



Microsoft Fabric

This presentation is the property of Microsoft and is intended for informational and educational purposes only. You may use, copy, and distribute this presentation for your personal, non-commercial purposes. You may not modify, alter, or create derivative works from this presentation without the prior written consent of Microsoft. You may not use this presentation to misrepresent, defame, or disparage Microsoft or its products, services, or affiliates. You may not use this presentation to endorse or promote any other products, services, or organizations without the prior written consent of Microsoft.

By using this presentation, you agree to abide by these terms. If you do not agree, you must not use this presentation. Microsoft reserves the right to change these terms and conditions at any time without notice. Microsoft disclaims any and all warranties, express or implied, relating to this presentation, including but not limited to the accuracy, completeness, timeliness, or suitability of the information contained herein. Microsoft is not liable for any damages, losses, or liabilities arising from your use of or reliance on this presentation.

Please review the terms of use posted in the content library.

#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

FABCON | **SQLCON**

Source: BSA | The Software Alliance Report Annual Report, 2025
ATLANTA26

JOIN THE
CONVERSATION **#FABCONSQLCON26**

Challenges with AI

#1

Priority for CISOs is securing enterprise AI adoption¹

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

¹CISO_Survey 2025_v10.pdf | ²Work 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 lifetime¹

Insider risk is significant

20%

Insiders account for 20% of data breaches, adding to costs²

Data leaks and oversharing are top of mind concerns

80%

Of leaders cited leakage of sensitive data as their main concern around adopting Generative AI³



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



Microsoft
Fabric

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



Microsoft
Purview

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

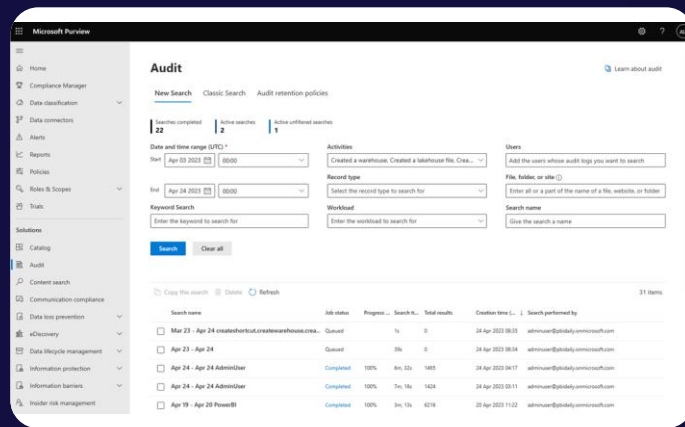
Problem

1. Data oversharing and leakage in Fabric

Solutions

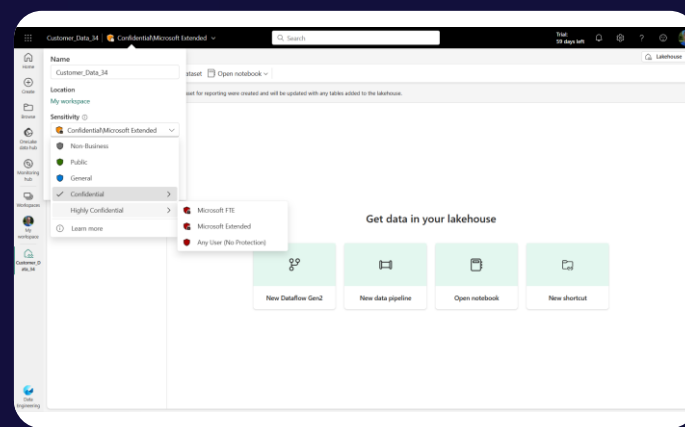
1. Discover and identify insider risks
2. Define and apply policies to sensitive data to prevent data leakage
3. Secure and Govern AI in Fabric

Purview Data Security & Compliance integration with Fabric



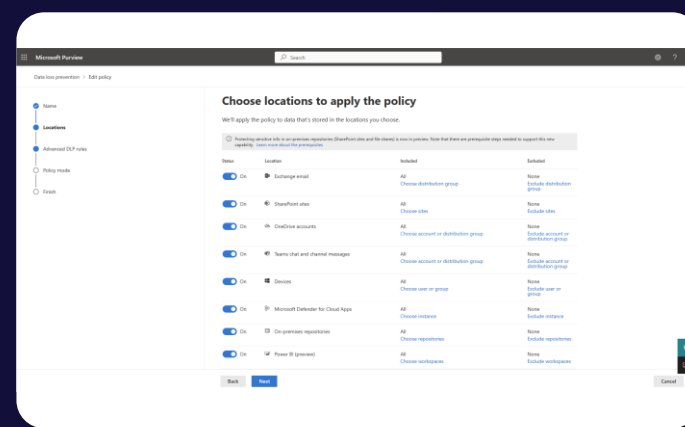
Audit

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



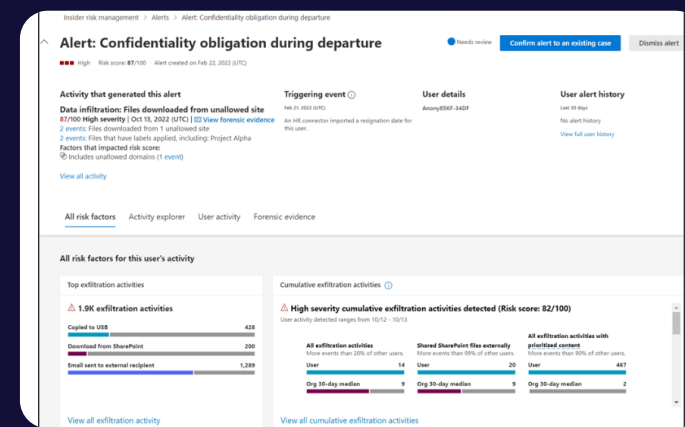
Information protection sensitivity labels and protection policies

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.



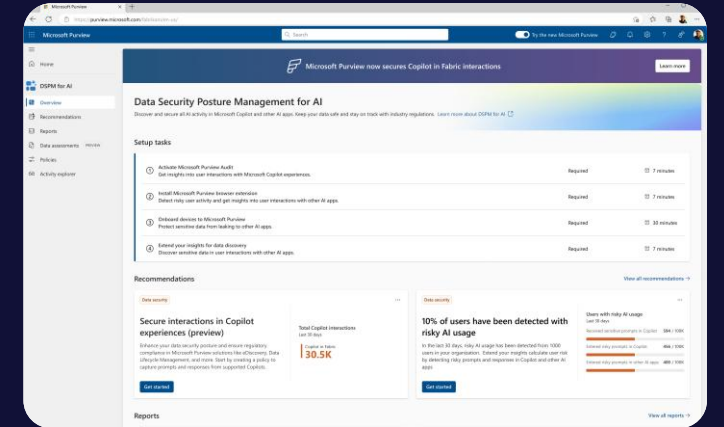
Data loss prevention policies

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 ▴

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

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

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

- Home
- Solutions
- Agents
- Learn
- Usage center (preview)
- Settings
- Insider Risk Management
 - Overview
 - Recommendations
 - Reports
 - Audit log
 - Policies
 - Users
 - Alerts
 - Cases
 - Users
 - Adaptive Protection
 - Forensic Evidence
 - Notice templates
 - Agents
- Related solutions
 - Communication Compliance
 - Data Security Investigations
 - Data Loss Prevention

Alerts > Alert: Confidentiality obligation during departure

(31ac5f2b) Alert: Confidentiality obligation during departure

Details Summarize

Created on: Feb 22, 2022 (UTC) • Status: Needs review • Severity: High • Risk score: 87/100

Activity explorer All risk factors User activity Data risk graph Forensic evidence

Filter: Show: All activity for user Risk category: Any Activity Type: Any Reset all

Sort by: Date occurred

- Exfiltration: Enabled external sharing of Microsoft Fabric data**
Nov 10, 2025 (UTC) | Risk score: 25/100
1 event(s): External sharing enabled from Fabric settings
- Deletion: Deleted Microsoft Fabric lakehouses**
Nov 10, 2025 (UTC) | Risk score: 50/100
5 event(s): Deleted Microsoft Fabric lakehouses
- Exfiltration: Data from lakehouse shared externally**
Nov 10, 2025 (UTC) | Risk score: 75/100
3 event(s): Lakehouse data shared with people outside the organization
- Deletion: Deleted lakehouse files or tables**
Nov 10, 2025 (UTC) | Risk score: 25/100
150 event(s): Deleted lakehouse files or tables
- Obfuscation: Downgraded sensitivity labels of lakehouses**
Nov 10, 2025 (UTC) | Risk score: 50/100
5 event(s): Downgraded sensitivity labels of lakehouses
- Obfuscation: Removed sensitivity labels of lakehouses**
Nov 10, 2025 (UTC) | Risk score: 50/100
5 event(s): Removed sensitivity labels of lakehouses

User activity scatter plot 6 Months 3 Months 1 Month



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

- Home
- Solutions
- Agents
- Learn
- Usage center (preview)
- Settings
- Insider Risk Management

Insider Risk Management

- Overview
- Recommendations
- Reports
- Audit log
- Policies**
- Users
- Agents

- Related solutions
- Communication Compliance
 - Data Security Investigations
 - Data Loss Prevention

Policies

User Policies Agent Policies

Policy warnings: 11 | Policy recommendations: 14 | Healthy policies: 0

Review collection policies. Collection policies control what activities can be detected by device indicators. We recommend reviewing your org's collection policies to ensure they detect in your insider risk policies. Learn more about collection policies.

+ Create policy Start scoring activity for users Refresh

Policy name	Status	Users in scope	Active alerts
DLP_Policy_1_with_Dlp_Alerts	1 warning, 1 recommendation	1	15
DLP_Policy_2	1 warning, 1 recommendation	1	15
DataLeakPolicy	1 warning, 1 recommendation	0	1
DoNotDelete - EmailToSelf	1 warning, 3 recommendations	1	0
Email exfiltration policy - 9/11/2025	1 warning, 1 recommendation	0	0
LH test 2	1 warning, 1 recommendation	0	1
Non-Microsoft 365 data theft (quick policy) - 2/9/2026	1 warning, 2 recommendations	1	0
Scope testing	2 warnings, 2 recommendations	1	0
SensitivityLabelUpdated-Karnika	1 warning, 1 recommendation	0	1
Test LH 234	1 warning, 1 recommendation	1	1

Create quick policies

Use preconfigured settings to quickly set up a policy based on common insider risk scenarios. Learn more about quick policies

- Data leaks**
Detect potential data leaks from all users in your org, which can range from accidental oversharing of sensitive info to data theft with malicious intent.
[Get started](#)
- Data theft from Microsoft 365 apps by users leaving your org**
Detects potential data theft from Microsoft 365 cloud apps by users leaving your org or whose account was deleted from Microsoft Entra ID.
[Get started](#)
- Data theft from non-Microsoft 365 apps by users leaving your org** New Pay-as-you-go
Detects potential data theft from non-Microsoft 365 cloud apps, including Microsoft Fabric, by users leaving your org or whose account was deleted from Microsoft Entra ID.
[Get started](#)
- Critical asset protection**
Detects activities involving your org's most valuable assets. Loss of these assets could result in legal liability, financial loss, or reputational damage.
[Get started](#)
- Email exfiltration**
Detects when users email sensitive assets outside your org. For example, users emailing sensitive assets to their personal email address.
[Get started](#)
- Risky AI Usage** New

Home

Solutions

Agents

Learn

Usage center (preview)

Settings

Insider Risk Management

Overview

Recommendations

Reports

Audit log

Policies

Users

Agents

Policies

User Policies Agent Policies

Policy warnings **11** Policy recommendations **14** Healthy policies **0**

Review collection policies. Collection policies control what activities can be detected by device indicators. We recommend reviewing your org's collection policies to ensure they detect in your insider risk policies. [Learn more about collection policies.](#)

+ Create policy Start scoring activity for users Refresh

Policy name	Status	Users in scope	Active alerts
DLP_Policy_1_with_Dlp_Alerts	1 warning, 1 recommendation	1	15
DLP_Policy_2	1 warning, 1 recommendation	1	15
DataLeakPolicy	1 warning, 1 recommendation	0	1
DoNotDelete - EmailToSelf	1 warning, 3 recommendations	1	0
Email exfiltration policy - 9/11/2025	1 warning, 1 recommendation	0	0
LH test 2	1 warning, 1 recommendation	0	1
Non-Microsoft 365 data theft (quick policy) - 2/9/2026	1 warning, 2 recommendations	1	0
Scope testing	2 warnings, 2 recommendations	1	0
SensitivityLabelUpdated-Karnika	1 warning, 1 recommendation	0	1
Test LH 234	1 warning, 1 recommendation	1	1

Create a data theft policy for non-Microsoft 365 apps

Pay-as-you-go 2 minutes to complete

This policy detects data theft by departing users near their resignation or termination date from non-Microsoft 365 apps including Fabric. Most organizations with insider risk programs have a data theft policy in place.

[How do quick policies work?](#)

Review the policy name we suggested and make changes if needed.

Policy name *

Non-Microsoft 365 data theft (quick policy) - 2/26/2026

Settings we filled in for you

Settings below are based on the latest analytics scan. You can edit them later or click 'Customize' now to configure settings using the full policy wizard.

User scope

Include all users and groups (Recommended for best coverage)

Triggering event

User account deleted from Microsoft Entra ID - requires all users and groups in policy scope

Indicators Pay-as-you-go

The following indicators are billed under pay-as-you-go. You'll be charged based on user activities processed. [Learn about pay-as-you-go billing.](#)

AWS, Dropbox, Box, Google Drive aren't connected yet. To use these indicators, you must first connect from the Microsoft 365 Defender portal. [Learn about connecting cloud apps](#)

[Go to Microsoft 365 Defender](#)

- Disabling Amazon S3 settings that block public access to data
- Downloading content from Dropbox
- Making Amazon S3 buckets publicly accessible

Home

Solutions

Agents

Learn

Usage center (preview)

Settings

Insider Risk Management

Insider Risk Management

Overview

Recommendations

Reports

Audit log

Policies

Users

Agents

Policies

User Policies Agent Policies

Policy warnings **11** Policy recommendations **14** Healthy policies **0**

Review collection policies. Collection policies control what activities can be detected by device indicators. We recommend reviewing your org's collection policies to ensure they detect in your insider risk policies. [Learn more about collection policies.](#)

+ Create policy Start scoring activity for users Refresh

Policy name	Status	Users in scope	Active alerts
DLP_Policy_1_with_Dlp_Alerts	1 warning, 1 recommendation	1	15
DLP_Policy_2	1 warning, 1 recommendation	1	15
DataLeakPolicy	1 warning, 1 recommendation	0	1
DoNotDelete - EmailToSelf	1 warning, 3 recommendations	1	0
Email exfiltration policy - 9/11/2025	1 warning, 1 recommendation	0	0
LH test 2	1 warning, 1 recommendation	0	1
Non-Microsoft 365 data theft (quick policy) - 2/9/2026	1 warning, 2 recommendations	1	0
Scope testing	2 warnings, 2 recommendations	1	0
SensitivityLabelUpdated-Karnika	1 warning, 1 recommendation	0	1
Test LH 234	1 warning, 1 recommendation	1	1

Create a data theft policy for non-Microsoft 365 apps

Settings we filled in for you

Settings below are based on the latest analytics scan. You can edit them later or click 'Customize' now to configure settings using the full policy wizard.

User scope

Include all users and groups (Recommended for best coverage)

Triggering event

User account deleted from Microsoft Entra ID - requires all users and groups in policy scope

Indicators Pay-as-you-go

The following indicators are billed under pay-as-you-go. You'll be charged based on user activities processed. [Learn about pay-as-you-go billing.](#)

AWS, Dropbox, Box, Google Drive aren't connected yet. To use these indicators, you must first connect from the Microsoft 365 Defender portal. [Learn about connecting cloud apps](#)

[Go to Microsoft 365 Defender](#)

- Disabling Amazon S3 settings that block public access to data
- Downloading content from Dropbox
- Making Amazon S3 buckets publicly accessible
- Elevating access to all Azure subscriptions and management groups
- Downloading content from Box
- Sharing Box files with people outside the organization
- Sharing Dropbox files with people outside the organization
- Sharing Google Drive files with people outside the organization
- Downloading Power BI reports
- Exporting Power BI reports
- Removing sensitivity labels from Power BI artifacts
- Downgrading sensitivity labels from Power BI artifacts
- Enabling external sharing of Microsoft Fabric data
- Sharing lakehouse data with people outside the organization
- Removing sensitivity labels of lakehouses
- Downgrading sensitivity labels of lakehouses

- Home
- solutions
- Learn
- Settings
- Insider Risk Management
- Insider Risk Management
- Reports
- Forensic evidence
- Adaptive protection (preview)
- Notice templates
- Audit log
- solutions
- Related
- Communication compliance
- Data Loss Prevention
- Information barriers

Reports > Pay-as-you-go usage report

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

i 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

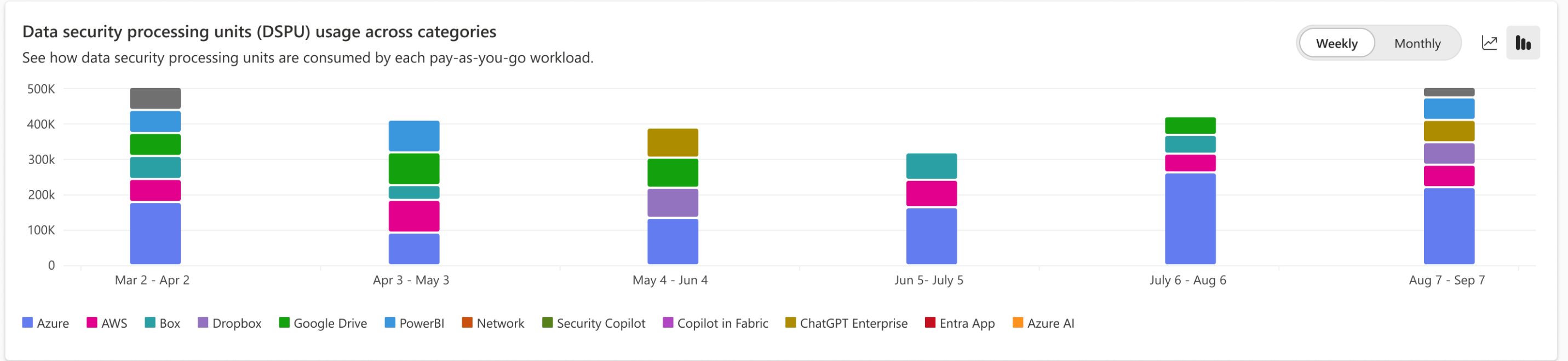
1.2M July 1-30, 2025

No. of paid indicators with usage

5 ↑ 28%

Avg. DSPUs used per day

40K ↑ 12%



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 sensitivi...	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

- 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

Power BI Finance Internal Search

Trials activated: 7 days left

Home Copilot Create Browse OneLake catalog Apps Scorecards Monitor Workspaces Finance Internal Customer Info

Finance Internal 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	Endorsement	Sensitivity	Included in app
2025_Info		Warehouse	—	King Solomon	—	—	—	General	
2025_Pipeline_1		Pipeline	—	Taras Shevc...	—	—	—	NewSDK_wi...	
2026_Data_Pipeline		Pipeline	—	Taras Shevc...	—	—	—	Confidentia...	
CopyJob_1		Copy job	—	King Solomon	—	—	Certified	General	
Customer_Info		Eventhouse	—	Taras Shevc...	—	—	—	General	
Customer_Info		KQL Database	—	Taras Shevc...	—	—	—	General	
Data_for_AWS_January_26		KQL Database	—	Taras Shevc...	—	—	—	NewSDK_wi...	
MirroredDatabase_1		KQL Database	—	Taras Shevc...	—	—	—	NewSDK_wi...	
KustoQueryWorkbench_1		KQL Database	—	Taras Shevc...	—	—	—	NewSDK_wi...	
Last_DLP_Retest		KQL Database	—	Taras Shevc...	—	—	—	NewSDK_wi...	
DB_ADD		KQL Database	—	Taras Shevc...	—	—	—	NewSDK_wi...	
RA2		SQL database	—	Taras Shevc...	—	—	—	Confidentia...	

This item is restricted.

Customer_Info

Data of customers

Access restricted

This KQL database is restricted because it contains sensitive info. Some people have lost access.

[See full details](#)

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”

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

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 Management
- 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

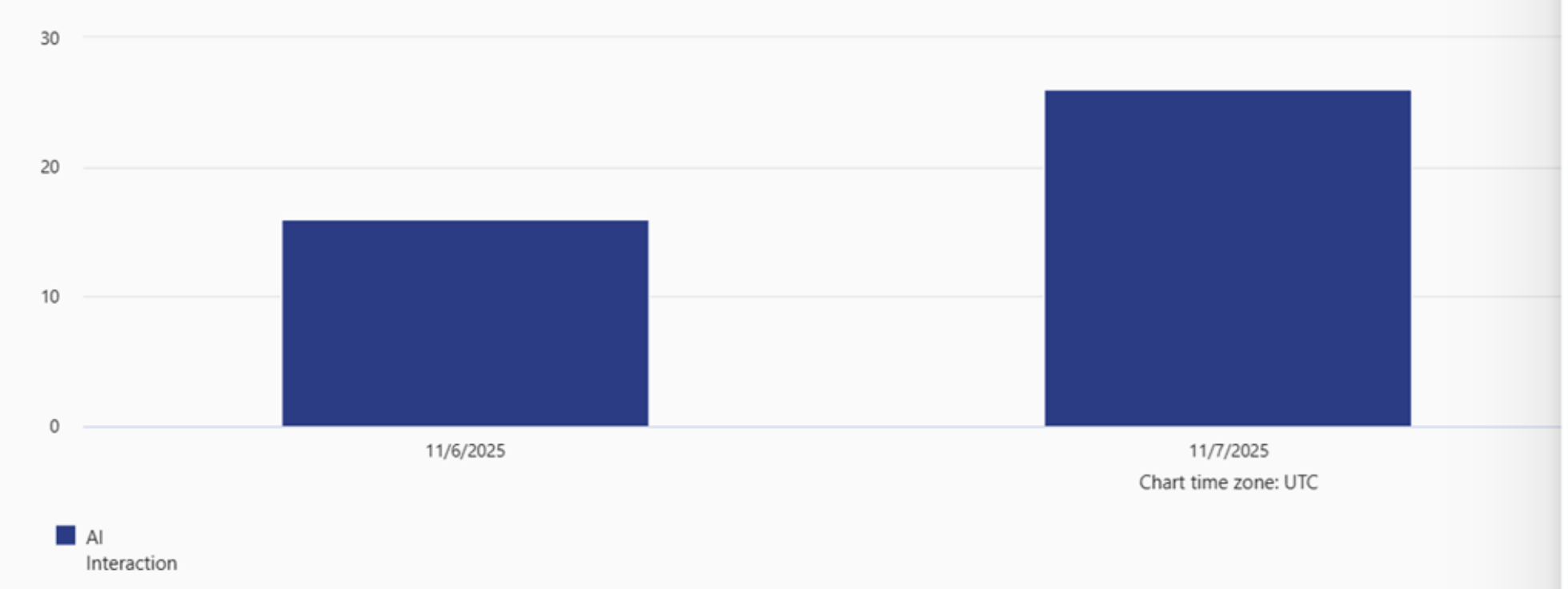
Review activity related to content that contains sensitive info or has labels applied, such as what labels were changed, files were modified, and more. Label activity is monitored across Exchange, SharePoint, OneDrive, and endpoint devices. Support for more data sources is coming soon.

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](#)

<input type="checkbox"/>	Activity type	Timestamp (UTC)	AI app category	App	App accessed in	Agent name
<input checked="" type="checkbox"/>	AI Interaction	Nov 13, 2025 6:55 PM	Enterprise AI apps	Fabric	Fabric - PowerBI	
<input type="checkbox"/>	AI Interaction	Nov 13, 2025 6:54 PM	Enterprise AI apps	Fabric	Fabric - PowerBI	
<input type="checkbox"/>	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

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.

All activity types **AI activities**

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

Filters: Timestamp: 3/11/2026-3/12/2026 Activity type: Any AI app category: Any App: Fabric - CopilotForDataScience, Copilot in Fabric, Fabric

User participant: Any Sensitive info type: Any Web searched: Any Sensitivity label: Any Add filter Reset all

3k
2k
1k
0

3/11/2026

Chart time zone: UTC

■ AI Interaction ■ Sensitive info types

Export selected item Refresh

<input type="checkbox"/>	Activity type	Timestamp (UTC)	AI app category	App	App accessed in	Agent name
<input type="checkbox"/>	AI Interaction	Mar 12, 2026 8:59 PM	Copilot experiences & agents	Fabric - DataAgent	DataScience	DataAgent
<input checked="" type="checkbox"/>	AI Interaction	Mar 12, 2026 8:59 PM	Copilot experiences & agents	Fabric - DataAgent	DataScience	DataAgent
<input type="checkbox"/>	AI Interaction	Mar 12, 2026 5:56 PM	Copilot experiences & agents	Copilot in Fabric	Power BI	PowerBICopilot
<input type="checkbox"/>	AI Interaction	Mar 12, 2026 5:55 PM	Copilot experiences & agents	Copilot in Fabric	Power BI	PowerBICopilot
<input type="checkbox"/>	AI Interaction	Mar 12, 2026 5:53 PM	Copilot experiences & agents	Copilot in Fabric	Power BI	PowerBICopilot
<input type="checkbox"/>	AI Interaction	Mar 12, 2026 5:53 PM	Copilot experiences & agents	Copilot in Fabric	Power BI	PowerBICopilot

AI Interaction

Activity details

Activity type: AI Interaction Timestamp: Mar 12, 2026 8:59 PM

Activity: Copilot Interaction Record ID: 0bae69a2-52e1-4271-a45b-711082711874

Client IP: 70.37.26.50

User participant details

User: AdminUser01

App details

AI app category: Copilot experiences & agents App: Fabric - DataAgent

App accessed in: DataScience

Agent details

Agent name: DataAgent Workload: Copilot

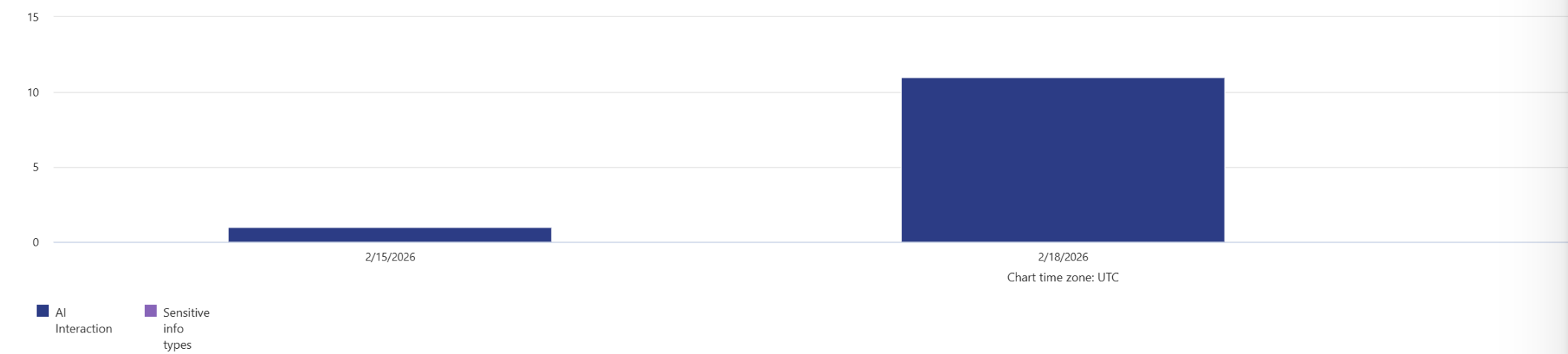
Agent ID: 00000000-0000-0000-0000-000000000000

Interaction details

Prompt: What are the historical trends across all my data? Copy

Data Agent Response

Filters: Timestamp: 2/13/2026-2/20/2026 Activity type: Any AI app category: Any App: Fabric - DataAgent App accessed in: Any Agents involved: Any User participant: Any Sensitive info type: Any Web searched:



Export selected item Refresh

<input type="checkbox"/>	Activity type	Timestamp (UTC)	AI app category	App	App accessed in	Agent name	User participant	Sensitive info types
<input type="checkbox"/>	AI Interaction	Feb 19, 2026 12:56 AM	Copilot experiences & agents	Fabric - DataAgent	DataScience	DataAgent	AdminUser01@daily01092...	
<input type="checkbox"/>	Sensitive info types	Feb 19, 2026 12:33 AM	Copilot experiences & agents	Fabric - DataAgent	DataScience	DataAgent	Testuser1@daily01092026...	Blood
<input type="checkbox"/>	AI Interaction	Feb 19, 2026 12:33 AM	Copilot experiences & agents	Fabric - DataAgent	DataScience	DataAgent	Testuser1@daily01092026...	
<input type="checkbox"/>	AI Interaction	Feb 19, 2026 12:13 AM	Copilot experiences & agents	Fabric - DataAgent	DataScience	DataAgent	AdminUser01@daily01092...	
<input type="checkbox"/>	AI Interaction	Feb 19, 2026 12:01 AM	Copilot experiences & agents	Fabric - DataAgent	DataScience	DataAgent	Testuser1@daily01092026...	
<input checked="" type="checkbox"/>	AI Interaction	Feb 19, 2026 12:01 AM	Copilot experiences & agents	Fabric - DataAgent	DataScience	DataAgent	Testuser1@daily01092026...	
<input type="checkbox"/>	AI Interaction	Feb 19, 2026 12:01 AM	Copilot experiences & agents	Fabric - DataAgent	DataScience	DataAgent	Testuser1@daily01092026...	
<input type="checkbox"/>	AI Interaction	Feb 18, 2026 11:59 PM	Copilot experiences & agents	Fabric - DataAgent	DataScience	DataAgent	Testuser1@daily01092026...	
<input type="checkbox"/>	AI Interaction	Feb 18, 2026 10:58 PM	Copilot experiences & agents	Fabric - DataAgent	DataScience	DataAgent	AdminUser01@daily01092...	
<input type="checkbox"/>	AI Interaction	Feb 18, 2026 7:14 PM	Copilot experiences & agents	Fabric - DataAgent	DataScience	DataAgent	AdminUser01@daily01092...	
<input type="checkbox"/>	AI Interaction	Feb 18, 2026 6:36 PM	Copilot experiences & agents	Fabric - DataAgent	DataScience	DataAgent	AdminUser01@daily01092...	
<input type="checkbox"/>	AI Interaction	Feb 18, 2026 6:09 PM	Copilot experiences & agents	Fabric - DataAgent	DataScience	DataAgent	AdminUser01@daily01092...	
<input type="checkbox"/>	AI Interaction	Feb 18, 2026 6:09 PM	Copilot experiences & agents	Fabric - DataAgent	DataScience	DataAgent	AdminUser01@daily01092...	
<input type="checkbox"/>	AI Interaction	Feb 18, 2026 6:00 PM	Copilot experiences & agents	Fabric - DataAgent	DataScience	DataAgent	AdminUser01@daily01092...	
<input type="checkbox"/>	AI Interaction	Feb 18, 2026 6:00 PM	Copilot experiences & agents	Fabric - DataAgent	DataScience	DataAgent	AdminUser01@daily01092...	

AI Interaction

Activity: Copilot Interaction
 Record ID: 832087db-e2b6-43af-aaa7-65a0e63a63d6

Client IP: 20.236.10.66

User participant details

User: Testuser1

App details

AI app category: Copilot experiences & agents
 App: Fabric - DataAgent

App accessed in: DataScience

Agent details

Agent name: DataAgent
 Workload: Copilot

Agent ID: 00000000-0000-0000-0000-000000000000

Interaction details

Response Copy

```
""sql SELECT TOP 1 soh.CustomerID, SUM(sod.LineTotal) AS TotalSalesValue FROM [Sales].[SalesOrderHeader] soh INNER JOIN [Sales].[SalesOrderDetail] sod ON soh.SalesOrderID = sod.SalesOrderID GROUP BY soh.CustomerID ORDER BY TotalSalesValue DESC "" ""sql SELECT TOP 1 soh.CustomerID, SUM(sod.LineTotal) AS TotalSalesValue FROM [Sales].
```

[Learn more about permissions to view prompts and responses](#)

Resources AI app accessed

Resource: Workspace-c92af354-3a17-48b7-bdc3-19e9...

PurviewTest-DA

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

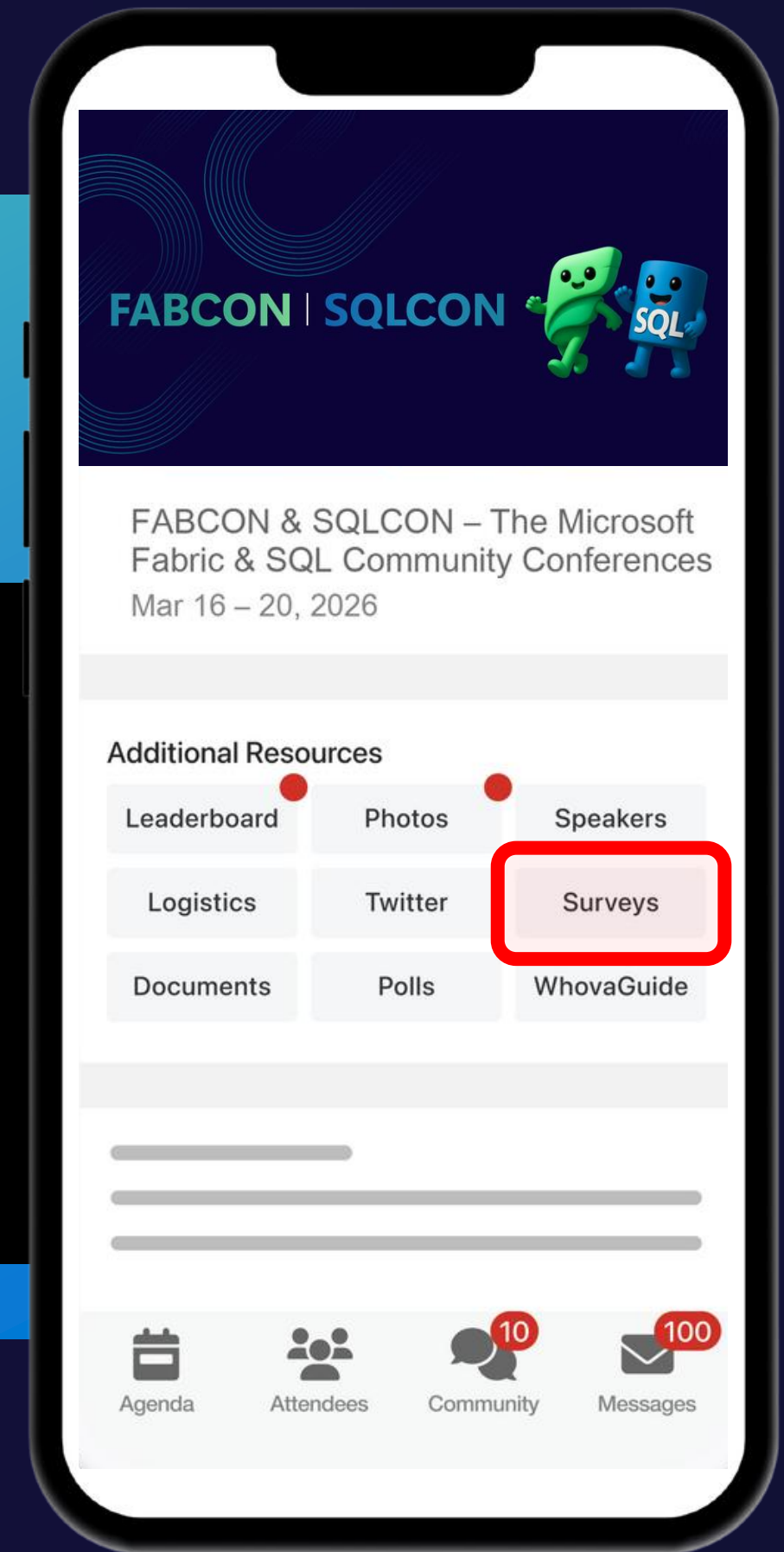
Influence our SQL roadmap and ensure it meets your real-life needs

<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

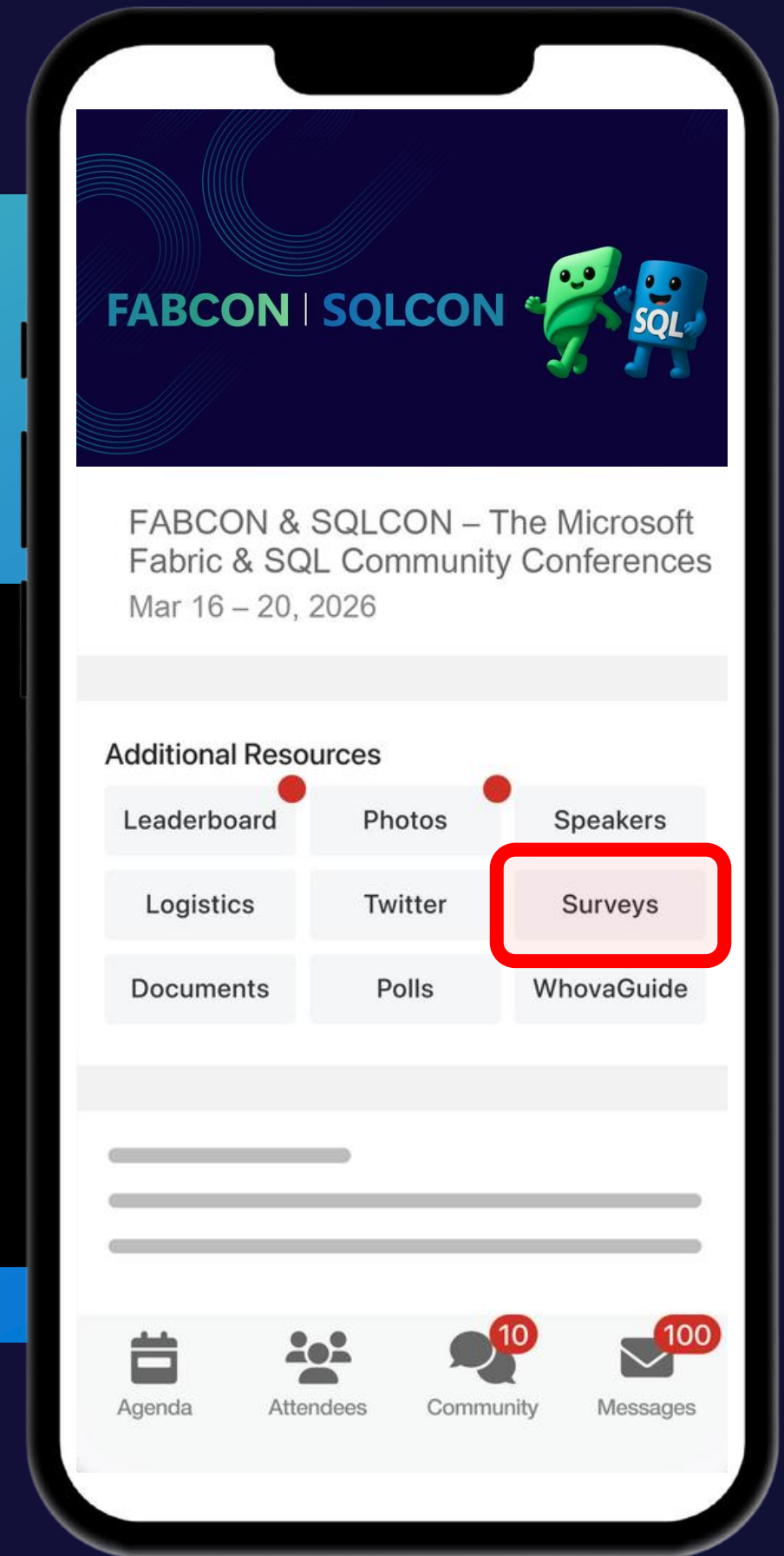
Influence our SQL roadmap and ensure it meets your real-life needs

<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>

