Microsoft Fabric

#FABCONSQLCON2026

FABCON
Microsoft Fabric
COMMUNITY CONFERENCE

SQLCON
Microsoft SQL
COMMUNITY CONFERENCE

ATLANTA MARCH 16 - 20, 2026

Microsoft Purview Data Security Protections in the Age of AI

“Insert location”

Anton Fritz

Principal PM Manager,
Microsoft Fabric

Sri Kutuva

Senior PM,
Microsoft Purview

Agenda

01 Current Data and AI landscape

02 What is Purview and Fabric?

03 How Purview features solve Fabric security scenarios

04 Demos

90%

of world's data has been
created in the past 2 years

Source: BSA | The Software Alliance Report Annual Report, 2025

Challenges with AI

#1 Priority for CISOs is securing enterprise AI adoption [1]

25% Of CISOs reported experiencing an AI-generated attack within the past 12 months

75% Of knowledge workers already using AI at work (doubled in the past 6 months)[2]

[1] CISO_Survey 2025_v10.pdf | [2] Work Trends Index,

Making data security essential for data in your data platforms

Data security incidents are widespread

83%

Of organizations experience more than one data breach in their lifetime[1]

Insider risk is significant

20%

Insiders account for 20% of data breaches, adding to costs[2]

Data leaks and oversharing are top of mind concerns

80%

Of leaders cited leakage of sensitive data as their main concern around adopting Generative AI[3]

Microsoft Purview

A unified approach to secure and govern your data

Microsoft Purview

Integrated solutions to secure & govern the world's data

Data security

Secure data across its lifecycle, wherever it lives

Data Loss Prevention

Insider Risk Management

Information Protection

Data Security Posture Management

Data Security Investigations

Unstructured & Structured data

Data governance

Confidently activate your data & accelerate time to insights

Unified Catalog:

Data Discovery

Curation

Data Quality

Data Health

Master Data Management

Traditional and AI generated data

Data compliance

Manage critical risks and regulatory requirements

Compliance Manager

eDiscovery and Audit

Communication Compliance

Data Lifecycle Management

Records Management

Microsoft and Multi-cloud

Shared platform capabilities

AI-based efficiency, Data Map, Classification, Labels, Audit Logs, Policies, Data Connectors

Purview + Fabric

Microsoft Fabric

The unified data platform for AI transformation

- Data Factory
- Analytics
- Databases
- Real-Time Intelligence
- Power BI

Fabric Platform

- AI
- OneLake
- Governance

Act on your trusted data with security and governance

Reshape how you access, manage, and act on data and insights by connecting every data source and analytics service together in Fabric

Seamlessly secure and confidently activate your data estate with security, governance and compliance solutions

Manage and use your Fabric data for data workloads and projects	Integrated security and governance	Enterprise oversight

End-to-end security in Microsoft Fabric

Secure by default with Microsoft's industry-leading protection

Always-on network security

Granular access management & storage

Standards and data residency compliance

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

Purview supports your Fabric personas

Tenant admins

Workspace and capacity admins

Data owners and consumers

Purview supports your Fabric personas

Tenant admins

Workspace and capacity admins

Data owners and consumers

Microsoft Purview

Comprehensive solution to discover, protect, and govern your data in Fabric

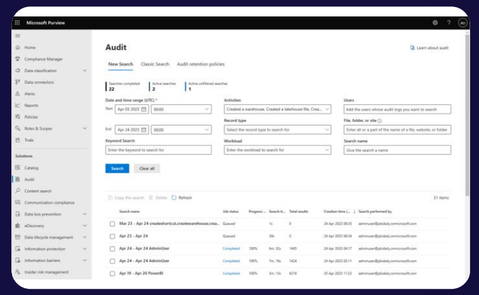
Problem

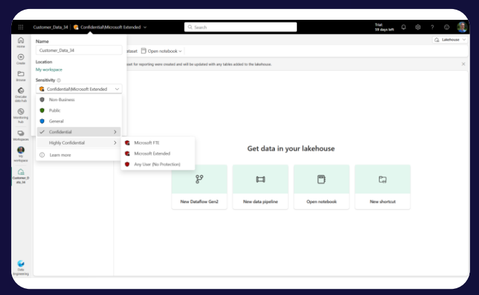
1. Data oversharing and leakage in Fabric

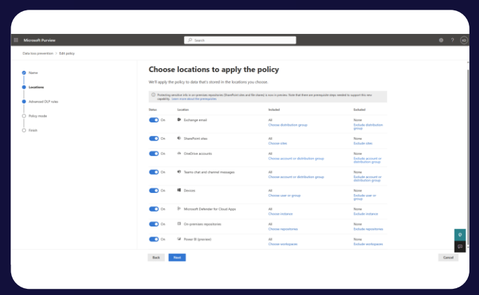
Solutions

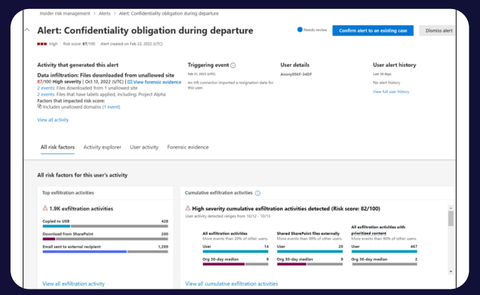
1. Discover and identify insider risks
2. Define and apply policies to sensitive data to prevent data leakage
3. Secure and Govern AI in Fabric

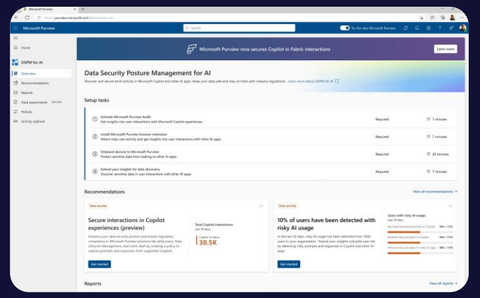
Purview Data Security & Compliance integration with Fabric











Audit

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

Information protection sensitivity labels and 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

Discover and identify risks in Fabric with Purview

Generally Available

Insider Risk Management extends to Lakehouse indicators

Security admins can create a data theft policy to detect Fabric data exfiltration in single click

Security admins can check the PAYG usage (processing units) across different workloads, sub workloads & activities through the usage report

- Policy template
- Name and description
- Users and groups
- Content to prioritize
- Triggering event
- **Indicators**
- Finish

Generative AI apps (3/5 selected) New

Microsoft Fabric indicators (14/14 selected) New

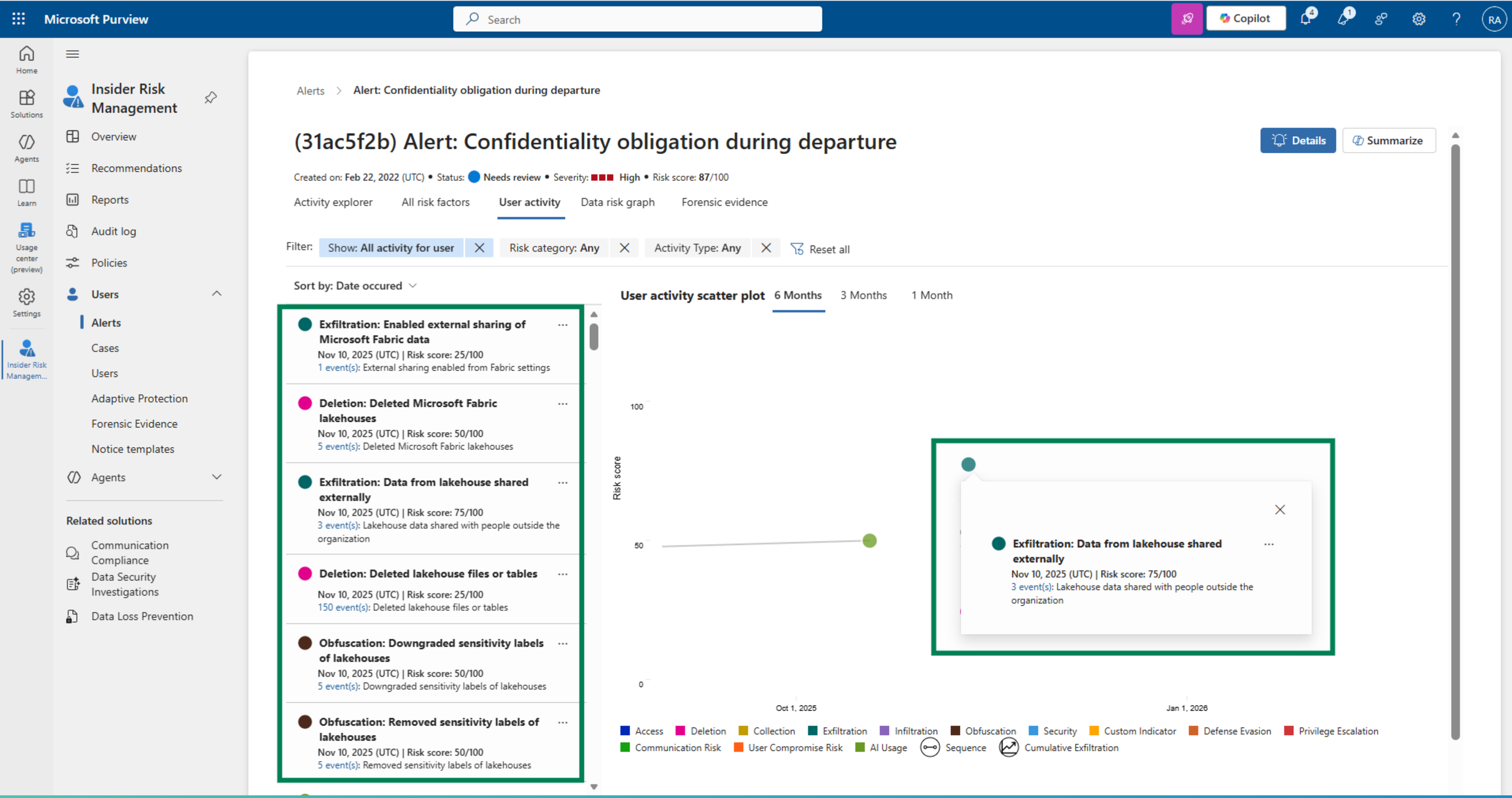
Power BI indicators (8/8 selected) New

- [x] Select all
- [x] Viewing Power BI reports
- [x] Downloading Power BI reports
- [x] Exporting Power BI reports
- [x] Removing sensitivity labels from Power BI artifacts
- [x] Downgrading sensitivity labels from Power BI artifacts
- [x] Deleting Power BI reports
- [x] Deleting Power BI dashboards
- [x] Deleting Power BI semantic models

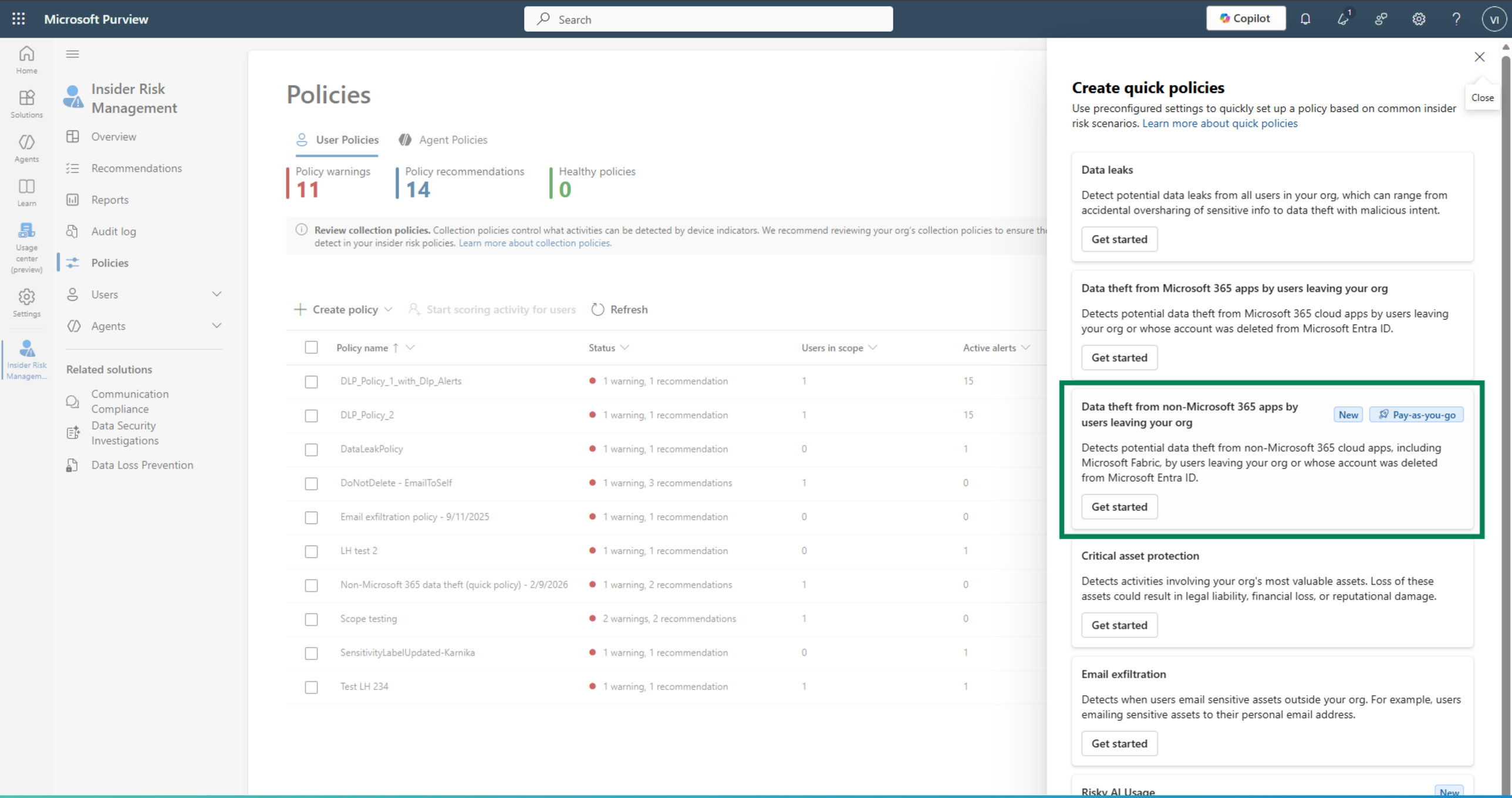
Lakehouse indicators (preview) (6/6 selected) New

- [x] Select all
- [x] Enabling external sharing of Microsoft Fabric data
- [x] Deleting Microsoft Fabric lakehouses
- [x] Sharing lakehouse data with people outside the organization
- [x] Deleted lakehouse files or tables
- [x] Downgrading sensitivity labels of lakehouses
- [x] Removing sensitivity labels of lakehouses

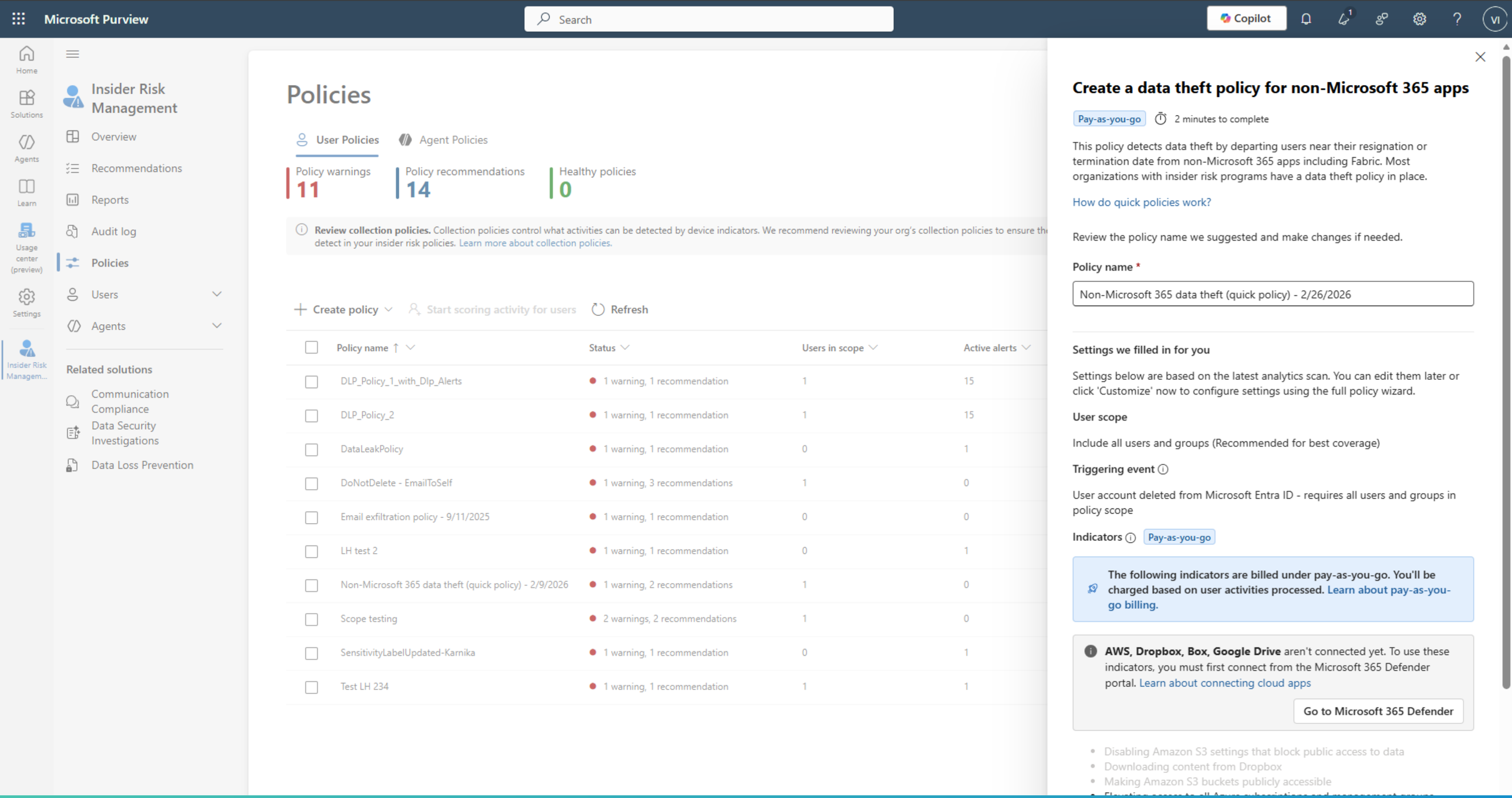
Security admins can also customize the policy to detect more activities from Power BI & Lakehouse



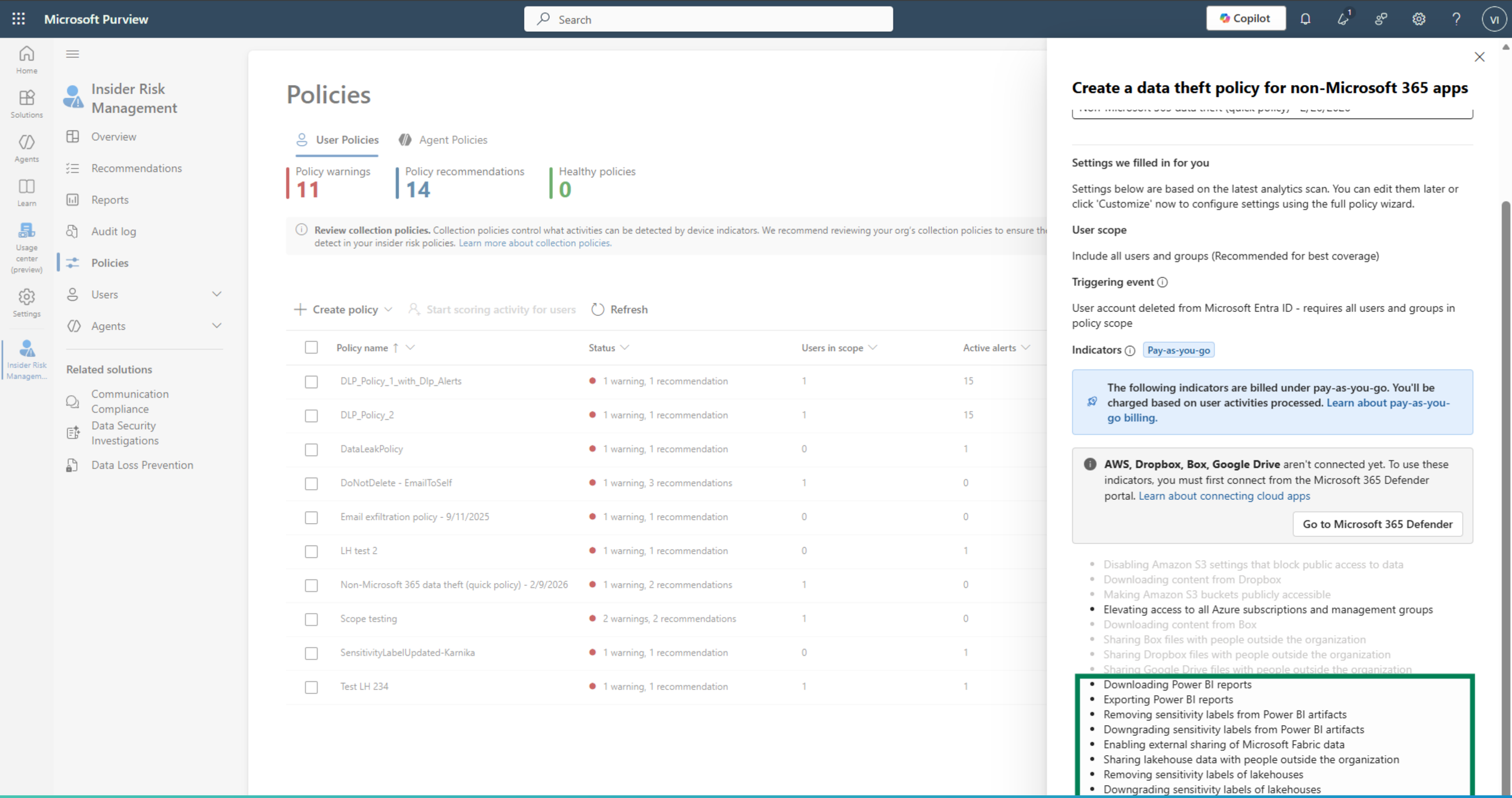
Security investigator finds insights from user activities across Fabric workloads, all at one place!



Security admins can create a data theft policy to detect Fabric data exfiltration in single click



Security admins can create a data theft policy to detect Fabric data exfiltration in single click



Security admins can create a data theft policy to detect Fabric data exfiltration in single click

Home
solutions
Learn
Settings
Insider Risk Management

Insider Risk Management
Overview
Recommended actions
Alerts
Cases
Policies
Users
Reports
Forensic evidence
Adaptive protection (preview)
Notice templates
Audit log
solutions

Related
Communication compliance
Data Loss Prevention
Information barriers

Pay-as-you-go usage report

Understand the usage trends of your pay-as-you-go capabilities in Insider Risk Management. Learn more

Last updated on: 09/07/2025

Get to know how much it might cost to run consumption based insider risk indicators for newly added indicators. Go to cost estimator

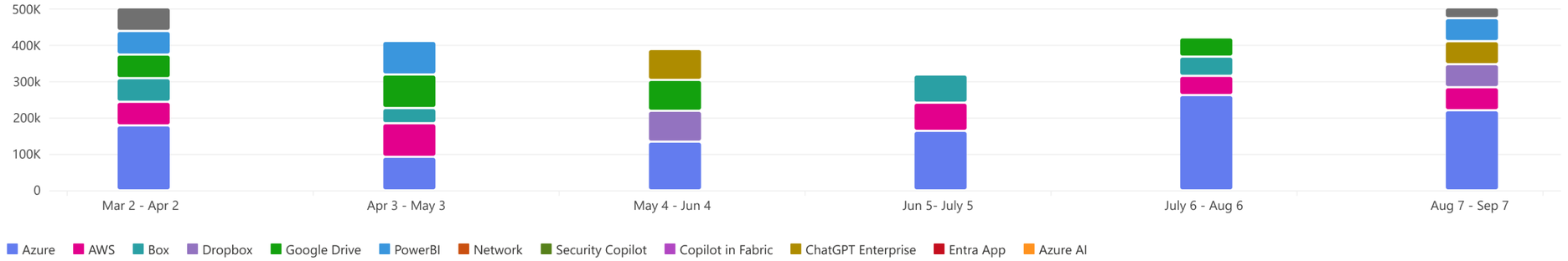
Workload: All | Subworkload: All | Activities: All | Policies: All | Date range:: This month | Add filter | Reset all | Insights & Action | Export as CSV

Total DSPUs used	No: of paid indicators with usage	Avg. DSPUs used per day
1.2M July 1-30, 2025	5 ↑ 28%	40K ↑ 12%

Data security processing units (DSPU) usage across categories

See how data security processing units are consumed by each pay-as-you-go workload.

Weekly | Monthly

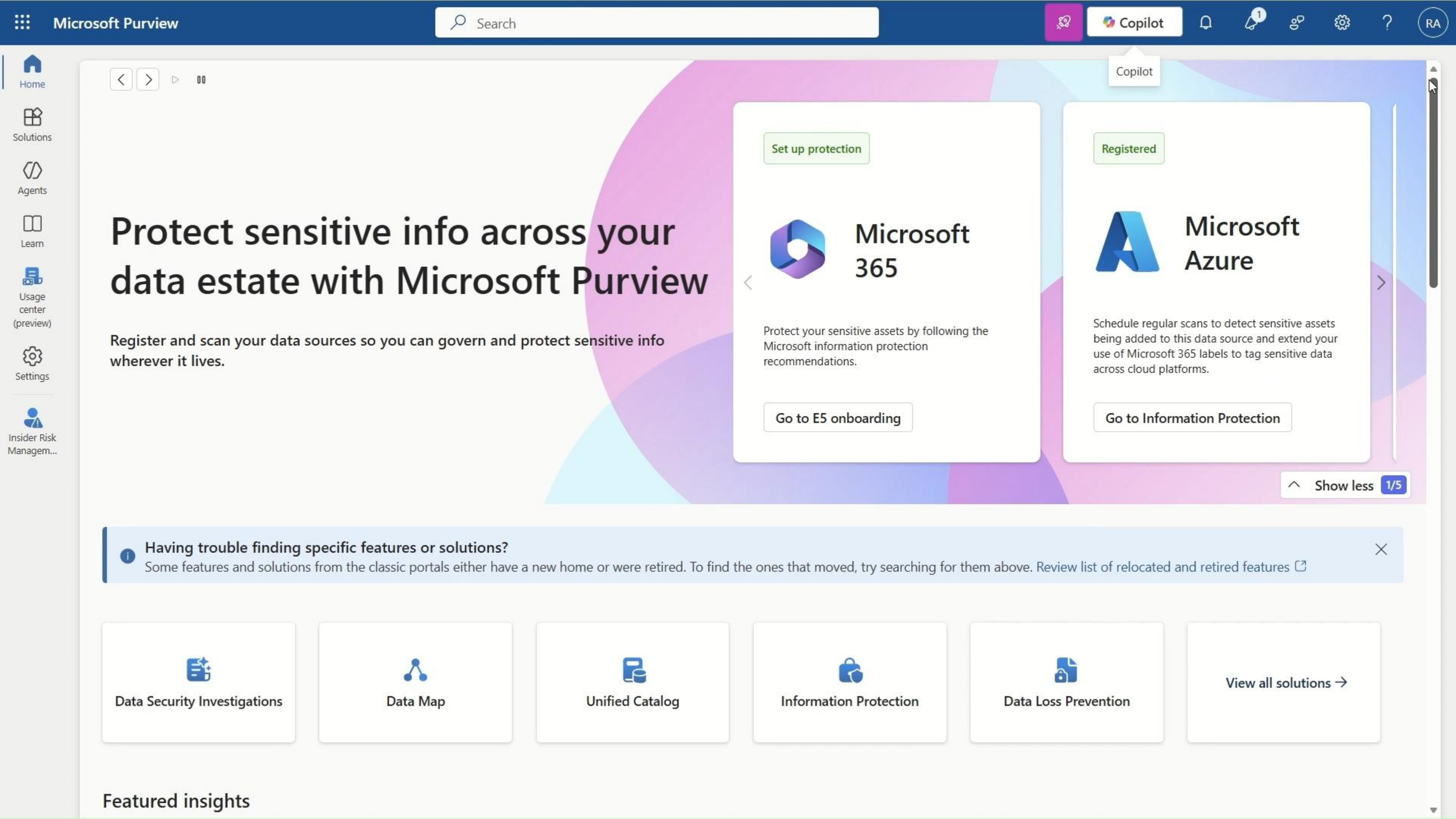


Usage breakdown by activity

20 items | Search by keyword

Date	Caused by	Workload	Subworkload	Activities	Policies	DSPUs used	Current status	
09/07/2025	Indicators	Cloud storage	Box	Downloading content f...	Marketing Data Leaks, I...	163 ↑ 12%	Active	View details
09/07/2025	Indicators	Microsoft Fabric	Power BI	Downgrading sensitiviti...	General Data Leaks - Gl...	84 ↑	Active	View details
09/07/2025	Indicators	Cloud storage	Box	Downloading content f...	Marketing Data Leaks, I...	21 ↓ -8%	Paused	View details

Security admins can check the PAYG usage (processing units) across different workloads, sub workloads & activities through the usage report


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

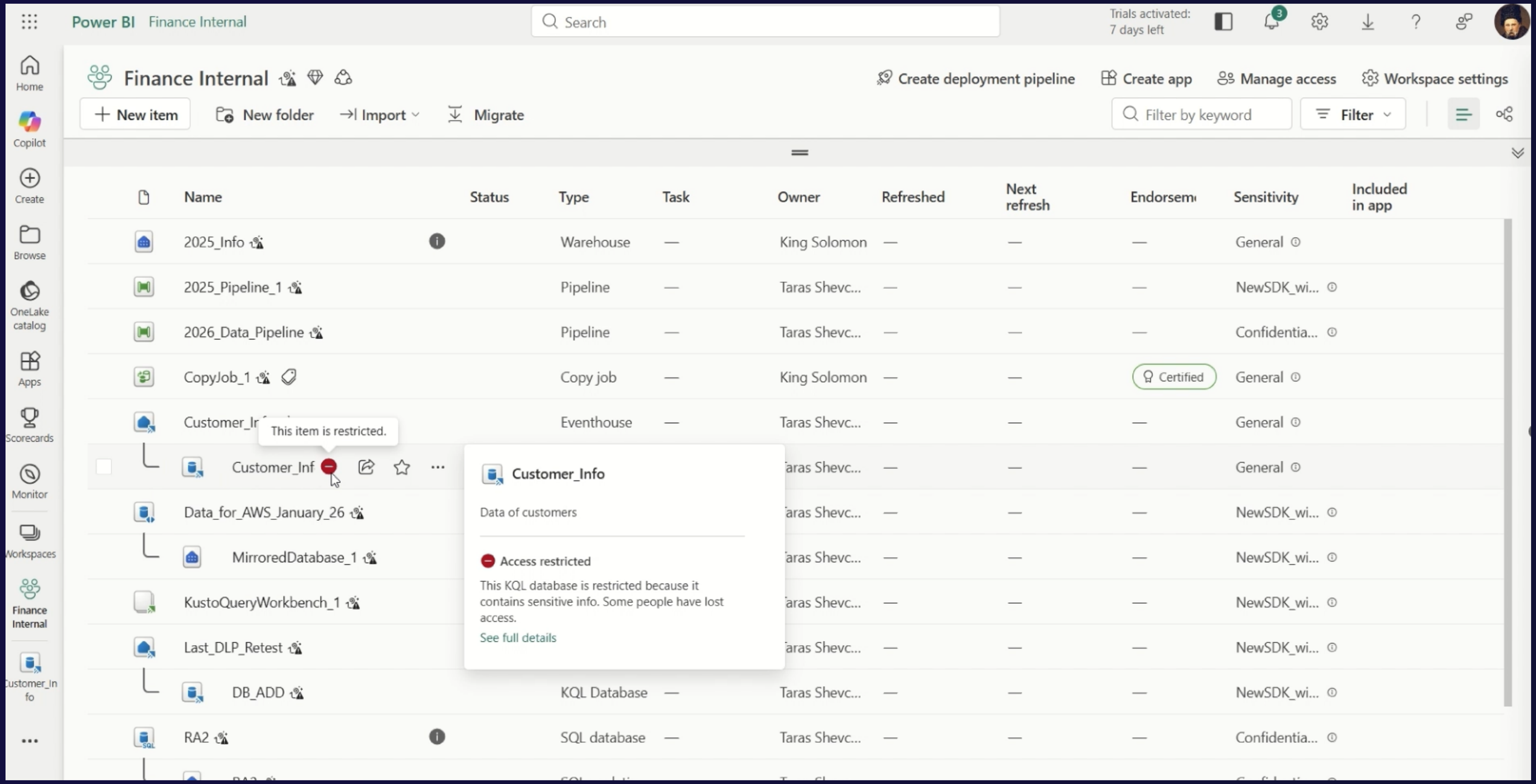
Define and apply policies to sensitive data to prevent data oversharing

Public Preview

Data Loss Prevention to restrict access to KQL/SQL/Cosmos DBs, Warehouse

Generally Available

Data Loss Prevention policies (audit + alerts + policy tips) for Warehouse and Cosmos DB



DLP restrict access preventing data oversharing of customer information stored in a KQL database

Secure and Govern AI in Fabric

Generally Available

DSPM for all Fabric Copilots and Agents to discover

“As an admin, Can I see what my users are asking my Copilots and Data Agent?”

Fabric does not natively offer an option to review a user’s prompts or responses from Data Agent

Purview DPSM (Data Posture Security Management) does!

01 Announcement – Public Preview at FabCon Atlanta 2026

02 Requires separate licensing for Purview! (docs)

03 Collection Policy “DSPM for AI – Capture interactions for Copilot experiences”

Fabric

https://app.fabric.microsoft.com/admin-portal/tenantSettings?experience=fabric-developer

Search

Admin portal

- Tenant settings New
- Users
- Premium Per User
- Audit logs
- Domains New
- Workloads
- Tags New
- Capacity settings
- Refresh summary
- Embed Codes
- Organizational visuals
- Organizational themes (preview)
- Azure connections
- Workspaces
- Custom branding
- Fabric identities
- Featured content
- Help + support

Information protection

- Allow users to apply sensitivity labels for content
  Disabled for the entire organization
- Apply sensitivity labels from data sources to their data in Power BI
  Disabled for the entire organization
- Automatically apply sensitivity labels to downstream content
  Disabled for the entire organization
- Allow workspace admins to override automatically applied sensitivity labels
  Disabled for the entire organization
- Restrict content with protected labels from being shared via link with everyone in your organization
  Disabled for the entire organization
- Domain admins can set default sensitivity labels for their domains (preview)
  Disabled for the entire organization

Allow Microsoft Purview to secure AI interactions

Enabled for the entire organization

Allow Microsoft Purview to access, process, and store prompts and responses-including metadata-for data security and compliance outcomes such as sensitive info type (SIT) classification, reporting in Microsoft Purview Data Security Posture Management for AI, Audit, Insider Risk Management, Communication Compliance, and eDiscovery. Note: This is a Microsoft Purview paid capability and is not included in the Copilot in Fabric pricing. Learn More

Enabled

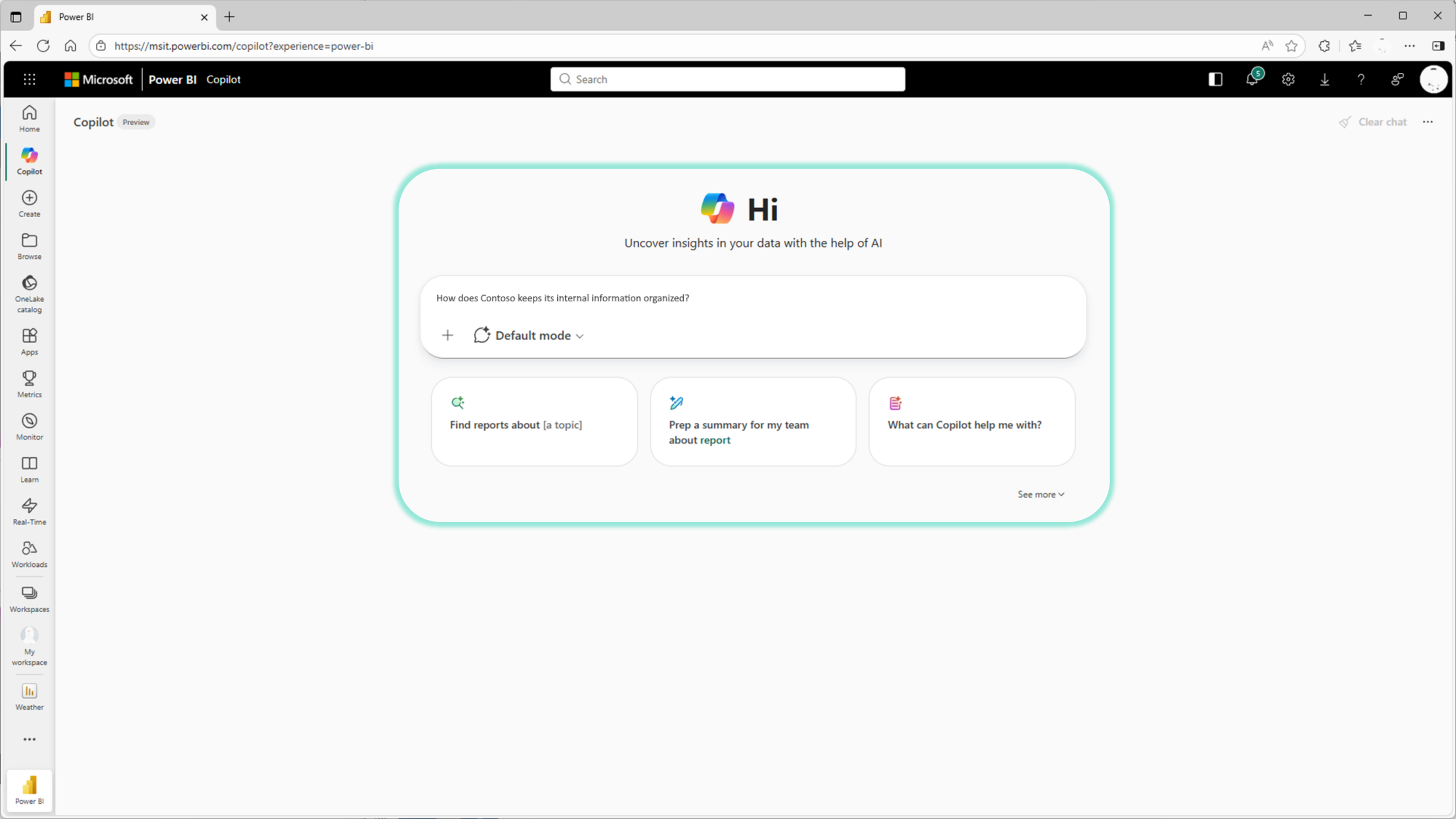
Disabling this setting means Microsoft Fabric AI interactions in your organization will not be protected by Microsoft Purview

This setting applies to the entire organization

Apply Cancel

Export and sharing settings

- External data sharing
  Disabled for the entire organization
- Users can accept external data shares
  Disabled for the entire organization
- Guest users can access Microsoft Fabric
  Enabled for the entire organization
- Users can invite guest users to collaborate through item sharing and permissions
  Enabled for the entire organization
- Guest users can browse and access Fabric content


Power BI
https://msit.powerbi.com/copilot?experience=power-bi
Microsoft
Power BI
Copilot
Search
Home
Copilot
Create
Browse
OneLake catalog
Apps
Metrics
Monitor
Learn
Real-Time
Workloads
Workspaces
My workspace
Weather
Power BI
Copilot
Preview
Clear chat
Hi
Uncover insights in your data with the help of AI
How does Contoso keeps its internal information organized?
Default mode
Find reports about [a topic]
Prep a summary for my team about report
What can Copilot help me with?
See more

Home
Solutions
Agents
Learn
Usage center (preview)
Settings
Data Security Posture Managem...
DSPM for AI (classic)

Data Security Posture Management
Posture
Objectives
Discover
Apps and agents
Activity explorer
Asset explorer
Data risk assessments
Actions
Reports

Additional permissions required. Your role can't view AI Visits or user risk levels. For permission, ask an administrator to change your role. Learn more about roles

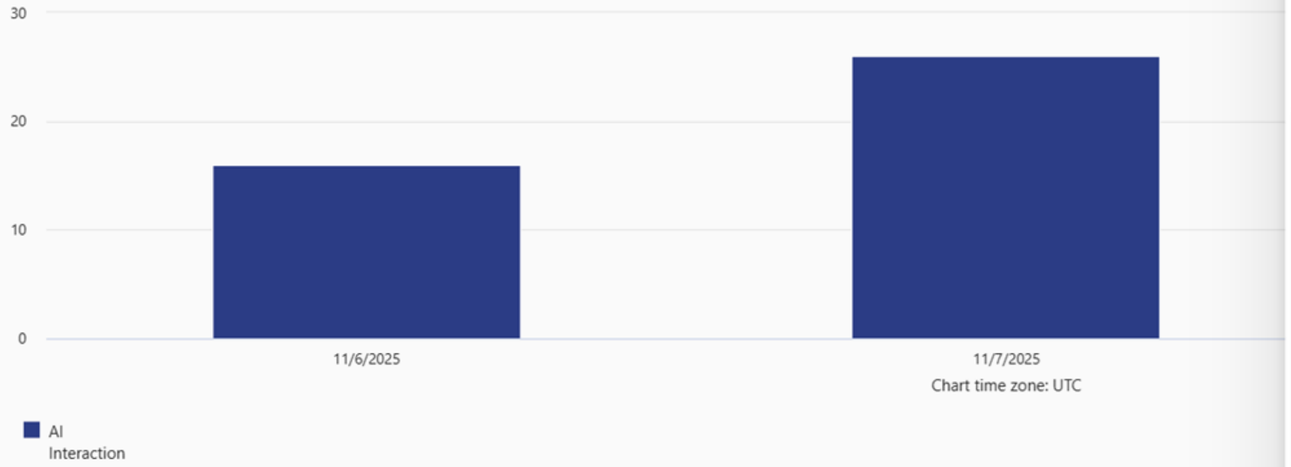
Activity explorer

Review activity related to content that contains sensitive info or has labels applied, such as what labels were changed, files were modified, and more. Label activity is monitored across Exchange, SharePoint, OneDrive, and endpoint devices. Support for more data sources is coming soon.

Activity explorer (IRM, DLP, MIP, DLM) | **Activity explorer (DSPM4AI)**

Review AI activity including AI interactions (prompts and responses), activity with sensitive info types, and more.

Filters: Timestamp: **11/6/2025-11/13/2025** | Activity type: **AI Interaction** | AI app category: **Any** | Sensitive info type: **Any** | Web searched: **Any** | Sensitivity label: **Any** | Add filter | Reset all



Export selected item | Refresh

Activity type	Timestamp (UTC)	AI app category	App	App accessed in	Agent name
AI Interaction	Nov 13, 2025 6:55 PM	Enterprise AI apps	Fabric	Fabric - PowerBI	
AI Interaction	Nov 13, 2025 6:54 PM	Enterprise AI apps	Fabric	Fabric - PowerBI	
AI Interaction	Nov 13, 2025 6:54 PM	Enterprise AI apps	Fabric	Fabric - PowerBI	

AI Interaction

Client IP
4.155.8.186

User details

User
Morgan Brown

App details

AI app category
Enterprise AI apps

App accessed in
Fabric - PowerBI

Interaction details

Prompt Copy

How does Contoso keep its internal information organized?

Response Copy

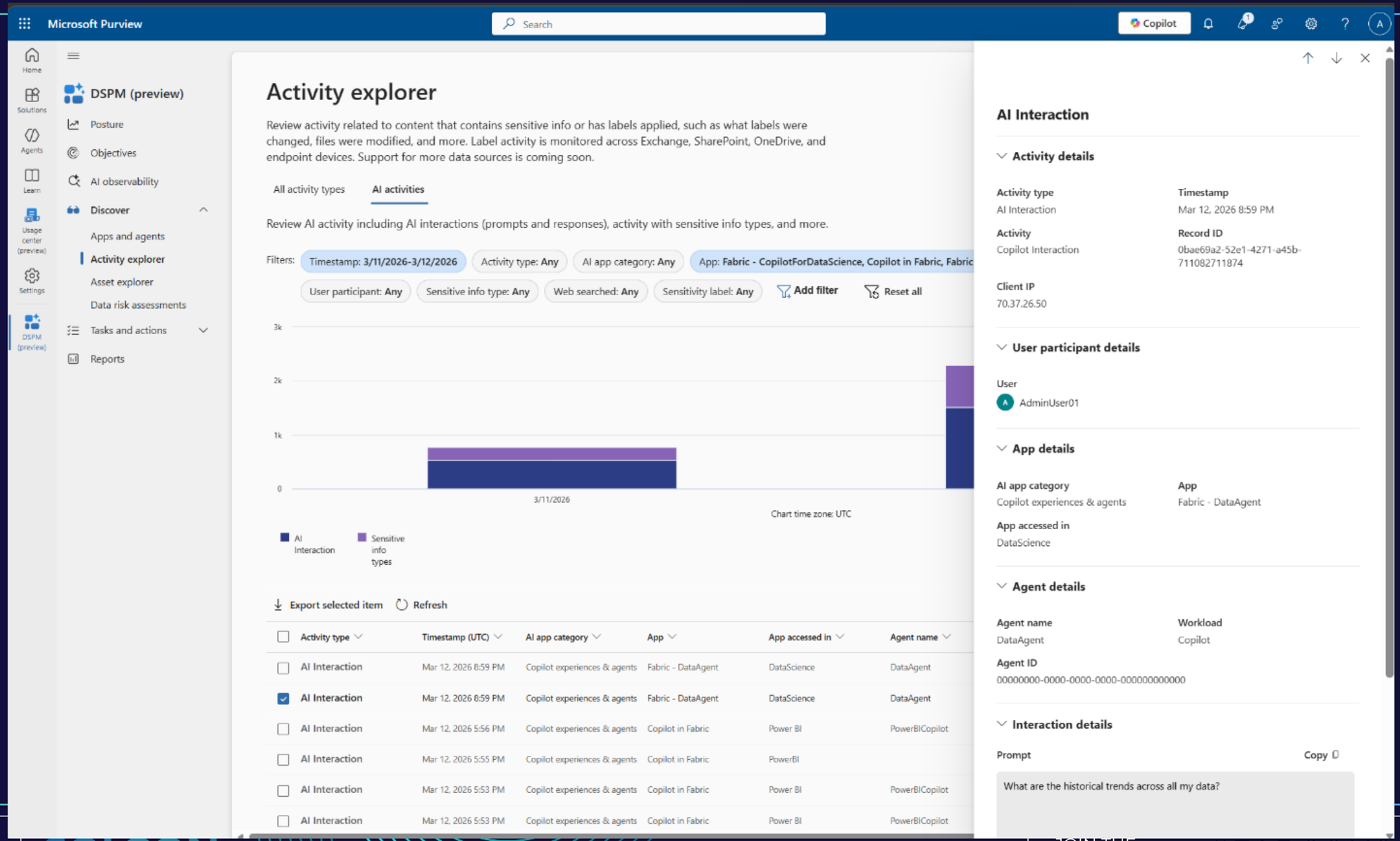
Contoson organizes information so that it's easy for employees to find and reuse.

Documents are labeled based on their audience (Public, Personal,

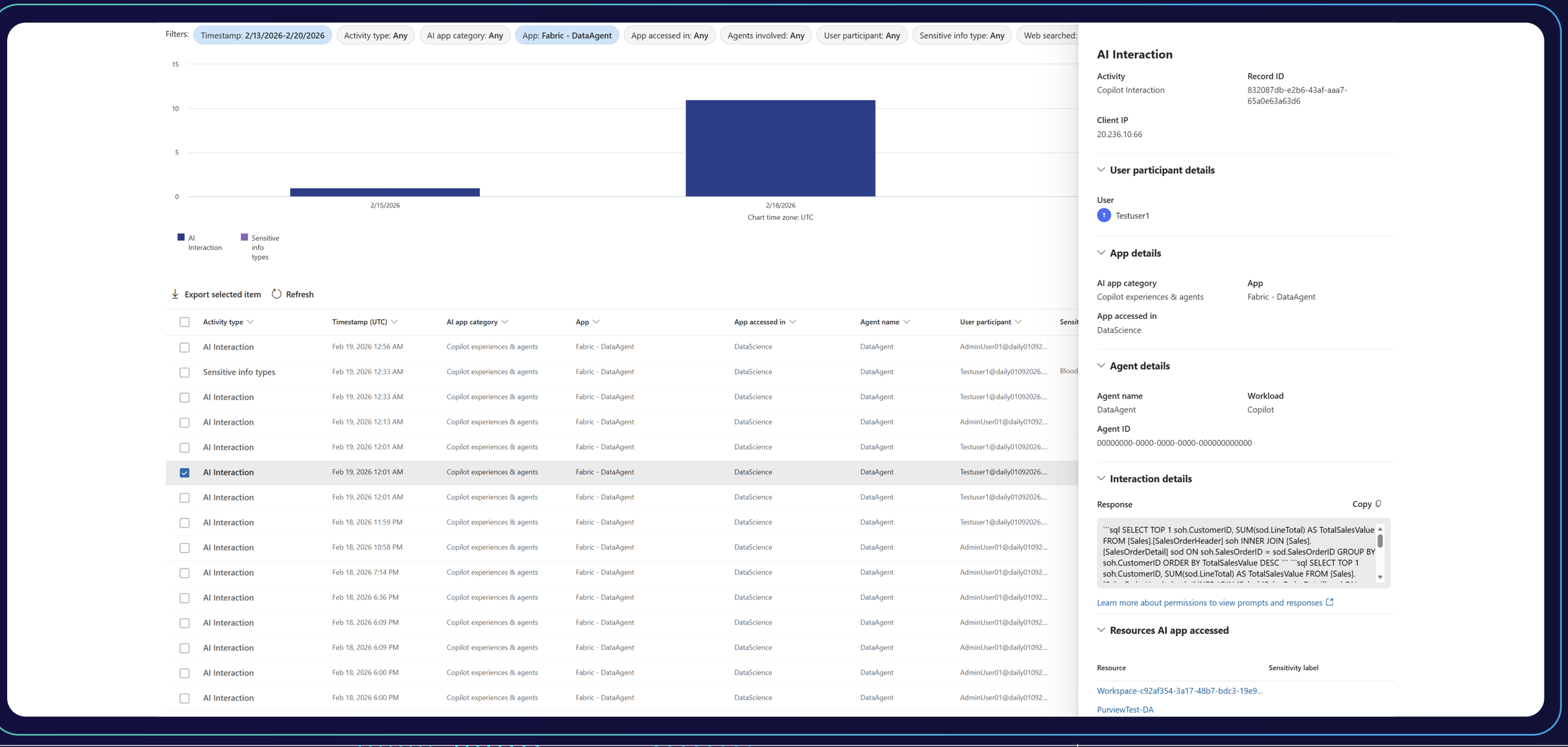
Sensitive info types detected | View related classification activity

Learn more about permissions to view prompts and responses

Data Agent Prompt



Data Agent Response



Summary

01 AI transformation is affecting the way we should think about protecting data

02 Microsoft Purview brings estate wide security to Fabric to protect your data with consistency

03 Securing data for AI is table stakes for proper AI activation

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

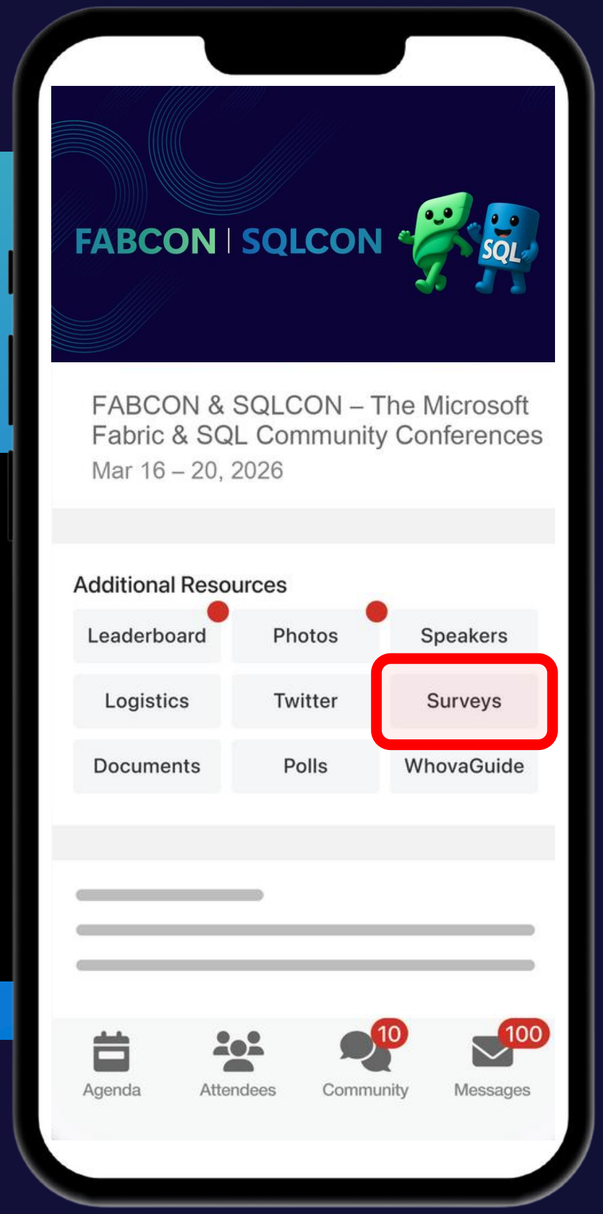
Join the SQL User Panel

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!**



Catalog and Search Announcements

Public Preview

- DSPM for all Fabric Copilots and Agents to discover
- Data Loss Prevention to restrict access to KQL/SQL/Cosmos DBs, Warehouse

General Availability

- IRM admins can check the PAYG usage (processing units) across different workloads, sub workloads & activities through the usage report
- IRM admins can create a data theft policy to detect Fabric data exfiltration in single click
- Insider Risk Management extends to Lakehouse indicators
- Data Loss Prevention policies (audit + alerts + policy tips) for Warehouse and Cosmos DB

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

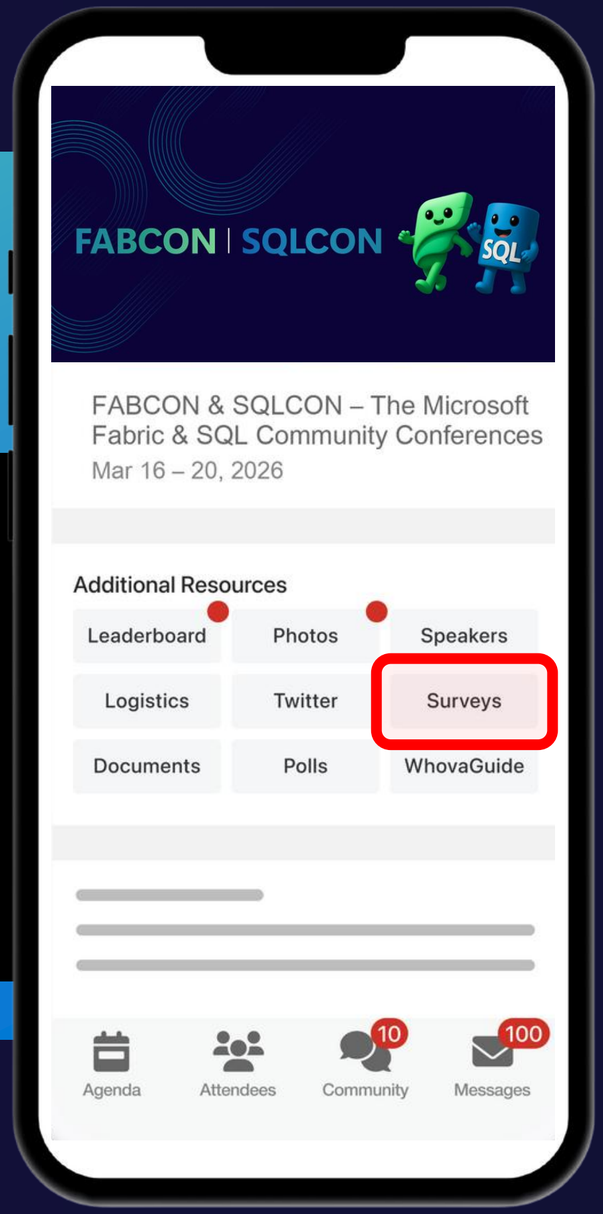
Join the SQL User Panel

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