Microsoft Fabric

#FABCONSQLCON2026

FABCON
Microsoft Fabric
COMMUNITY CONFERENCE

SQLCON
Microsoft SQL
COMMUNITY CONFERENCE

ATLANTA MARCH 16 - 20, 2026

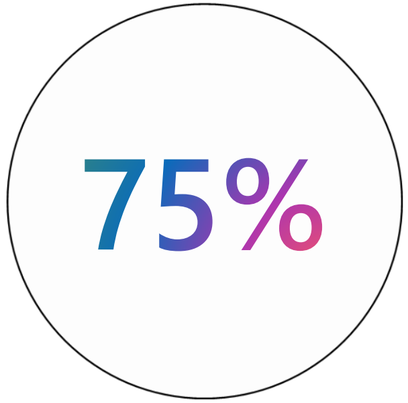
Enforce Your Governance and Security Regulations in Fabric

Benni De Jagere, Principal PM – Azure Data CAT

Darren Portillo, Product Marketing Manager

Data culture and AI transformation are happening now

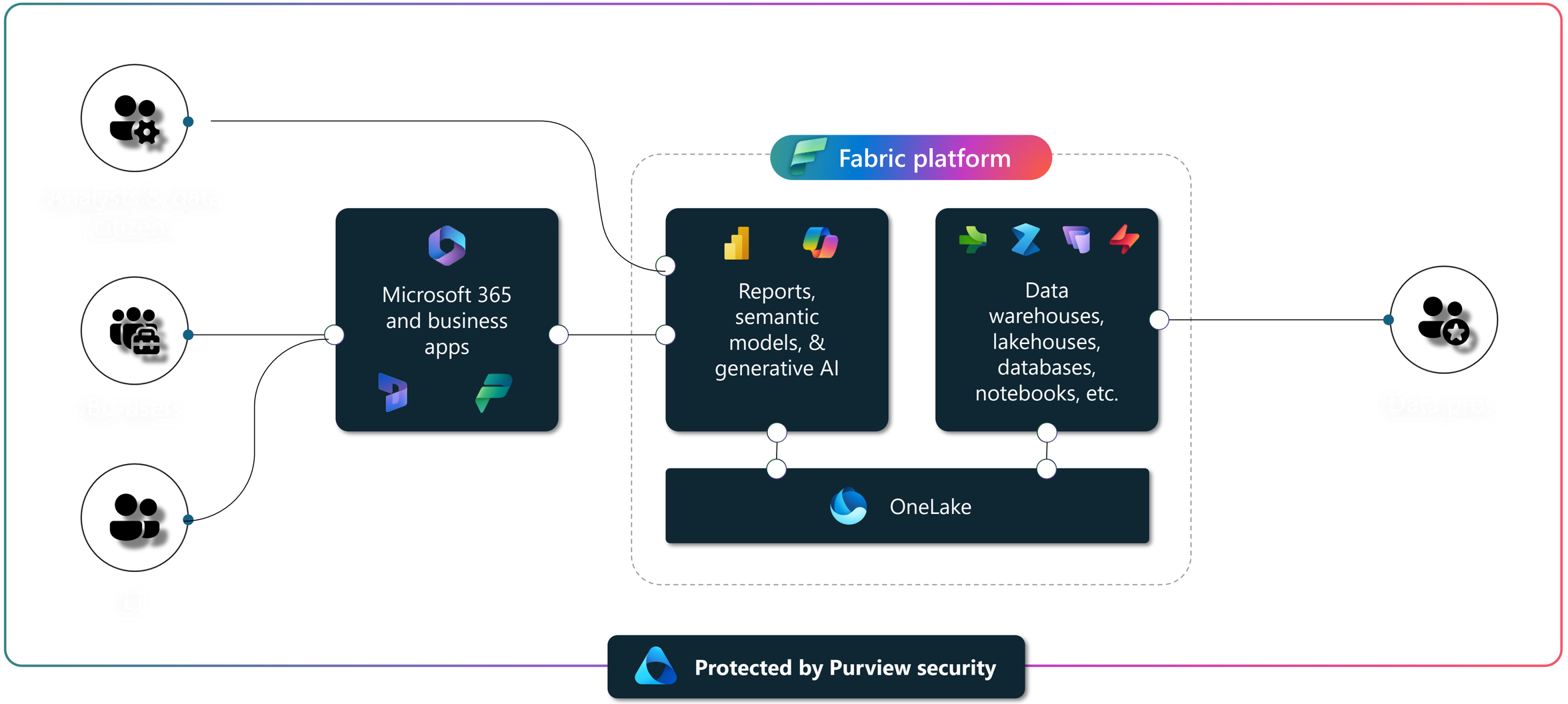
of organizations are implementing or developing a company wide data foundation[1]



of knowledge workers already using AI at work (doubled in the past 6 months)[2]

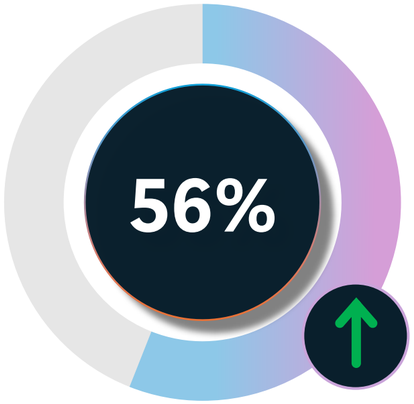
1. The Alation State of Data Culture Report
2. Microsoft 2024 Work Trend Index Annua

AI-powered data cultures require broad data access



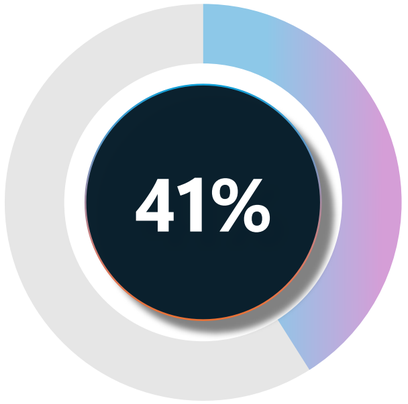
Broad data access bring additional risk

Data oversharing from AI



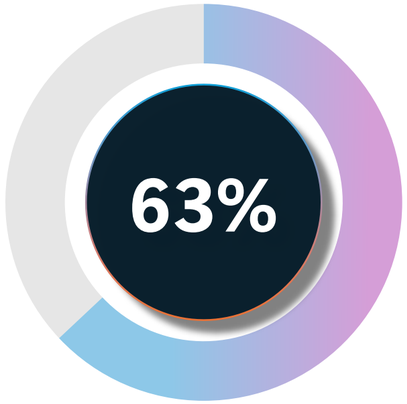
Cybersecurity incidents involving AI surged by more than 56% in 2024[1]

Identification of risky AI use



Of security leaders cited that the identification of risky users based on queries into AI was one of the top AI controls they want to implement[2]

AI governance and risk visibility



Of data breaches stem from inadvertent, negligent or malicious insiders[3]

1. Stanford's 2025 AI Index Report
2. Microsoft data security index 2024 report
3. Microsoft Security Rethinking Security from the Inside Out 2024 report

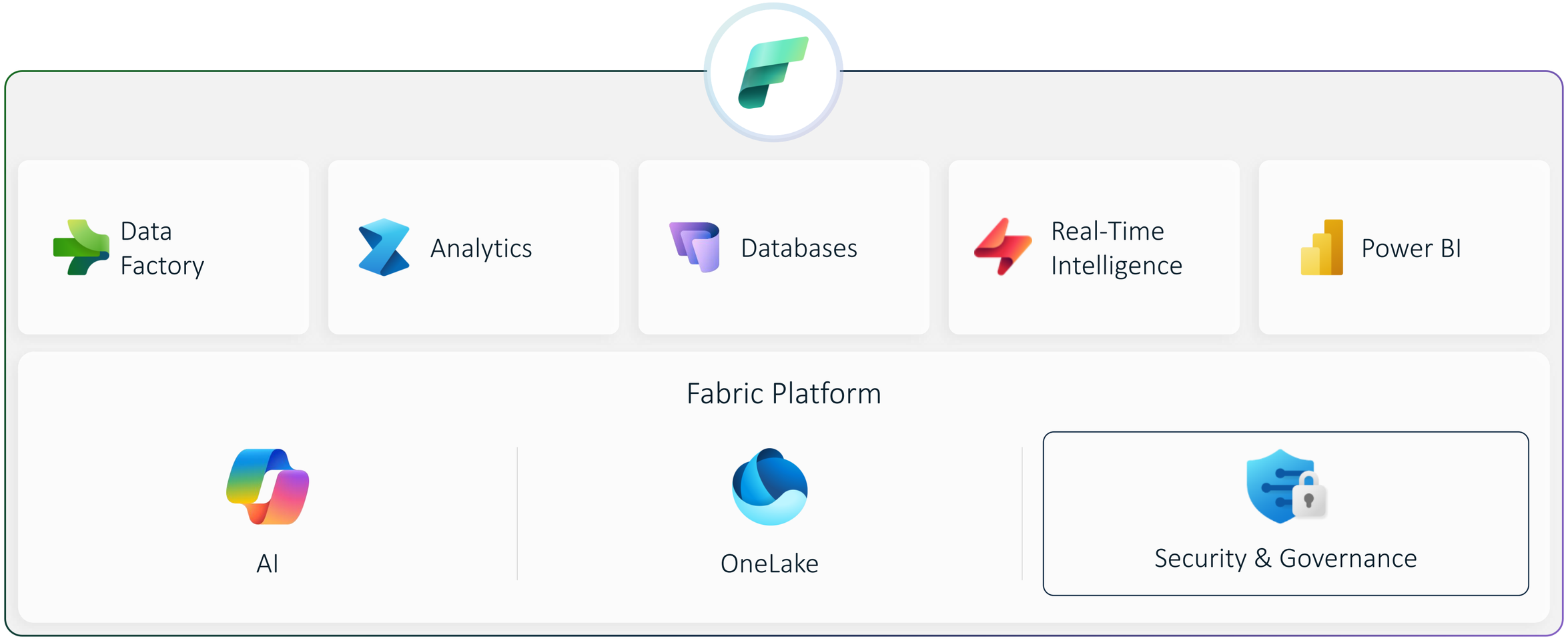
Achieving both goals can prove challenging

Ensuring your data is secure

Fostering a data-driven culture

Microsoft Fabric

The unified SaaS data platform for AI transformation



Gain full visibility and control with industry-leading features

Governance and security features built into Microsoft Fabric

Manage your data estate

- Admin portal
- Tenant and workspace settings
- Metadata scanning
- Capacities
- Domains
- Workspaces

Secure, protect, and comply

- Fabric inbound and outbound security
- Conditional access
- Compute security
- Workspace & item security
- Data encryption
- OneLake security
- Purview sensitivity labeling**
- Purview Data Loss Prevention policies**
- Certificates & standards
- Data residency
- Purview Audit**

Encourage data discovery, trust, and use

- OneLake catalog (Explore tab)
- Endorsement & tags
- Data lineage & impact analysis
- External data sharing
- Metadata curation
- Discover & Reuse
- Purview Data Quality**

Monitor, uncover insights, and act

- OneLake catalog Govern tab
- Monitoring hub
- Workspace monitoring
- Capacity metrics
- Admin monitoring

Fabric metadata

Advanced Govern and secure Fabric data

Microsoft Purview for estate-wide governance and protection

Comprehensive data security

Data Loss Prevention
Information Protection
Insider Risk Management

Federated data governance

Data Discovery
Catalog Management
Health Management

Risk & compliance posture

Purview Audit

MS Apps

- M365, D365
- Power Platform, IoT, PBI ...

Azure

- SQL
- Cosmos DB
- Postgres
- AML
- ADF
- ...

3rd Party

- AWS
- GCP
- SAP
- Teradata
- ...

**Additional Microsoft Purview purchase required

Fabric Policies

Simplify rollout

- Provide admins with granular controls to deploy Fabric according to compliance requirements
- Enable scaling usage incrementally in a secure and controlled manner
- Empower centralized governance controls

Central & consistent platform

- Provide central & consistent controls across Fabric features and workloads through Policies
- Improve developer velocity & quality
- Improve admins satisfaction

Introduce new controls

- Tenant level Network security policies to control OAP, CMK and external data sharing
- Capacity admins resources management with policies over who is allowed to be create specific items in their capacity.
- Granular access controls - define who can do what (Future)

Manage and Govern with Fabric Policies

Coming soon

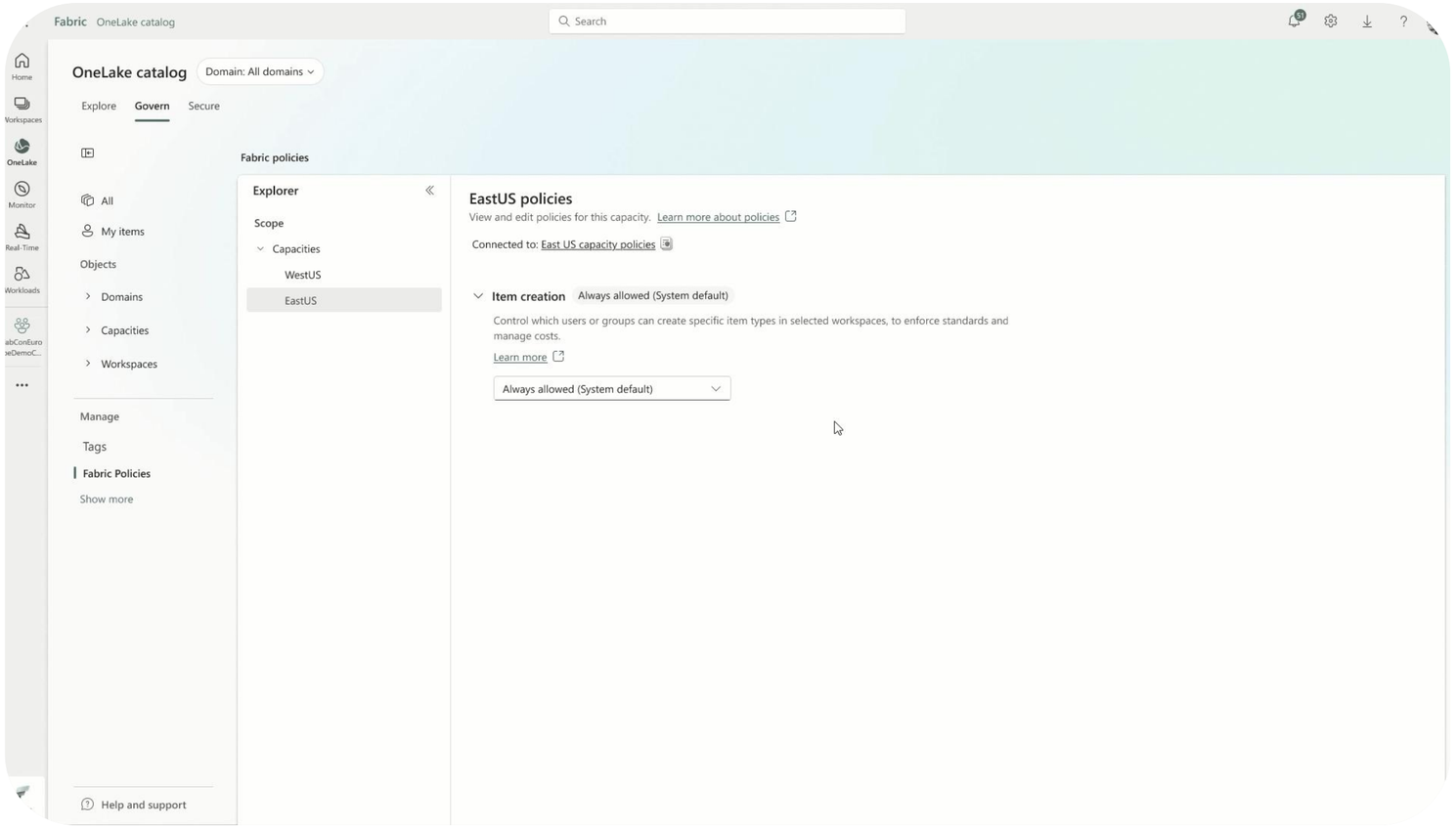
Manage and govern Fabric with centralized policy framework

Create policies to enforce compliance, security and regulation requirements across your tenant

Define granular, attribute-based policies to govern user and system actions.

Manage policies in a single place with the new policies center in the OneLake Catalog

Support policies at scale via APIs and Git



Fabric Policies Demo

Home
Workspaces
OneLake
Monitor
Real-Time
Workloads
FabConEuropeDemoC...
...

OneLake catalog

Domain: All domains

Explore Govern Secure

All
My items
Objects
Domains
Capacities
Workspaces

Manage
Tags
Policies (preview)
Show more

Help and support

Explorer

Scope

- Capacities
  - WestUS
  - EastUS

EastUS policies

View and edit policies for this capacity. Learn more about policies

Connected to: East US capacity policies

Item creation — Advanced

Control which users or groups can create specific item types in selected workspaces, to enforce standards and manage costs.

Learn more

Advanced

Allow all item creation except Notebooks
Last modified 8 hours ago by Kathryn Murphy

All users in this capacity can create any item type except Notebooks.

Allow under certain conditions
If Item type **Is none of** Notebook

+ Add policy rule

Control Plane Access — Not allowed (System default)

Surge Protection — Not allowed (System default)

Disaster Recovery — Advanced

Monitorying for workspaces — Advanced

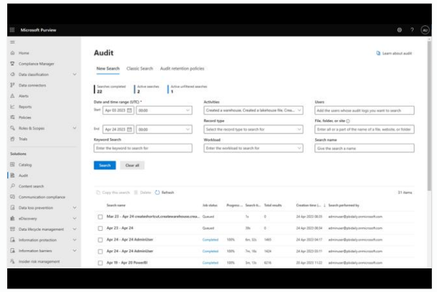
Copilot and other features powered by Azure OpenAI — Advanced

Fabric Policies – What Did We See

1. In OneLake catalog, in the new Policies Center, a capacity admin creates a policy to define which users can create one type of items.
2. They choose that only specific users can create *Notebooks* in specific workspaces.
3. Fabric automatically enforces the rule without manual intervention.
4. When an authorized user attempts to create a Notebook in an unauthorized workspace – the operation is blocked by the Policy.
5. The user sees a message explaining why he couldn't perform the action.
6. Only an action that answers both policy conditions succeeds.

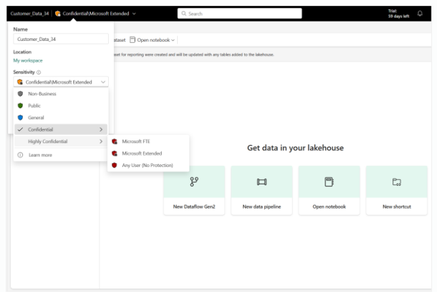
The first policies to roll out will be for **Item Creation** and **Data Sharing** controls, with more coming soon!

Purview Data Security & Compliance integration with Fabric



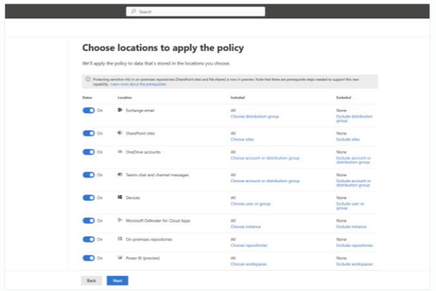
Audit

Log user activities from Microsoft Fabric in MS Purview Audit to support security, forensic, and internal investigations.



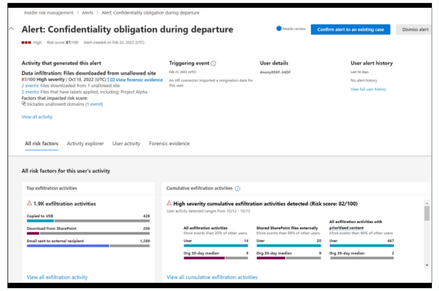
Information protection sensitivity labels & protection policies

Classify sensitive Fabric data using the same sensitivity labels that are used in Microsoft 365—the label and protection travels with the data within Fabric and enforced even when the data is exported to Office.



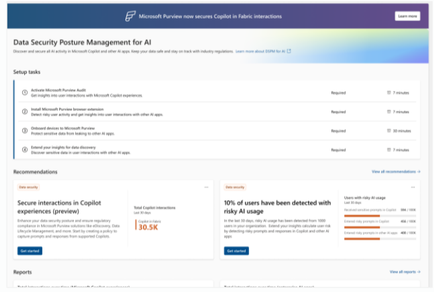
Data loss prevention policies

Automatically detect sensitive data such as PII or SSN in structured data in OneLake and trigger automatic risk remediation actions such as alerts or restrict access.



Insider Risk Management

Ingest audit logs from Fabric in addition to other millions of signals to identify potential malicious or inadvertent insider risks.

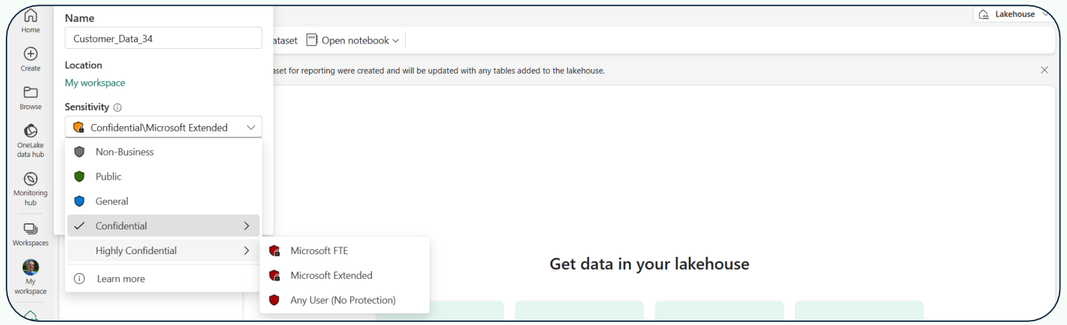


Data Security Posture Management

DSPM provides admins with comprehensive reports on user activities and data interactions in Fabric Copilot and Agents

Additional Microsoft Purview purchase required

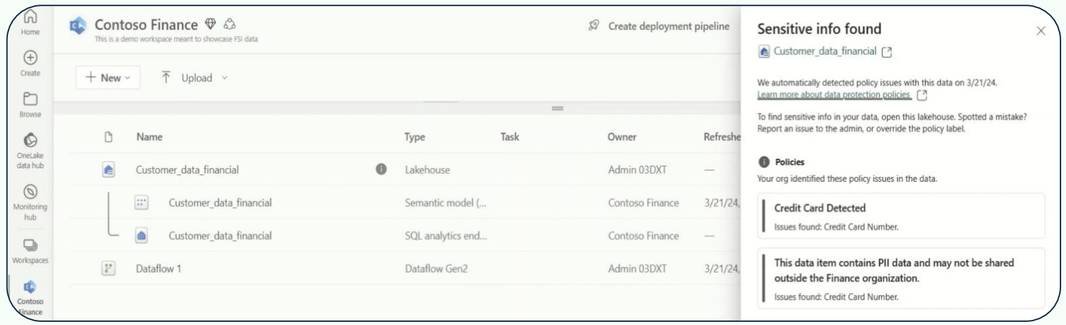
Protect data consistently across your estate with Microsoft Purview



Purview Information Protection labels

Protect Fabric data using the same sensitivity labels used in Microsoft 365—enforced even when the data is exported

Generally available

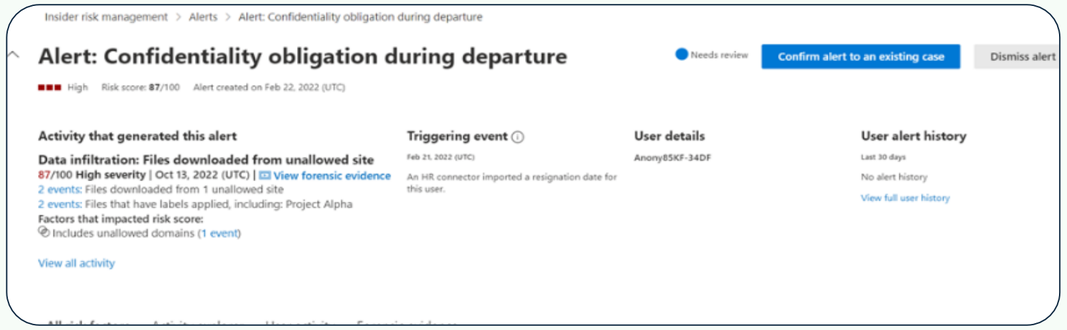


Purview Data Loss Prevention policies

Automatically detect the upload of sensitive data and trigger automatic actions

Public preview	Access restriction to KQL, SQL, Cosmos DBs, and warehouses
General availability	Support for warehouses and Cosmos DB

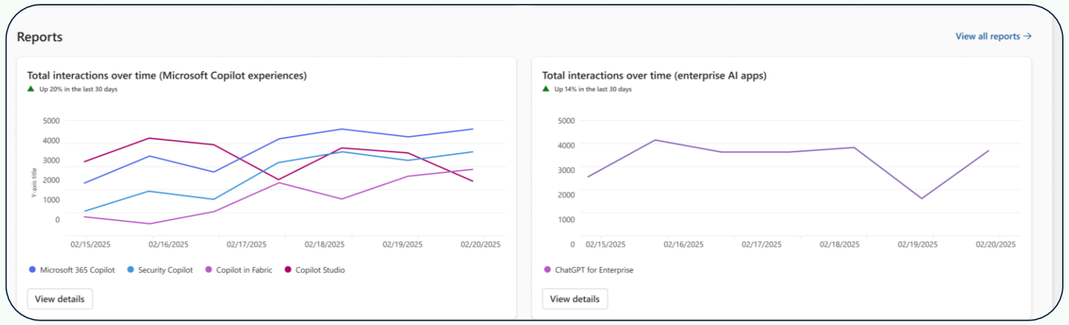
Protect data consistently across your estate with Microsoft Purview



Purview Insider Risk Management

Ingest audit logs from Fabric and millions of other signals to identify malicious or inadvertent risk

General availability	Lakehouse signals & Quick policy for Data Theft
General availability	IRM Pay-as-you-go Usage Report



Purview Data Security Posture Management

Discover risks of data leaks for Copilot in Fabric, Copilot in Power BI, and Fabric data agents usage

Public preview	DSPM monitoring for Fabric Copilots and data agents

Purview Data Loss Prevention for Fabric

Generally Available

Automatically detect and secure sensitive data to meet business, compliance and security needs

Automatic scan to detect sensitive data in OneLake structured data and semantic models

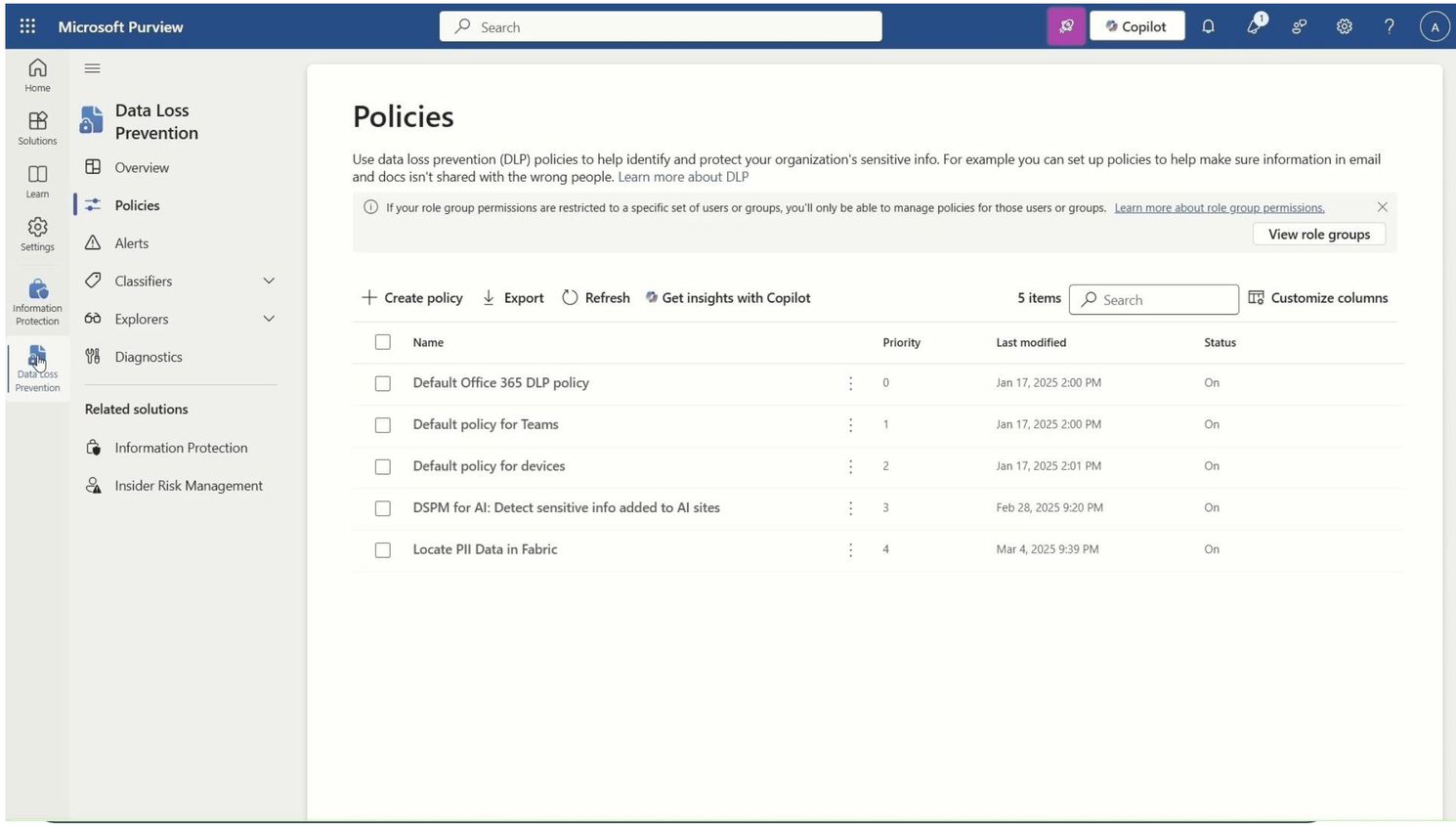
Security policy tip for data owners, security audit and alerts for security admins

Announcing: Restrict access to all structured data in OneLake (PuPr)

SQL, KQL, Cosmos* and Mirrored* DBs

Warehouse

(Lakehouses and Models already in Preview)



Additional Microsoft Purview purchase required

*Cosmos and Mirrored databases coming soon

DLP Restrict Access for KQL DBs in Fabric Demo

Template or custom policy
Name
Admin units
Locations
Policy settings
Policy mode
Finish

Choose where to apply the policy

We'll apply the policy to data that's stored in the locations you choose.

If your role group permissions are restricted to a specific set of users or groups, you'll only be able to apply this policy to those users or groups. Learn more about role group permissions.

View role groups

Protecting sensitive info in on-premises repositories (SharePoint sites and file shares) is now in preview. Note that there are prerequisite steps needed to support this new capability. Learn more about the prerequisites

Location	Scope	Actions
Exchange email	Turn on location to scope	
SharePoint sites	Turn on location to scope	
OneDrive accounts	Turn on location to scope	
Teams chat and channel messages	Turn on location to scope	
Devices	Turn on location to scope	
Instances	Turn on location to scope	

DLP Restrict Access for KQL DB – What Did We See

1. We set up a DLP policy in the Purview portal, and after selecting the condition, we were able to set an action to restrict access when the policy conditions are met.
2. We could have chosen between blocking all users, or blocking all guest users in the tenant, and we chose the latter.
3. When a KQL DB was updated in Fabric, the DLP policy was triggered and it evaluated the KQL database's content.
4. Since we uploaded sensitive information, the policy found a match, and the item became restricted to guest users.
5. The indications on the item (icon, hover card, side panel and policy tips) display that users are restricted from the item, for visibility and caution of the users who still regain access.
6. Workspace admins can take action: override the policy or report an issue to the security admin.

Security Observability (OneLake Catalog – Govern)

Generally Available

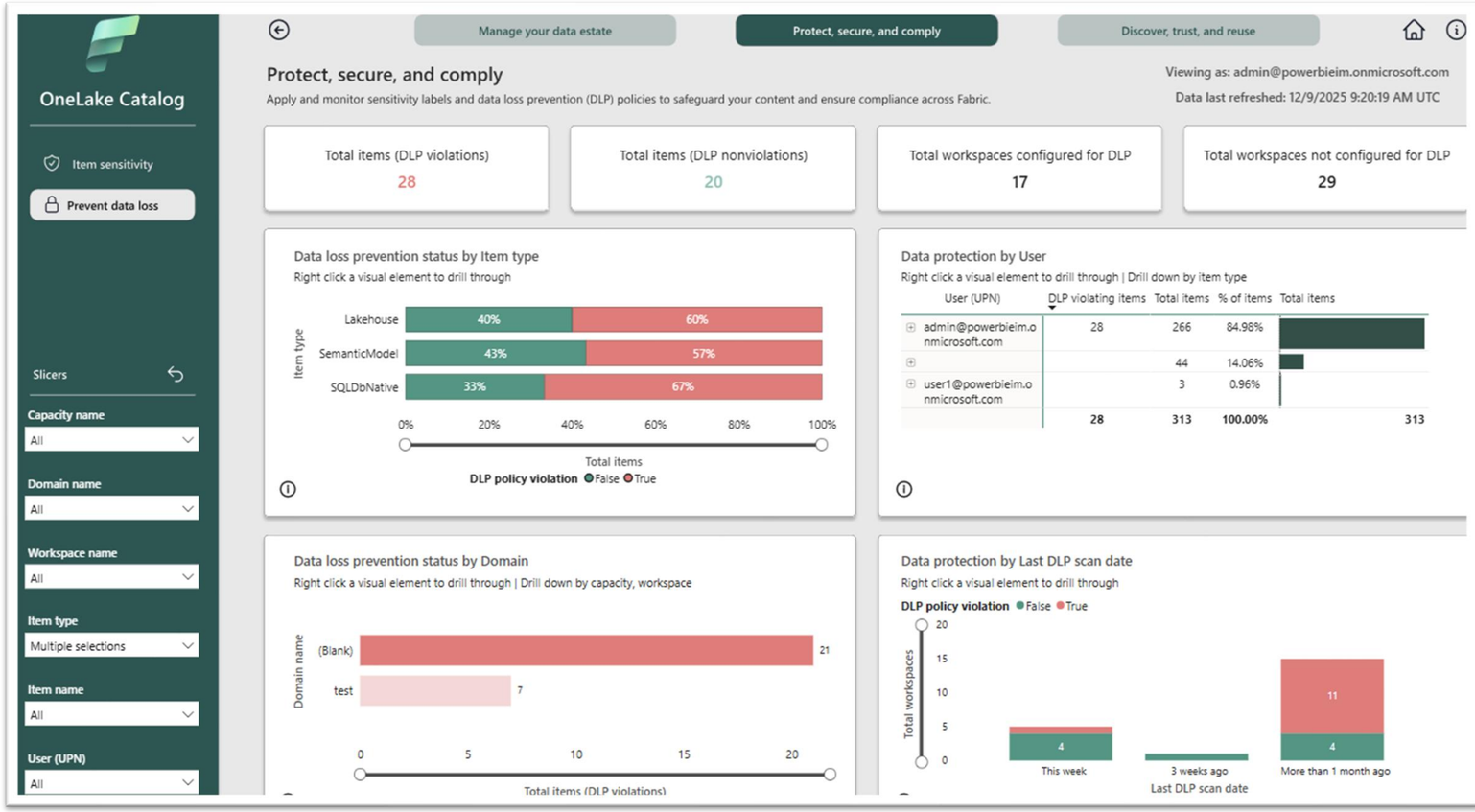
Learn about your data so you can protect it better

Insights can now be found side-by-side with your data in **OneLake catalog - Govern**

Discover where sensitive data is in your organization, set the label coverage goal and track it

Track DLP policies activities coverage

View your Fabric security insights directly in **Purview portal**



Insider Risk Management for Fabric

Generally Available

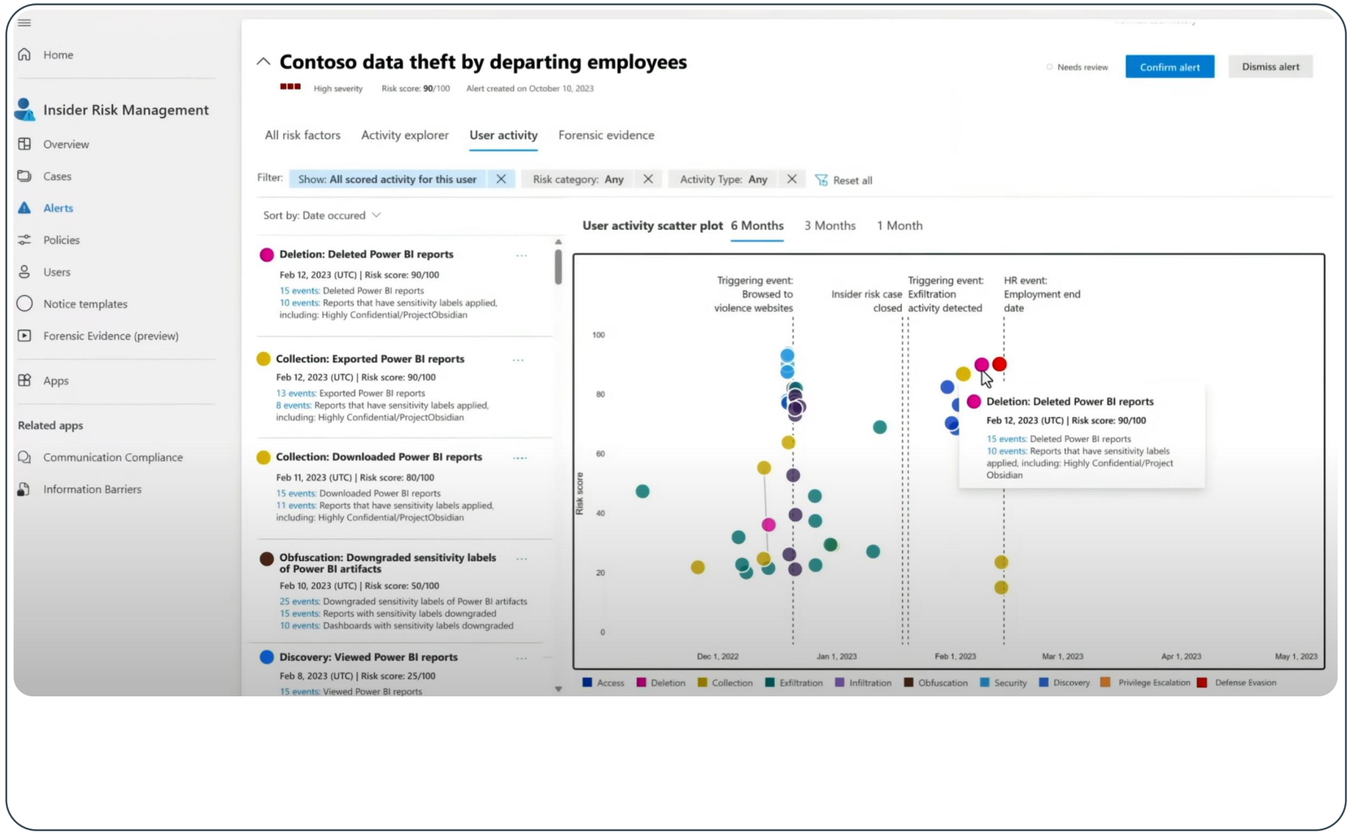
Identify potential malicious or inadvertent insider risk

Ingest audit logs from Fabric in addition to other millions of signals

Detect and investigate malicious and inadvertent activities in your organization based on your organization's compliance standards.

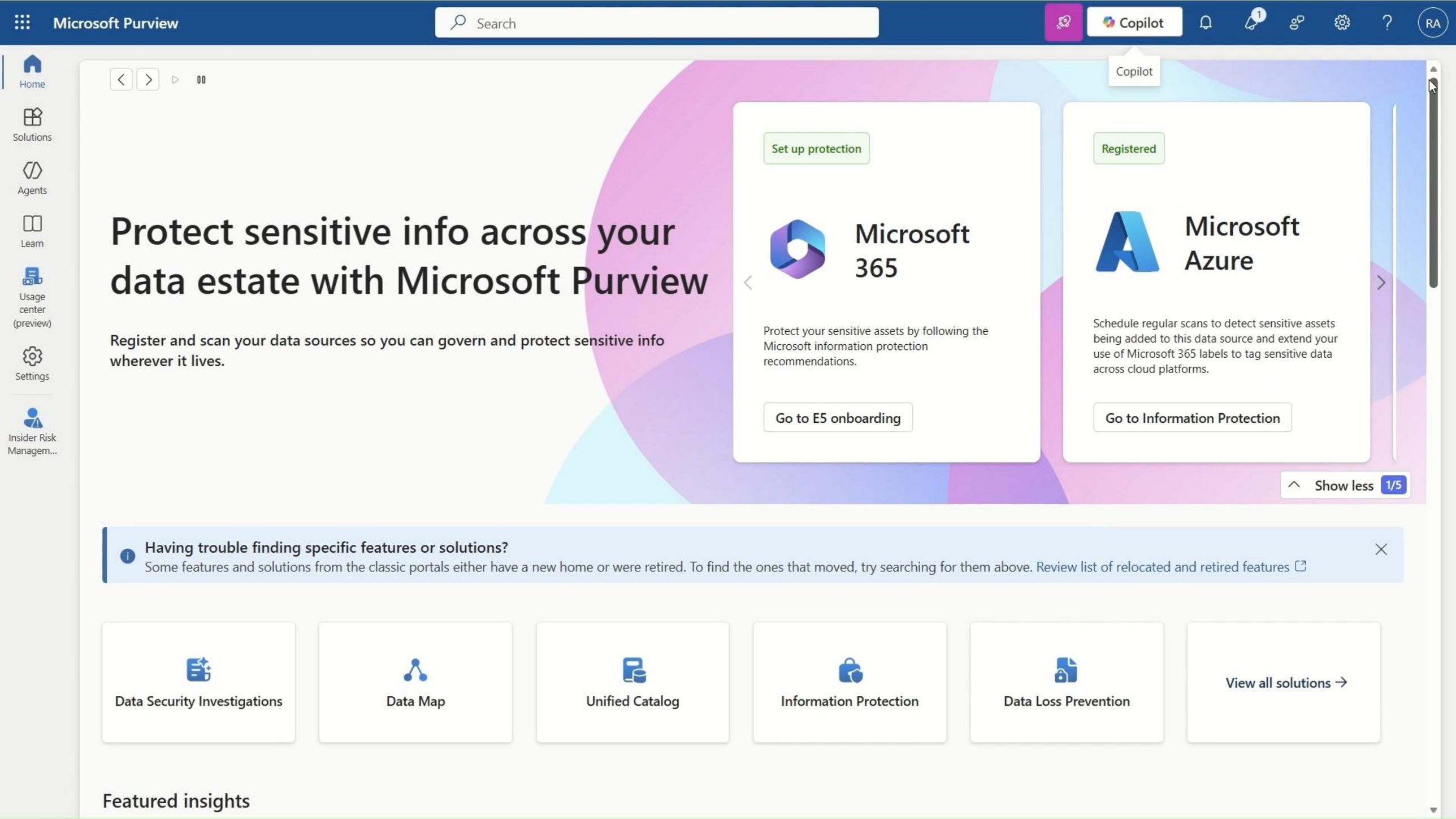
Announcing:

- New signals from Lakehouses
- Quick IRM creation for Fabric
- And PAYG usage report



Additional Microsoft Purview purchase required

Insider Risk Management for Fabric Demo


Microsoft Purview
Search
Copilot
RA
Copilot
Home
Solutions
Agents
Learn
Usage center (preview)
Settings
Insider Risk Managem...
Protect sensitive info across your data estate with Microsoft Purview
Register and scan your data sources so you can govern and protect sensitive info wherever it lives.
Set up protection
Microsoft 365
Protect your sensitive assets by following the Microsoft information protection recommendations.
Go to E5 onboarding
Registered
Microsoft Azure
Schedule regular scans to detect sensitive assets being added to this data source and extend your use of Microsoft 365 labels to tag sensitive data across cloud platforms.
Go to Information Protection
Show less 1/5
Having trouble finding specific features or solutions?
Some features and solutions from the classic portals either have a new home or were retired. To find the ones that moved, try searching for them above. Review list of relocated and retired features
Data Security Investigations
Data Map
Unified Catalog
Information Protection
Data Loss Prevention
View all solutions
Featured insights

Insider Risk Management for Fabric – What Did We See

1. In Insider Risk Management you can create a quick policy for Data Theft in Fabric in one click, and the policy is created.
2. When creating custom policies and selecting the signal you want to track, there are new Lakehouse indicators under the Power BI indicators, that allow you to create broader user profiles in IRM.
3. Once you review the reporting of an IRM policy, you can see the Lakehouse signals along other products, and you can hover on a specific signal to see its details.
4. Admins can monitor their IRM processing units' distribution through a new Pay-as-you-go usage report, to better understand the cost of each product.

Data Risk Assessment

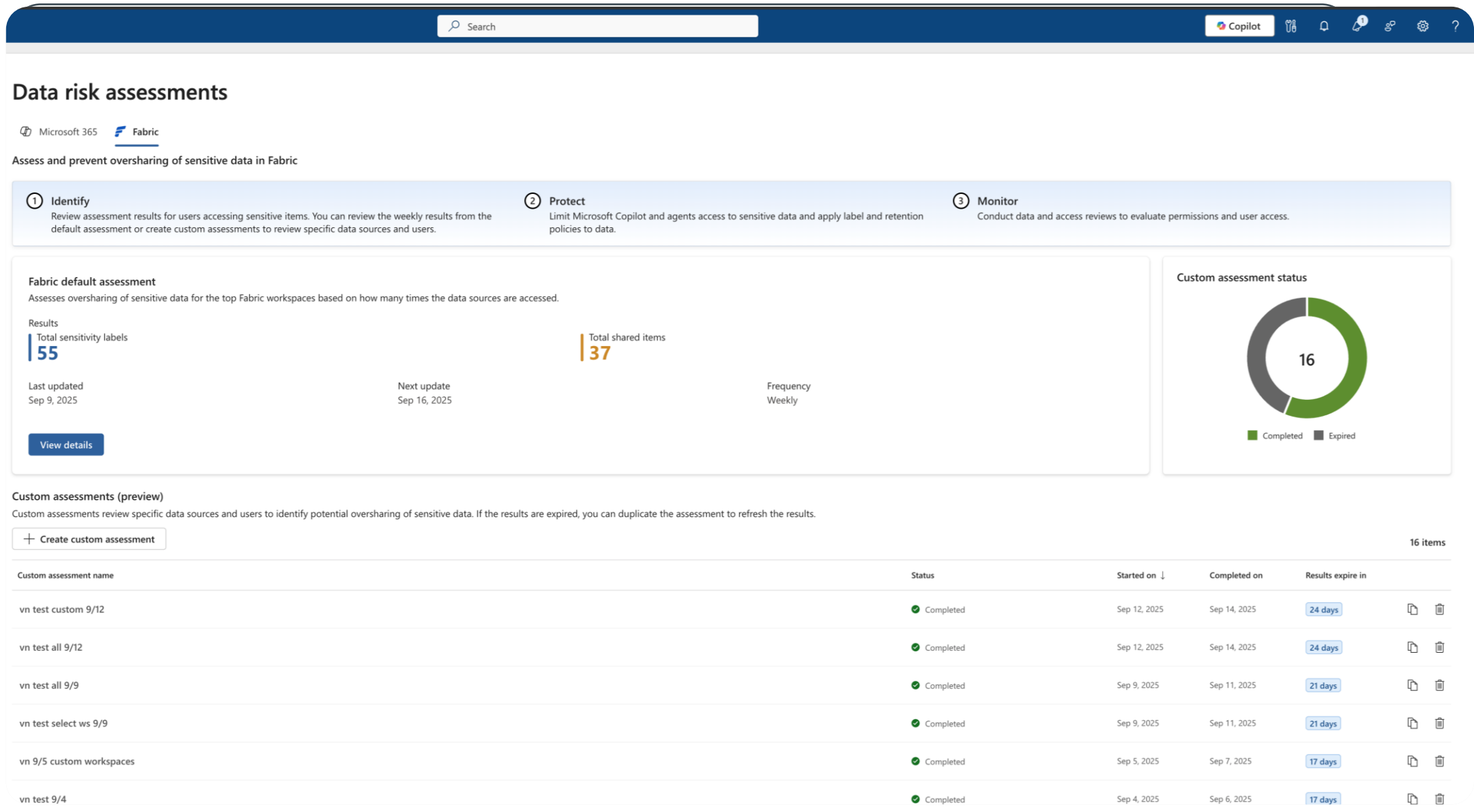
Insight into sensitive data exposure and oversharing risks, enabling targeted risk reduction

Scan your Fabric workspaces to discovering overshared data

Identifying what data is most at risk of leakage

Security admins can take action to remediate risks

No additional licensing required!



Data Risk Assessment for Fabric Demo

Home
Solutions
Agents
Learn
Settings
DSPM for AI

Data risk assessments

Microsoft 365 | Fabric

Assess and prevent oversharing of sensitive data in Fabric

1 Identify
Review assessment results for users accessing sensitive items. You can review the weekly results from the default assessment or create custom assessments to review specific data sources and users.

2 Protect
Limit Microsoft Copilot and agents access to sensitive data and apply label and retention policies to data.

3 Monitor
Conduct data and access reviews to evaluate permissions and user access.

Fabric default assessment

Assesses oversharing of sensitive data for the top Fabric workspaces based on how many times the data sources are accessed.

Results

Total sensitivity labels
55

Total shared items
37

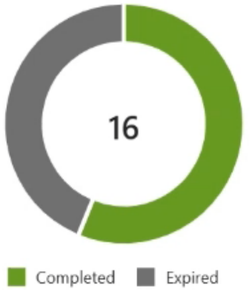
Last updated
Sep 9, 2025

Next update
Sep 16, 2025

Frequency
Weekly

View details

Custom assessment status



Custom assessments (preview)

Custom assessments review specific data sources and users to identify potential oversharing of sensitive data. If the results are expired, you can duplicate the assessment to refresh the results.

+ Create custom assessment

16 items

Custom assessment name	Status	Started on ↓	Completed on	Results expire in
vn test custom 9/12	Completed	Sep 12, 2025	Sep 14, 2025	24 days
vn test all 9/12	Completed	Sep 12, 2025	Sep 14, 2025	24 days
vn test all 9/9	Completed	Sep 9, 2025	Sep 11, 2025	21 days
vn test select ws 9/9	Completed	Sep 9, 2025	Sep 11, 2025	21 days

Data Risk Assessment for Fabric – What Did We See

1. DSPM for AI's default assessment for Fabric **scans top accessed workspaces** to look for overshared items.
2. The report shows Sensitive Info Types (SIT) and labeled items in those workspaces, as well as items that have been widely accessed by users.
3. Each workspace in the report produces a side panel with additional information.
4. The Protect tab prompts users to take immediate action, such as configuring new DLP policies or setup default labels for the tenant, to increase the security posture.
5. The Monitor tab allows you to review workspace access details and start an access review in Microsoft Entra.
6. Custom risk assessments allows to choose specific workspaces to run the scan on, to produce similar insights.

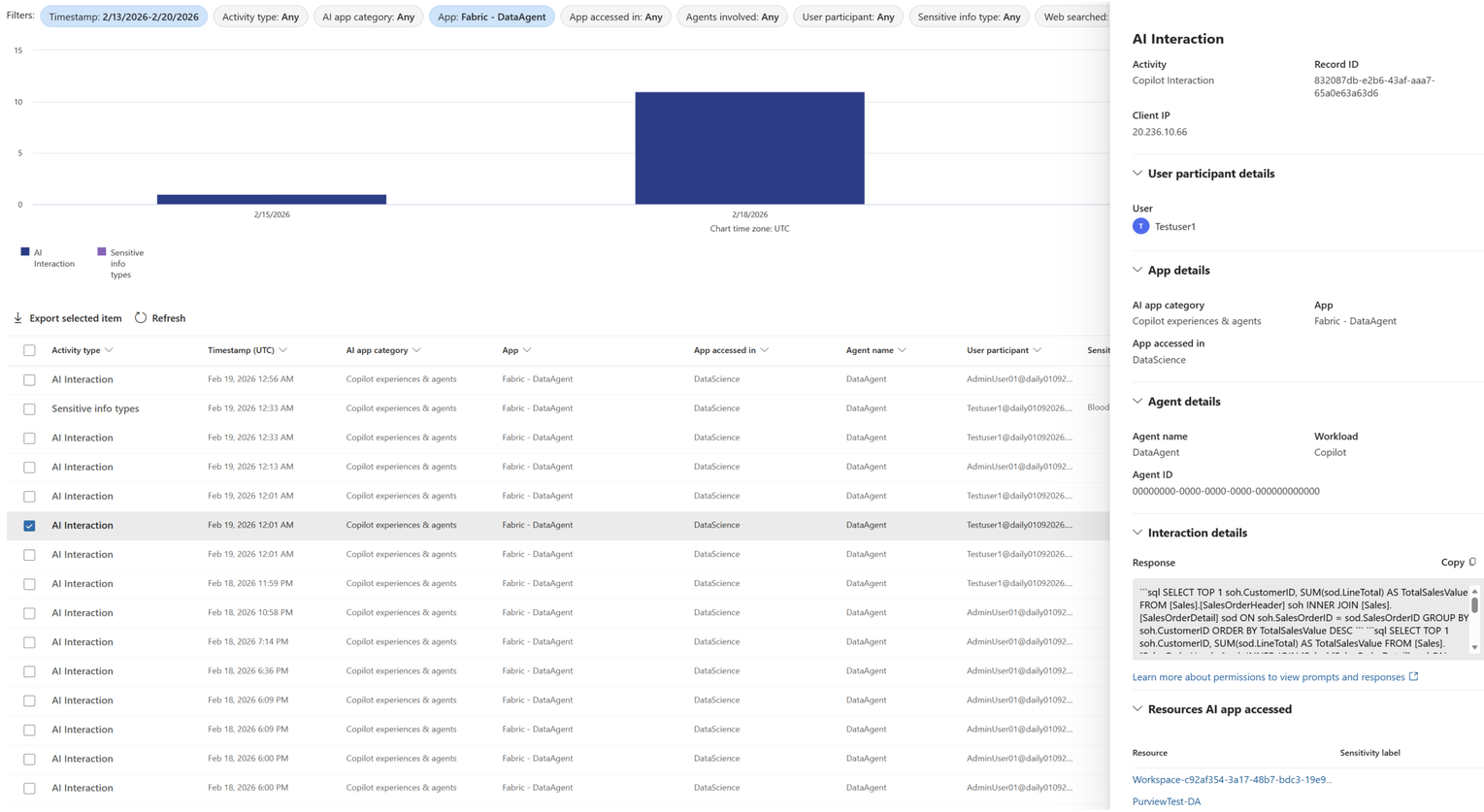
Data Security Posture Management for AI in Fabric

Comprehensive reports on user activities and data within Fabric Copilots and Data Agents

Whenever a user performs an action within **Fabric Copilot or Data Agent, an audit log** entry is created

Protect your Fabric data **consistently**, which means **your AI** as well

Activate AI responsibly with monitoring and reports



Additional Microsoft Purview purchase required

Generally Available

Purview Information Protection for Fabric

Classify and protect sensitive data as it travels across Azure, Microsoft Fabric and Office

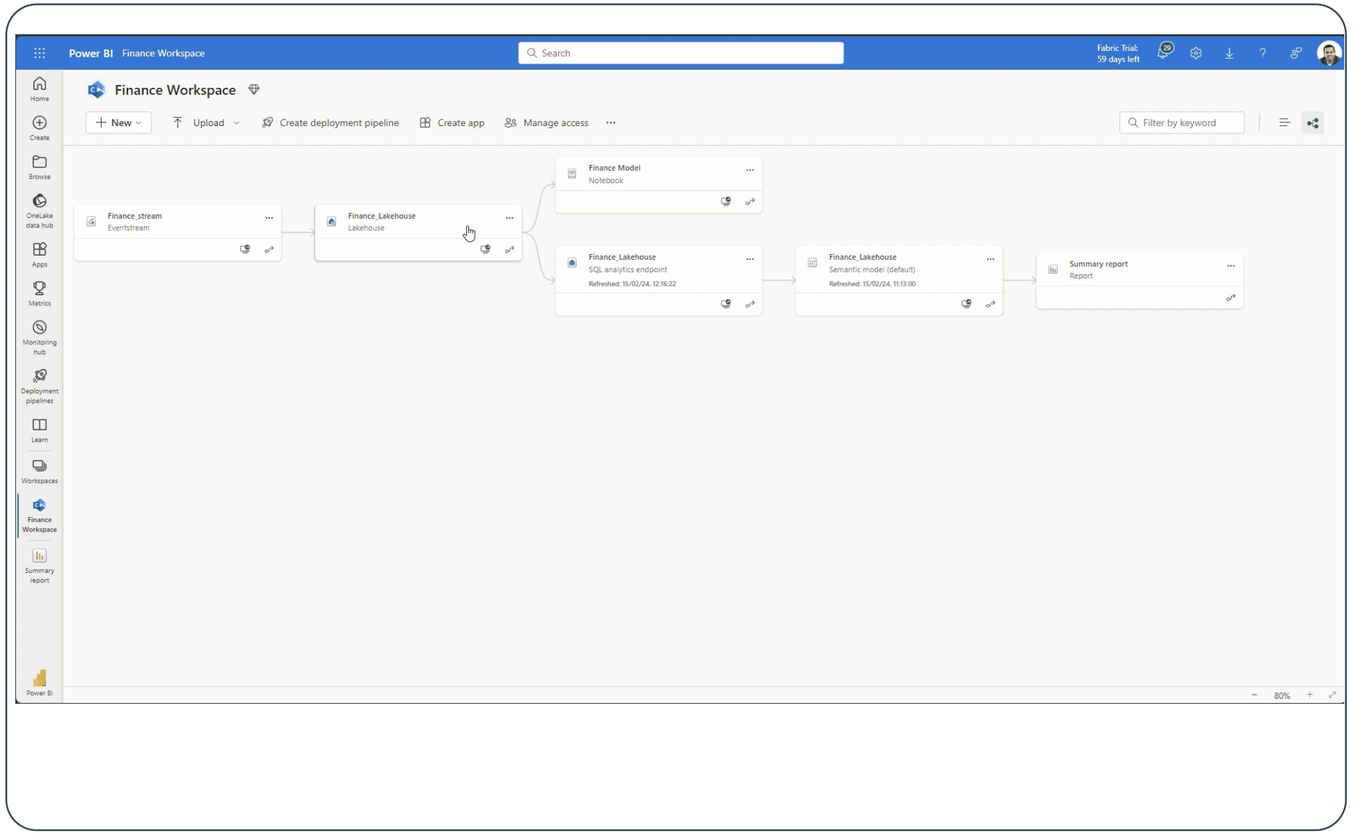
Label data using the same sensitivity labels used in Office, SharePoint, and Azure

Label based **data protection** providing dynamic access controls

Label and protection follow the data within Fabric and to Office, Power BI and PDF files

Enforce labeling with mandatory and default label policies, also at domain level

Labels available in Get, List ,Create and Update **public APIs**



*Protection policies don't yet support Power BI reports and dashboards

Additional Microsoft Purview purchase required

MIP Sensitivity Labels End-to-End Demo

MIP Demo

MIP Sensitivity Labels End-to-End – What Did We See

1. Users can manually apply sensitivity labels to items in Fabric.
2. Labels are automatically inherited to downstream items in Fabric; when you label a data item, all items reading data from it are labeled as well.
3. When a Protection Policy is applied on a label – it restricts access from users who are not in the policy, even if they previously had permissions to an item.
4. The label – and its protection – travel with the data when it leaves Fabric. Exported items maintain the label and the access restriction on Office files.

Best Practices for Enterprises

Deploying Security in Microsoft Fabric: Enterprise Best Practices

A layered approach that accelerates adoption of Fabric + Purview security

1) Establish the security foundation

- Use Entra ID + Conditional Access for consistent identity controls
- Harden network paths: Private Link/managed VNets + managed private endpoints
- Design workspace boundaries (Dev/Test/Prod, BU separation) with least privilege *(recommended practice)*
- Prefer groups over individuals for role assignments (repeatable operations) *(recommended practice)*

2) Apply fine-grained access controls

- Use workspace roles + item permissions to prevent oversharing
- Add RLS/OLS/CLS where needed for “same dataset, different views” scenarios
- Document ownership (data owner vs. security admin) and escalation paths *(recommended practice)*

Deploying Security in Microsoft Fabric: Enterprise Best Practices

A layered approach that accelerates adoption of Fabric + Purview security

3) Standardize classification & policy

- Adopt sensitivity labels; consider mandatory and default labeling for coverage
- Use Protection Policies to enforce org-wide access based on labels
- Use Purview DLP for Fabric to detect sensitive info and drive alerts/policy tips
- Add DLP “Restrict access” for high-risk items (e.g., internal data, PII)

4) Monitor, respond, and drive adoption

- Centralize visibility: Purview Audit + alerting for Fabric activities
- Extend to Insider Risk Management using Fabric signals for investigations
- Start with 1–2 test workspaces before expanding; publish a playbook for your users *(recommended practice)*
- Ensure AI interactions are monitored with DSPM for AI (Copilot and data agents) to unlock faster adoption *(recommended practice)*

End-to-end security in Microsoft Fabric

Secure by default with Microsoft’s industry-leading protection

Faster AI

Lower Risk

Trusted Insights

Discover risks and protect data consistently across your entire estate with Microsoft Purview

Summary

1. AI transformation is affecting the way we should think about protecting data
2. Microsoft Fabric makes your organization AI-ready by design, so that you can focus on acceleration
3. Purview’s native integration with Fabric brings estate-wide security to protect your data at industry highest standards

THANK YOU!

Microsoft Customer Connection Program

Microsoft Purview MS Learn Documentation

Try Purview Unified Catalog

Microsoft Purview Partner Training Resources

Try Microsoft Fabric

Try Purview Data Security

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

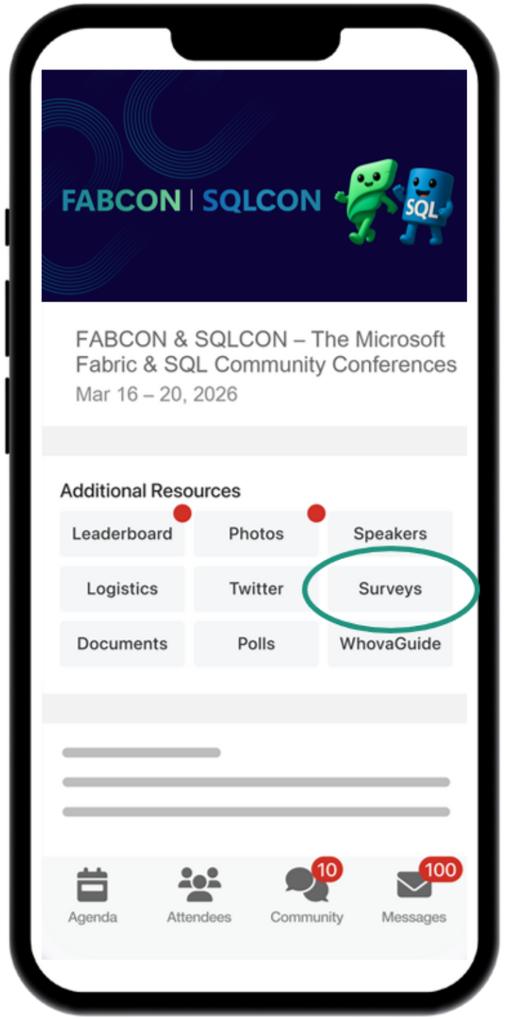
Join the SQL User Panel

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!



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