S.: Report and Stati...

44%
of breaches involve ransomware

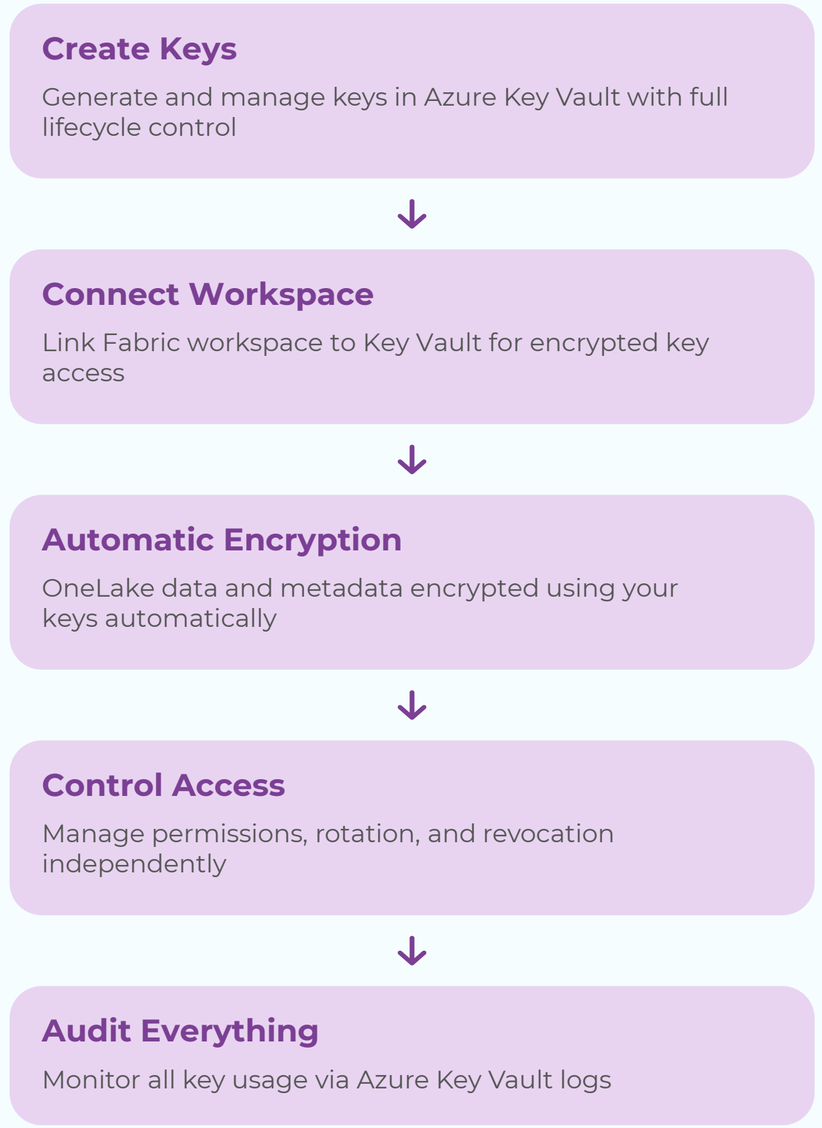
75%
of attacks are identity-based

$5M+
average recovery cost

- Network breaches are initial entry points—phishing (16%) and credentials (12-14%) bypass perimeter defenses
- Credential theft surged 800% in 2025: 1.8B credentials stolen via infostealer malware post-compromise
- Attackers stay hidden for months (63% for 6+ months), mapping cloud resources and stealing credentials
- Once inside, attackers conduct reconnaissance to identify cloud connections and privileged accounts
- Attack chain: network breach → credential theft → cloud access → encryption

Fabric Customer Managed Keys (CMK)

- Fabric encrypts all data by default with Microsoft-managed keys, providing strong baseline security across workspaces
- CMK adds encryption layer via envelope encryption—your Key Vault key encrypts Microsoft's data encryption keys
- Keys stay in your Key Vault—Fabric accesses via secure APIs with logged, policy-validated calls
- Workspace-level granularity lets you apply enhanced encryption selectively to sensitive environments



CMK Implementation in Fabric Warehouse

OneLake Data

All persisted data encrypted with your CMK including tables, Delta Parquet files, and analytics datasets

Warehouse Metadata

Table definitions, stored procedures, functions, and schema information encrypted with your key

Backend Compute

Ephemeral caches use Microsoft-managed keys and auto-clear after sessions, no data persists

3 Encryption Layers

Protection depth

Zero Performance Impact

No speed reduction

Ephemeral Compute

Auto-clearing caches

- SQL frontend encrypts all metadata including table definitions, views, and functions using your key to protect schema information
- All OneLake data uses your Azure Key Vault key through envelope encryption, providing comprehensive protection for persisted information
- Backend compute processes queries in ephemeral cache environments that auto-evict content after use, with no data at rest
- Once enabled, both existing and new Warehouse items automatically use your encryption keys without manual configuration

Demo

CMK

Home
Create
OneLake catalog
Monitor
Workspaces
MyCMK-Workspace
MyDemoDW

MyCMK-Workspace

Recycle bin | Create deployment pipeline | Create app | Manage access | Workspace settings

New item | New folder | Import | Migrate

Filter by keyword | Filter

Choose from predesigned task flows or add a task to build one

Select from one of Microsoft's predesigned task flows or add a task to start building one yourself.

Select a predesigned task flow | Add a task

Import a task flow

Name	Status	Type	Task	Owner	Refreshed	Next refres
MyDemoDW		Warehouse	—	AdminUser01	—	—

Power BI

Layer 4: Limiting Data Exposure

Why Ingestion Must Be Controlled

Arbitrary storage path access

Silent data exfiltration risk

Corrupted analytical datasets

Complex incident response

Threat Vectors

- **COPY INTO & OPENROWSET**
  Only 2 SQL commands with external access in Data Warehouse
- **Abuse - Arbitrary Storage Paths**
  Attackers specify external storage locations as data sources, bypassing access controls and reading unintended files
- **High-Bandwidth Attack Channel**
  Ingestion processes large volumes rapidly, enabling significant data movement without triggering monitoring
- **Privilege Escalation Vector**
  COPY INTO runs with elevated permissions, making it attractive for unauthorized data access

Real Harm Impact

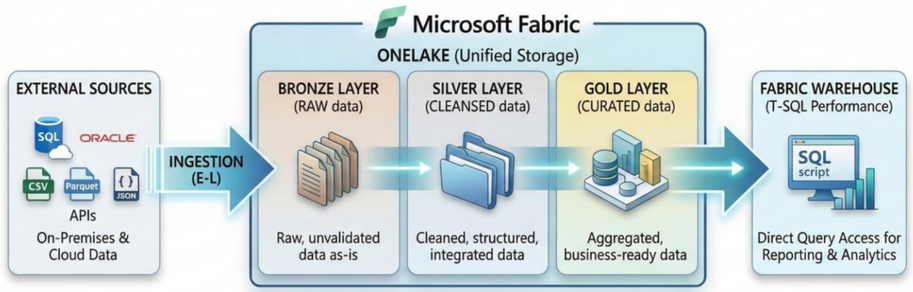
- **Silent Data Exfiltration to Attacked-Controlled Warehouses**
  Sensitive data copied to attacker-controlled storage without detection, appearing as legitimate operations
- **Compliance Violations**
  Unauthorized data movement creates regulatory failures, legal penalties, and breach notification requirements
- **Dataset Corruption and Integrity Loss**
  Malicious data injection undermines analytical integrity, leading to incorrect business decisions
- **Loss of Trust and Incident Response Complexity**
  Discovered abuse erodes stakeholder trust and requires complex forensic investigations

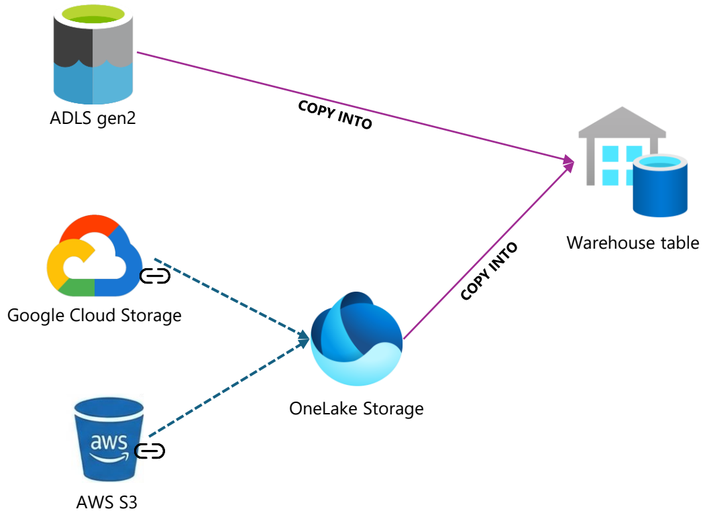
Hardening Ingestion in Warehouse

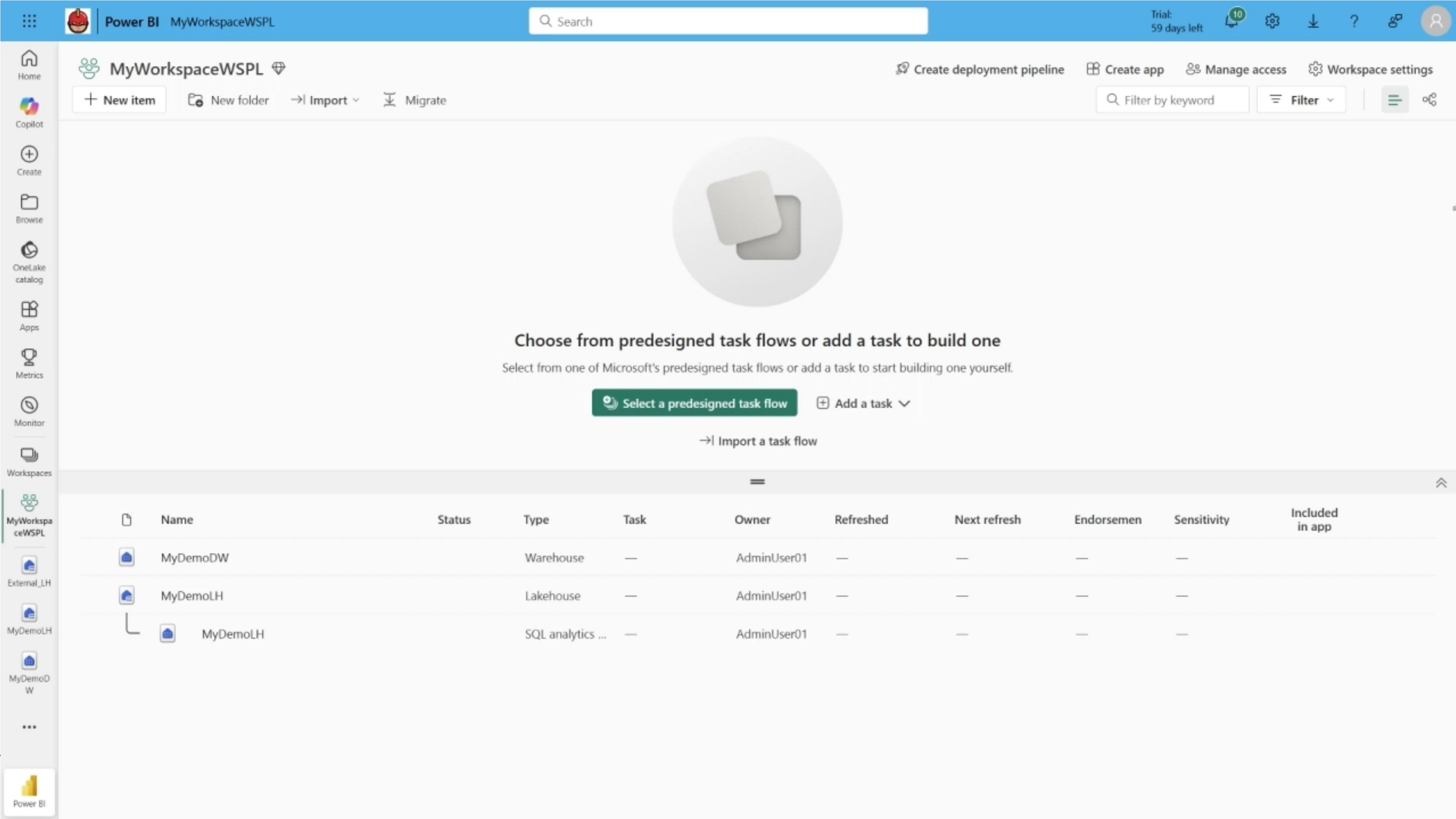
Fabric Warehouse implements defense layers to control ingestion operation

Validated OneLake paths only	**System-controlled staging**
Outbound Access Protection	**Identity-scoped permissions**

- **Source Validation:** Only validated OneLake paths from trusted workspaces eliminating arbitrary storage access.
- **Network Protection:** Private Link limits inbound access while Outbound Access Protection prevents data exfiltration.
- **Identity Checks:** COPY INTO evaluated under Entra identity with least privilege (Granular Insert Permission).
- **Audit Trail:** All operations logged with staging and execution tracing for forensics-ready compliance reporting.

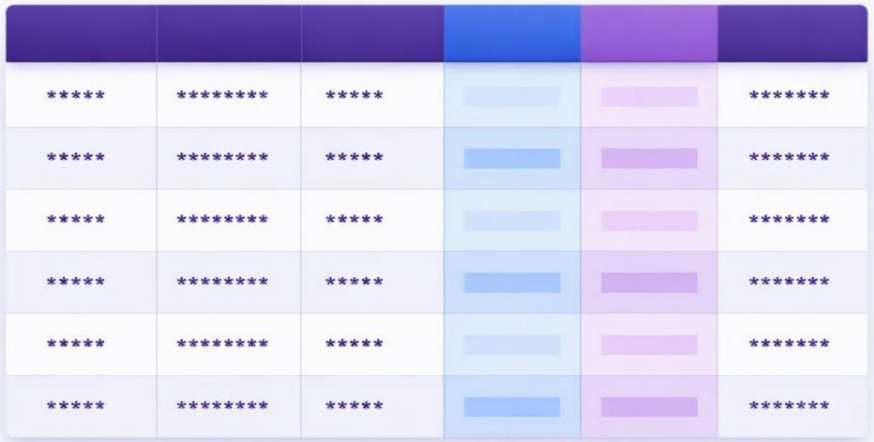





Power BI
MyWorkspaceWSPL
Search
Trial:
59 days left
10
Home
Copilot
Create
Browse
OneLake catalog
Apps
Metrics
Monitor
Workspaces
MyWorkspaceWSPL
External_LH
MyDemoLH
MyDemoDW
Power BI
MyWorkspaceWSPL
Create deployment pipeline
Create app
Manage access
Workspace settings
New item
New folder
Import
Migrate
Filter by keyword
Filter
Choose from predesigned task flows or add a task to build one
Select from one of Microsoft's predesigned task flows or add a task to start building one yourself.
Select a predesigned task flow
Add a task
Import a task flow
Name
Status
Type
Task
Owner
Refreshed
Next refresh
Endorsemen
Sensitivity
Included in app
MyDemoDW
Warehouse
AdminUser01
MyDemoLH
Lakehouse
AdminUser01
MyDemoLH
SQL analytics ...
AdminUser01

Layer 4: Data Protection – Tight Permission Controls

Fine-Grained Data Protection



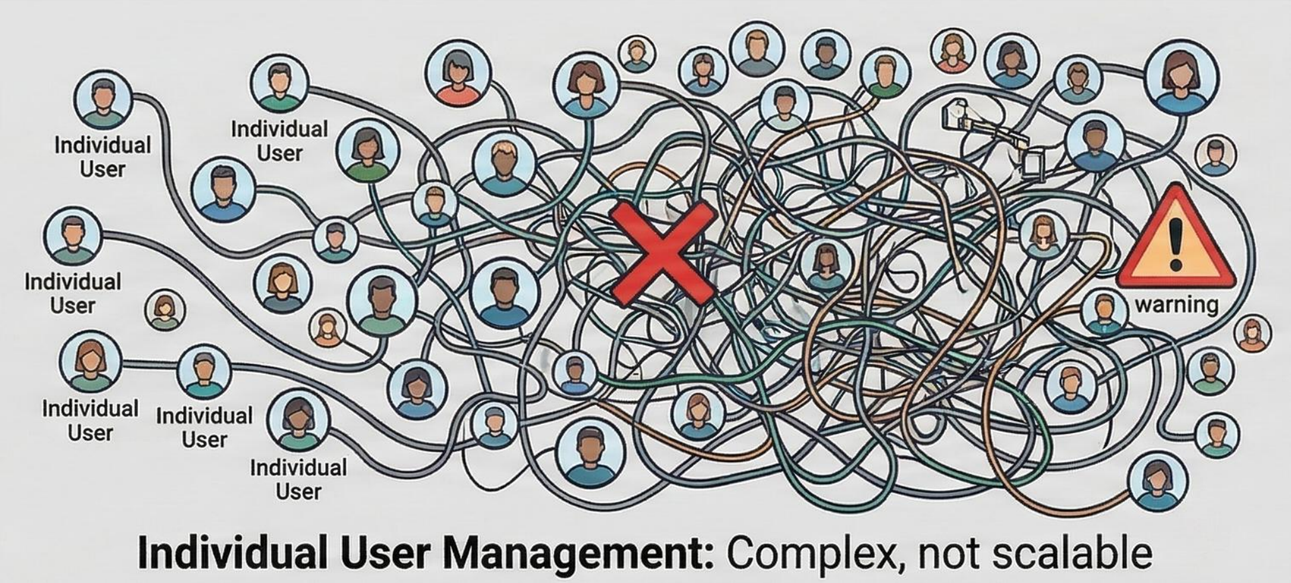
GRANT/DENY Columns

Masking Functions

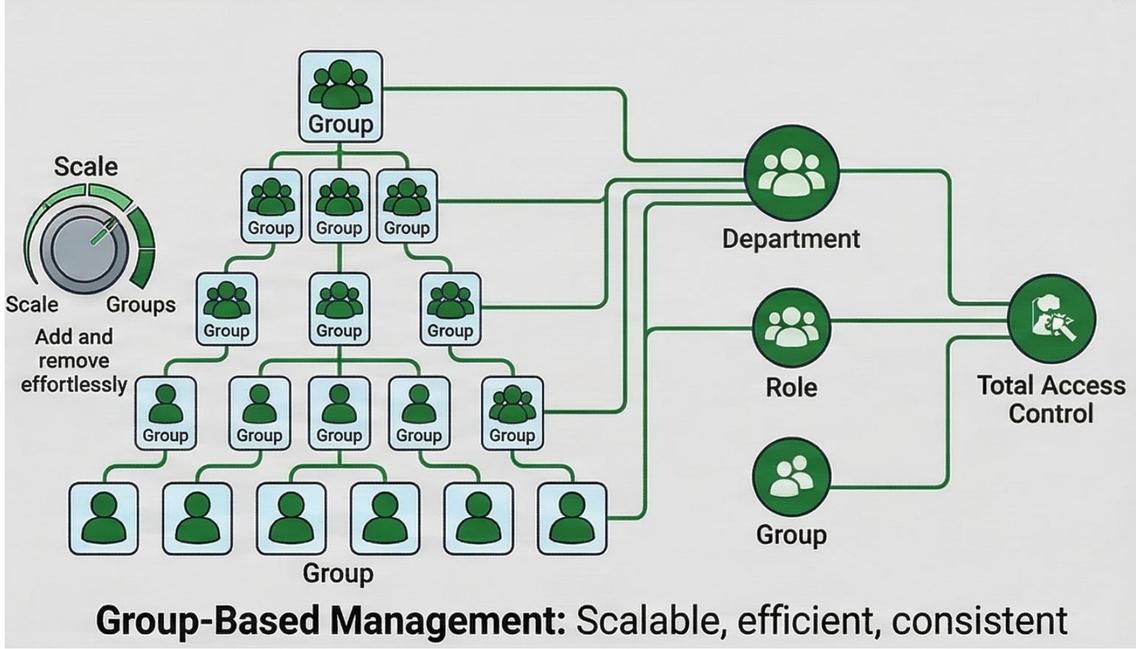
- **Column-Level Security (CLS):** Use GRANT and DENY statements to control access to columns with sensitive information
- **Dynamic Data Masking (DDM):** Apply functions that obfuscate sensitive data, showing 'XXX-XX-1234' instead of full social security numbers
- **Row Level Security:** Choose Role-Based Filtering to define filter conditions based on user identity, role membership, or attributes to automatically restrict rows
- **Prevent Elevated Access:** Designate groups, roles and permission to the granular level, avoiding granting more access than users should have.
- **Layered Approach:** Combine RLS, CLS, and DDM to create multiple barriers against attacks

Don't Ignore SQL Security: The Principle of Least Privilege

- **Move Beyond "All or Nothing":** Avoid granting high-level administrative roles to general users.
- **Precision Control:** Use explicit GRANT, DENY, and REVOKE statements at the object level (Tables, Views, Stored Procedures).
- **Layered Defense:** Apply Row-Level Security (RLS) and Column-Level Security (CLS) to protect sensitive data cells within a shared table.



Individual User Management: Complex, not scalable

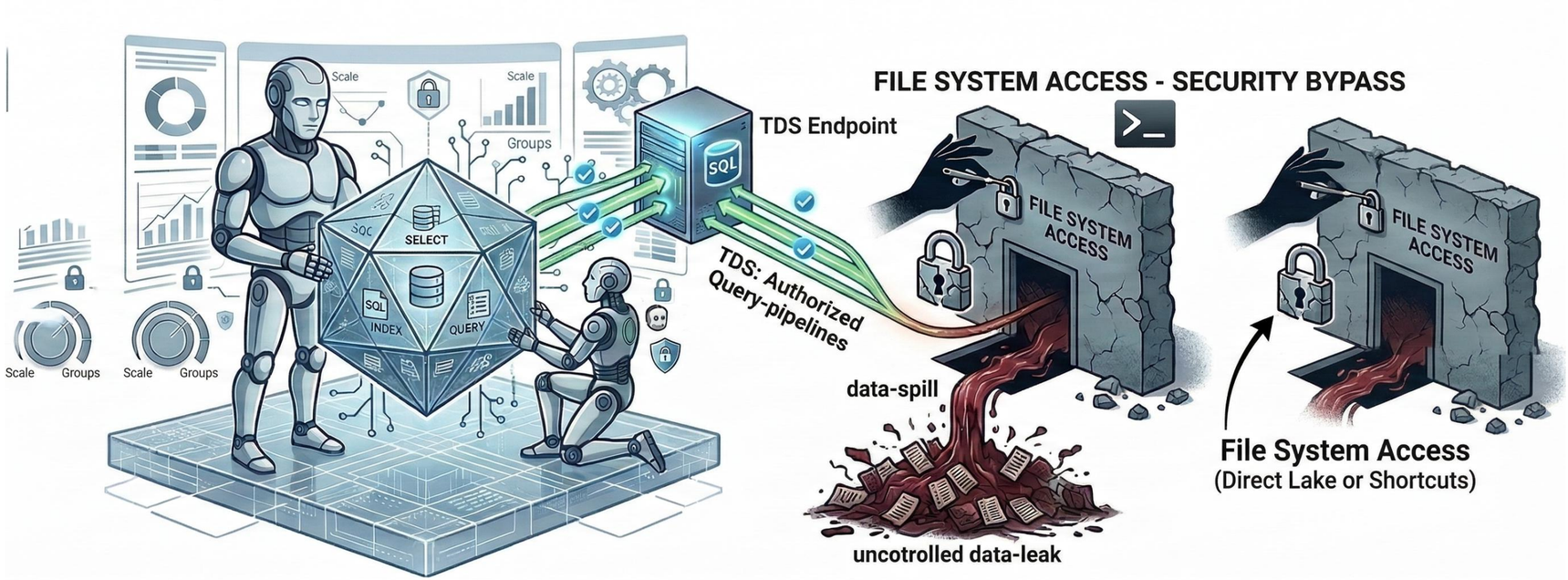


Group-Based Management: Scalable, efficient, consistent

T-SQL Security – Best Practices

CRITICAL!

SQL Security is enforced exclusively via **TDS Endpoints**. Accessing the underlying file system through **Direct Lake** or **Shortcuts** bypasses these SQL-level permissions entirely.



*__Sneak Peak__: We have a say about this later

Layer 5: Monitoring and Detection

Monitoring & Detection: The "Assume Breach" Foundation

Correlating Control Plane & Data Plane telemetry to validate Zero Trust.

Control Plane

- **Workspace Lifecycle:** Trace all creation, deletion, and configuration changes of the workspace.
- **Security Controls:** Audit who enabled Customer Managed Keys (CMK) or modified any workspace setting.

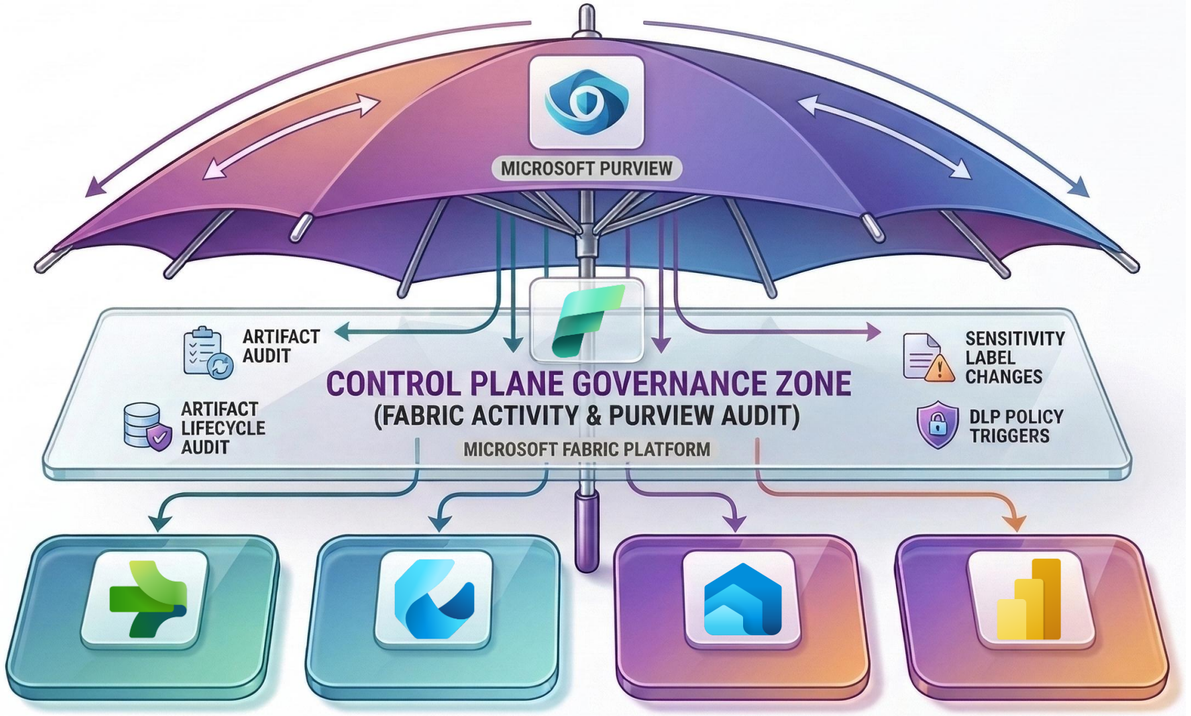
Data Plane

- **Full SQL Audit:** Capture comprehensive T-SQL command text, execution parameters, and precise timestamps.
- **Access Forensics:** Enable deep "Who, When, and What" tracing for every granular data interaction.
- **Integrity Validation:** Verify that data access aligns with the governance and security controls.

Control Plane: Fabric & Purview Governance

Governing the Fabric Ecosystem

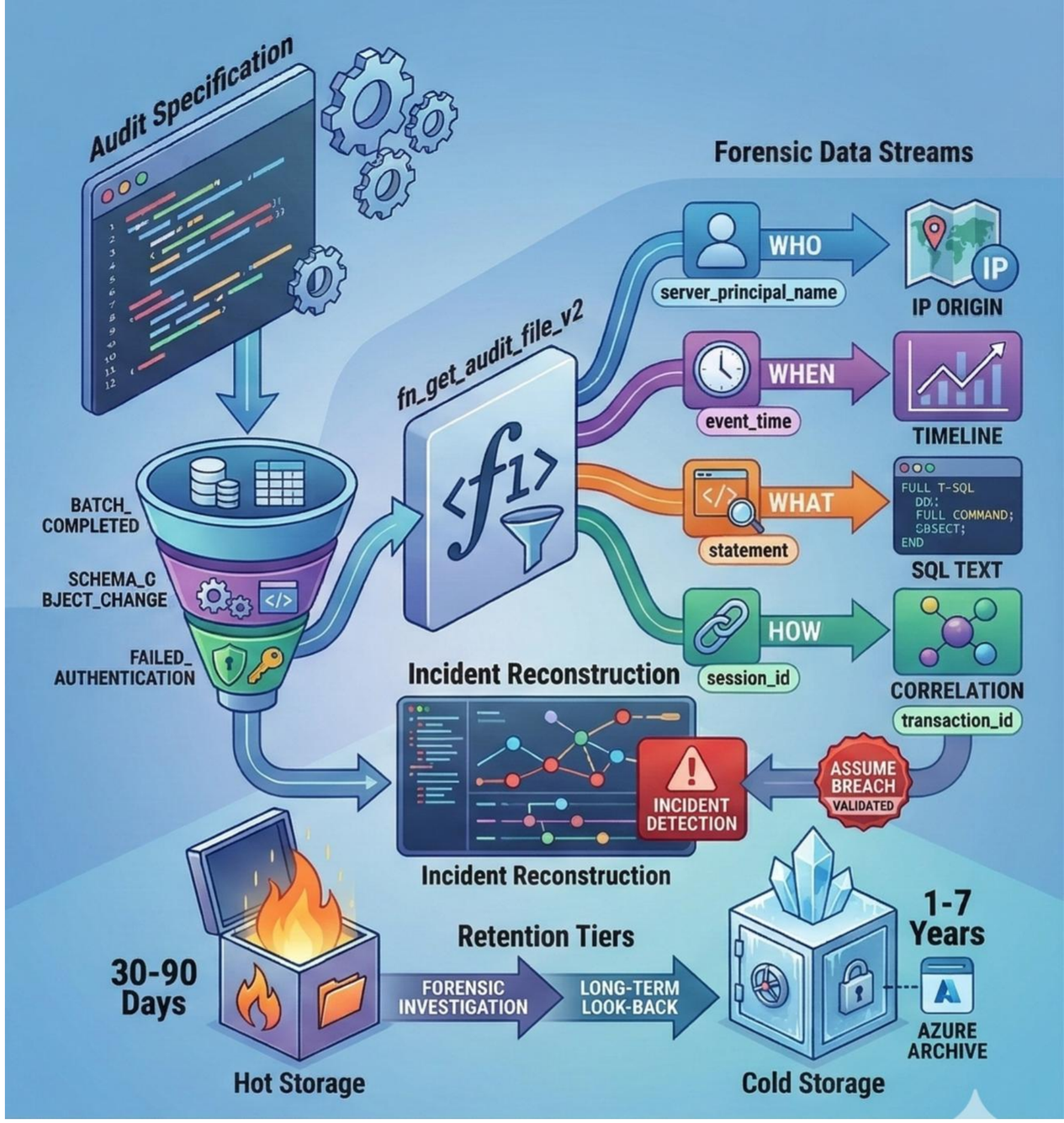
- **Platform Activity Strategy:** Track high-level operations such as CreateWorkspace, UpdateCapacity, and DeleteArtifact (Lakehouses, Pipelines, Warehouses) to maintain environment integrity.
- **Metadata Traceability:** Utilize the Microsoft Fabric Operation List to capture the "Who" and "When" for structural changes, such as moving artifacts or changing workspace permissions.
- **Purview & Label Governance:** Monitor sensitivity label changes (upgrading/downgrading) and Data Loss Prevention (DLP) policy triggers to ensure data remains classified correctly.
- **Administrative Forensics:** Audit "Power User" actions, including capacity setting modifications and tenant-level configuration drifts that could bypass lower-level security testing) that precede targeted data extraction



SQL Audit Logs– From Configuration to Forensics

Knowing the questions help you find the answers

- **Capture Strategy:** Focus on "high-signal" Action Groups—*BATCH_COMPLETED*, *SCHEMA_OBJECT_CHANGE*—to bridge the gap between Control Plane metadata and Data Plane execution.
- **The Forensic Result:** Leverage *sys.fn_get_audit_file_v2* to extract the **Who** (server_principal_name), **When** (event_time), **What** (statement), **and How** (session_id) for every data interaction.
- **Retention Policy:** Implement a **tiered retention strategy**: 30–90 days in hot storage for immediate forensic response and 1–7 years in cold storage (Azure Archive) to satisfy long-term compliance and "Assume Breach" look-back requirements.



Demo

SQL Audit Logs

ContosoDW | This item is restricted

Search

Trials activated: 44 days left

10

Home | Management | Help

Share

Home
Copilot
Create
Browse
OneLake catalog
Apps
Scorecards
Workspaces
Contoso Corp
ContosoDW
Power BI

Explorer

Query and preview your data

You can use this editor to query and preview your data for analysis. Start with a new query.

New SQL query

Copy SQL connection string

Best Practices: Incident Investigation & Replay

Closing the Loop – From Logs to Actionable Forensics

- **Reconstruction Strategy:**
Identify compromised accounts and unusual access patterns by cross-referencing authentication logs with specific query execution histories.

- **Systematic Timeline Analysis:**
Query audit logs chronologically to map the entire attack chain, from initial unauthorized access through privilege escalation to final data exfiltration.

- **Pattern Recognition:**
Perform query pattern analysis on captured T-SQL text to identify reconnaissance activities, such as schema enumeration or permission testing, that precede an attack.

.

- **Detecting Malicious Intent**
Detect lateral movement by tracking GRANT operations, role membership changes, and subsequent attempts to access previously restricted resources.

- **Beyond Native Queries:**
Use Semantic Link (SemPy) to export audit files into a dedicated Fabric Lakehouse to bypass standard log retention limits and create a permanent, queryable "Forensic Vault.“

- **Root Cause & Scope Assessment**
Trace malicious activity back to the initial entry point, whether it was a compromised credential, a misconfigured permission, or a vulnerable application.

**Determine the exact scope of data exposure by correlating query logs with table sensitivity classifications and data volume metrics*

Closing

Building Comprehensive Warehouse Security - Recap

- **Identity as Foundation:**
  Strong authentication reduce the risk of credential-based attacks that represent the primary breach vector
- **Network Isolation Reduces Attack Surface:**
  Create zero-trust boundaries that force attackers through monitored chokepoints and prevent data exfiltration
- **Data Policies Limit Blast Radius:**
  Ensure that even compromised accounts cannot access all sensitive data, containing damage from successful breaches
- **Monitoring Enables Detection and Response:**
  Comprehensive audit logging with provides visibility to detect anomalous behavior and respond before significant data loss
- **Defense in Depth Philosophy:**
  Each security layer compounds difficulty for attackers

If you are starting today, plan for a zero-trust architecture. Prioritize Layer 1 (Identity) with strict Least Privilege and Layer 5 (Monitoring) as your non-negotiable pillars. These ensure that no identity has more permission than necessary and the network has the right controls in place—no exceptions

What's Next: Security Roadmap

Continuous innovation in security capabilities to address evolving threat landscape

- **Granular Data Lineage**
  Column-level lineage showing sensitive data flow
- **OneLake Security for DW**
  Support OneLake Security with Fabric DW
- **Improved SQL Security Experience**
  Improved experience, and traceability for security management on Fabric DW
- **SQL Audit Logs Improvements**
  Improved navigation experience, introducing predicate filtering and more.
- **COPY INTO support Workspace Identity**
  Support COPY INTO operations to support the Workspace Identities
- **..and more**

Quick Survey:

Tell us what works — and what does not — in Fabric Data Warehouse!

https://aka.ms/fabric-data-warehouse-survey

It’s your time!

Sound off.
The mic is all yours.
Influence the product roadmap.

Join the Fabric User Panel

Share your feedback directly with our Fabric product group and researchers.

https://aka.ms/JoinFabricUserPanel

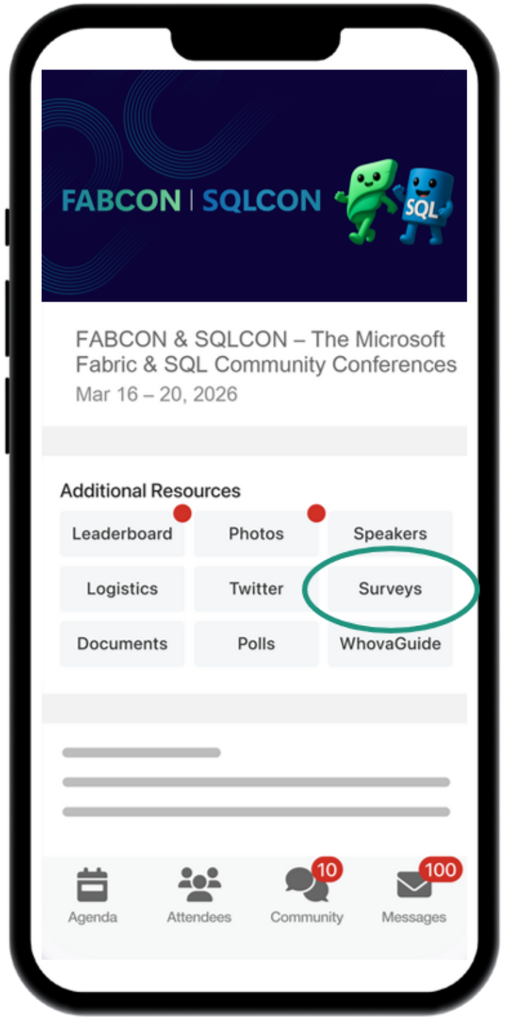
Join the SQL User Panel

Influence our SQL roadmap and ensure it meets your real-life needs

https://aka.ms/JoinSQLUserPanel

How was the session?

Complete Session Surveys in Whova for your chance to WIN PRIZES!



References

[1] Microsoft Entra Authentication in Fabric Data Warehou...

[2] About private Links for secure access to Fabric - Mic...

[3] 50 Identity And Access Security Stats You Should Know...

[4] Identity Theft Resource Center 2025 Annual Data Breac...

[5] Identity Security: Cloud's Weakest Link in 2025 | CSA

[6] Connect to your most sensitive data with end-to-end n...

[7] Workspace-Level Private Link in Microsoft Fabric (Gen...

[8] Track user activities in Power BI - Microsoft Fabric | Microsoft Learn

[9] Frequently Asked Questions (FAQ) · microsoft/semantic-link-labs Wiki

Get Two Fabric Certifications for FREE

Attendees of FABCON can take the Fabric Analytics Engineer or Fabric Data Engineer exam for free. Be part of the 2 fastest growing role-based certifications in Microsoft history.

Request your voucher by March 23, 2026.

https://aka.ms/fabcon/cert100