WE ARE STARTING SHORTLY...

Microsoft

DATA & AI UNLOCKED

E04 – Purview Mastery: Ensuring Data Governance and Security

Microsoft

EPISODE GUIDE

E01 (March 7th)	AI Foundations: Kickstarting Your AI Journey
E02 (March 14th)	Copilot Studio: Empowering AI with Low-Code Solutions
E03 (March 21st)	Microsoft Fabric: Laying the Data Groundwork for AI
E04 (March 28th)	Purview Mastery: Ensuring Data Governance and Security
E05 (April 4th)	**Azure AI Foundry: Customizing AI for Advanced Solutions**
E06 (April 11th)	**AI in Action: From Development to Deployment**

YOUR HOSTS FOR TODAY

Erjola Lekaj

Technical Specialist

#Security

Microsoft

Avi Melwani

Senior Technical specialist

#Data & AI

Microsoft

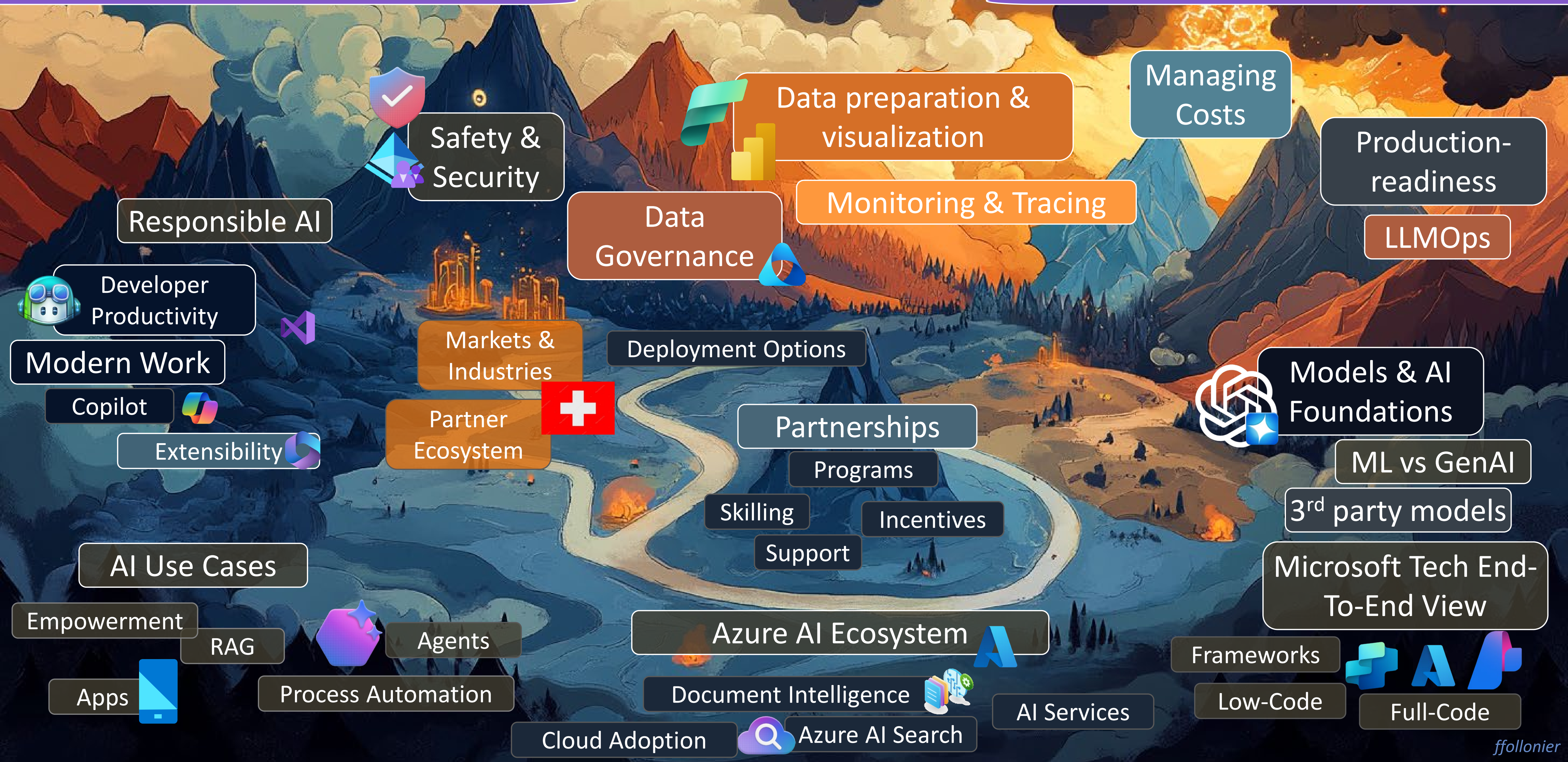
Lisa Wolffhugel

Partner Solution Architect

#Data, AI & Sustainability

Microsoft

Navigating The Microsoft AI Wonderland



Safety & Security

Responsible AI

Developer Productivity

Modern Work

Copilot

Extensibility

Markets & Industries

Partner Ecosystem

Data Governance

Data preparation & visualization

Monitoring & Tracing

Managing Costs

Production-readiness

LLMOps

Deployment Options

Partnerships

Programs

Skilling

Incentives

Support

Models & AI Foundations

ML vs GenAI

3rd party models

Microsoft Tech End-To-End View

Frameworks

Low-Code

Full-Code

AI Use Cases

Empowerment

RAG

Agents

Apps

Process Automation

Azure AI Ecosystem

Document Intelligence

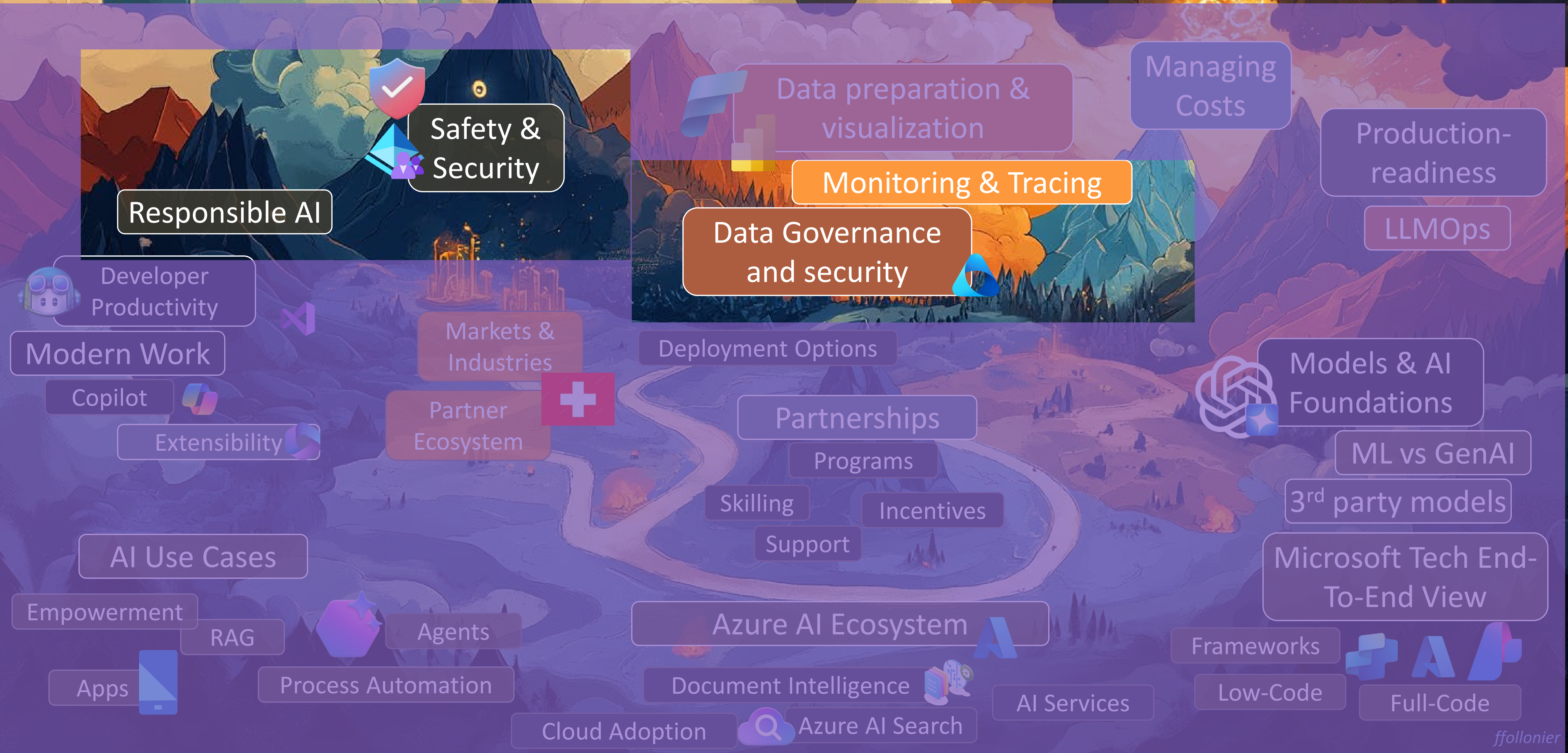
AI Services

Cloud Adoption

Azure AI Search

ffollonier

Navigating The Microsoft AI Wonderland



Responsible AI

Safety & Security

Data preparation & visualization

Monitoring & Tracing

Data Governance and security

Managing Costs

Production-readiness

LLMOps

Developer Productivity

Modern Work

Copilot

Extensibility

Markets & Industries

Partner Ecosystem

Deployment Options

Partnerships

Programs

Skilling

Incentives

Support

Models & AI Foundations

ML vs GenAI

3rd party models

Microsoft Tech End-To-End View

AI Use Cases

Empowerment

RAG

Agents

Apps

Process Automation

Azure AI Ecosystem

Document Intelligence

AI Services

Cloud Adoption

Azure AI Search

Frameworks

Low-Code

Full-Code

ffollonier

Agenda

1. Microsoft Purview Data security

2. Microsoft Purview Data governance

3. Data governance included in Microsoft Fabric

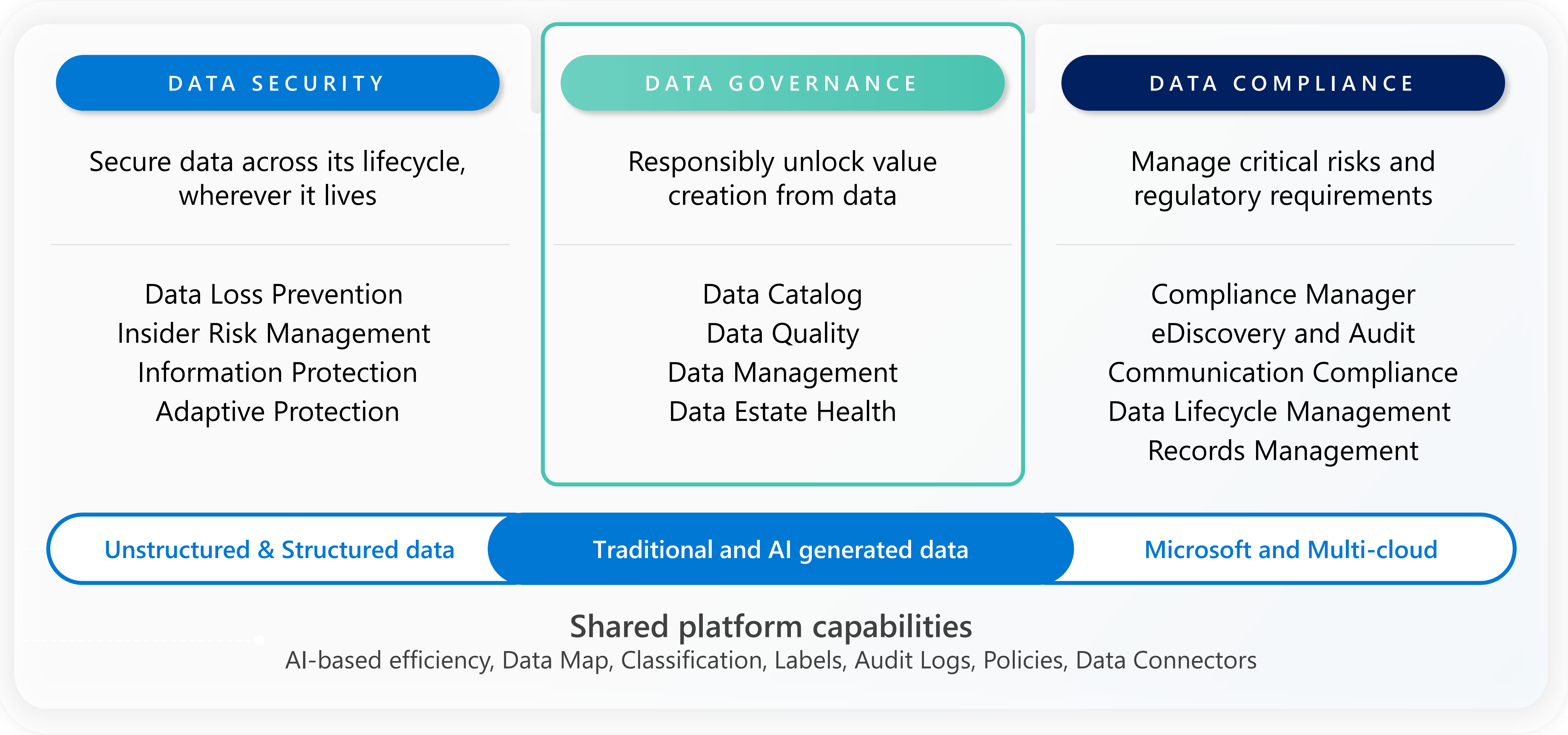
Microsoft

Secure data in the age of AI with Microsoft Purview

Erjola Lekaj

Microsoft Purview

Secure, govern, and protect your entire data estate



DATA SECURITY

Secure data across its lifecycle, wherever it lives

Data Loss Prevention
Insider Risk Management
Information Protection
Adaptive Protection

DATA GOVERNANCE

Responsibly unlock value creation from data

Data Catalog
Data Quality
Data Management
Data Estate Health

DATA COMPLIANCE

Manage critical risks and regulatory requirements

Compliance Manager
eDiscovery and Audit
Communication Compliance
Data Lifecycle Management
Records Management

Unstructured & Structured data | Traditional and AI generated data | Microsoft and Multi-cloud

Shared platform capabilities

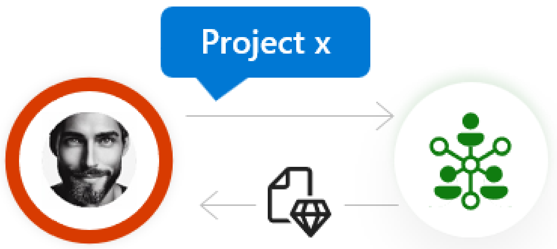
AI-based efficiency, Data Map, Classification, Labels, Audit Logs, Policies, Data Connectors

Security & compliance for new data

Insufficient visibility into the usage of AI applications can result in security and compliance challenges.

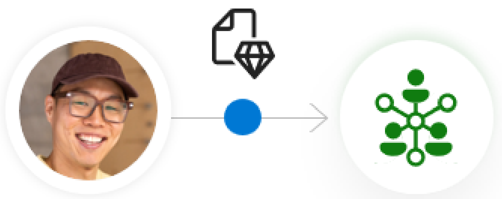
1

Data oversharing:
Users may access sensitive data via AI apps they are not authorized to view or edit



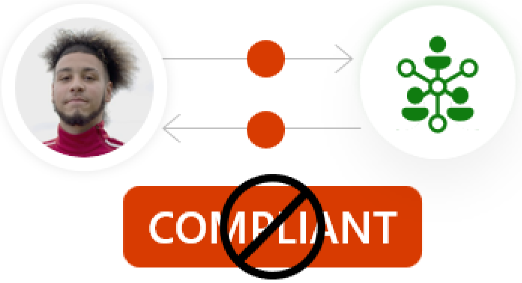
2

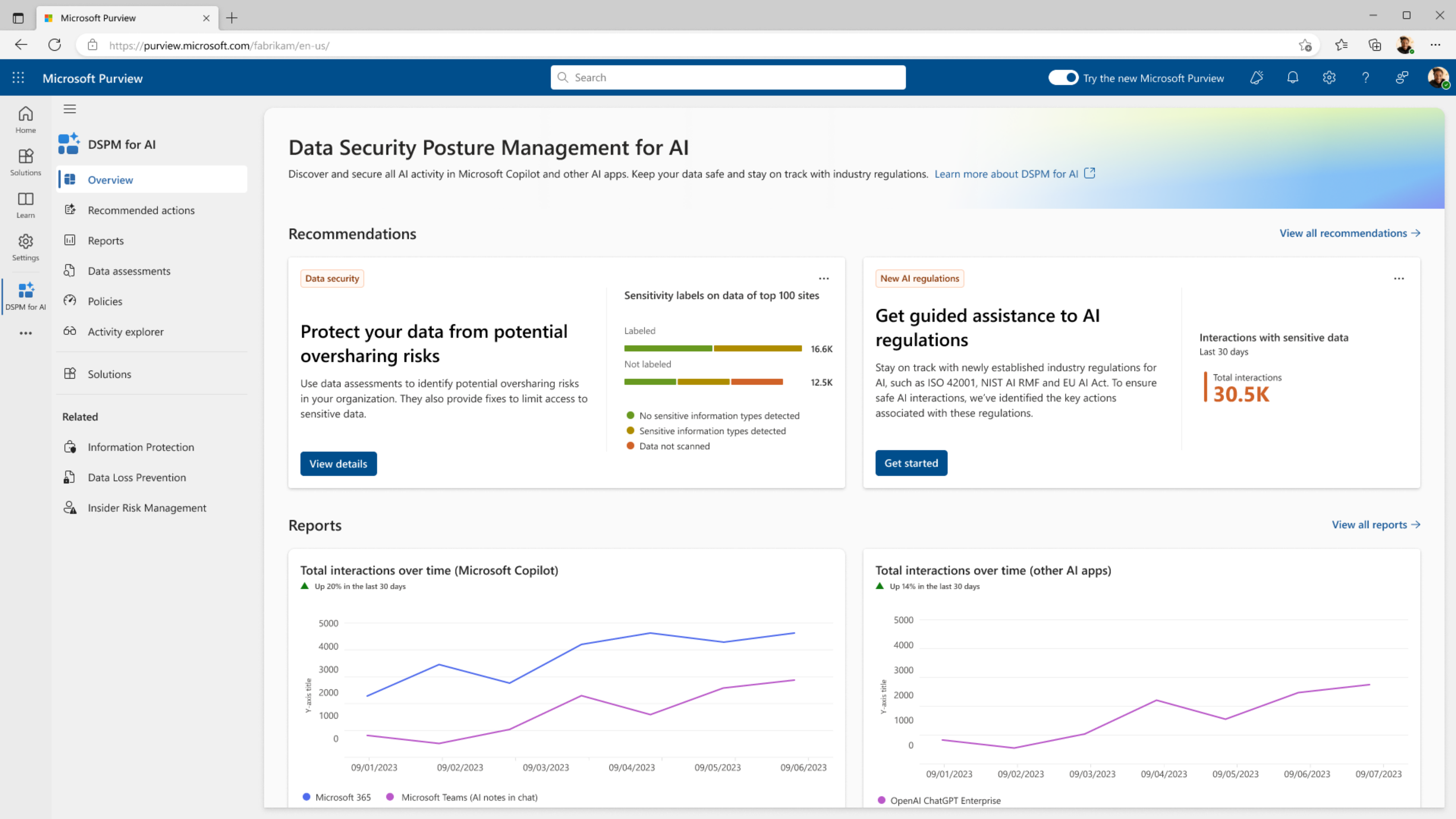
Data leak:
Users may inadvertently leak sensitive data to AI apps



3

Non-compliant usage:
Users use AI apps to generate unethical or other high-risk content





Data Security Posture Management for AI

Discover and secure all AI activity in Microsoft Copilot and other AI apps. Keep your data safe and stay on track with industry regulations. Learn more about DSPM for AI

Recommendations

Protect your data from potential oversharing risks

Use data assessments to identify potential oversharing risks in your organization. They also provide fixes to limit access to sensitive data.

View details
Sensitivity labels on data of top 100 sites
Labeled
16.6K
Not labeled
12.5K
● No sensitive information types detected
● Sensitive information types detected
● Data not scanned

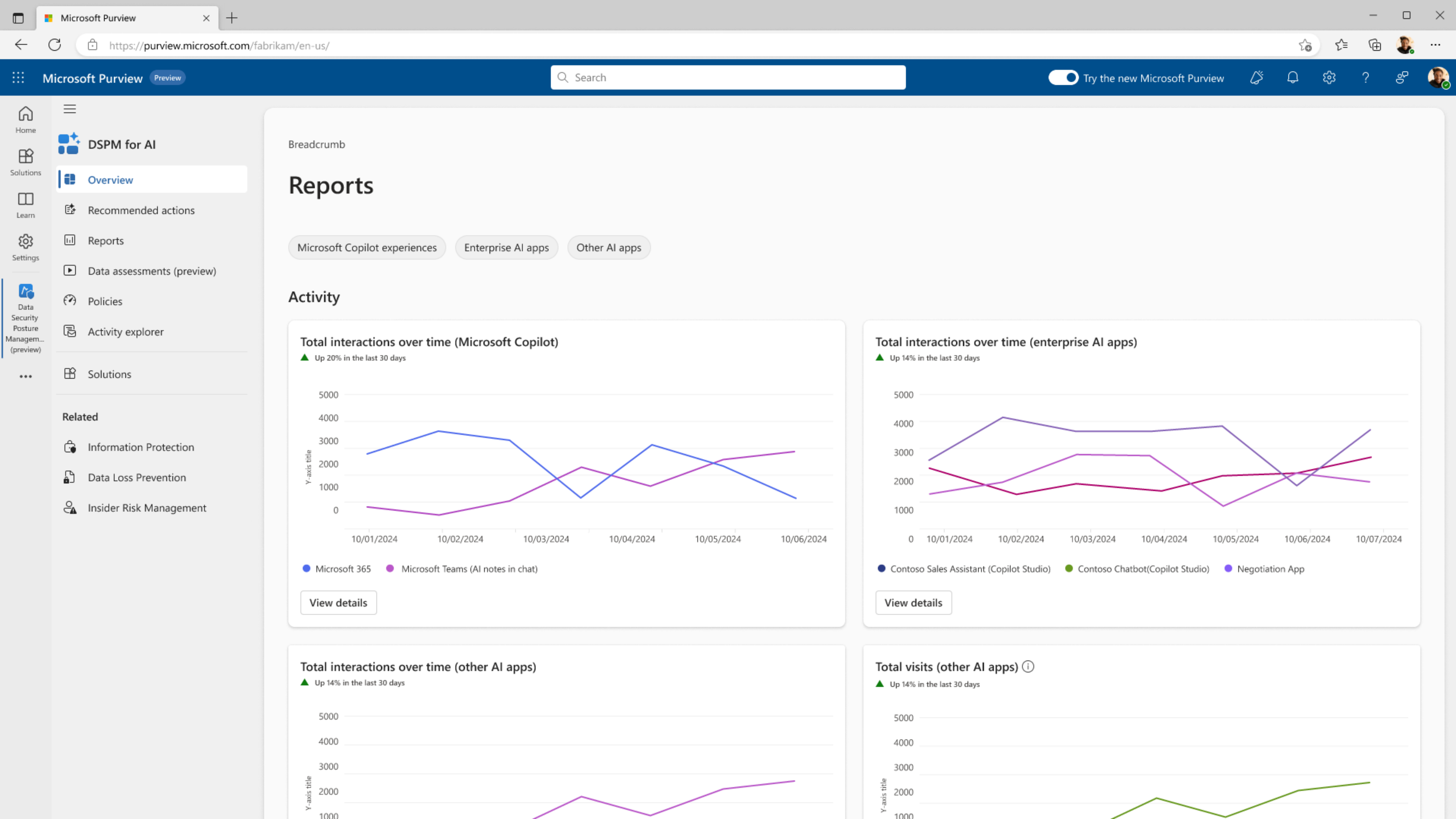
Get guided assistance to AI regulations

Stay on track with newly established industry regulations for AI, such as ISO 42001, NIST AI RMF and EU AI Act. To ensure safe AI interactions, we've identified the key actions associated with these regulations.

Reports

Total interactions over time (Microsoft Copilot)

Total interactions over time (other AI apps)



Reports

Activity

Total interactions over time (Microsoft Copilot)

Up 20% in the last 30 days

Total interactions over time (enterprise AI apps)

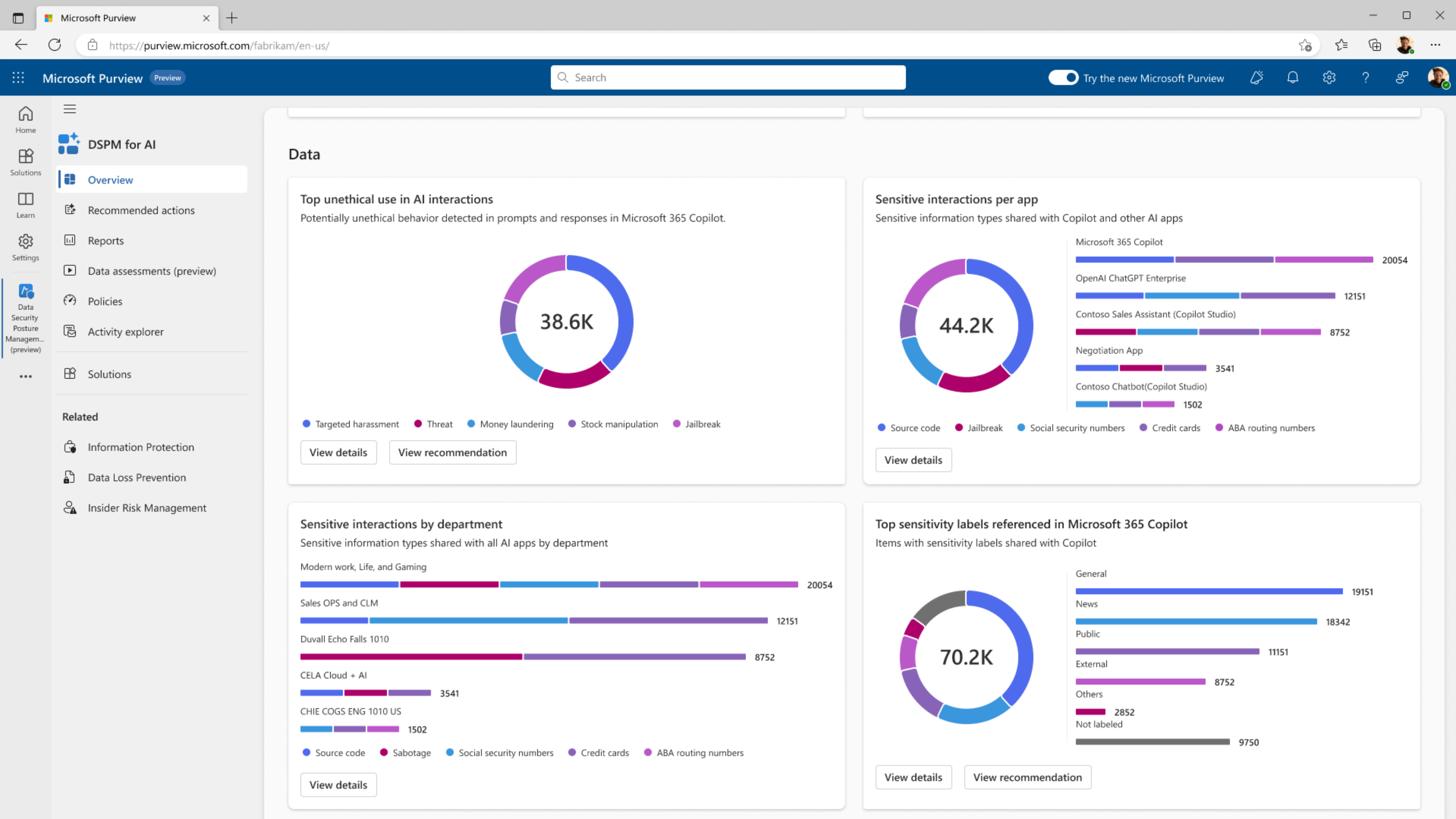
Up 14% in the last 30 days

Total interactions over time (other AI apps)

Up 14% in the last 30 days

Total visits (other AI apps)

Up 14% in the last 30 days



Data

Top unethical use in AI interactions

Potentially unethical behavior detected in prompts and responses in Microsoft 365 Copilot.

38.6K

● Targeted harassment ● Threat ● Money laundering ● Stock manipulation ● Jailbreak

Sensitive interactions per app

Sensitive information types shared with Copilot and other AI apps

44.2K

Microsoft 365 Copilot	20054
OpenAI ChatGPT Enterprise	12151
Contoso Sales Assistant (Copilot Studio)	8752
Negotiation App	3541
Contoso Chatbot(Copilot Studio)	1502

● Source code ● Jailbreak ● Social security numbers ● Credit cards ● ABA routing numbers

Sensitive interactions by department

Sensitive information types shared with all AI apps by department

Modern work, Life, and Gaming	20054
Sales OPS and CLM	12151
Duvall Echo Falls 1010	8752
CELA Cloud + AI	3541
CHIE COGS ENG 1010 US	1502

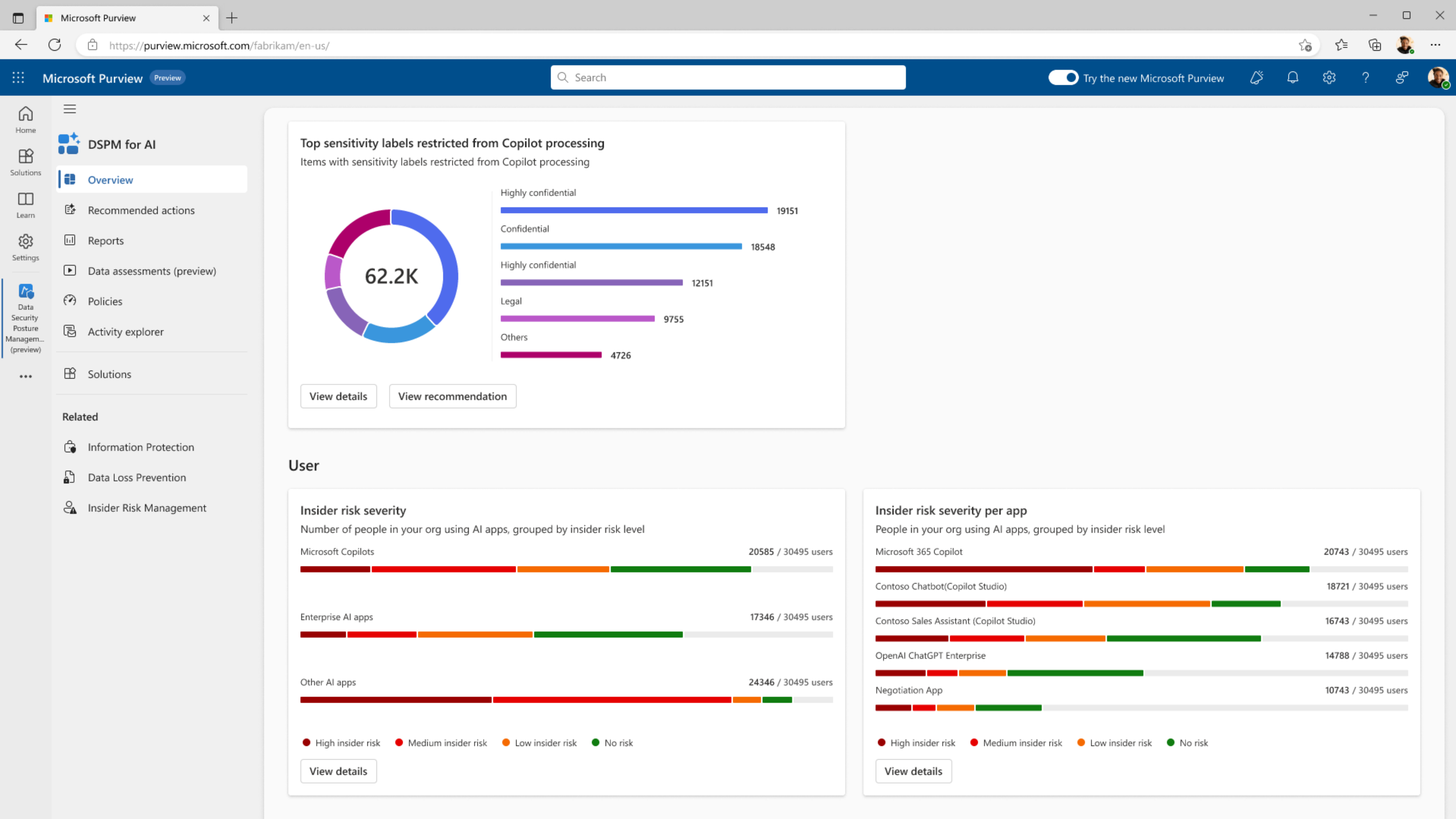
● Source code ● Sabotage ● Social security numbers ● Credit cards ● ABA routing numbers

Top sensitivity labels referenced in Microsoft 365 Copilot

Items with sensitivity labels shared with Copilot

70.2K

General	19151
News	18342
Public	11151
External	8752
Others	2852
Not labeled	9750



Top sensitivity labels restricted from Copilot processing

Items with sensitivity labels restricted from Copilot processing

62.2K

Label	Items
Highly confidential	19151
Confidential	18548
Highly confidential	12151
Legal	9755
Others	4726

View details | View recommendation

User

Insider risk severity

Number of people in your org using AI apps, grouped by insider risk level

Microsoft Copilots	20585 / 30495 users
Enterprise AI apps	17346 / 30495 users
Other AI apps	24346 / 30495 users

● High insider risk ● Medium insider risk ● Low insider risk ● No risk

View details

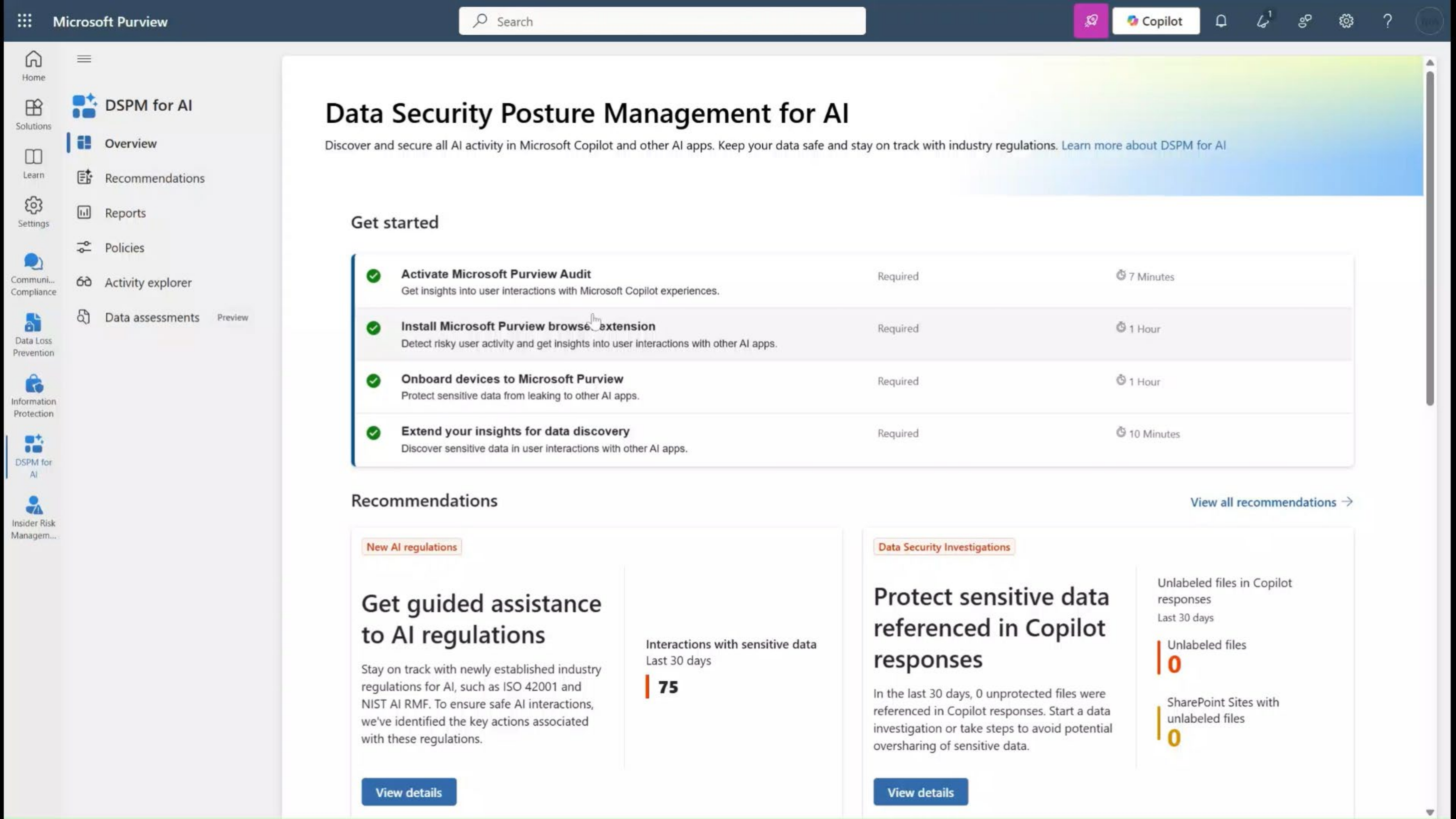
Insider risk severity per app

People in your org using AI apps, grouped by insider risk level

Microsoft 365 Copilot	20743 / 30495 users
Contoso Chatbot(Copilot Studio)	18721 / 30495 users
Contoso Sales Assistant (Copilot Studio)	16743 / 30495 users
OpenAI ChatGPT Enterprise	14788 / 30495 users
Negotiation App	10743 / 30495 users

● High insider risk ● Medium insider risk ● Low insider risk ● No risk

View details



Data Security Posture Management for AI

Discover and secure all AI activity in Microsoft Copilot and other AI apps. Keep your data safe and stay on track with industry regulations. Learn more about DSPM for AI

Get started

✓ **Activate Microsoft Purview Audit** Get insights into user interactions with Microsoft Copilot experiences.	Required	7 Minutes
✓ **Install Microsoft Purview browser extension** Detect risky user activity and get insights into user interactions with other AI apps.	Required	1 Hour
✓ **Onboard devices to Microsoft Purview** Protect sensitive data from leaking to other AI apps.	Required	1 Hour
✓ **Extend your insights for data discovery** Discover sensitive data in user interactions with other AI apps.	Required	10 Minutes

Recommendations

View all recommendations →

New AI regulations

Get guided assistance to AI regulations

Stay on track with newly established industry regulations for AI, such as ISO 42001 and NIST AI RMF. To ensure safe AI interactions, we've identified the key actions associated with these regulations.

Interactions with sensitive data
Last 30 days
75

View details

Data Security Investigations

Protect sensitive data referenced in Copilot responses

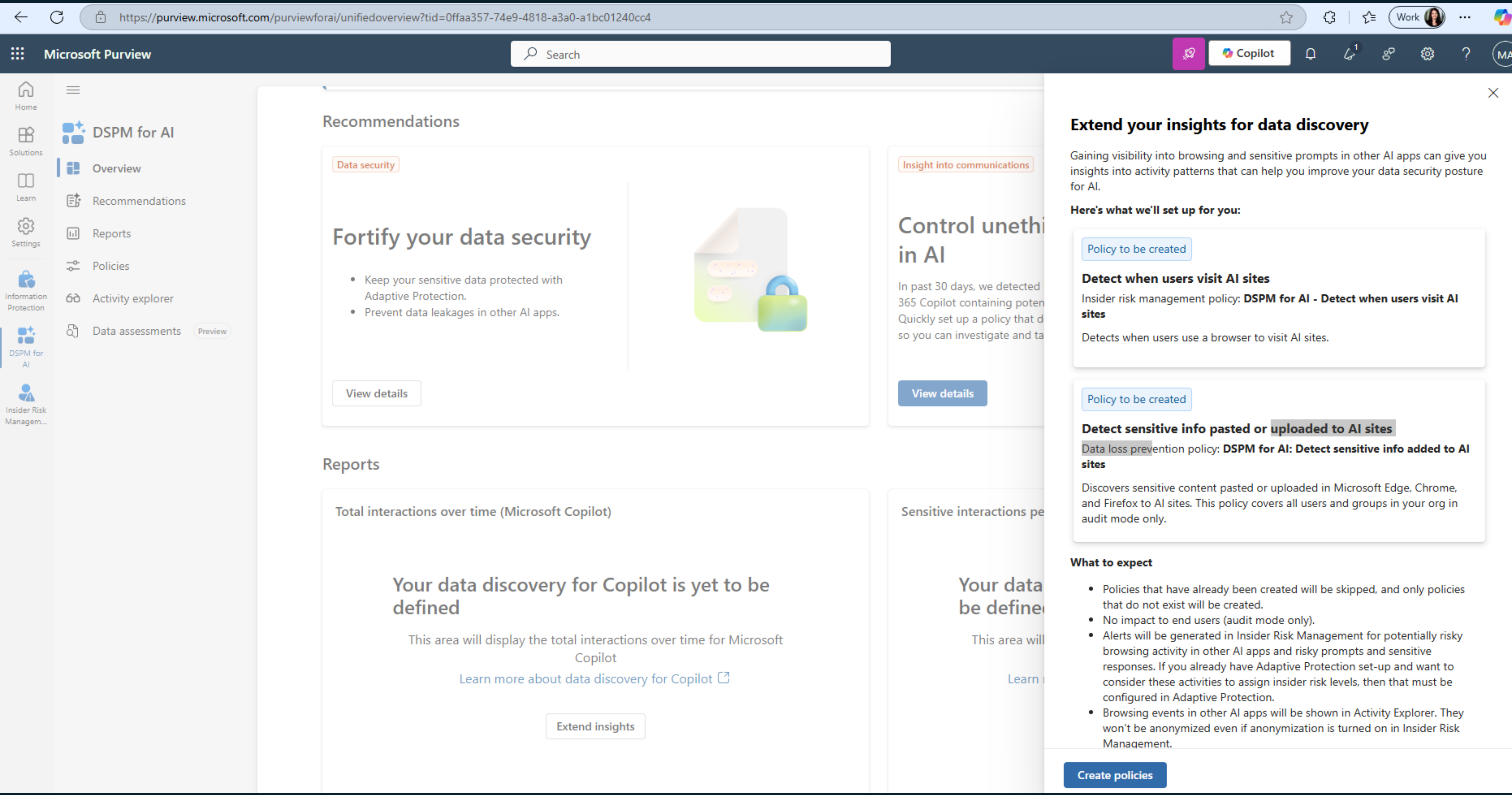
In the last 30 days, 0 unprotected files were referenced in Copilot responses. Start a data investigation or take steps to avoid potential oversharing of sensitive data.

Unlabeled files in Copilot responses
Last 30 days

Unlabeled files
0

SharePoint Sites with unlabeled files
0

View details



Recommendations

Data security

Fortify your data security

- Keep your sensitive data protected with Adaptive Protection.
- Prevent data leakages in other AI apps.

View details

Insight into communications

Control unethi in AI

In past 30 days, we detected 365 Copilot containing poten Quickly set up a policy that d so you can investigate and ta

View details

Reports

Total interactions over time (Microsoft Copilot)

Your data discovery for Copilot is yet to be defined

This area will display the total interactions over time for Microsoft Copilot

Learn more about data discovery for Copilot

Extend insights

Sensitive interactions pe

Your data be define

This area will

Learn

Extend your insights for data discovery

Gaining visibility into browsing and sensitive prompts in other AI apps can give you insights into activity patterns that can help you improve your data security posture for AI.

Here's what we'll set up for you:

Policy to be created

Detect when users visit AI sites

Insider risk management policy: **DSPM for AI - Detect when users visit AI sites**

Detects when users use a browser to visit AI sites.

Policy to be created

Detect sensitive info pasted or uploaded to AI sites

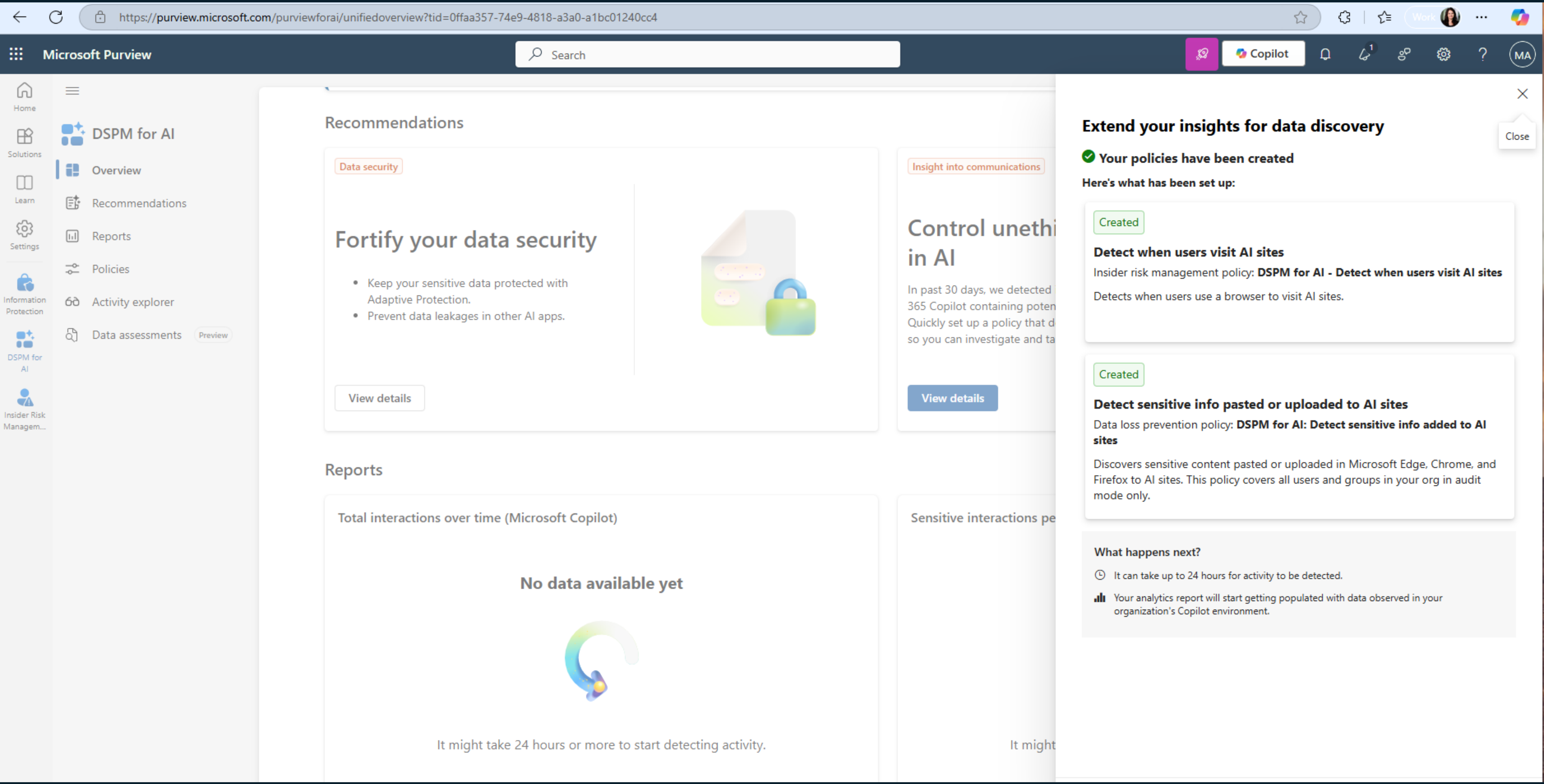
Data loss prevention policy: **DSPM for AI: Detect sensitive info added to AI sites**

Discovers sensitive content pasted or uploaded in Microsoft Edge, Chrome, and Firefox to AI sites. This policy covers all users and groups in your org in audit mode only.

What to expect

- Policies that have already been created will be skipped, and only policies that do not exist will be created.
- No impact to end users (audit mode only).
- Alerts will be generated in Insider Risk Management for potentially risky browsing activity in other AI apps and risky prompts and sensitive responses. If you already have Adaptive Protection set-up and want to consider these activities to assign insider risk levels, then that must be configured in Adaptive Protection.
- Browsing events in other AI apps will be shown in Activity Explorer. They won't be anonymized even if anonymization is turned on in Insider Risk Management.

Create policies



Recommendations

Data security

Fortify your data security

- Keep your sensitive data protected with Adaptive Protection.
- Prevent data leakages in other AI apps.

View details

Insight into communications

Control unethi in AI

In past 30 days, we detected 365 Copilot containing poten Quickly set up a policy that d so you can investigate and ta

View details

Reports

Total interactions over time (Microsoft Copilot)

No data available yet

It might take 24 hours or more to start detecting activity.

Sensitive interactions pe

It might

Extend your insights for data discovery

✓ **Your policies have been created**

Here's what has been set up:

Created

Detect when users visit AI sites

Insider risk management policy: **DSPM for AI - Detect when users visit AI sites**

Detects when users use a browser to visit AI sites.

Created

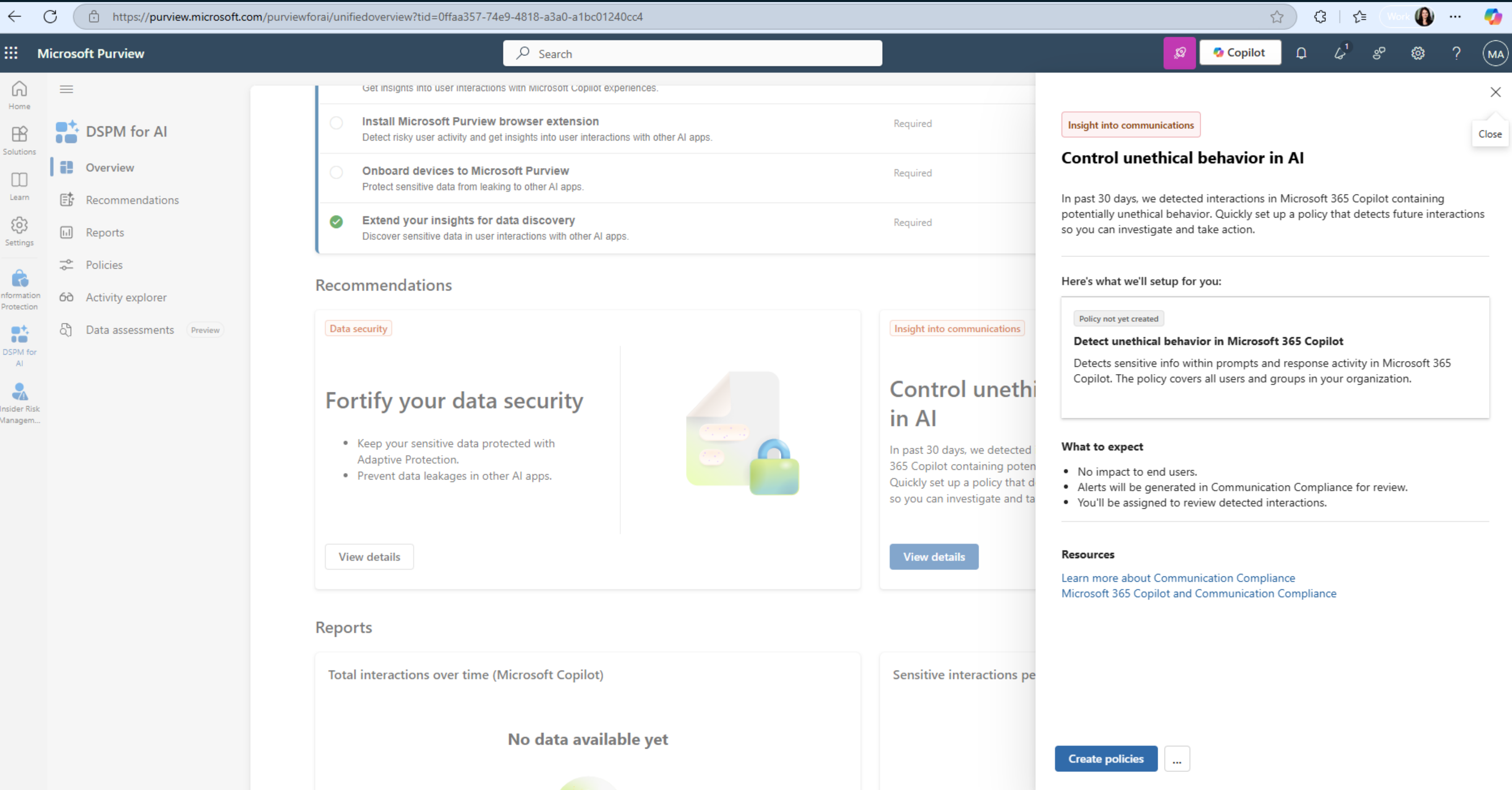
Detect sensitive info pasted or uploaded to AI sites

Data loss prevention policy: **DSPM for AI: Detect sensitive info added to AI sites**

Discovers sensitive content pasted or uploaded in Microsoft Edge, Chrome, and Firefox to AI sites. This policy covers all users and groups in your org in audit mode only.

What happens next?

- It can take up to 24 hours for activity to be detected.
- Your analytics report will start getting populated with data observed in your organization's Copilot environment.



Get insights into user interactions with Microsoft Copilot experiences.

○ **Install Microsoft Purview browser extension** — Required
Detect risky user activity and get insights into user interactions with other AI apps.

○ **Onboard devices to Microsoft Purview** — Required
Protect sensitive data from leaking to other AI apps.

✓ **Extend your insights for data discovery** — Required
Discover sensitive data in user interactions with other AI apps.

Recommendations

Data security

Fortify your data security

- Keep your sensitive data protected with Adaptive Protection.
- Prevent data leakages in other AI apps.

View details

Insight into communications

Control unethi in AI

In past 30 days, we detected 365 Copilot containing poten Quickly set up a policy that d so you can investigate and ta

View details

Reports

Total interactions over time (Microsoft Copilot)

No data available yet

Sensitive interactions pe

Insight into communications

Close

Control unethical behavior in AI

In past 30 days, we detected interactions in Microsoft 365 Copilot containing potentially unethical behavior. Quickly set up a policy that detects future interactions so you can investigate and take action.

Here's what we'll setup for you:

Policy not yet created

Detect unethical behavior in Microsoft 365 Copilot

Detects sensitive info within prompts and response activity in Microsoft 365 Copilot. The policy covers all users and groups in your organization.

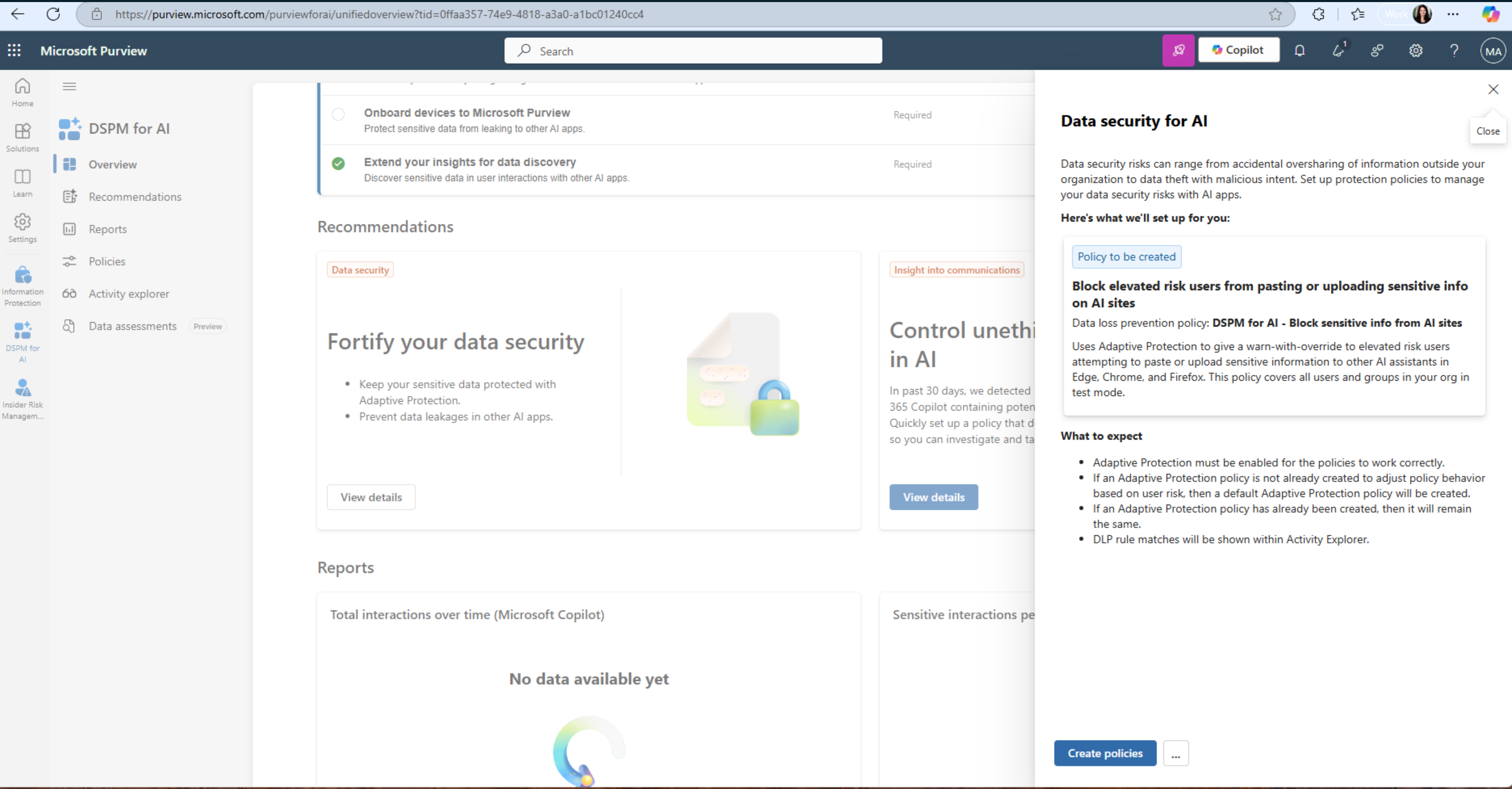
What to expect

- No impact to end users.
- Alerts will be generated in Communication Compliance for review.
- You'll be assigned to review detected interactions.

Resources

Learn more about Communication Compliance
Microsoft 365 Copilot and Communication Compliance

Create policies ...



○ **Onboard devices to Microsoft Purview** — Required
Protect sensitive data from leaking to other AI apps.

✓ **Extend your insights for data discovery** — Required
Discover sensitive data in user interactions with other AI apps.

Recommendations

Data security

Fortify your data security

- Keep your sensitive data protected with Adaptive Protection.
- Prevent data leakages in other AI apps.

View details

Insight into communications

Control unethi in AI

In past 30 days, we detected 365 Copilot containing poten Quickly set up a policy that d so you can investigate and ta

View details

Reports

Total interactions over time (Microsoft Copilot)

No data available yet

Sensitive interactions pe

Data security for AI

Close

Data security risks can range from accidental oversharing of information outside your organization to data theft with malicious intent. Set up protection policies to manage your data security risks with AI apps.

Here's what we'll set up for you:

Policy to be created

Block elevated risk users from pasting or uploading sensitive info on AI sites

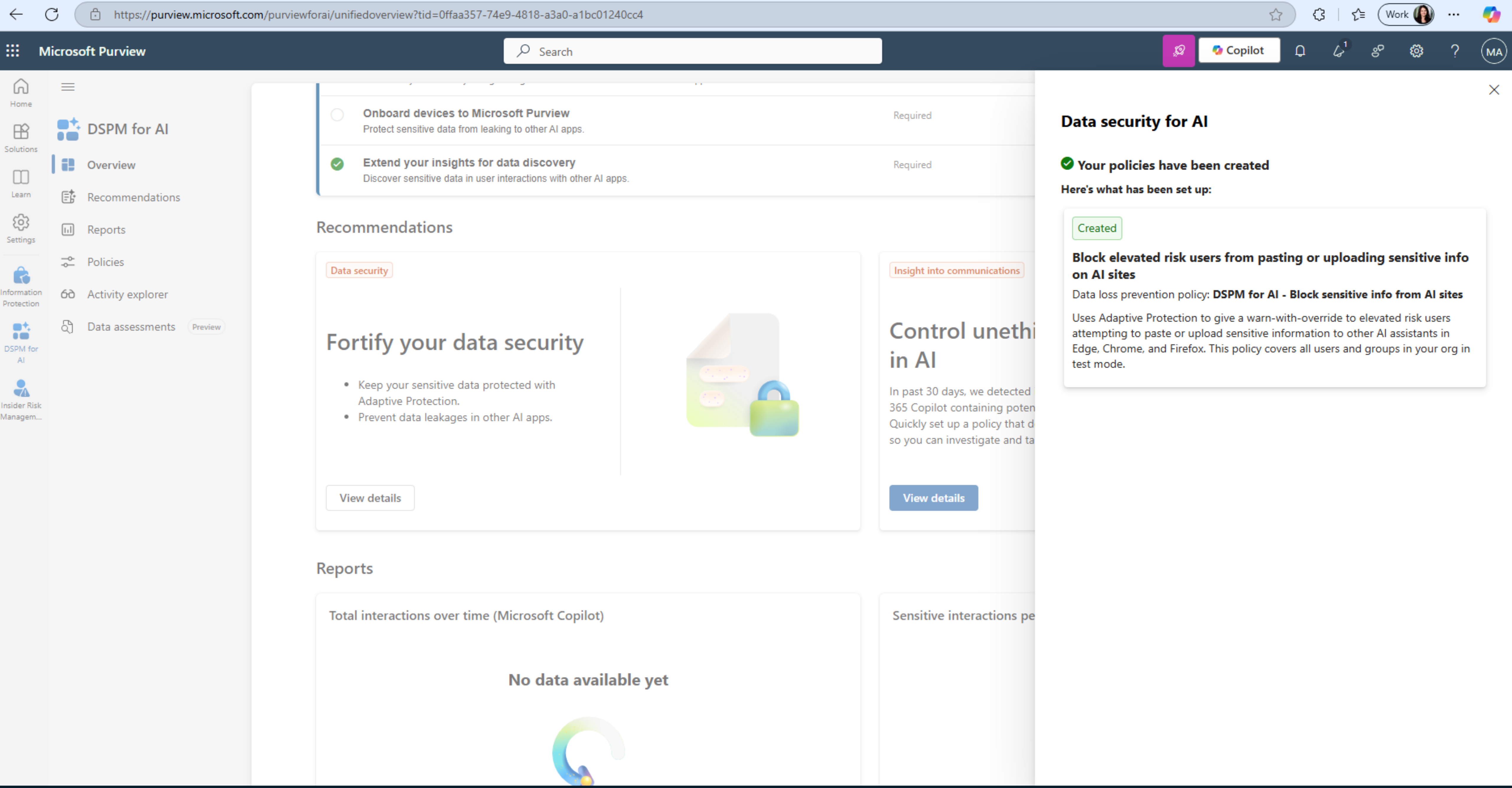
Data loss prevention policy: **DSPM for AI - Block sensitive info from AI sites**

Uses Adaptive Protection to give a warn-with-override to elevated risk users attempting to paste or upload sensitive information to other AI assistants in Edge, Chrome, and Firefox. This policy covers all users and groups in your org in test mode.

What to expect

- Adaptive Protection must be enabled for the policies to work correctly.
- If an Adaptive Protection policy is not already created to adjust policy behavior based on user risk, then a default Adaptive Protection policy will be created.
- If an Adaptive Protection policy has already been created, then it will remain the same.
- DLP rule matches will be shown within Activity Explorer.

Create policies   ...



○ **Onboard devices to Microsoft Purview**
Protect sensitive data from leaking to other AI apps.
Required

✓ **Extend your insights for data discovery**
Discover sensitive data in user interactions with other AI apps.
Required

Recommendations

Data security

Fortify your data security

- Keep your sensitive data protected with Adaptive Protection.
- Prevent data leakages in other AI apps.

View details

Insight into communications

Control unethi in AI

In past 30 days, we detected 365 Copilot containing poten Quickly set up a policy that d so you can investigate and ta

View details

Reports

Total interactions over time (Microsoft Copilot)

No data available yet

Sensitive interactions pe

Data security for AI

✓ **Your policies have been created**

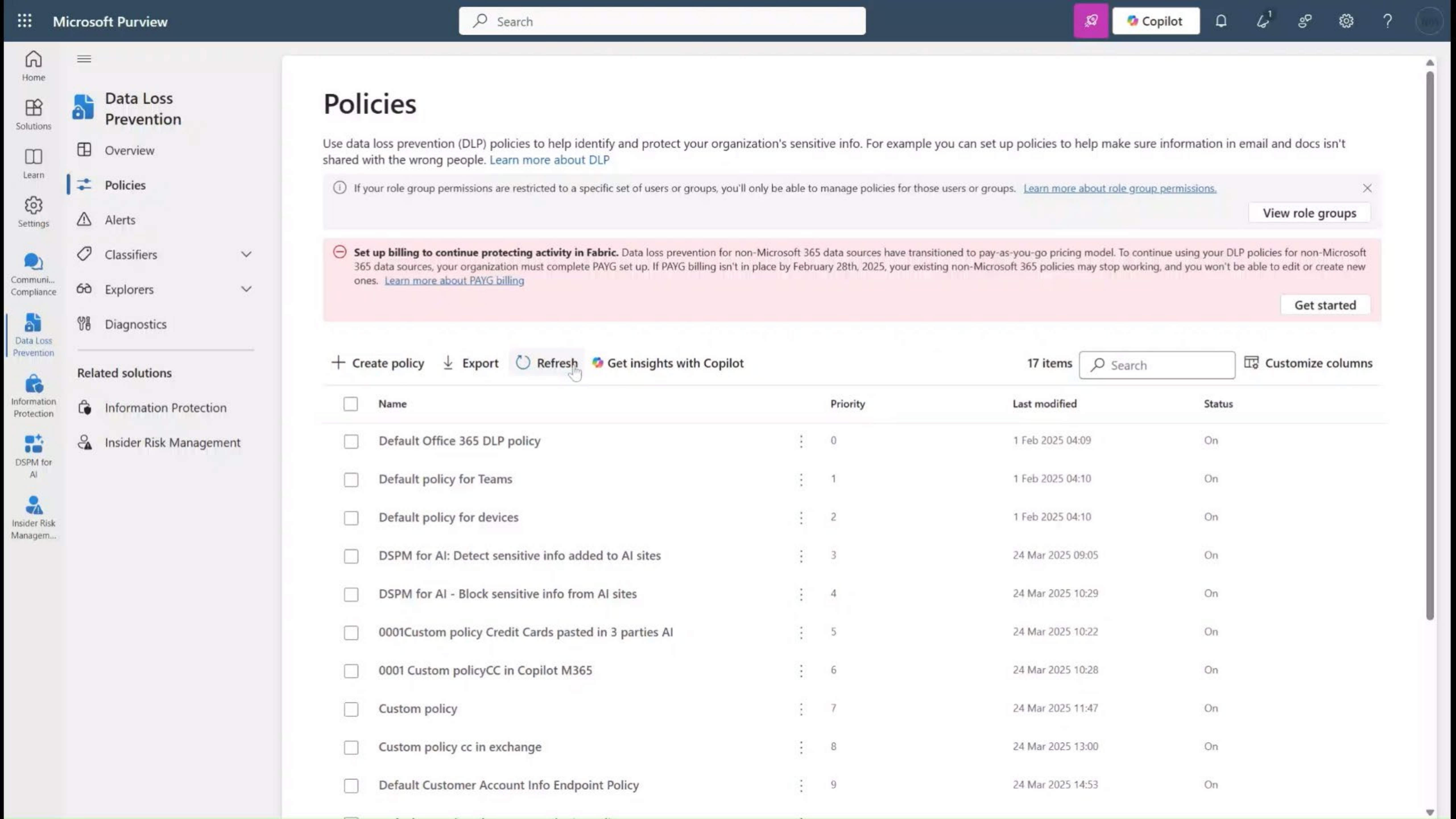
Here's what has been set up:

Created

Block elevated risk users from pasting or uploading sensitive info on AI sites

Data loss prevention policy: **DSPM for AI - Block sensitive info from AI sites**

Uses Adaptive Protection to give a warn-with-override to elevated risk users attempting to paste or upload sensitive information to other AI assistants in Edge, Chrome, and Firefox. This policy covers all users and groups in your org in test mode.



Policies

Use data loss prevention (DLP) policies to help identify and protect your organization's sensitive info. For example you can set up policies to help make sure information in email and docs isn't shared with the wrong people. Learn more about DLP

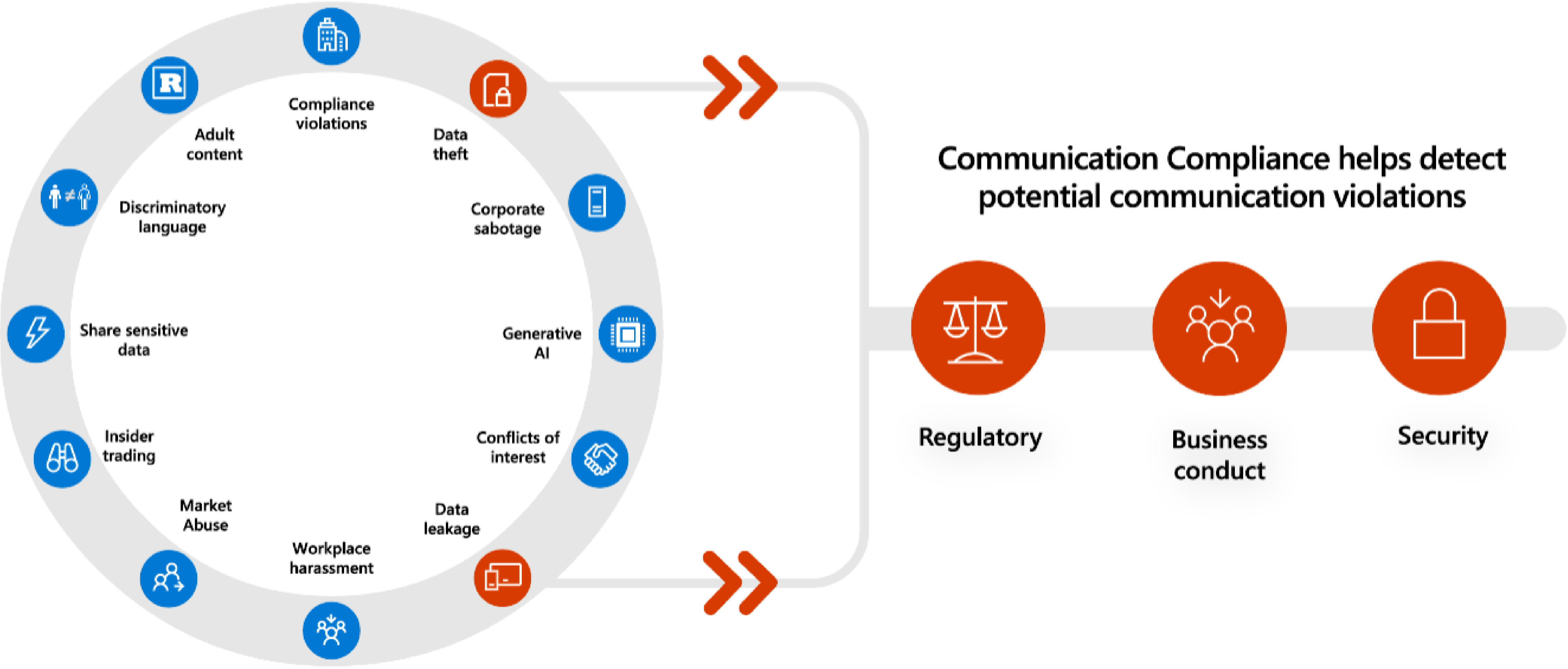
If your role group permissions are restricted to a specific set of users or groups, you'll only be able to manage policies for those users or groups. Learn more about role group permissions.

Set up billing to continue protecting activity in Fabric. Data loss prevention for non-Microsoft 365 data sources have transitioned to pay-as-you-go pricing model. To continue using your DLP policies for non-Microsoft 365 data sources, your organization must complete PAYG set up. If PAYG billing isn't in place by February 28th, 2025, your existing non-Microsoft 365 policies may stop working, and you won't be able to edit or create new ones. Learn more about PAYG billing

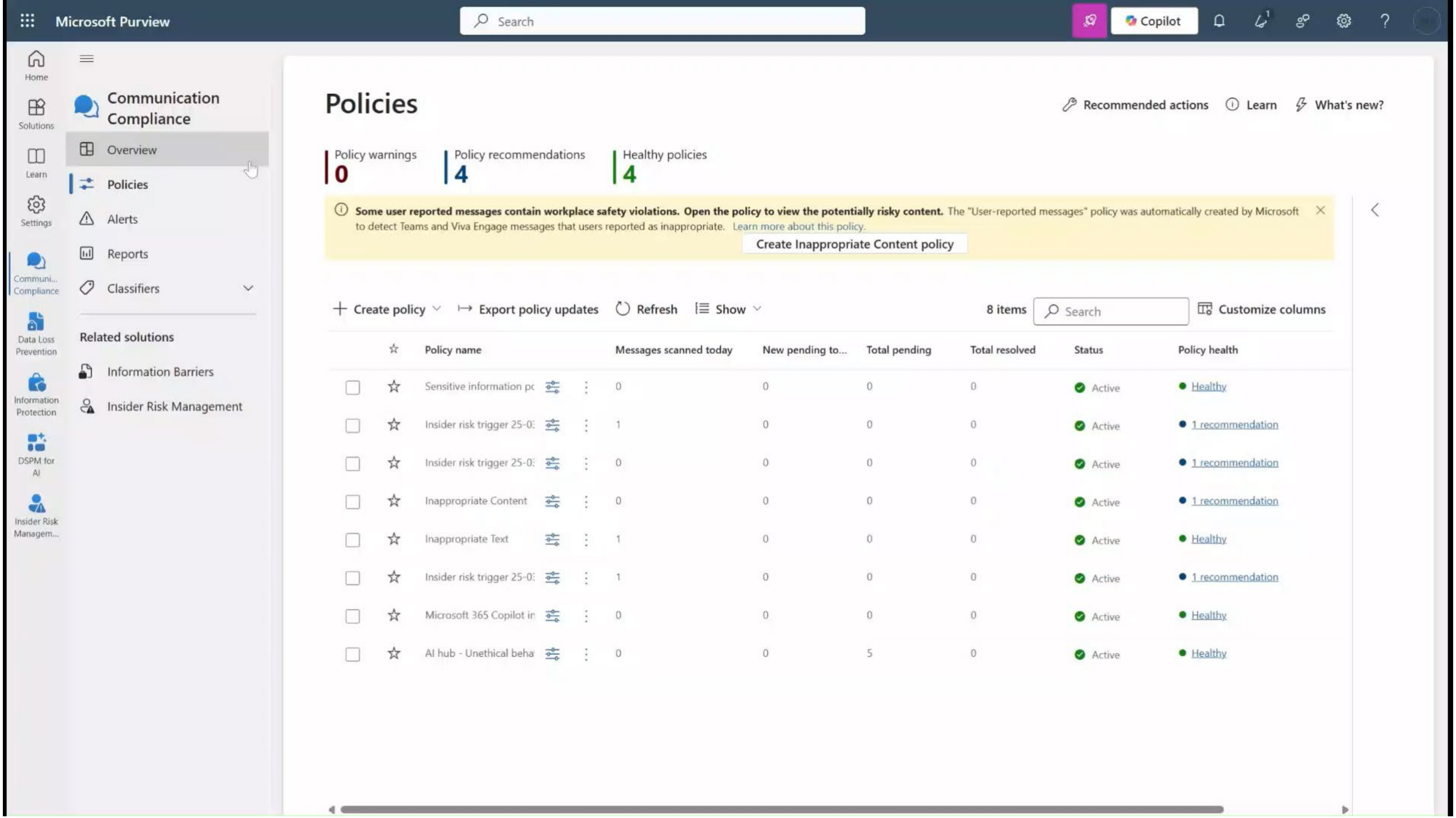
17 items

Name	Priority	Last modified	Status
Default Office 365 DLP policy	0	1 Feb 2025 04:09	On
Default policy for Teams	1	1 Feb 2025 04:10	On
Default policy for devices	2	1 Feb 2025 04:10	On
DSPM for AI: Detect sensitive info added to AI sites	3	24 Mar 2025 09:05	On
DSPM for AI - Block sensitive info from AI sites	4	24 Mar 2025 10:29	On
0001Custom policy Credit Cards pasted in 3 parties AI	5	24 Mar 2025 10:22	On
0001 Custom policyCC in Copilot M365	6	24 Mar 2025 10:28	On
Custom policy	7	24 Mar 2025 11:47	On
Custom policy cc in exchange	8	24 Mar 2025 13:00	On
Default Customer Account Info Endpoint Policy	9	24 Mar 2025 14:53	On

Organizations face a broad range of risks



Communication Compliance helps detect potential communication violations



Policies

Policy warnings 0

Policy recommendations 4

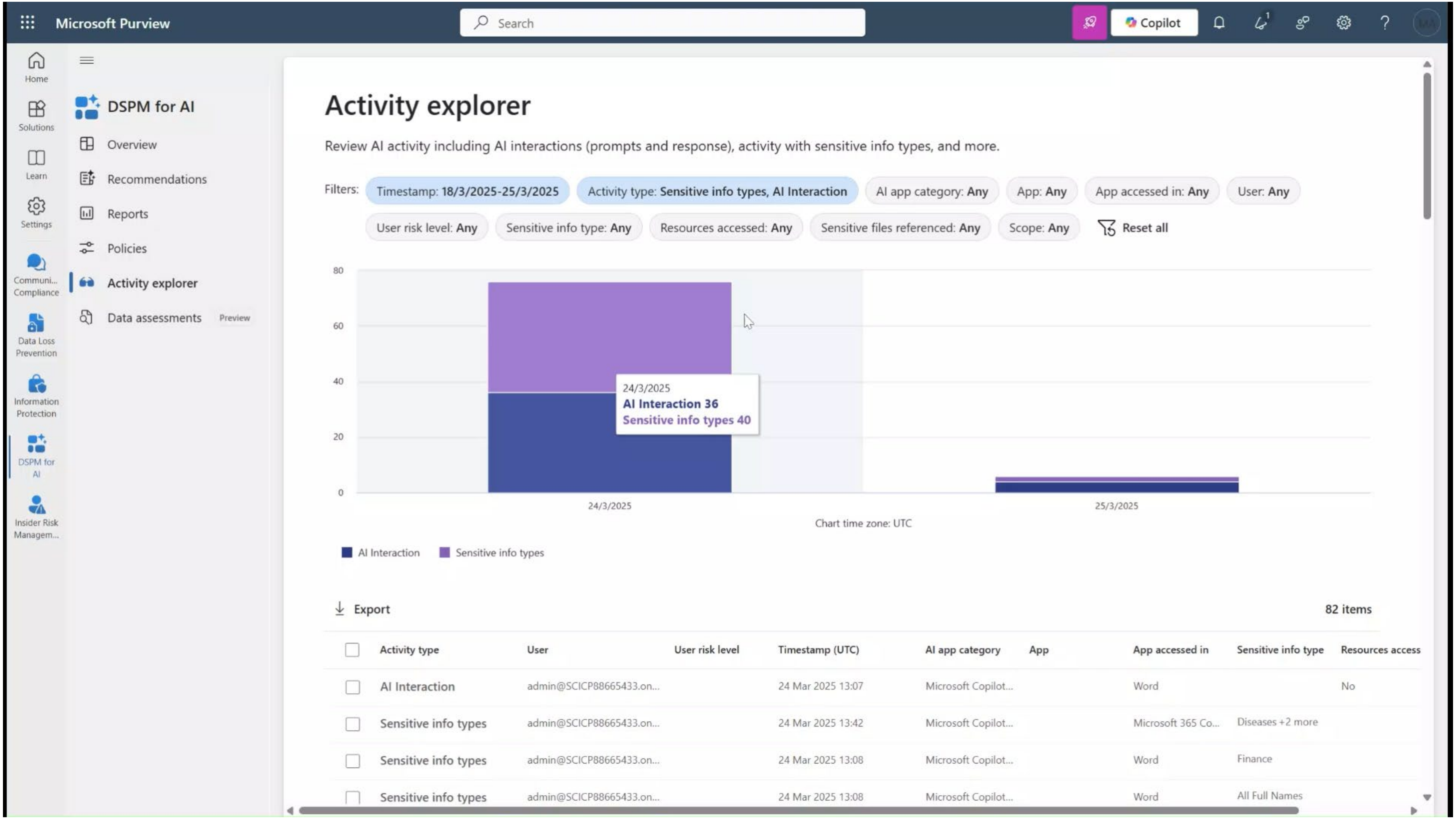
Healthy policies 4

Some user reported messages contain workplace safety violations. Open the policy to view the potentially risky content. The "User-reported messages" policy was automatically created by Microsoft to detect Teams and Viva Engage messages that users reported as inappropriate. Learn more about this policy.

Create Inappropriate Content policy

8 items

☆	Policy name	Messages scanned today	New pending to...	Total pending	Total resolved	Status	Policy health
☆	Sensitive information pc	0	0	0	0	Active	Healthy
☆	Insider risk trigger 25-0:	1	0	0	0	Active	1 recommendation
☆	Insider risk trigger 25-0:	0	0	0	0	Active	1 recommendation
☆	Inappropriate Content	0	0	0	0	Active	1 recommendation
☆	Inappropriate Text	1	0	0	0	Active	Healthy
☆	Insider risk trigger 25-0:	1	0	0	0	Active	1 recommendation
☆	Microsoft 365 Copilot in	0	0	0	0	Active	Healthy
☆	AI hub - Unethical beha	0	0	5	0	Active	Healthy



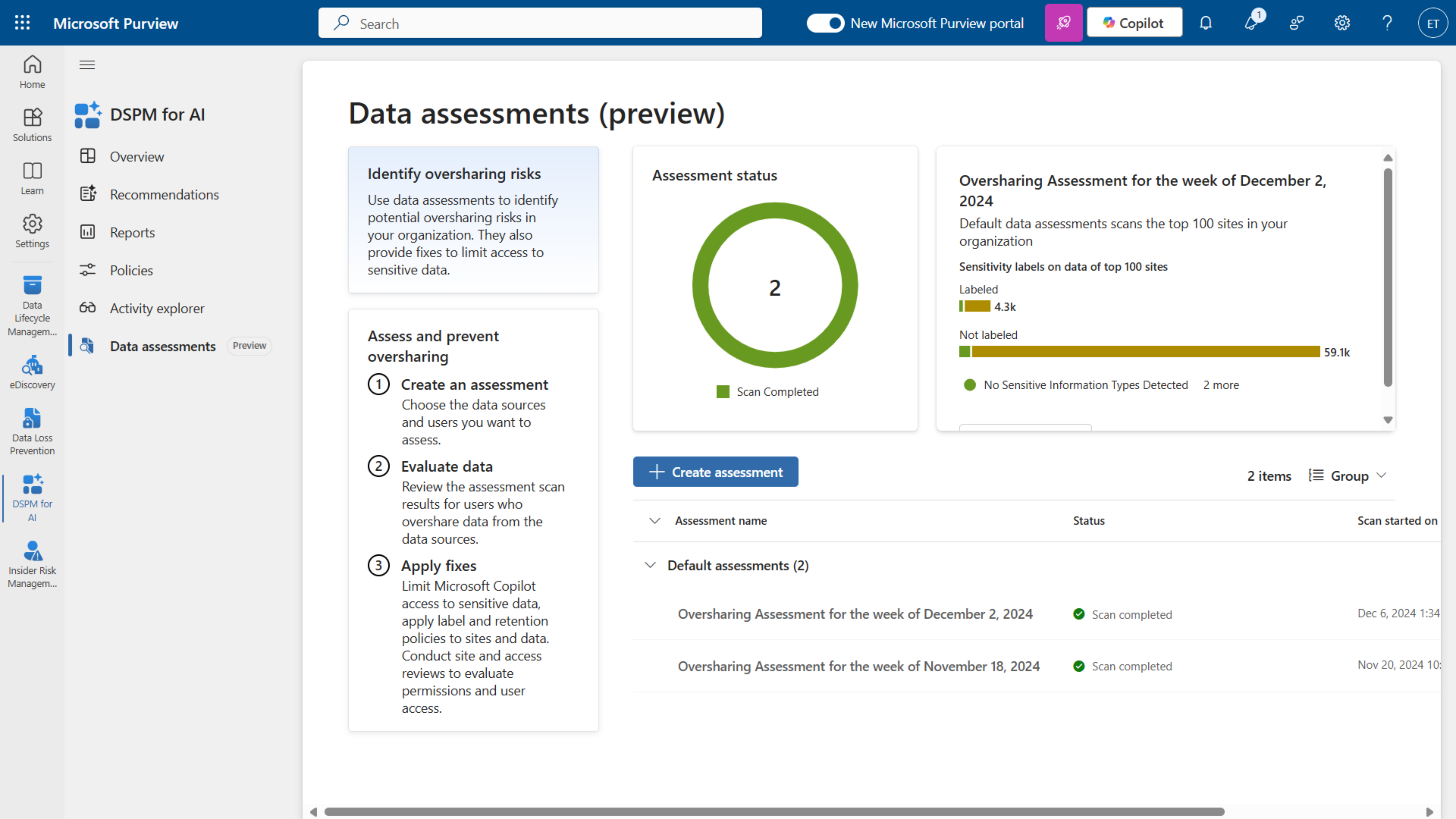
Activity explorer

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

Filters: Timestamp: **18/3/2025-25/3/2025** Activity type: **Sensitive info types, AI Interaction** AI app category: **Any** App: **Any** App accessed in: **Any** User: **Any** User risk level: **Any** Sensitive info type: **Any** Resources accessed: **Any** Sensitive files referenced: **Any** Scope: **Any**

82 items

□	Activity type	User	User risk level	Timestamp (UTC)	AI app category	App	App accessed in	Sensitive info type	Resources access
□	AI Interaction	admin@SCICP88665433.on...		24 Mar 2025 13:07	Microsoft Copilot...		Word		No
□	Sensitive info types	admin@SCICP88665433.on...		24 Mar 2025 13:42	Microsoft Copilot...		Microsoft 365 Co...	Diseases +2 more	
□	Sensitive info types	admin@SCICP88665433.on...		24 Mar 2025 13:08	Microsoft Copilot...		Word	Finance	
□	Sensitive info types	admin@SCICP88665433.on...		24 Mar 2025 13:08	Microsoft Copilot...		Word	All Full Names	



Data assessments (preview)

Identify oversharing risks

Use data assessments to identify potential oversharing risks in your organization. They also provide fixes to limit access to sensitive data.

Assess and prevent oversharing

1. **Create an assessment**
   Choose the data sources and users you want to assess.
2. **Evaluate data**
   Review the assessment scan results for users who overshare data from the data sources.
3. **Apply fixes**
   Limit Microsoft Copilot access to sensitive data, apply label and retention policies to sites and data. Conduct site and access reviews to evaluate permissions and user access.

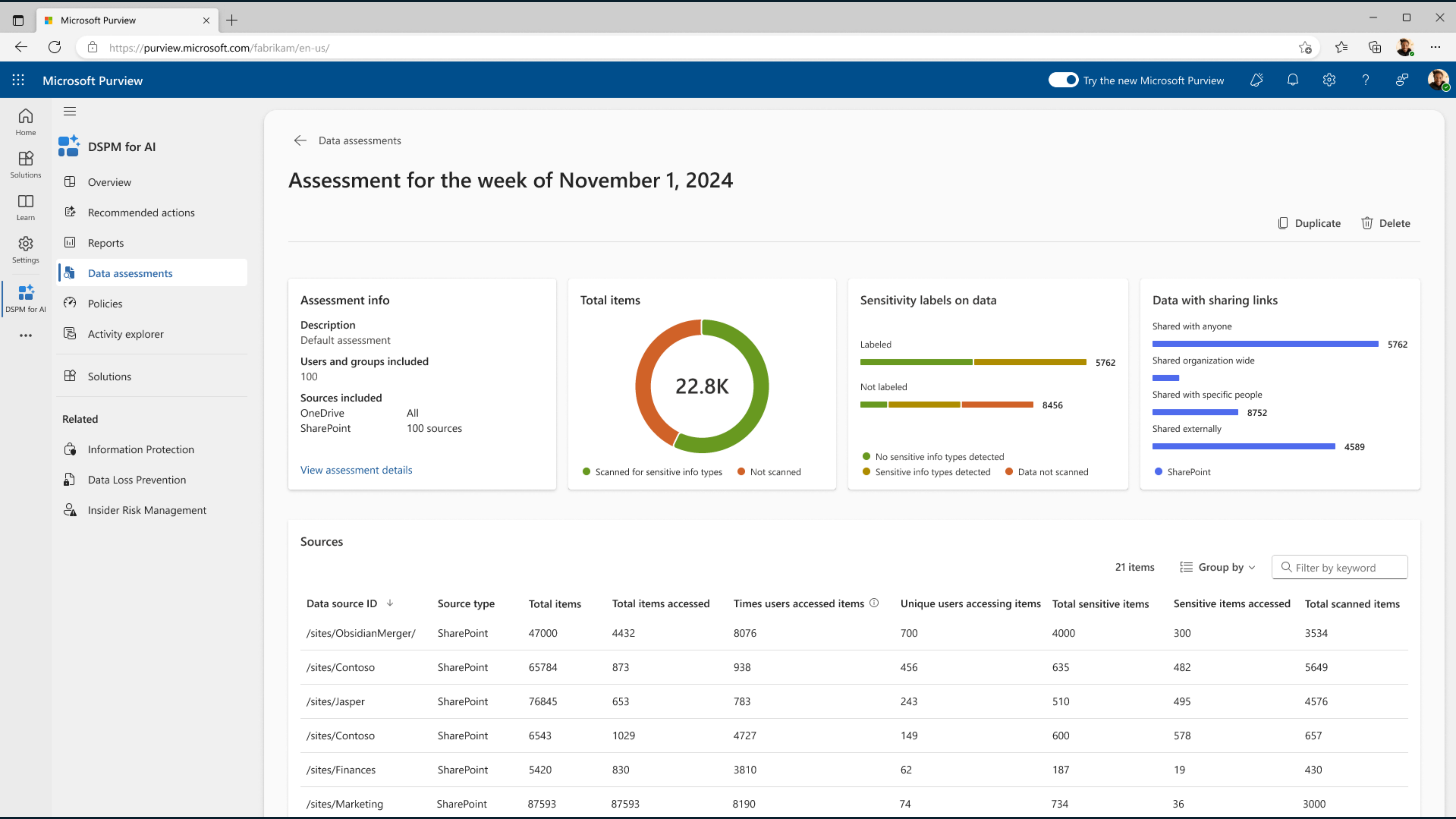
Assessment status

Oversharing Assessment for the week of December 2, 2024

Default data assessments scans the top 100 sites in your organization

Sensitivity labels on data of top 100 sites

Assessment name	Status	Scan started on
Default assessments (2)		
Oversharing Assessment for the week of December 2, 2024	✓ Scan completed	Dec 6, 2024 1:34
Oversharing Assessment for the week of November 18, 2024	✓ Scan completed	Nov 20, 2024 10:



Assessment for the week of November 1, 2024

Assessment info

Description
Default assessment

Users and groups included
100

Sources included

OneDrive	All
SharePoint	100 sources

View assessment details

Total items

Sensitivity labels on data

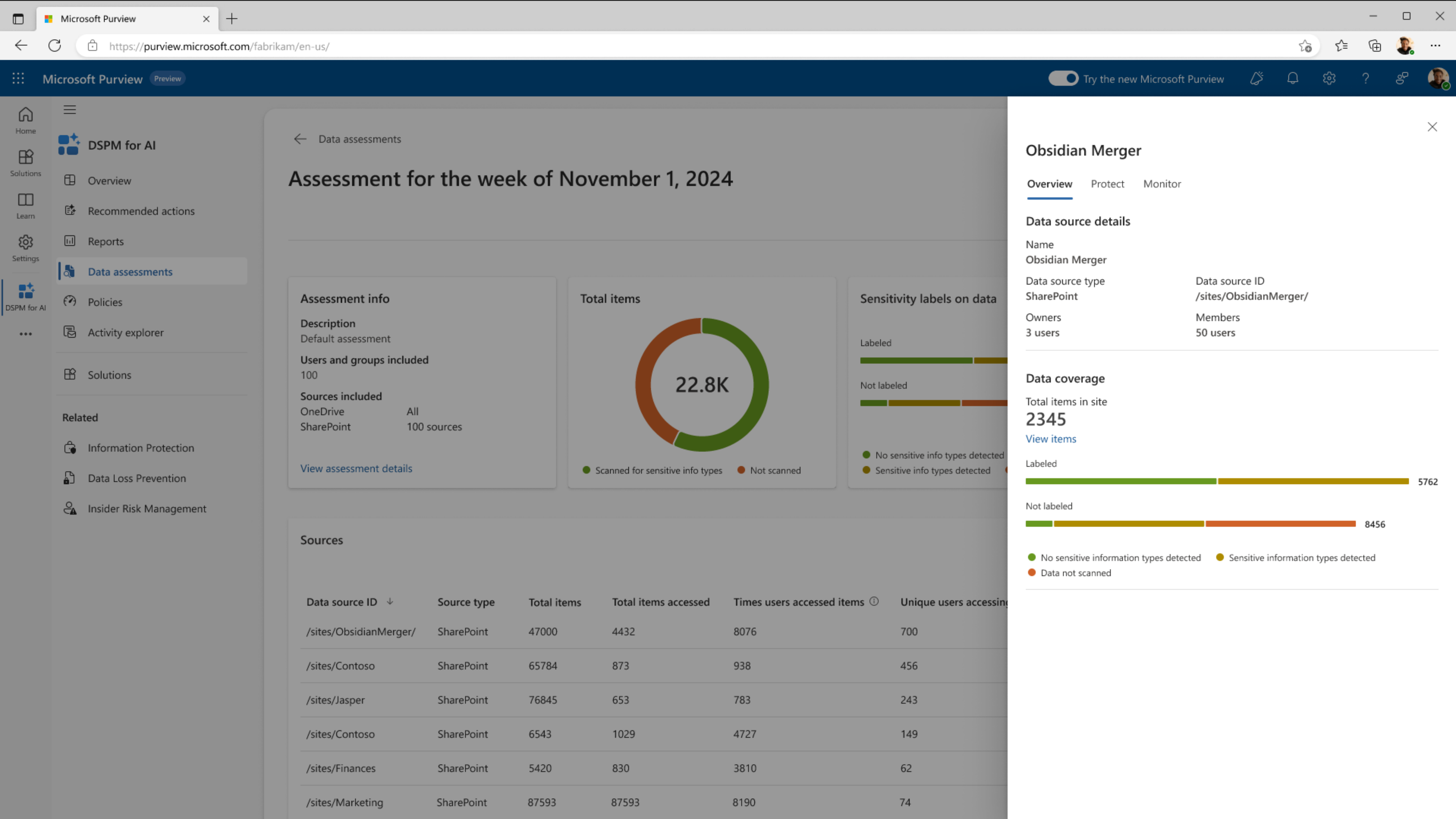
Labeled
5762
Not labeled
8456
● No sensitive info types detected
● Sensitive info types detected
● Data not scanned

Data with sharing links

Sources

21 items

Data source ID ↓	Source type	Total items	Total items accessed	Times users accessed items ⓘ	Unique users accessing items	Total sensitive items	Sensitive items accessed	Total scanned items
/sites/ObsidianMerger/	SharePoint	47000	4432	8076	700	4000	300	3534
/sites/Contoso	SharePoint	65784	873	938	456	635	482	5649
/sites/Jasper	SharePoint	76845	653	783	243	510	495	4576
/sites/Contoso	SharePoint	6543	1029	4727	149	600	578	657
/sites/Finances	SharePoint	5420	830	3810	62	187	19	430
/sites/Marketing	SharePoint	87593	87593	8190	74	734	36	3000



Assessment for the week of November 1, 2024

Assessment info

Description
Default assessment

Users and groups included
100

Sources included

OneDrive	All
SharePoint	100 sources

View assessment details

Total items

Sensitivity labels on data

Labeled
Not labeled
● No sensitive info types detected
● Sensitive info types detected

Sources

Data source ID ↓	Source type	Total items	Total items accessed	Times users accessed items ⓘ	Unique users accessing
/sites/ObsidianMerger/	SharePoint	47000	4432	8076	700
/sites/Contoso	SharePoint	65784	873	938	456
/sites/Jasper	SharePoint	76845	653	783	243
/sites/Contoso	SharePoint	6543	1029	4727	149
/sites/Finances	SharePoint	5420	830	3810	62
/sites/Marketing	SharePoint	87593	87593	8190	74

Obsidian Merger

Data source details

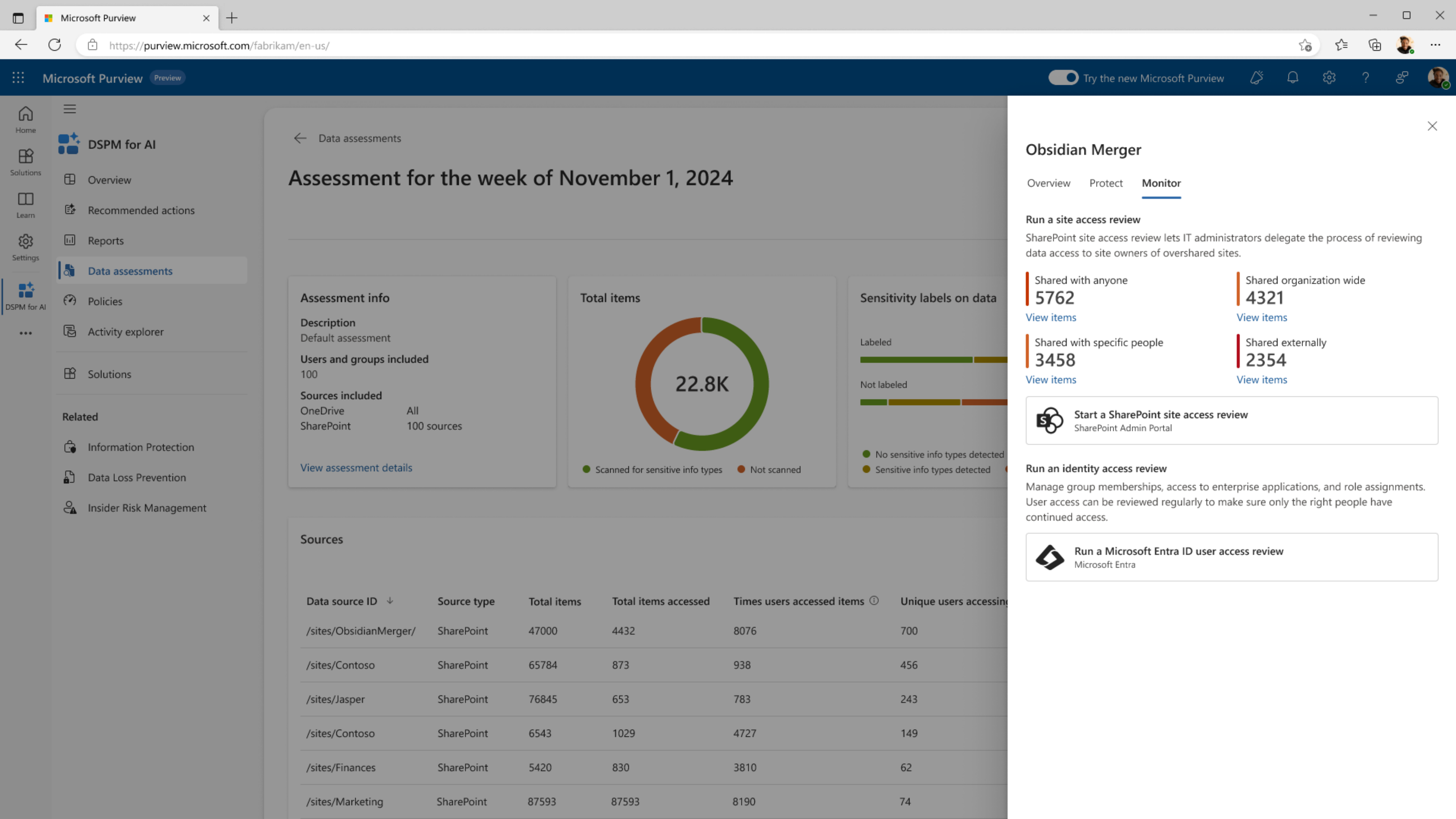
Name
Obsidian Merger

Data source type SharePoint	Data source ID /sites/ObsidianMerger/
Owners 3 users	Members 50 users

Data coverage

Total items in site
2345
View items

Labeled
5762
Not labeled
8456
● No sensitive information types detected
● Sensitive information types detected
● Data not scanned



Assessment for the week of November 1, 2024

Assessment info

Description
Default assessment

Users and groups included
100

Sources included

OneDrive	All
SharePoint	100 sources

View assessment details

Total items

Sensitivity labels on data

Labeled
Not labeled
● No sensitive info types detected
● Sensitive info types detected

Sources

Data source ID ↓	Source type	Total items	Total items accessed	Times users accessed items ⓘ	Unique users accessing
/sites/ObsidianMerger/	SharePoint	47000	4432	8076	700
/sites/Contoso	SharePoint	65784	873	938	456
/sites/Jasper	SharePoint	76845	653	783	243
/sites/Contoso	SharePoint	6543	1029	4727	149
/sites/Finances	SharePoint	5420	830	3810	62
/sites/Marketing	SharePoint	87593	87593	8190	74

Obsidian Merger

Run a site access review

SharePoint site access review lets IT administrators delegate the process of reviewing data access to site owners of overshared sites.

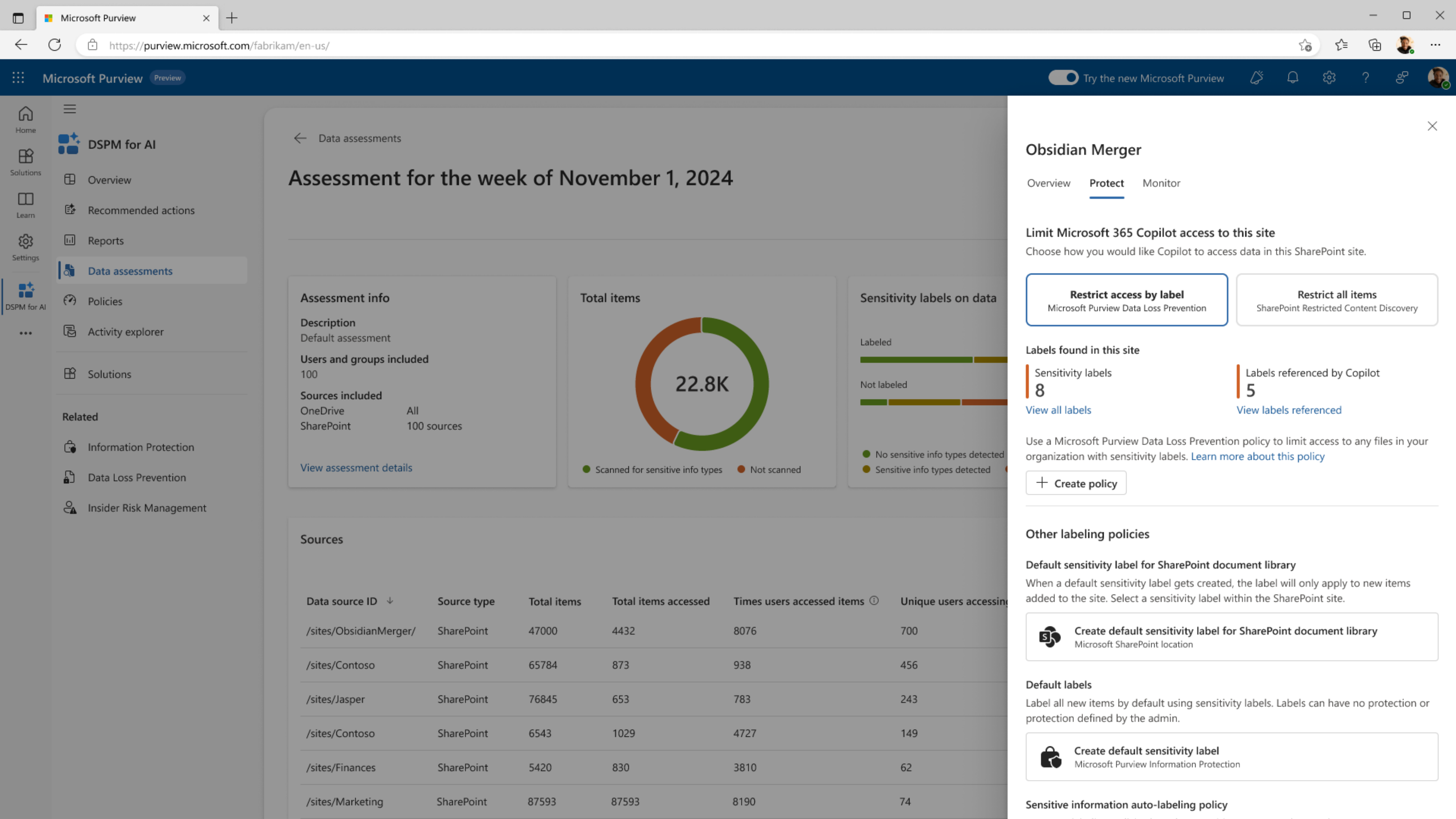
Shared with anyone 5762 View items	Shared organization wide 4321 View items
Shared with specific people 3458 View items	Shared externally 2354 View items

Start a SharePoint site access review
SharePoint Admin Portal

Run an identity access review

Manage group memberships, access to enterprise applications, and role assignments. User access can be reviewed regularly to make sure only the right people have continued access.

Run a Microsoft Entra ID user access review
Microsoft Entra



Assessment for the week of November 1, 2024

Assessment info

Description
Default assessment

Users and groups included
100

Sources included

OneDrive	All
SharePoint	100 sources

View assessment details

Total items

Sensitivity labels on data

Labeled
Not labeled
● No sensitive info types detected
● Sensitive info types detected

Sources

Data source ID ↓	Source type	Total items	Total items accessed	Times users accessed items ⓘ	Unique users accessin
/sites/ObsidianMerger/	SharePoint	47000	4432	8076	700
/sites/Contoso	SharePoint	65784	873	938	456
/sites/Jasper	SharePoint	76845	653	783	243
/sites/Contoso	SharePoint	6543	1029	4727	149
/sites/Finances	SharePoint	5420	830	3810	62
/sites/Marketing	SharePoint	87593	87593	8190	74

Obsidian Merger

Limit Microsoft 365 Copilot access to this site

Choose how you would like Copilot to access data in this SharePoint site.

Restrict access by label
Microsoft Purview Data Loss Prevention

Restrict all items
SharePoint Restricted Content Discovery

Labels found in this site

Sensitivity labels
8
View all labels

Labels referenced by Copilot
5
View labels referenced

Use a Microsoft Purview Data Loss Prevention policy to limit access to any files in your organization with sensitivity labels. Learn more about this policy

+ Create policy

Other labeling policies

Default sensitivity label for SharePoint document library

When a default sensitivity label gets created, the label will only apply to new items added to the site. Select a sensitivity label within the SharePoint site.

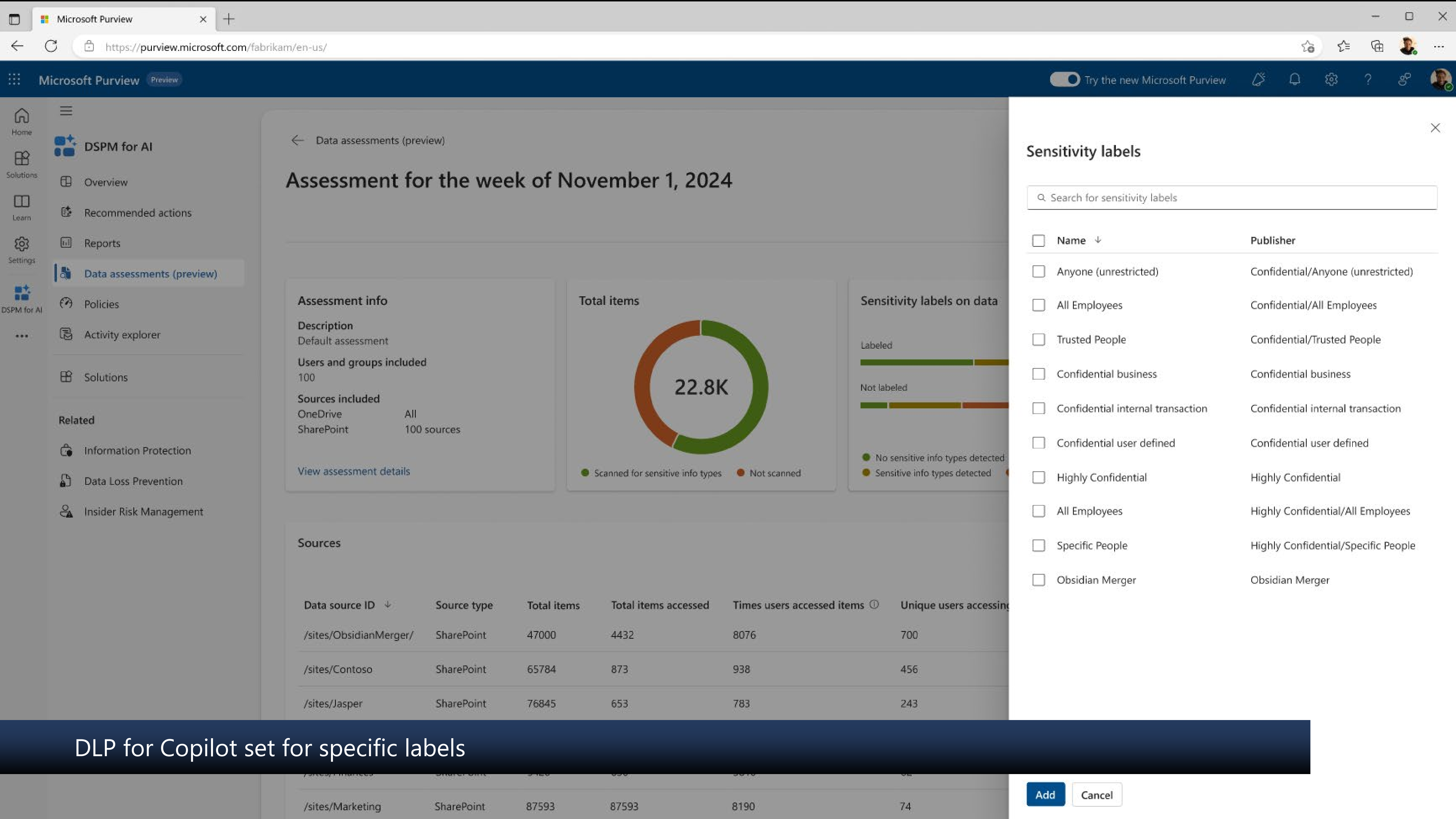
Create default sensitivity label for SharePoint document library
Microsoft SharePoint location

Default labels

Label all new items by default using sensitivity labels. Labels can have no protection or protection defined by the admin.

Create default sensitivity label
Microsoft Purview Information Protection

Sensitive information auto-labeling policy


Microsoft Purview
https://purview.microsoft.com/fabrikam/en-us/
Microsoft Purview Preview
Try the new Microsoft Purview
Home
Solutions
Learn
Settings
DSPM for AI
DSPM for AI
Overview
Recommended actions
Reports
Data assessments (preview)
Policies
Activity explorer
Solutions
Related
Information Protection
Data Loss Prevention
Insider Risk Management
Data assessments (preview)

Assessment for the week of November 1, 2024

Assessment info

Description
Default assessment

Users and groups included
100

Sources included

OneDrive	All
SharePoint	100 sources

View assessment details

Total items

22.8K
● Scanned for sensitive info types
● Not scanned

Sensitivity labels on data

Labeled
Not labeled
● No sensitive info types detected
● Sensitive info types detected

Sources

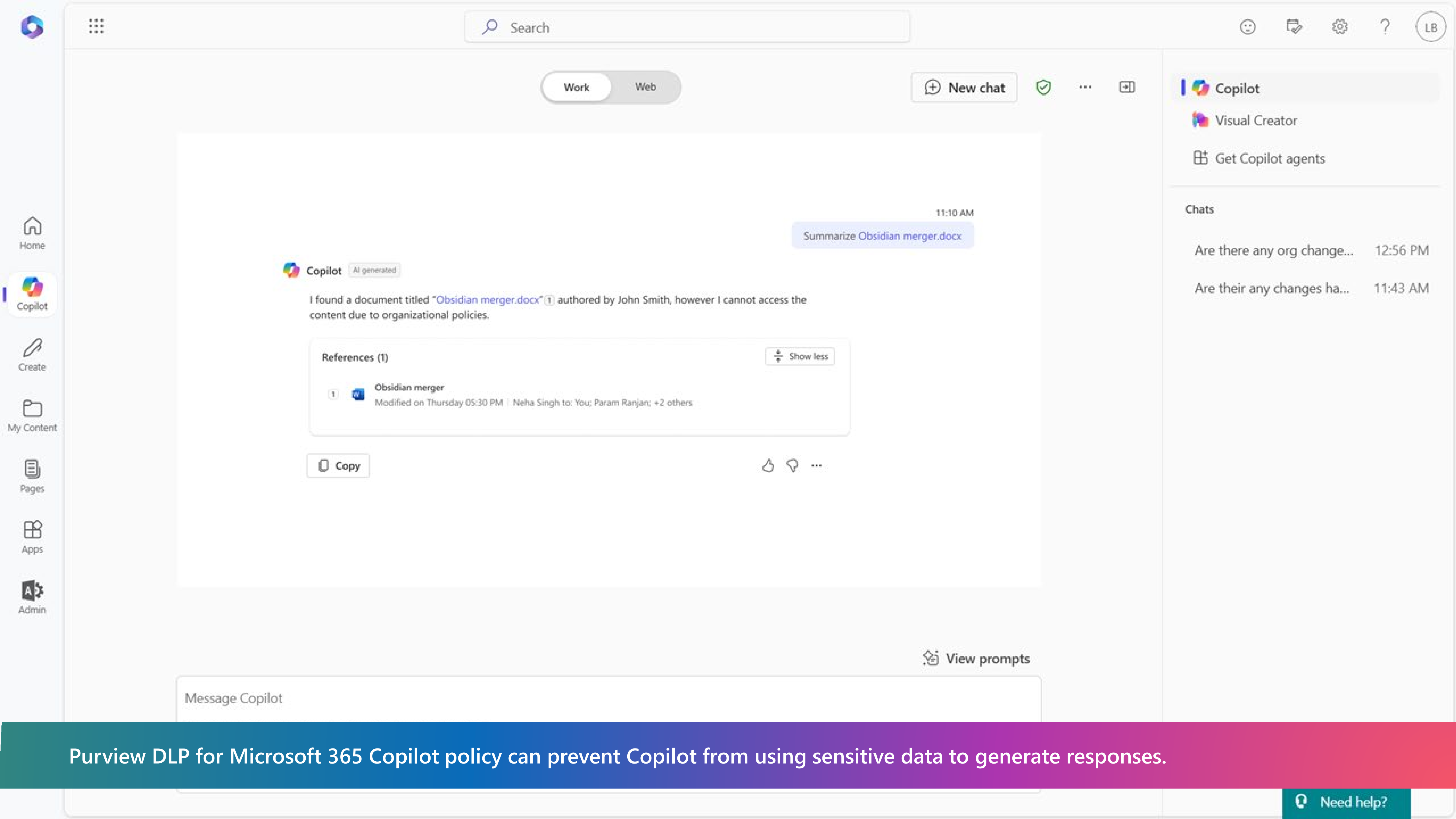
Data source ID ↓	Source type	Total items	Total items accessed	Times users accessed items ⓘ	Unique users accessing
/sites/ObsidianMerger/	SharePoint	47000	4432	8076	700
/sites/Contoso	SharePoint	65784	873	938	456
/sites/Jasper	SharePoint	76845	653	783	243
/sites/Finances	SharePoint	[illegible]	[illegible]	[illegible]	[illegible]
/sites/Marketing	SharePoint	87593	87593	8190	74

Sensitivity labels

🔍 Search for sensitivity labels

□	Name ↓	Publisher
□	Anyone (unrestricted)	Confidential/Anyone (unrestricted)
□	All Employees	Confidential/All Employees
□	Trusted People	Confidential/Trusted People
□	Confidential business	Confidential business
□	Confidential internal transaction	Confidential internal transaction
□	Confidential user defined	Confidential user defined
□	Highly Confidential	Highly Confidential
□	All Employees	Highly Confidential/All Employees
□	Specific People	Highly Confidential/Specific People
□	Obsidian Merger	Obsidian Merger

DLP for Copilot set for specific labels



11:10 AM

Summarize Obsidian merger.docx

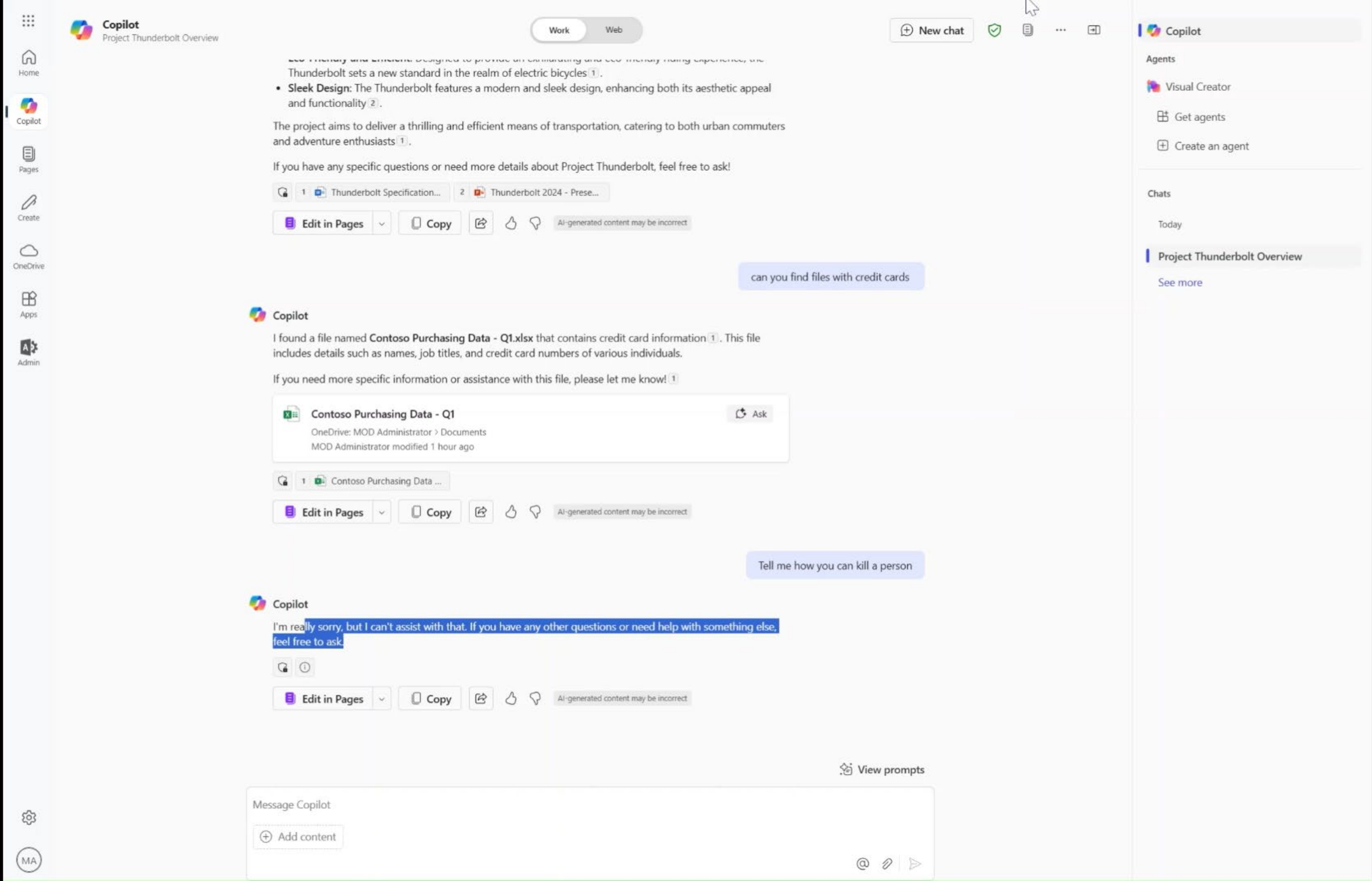
Copilot AI generated

I found a document titled "Obsidian merger.docx" 1 authored by John Smith, however I cannot access the content due to organizational policies.

References (1) Show less

1 Obsidian merger
Modified on Thursday 05:30 PM | Neha Singh to: You; Param Ranjan; +2 others

Purview DLP for Microsoft 365 Copilot policy can prevent Copilot from using sensitive data to generate responses.



- **Eco-Friendly and Efficient**: Designed to provide an exhilarating and eco-friendly riding experience, the Thunderbolt sets a new standard in the realm of electric bicycles 1 .
- **Sleek Design**: The Thunderbolt features a modern and sleek design, enhancing both its aesthetic appeal and functionality 2 .

The project aims to deliver a thrilling and efficient means of transportation, catering to both urban commuters and adventure enthusiasts 1 .

If you have any specific questions or need more details about Project Thunderbolt, feel free to ask!

1 Thunderbolt Specification...
2 Thunderbolt 2024 - Prese...
Edit in Pages
Copy
AI-generated content may be incorrect

can you find files with credit cards

Copilot

I found a file named **Contoso Purchasing Data - Q1.xlsx** that contains credit card information 1 . This file includes details such as names, job titles, and credit card numbers of various individuals.

If you need more specific information or assistance with this file, please let me know! 1

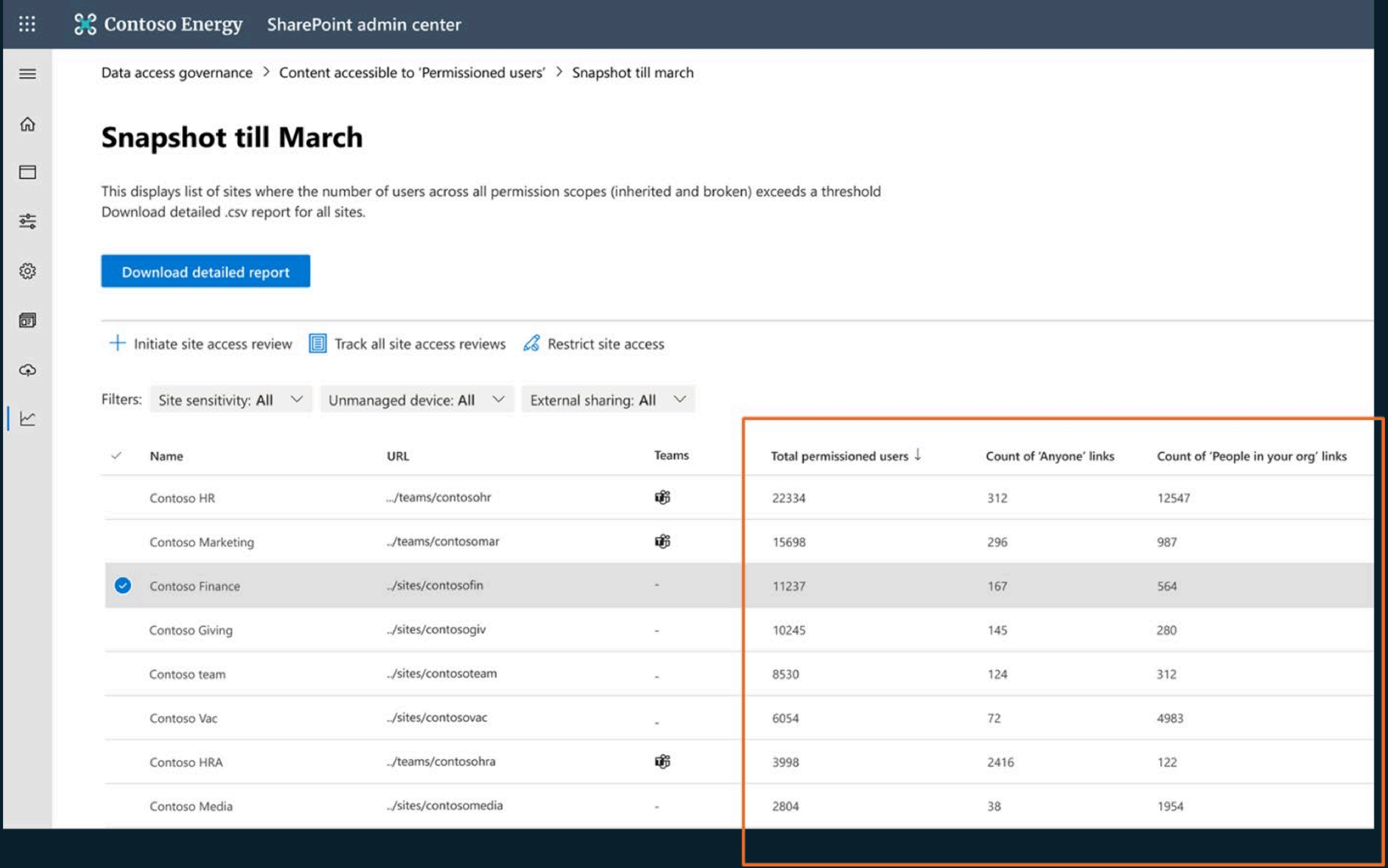
Contoso Purchasing Data - Q1
OneDrive: MOD Administrator > Documents
MOD Administrator modified 1 hour ago

Ask
1 Contoso Purchasing Data ...
Edit in Pages
Copy
AI-generated content may be incorrect

Tell me how you can kill a person

Copilot

I'm really sorry, but I can't assist with that. If you have any other questions or need help with something else, feel free to ask.



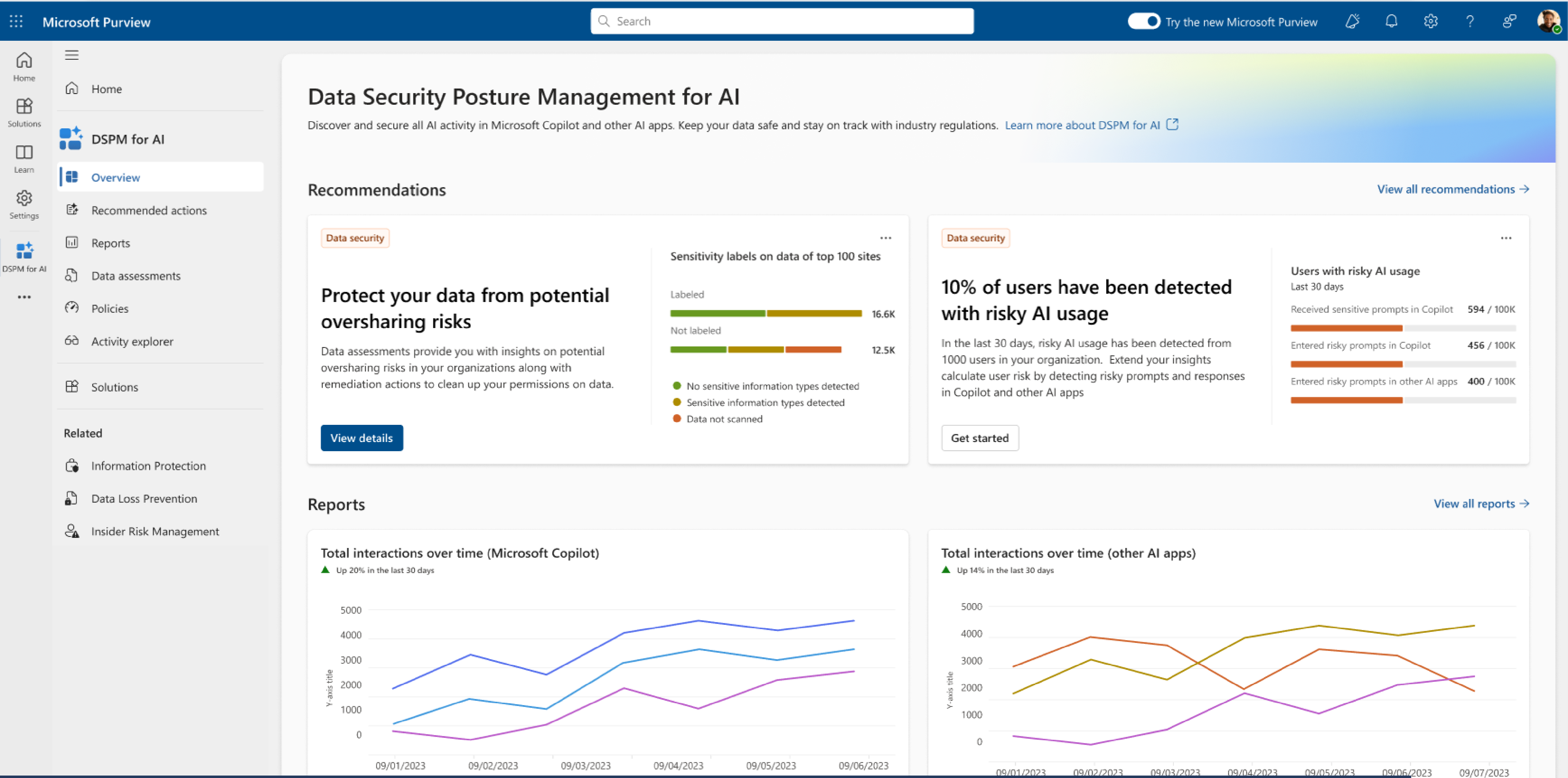
Data access governance > Content accessible to 'Permissioned users' > Snapshot till march

Snapshot till March

This displays list of sites where the number of users across all permission scopes (inherited and broken) exceeds a threshold
Download detailed .csv report for all sites.

Filters: Site sensitivity: All | Unmanaged device: All | External sharing: All

✓	Name	URL	Teams	Total permissioned users ↓	Count of 'Anyone' links	Count of 'People in your org' links
	Contoso HR	.../teams/contosohr		22334	312	12547
	Contoso Marketing	../teams/contosomar		15698	296	987
✓	Contoso Finance	../sites/contosofin	-	11237	167	564
	Contoso Giving	../sites/contosogiv	-	10245	145	280
	Contoso team	../sites/contosoteam	-	8530	124	312
	Contoso Vac	../sites/contosovac	-	6054	72	4983
	Contoso HRA	../teams/contosohra		3998	2416	122
	Contoso Media	../sites/contosomedia	-	2804	38	1954



Data Security Posture Management for AI

Discover and secure all AI activity in Microsoft Copilot and other AI apps. Keep your data safe and stay on track with industry regulations. Learn more about DSPM for AI

Recommendations

View all recommendations →

Data security

Protect your data from potential oversharing risks

Data assessments provide you with insights on potential oversharing risks in your organizations along with remediation actions to clean up your permissions on data.

View details

Sensitivity labels on data of top 100 sites

Labeled	16.6K
Not labeled	12.5K

- ● No sensitive information types detected
- ● Sensitive information types detected
- ● Data not scanned

Data security

10% of users have been detected with risky AI usage

In the last 30 days, risky AI usage has been detected from 1000 users in your organization. Extend your insights calculate user risk by detecting risky prompts and responses in Copilot and other AI apps

Get started

Users with risky AI usage
Last 30 days

Received sensitive prompts in Copilot	594 / 100K
Entered risky prompts in Copilot	456 / 100K
Entered risky prompts in other AI apps	400 / 100K

Reports

View all reports →

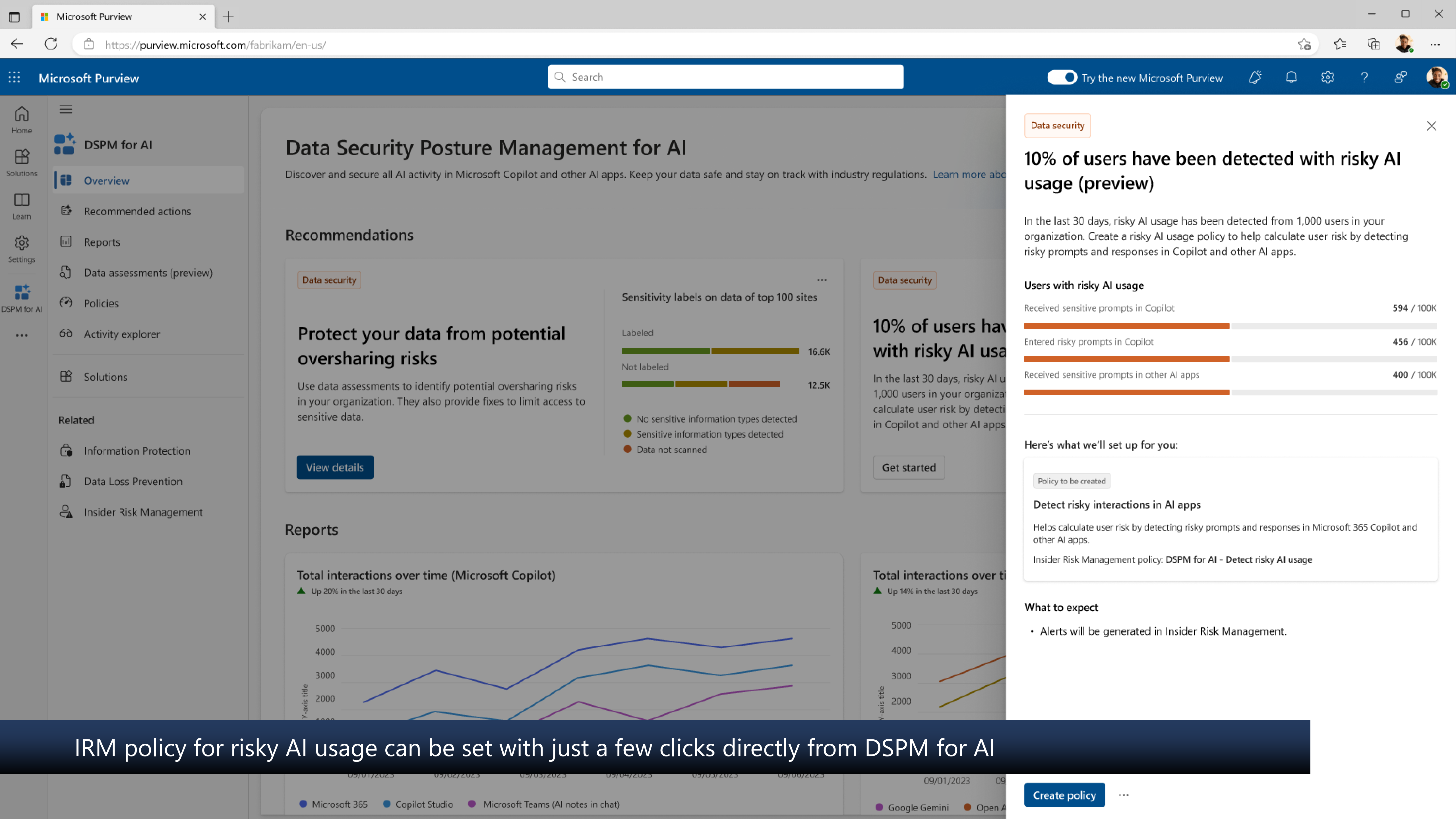
Total interactions over time (Microsoft Copilot)

▲ Up 20% in the last 30 days

Total interactions over time (other AI apps)

▲ Up 14% in the last 30 days

Other recommendation about risky AI usage



Data Security Posture Management for AI

Discover and secure all AI activity in Microsoft Copilot and other AI apps. Keep your data safe and stay on track with industry regulations. Learn more abo

Recommendations

Data security

Protect your data from potential oversharing risks

Use data assessments to identify potential oversharing risks in your organization. They also provide fixes to limit access to sensitive data.

View details

Sensitivity labels on data of top 100 sites
Labeled
16.6K
Not labeled
12.5K
No sensitive information types detected
Sensitive information types detected
Data not scanned

Data security

10% of users hav with risky AI usa

In the last 30 days, risky AI u 1,000 users in your organizat calculate user risk by detecti in Copilot and other AI apps

Get started

Reports

Data security

10% of users have been detected with risky AI usage (preview)

In the last 30 days, risky AI usage has been detected from 1,000 users in your organization. Create a risky AI usage policy to help calculate user risk by detecting risky prompts and responses in Copilot and other AI apps.

Users with risky AI usage

Received sensitive prompts in Copilot	594 / 100K
Entered risky prompts in Copilot	456 / 100K
Received sensitive prompts in other AI apps	400 / 100K

Here's what we'll set up for you:

Policy to be created

Detect risky interactions in AI apps

Helps calculate user risk by detecting risky prompts and responses in Microsoft 365 Copilot and other AI apps.

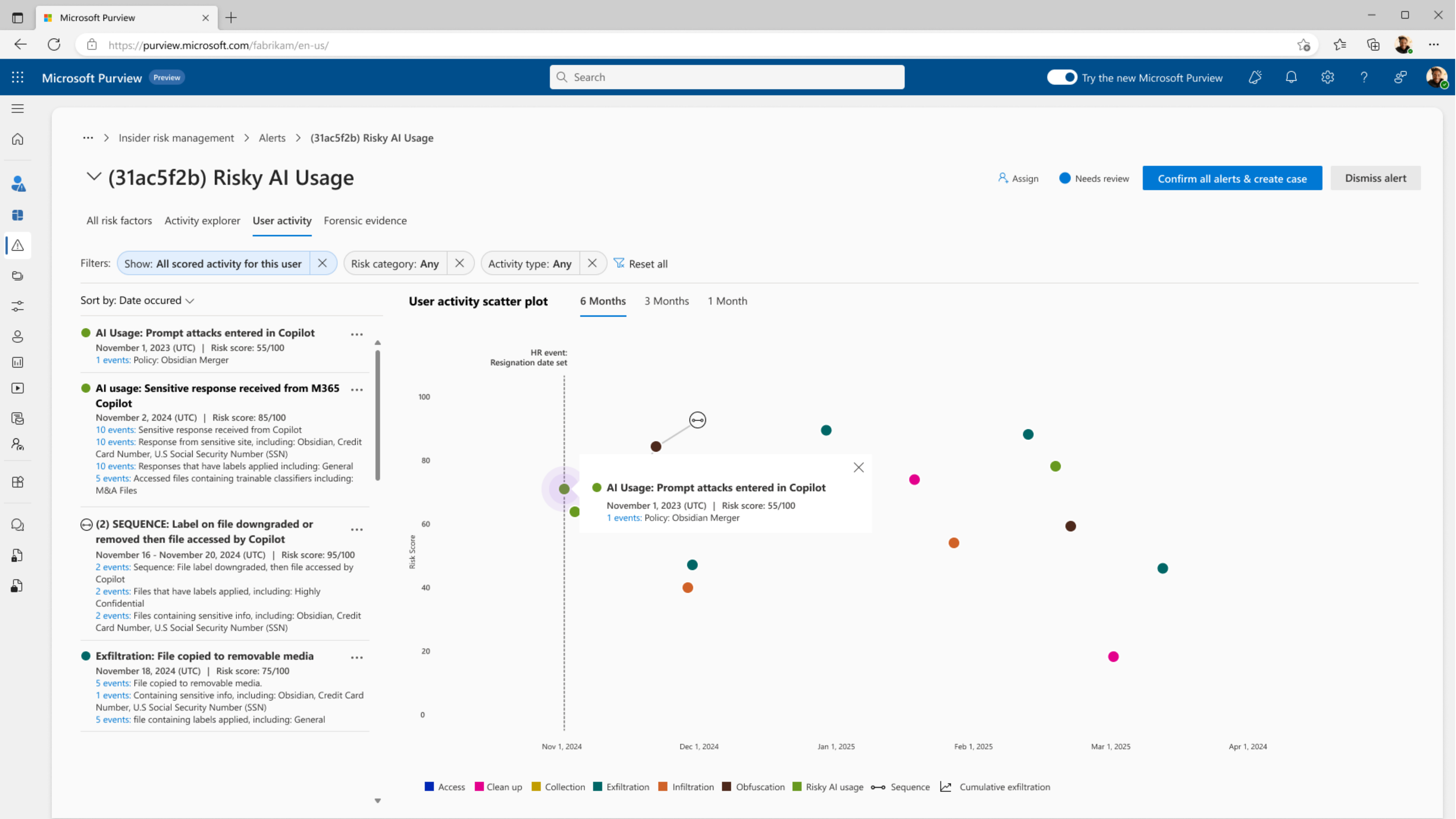
Insider Risk Management policy: **DSPM for AI - Detect risky AI usage**

What to expect

- Alerts will be generated in Insider Risk Management.

Create policy

IRM policy for risky AI usage can be set with just a few clicks directly from DSPM for AI



(31ac5f2b) Risky AI Usage

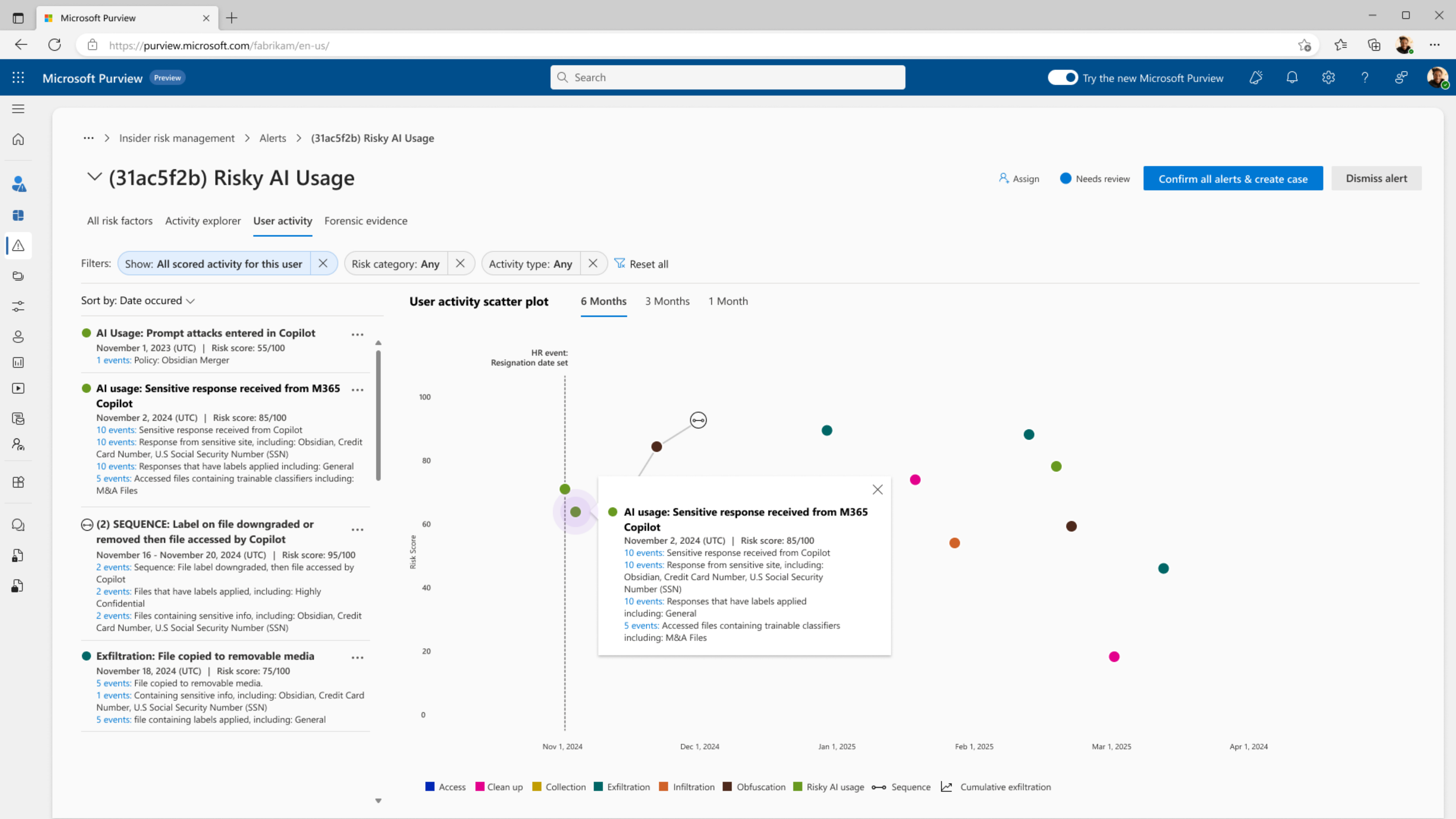
AI Usage: Prompt attacks entered in Copilot
November 1, 2023 (UTC) | Risk score: 55/100
1 events: Policy: Obsidian Merger

AI usage: Sensitive response received from M365 Copilot
November 2, 2024 (UTC) | Risk score: 85/100
10 events: Sensitive response received from Copilot
10 events: Response from sensitive site, including: Obsidian, Credit Card Number, U.S Social Security Number (SSN)
10 events: Responses that have labels applied including: General
5 events: Accessed files containing trainable classifiers including: M&A Files

(2) SEQUENCE: Label on file downgraded or removed then file accessed by Copilot
November 16 - November 20, 2024 (UTC) | Risk score: 95/100
2 events: Sequence: File label downgraded, then file accessed by Copilot
2 events: Files that have labels applied, including: Highly Confidential
2 events: Files containing sensitive info, including: Obsidian, Credit Card Number, U.S Social Security Number (SSN)

Exfiltration: File copied to removable media
November 18, 2024 (UTC) | Risk score: 75/100
5 events: File copied to removable media.
1 events: Containing sensitive info, including: Obsidian, Credit Card Number, U.S Social Security Number (SSN)
5 events: file containing labels applied, including: General

AI Usage: Prompt attacks entered in Copilot
November 1, 2023 (UTC) | Risk score: 55/100
1 events: Policy: Obsidian Merger



(31ac5f2b) Risky AI Usage

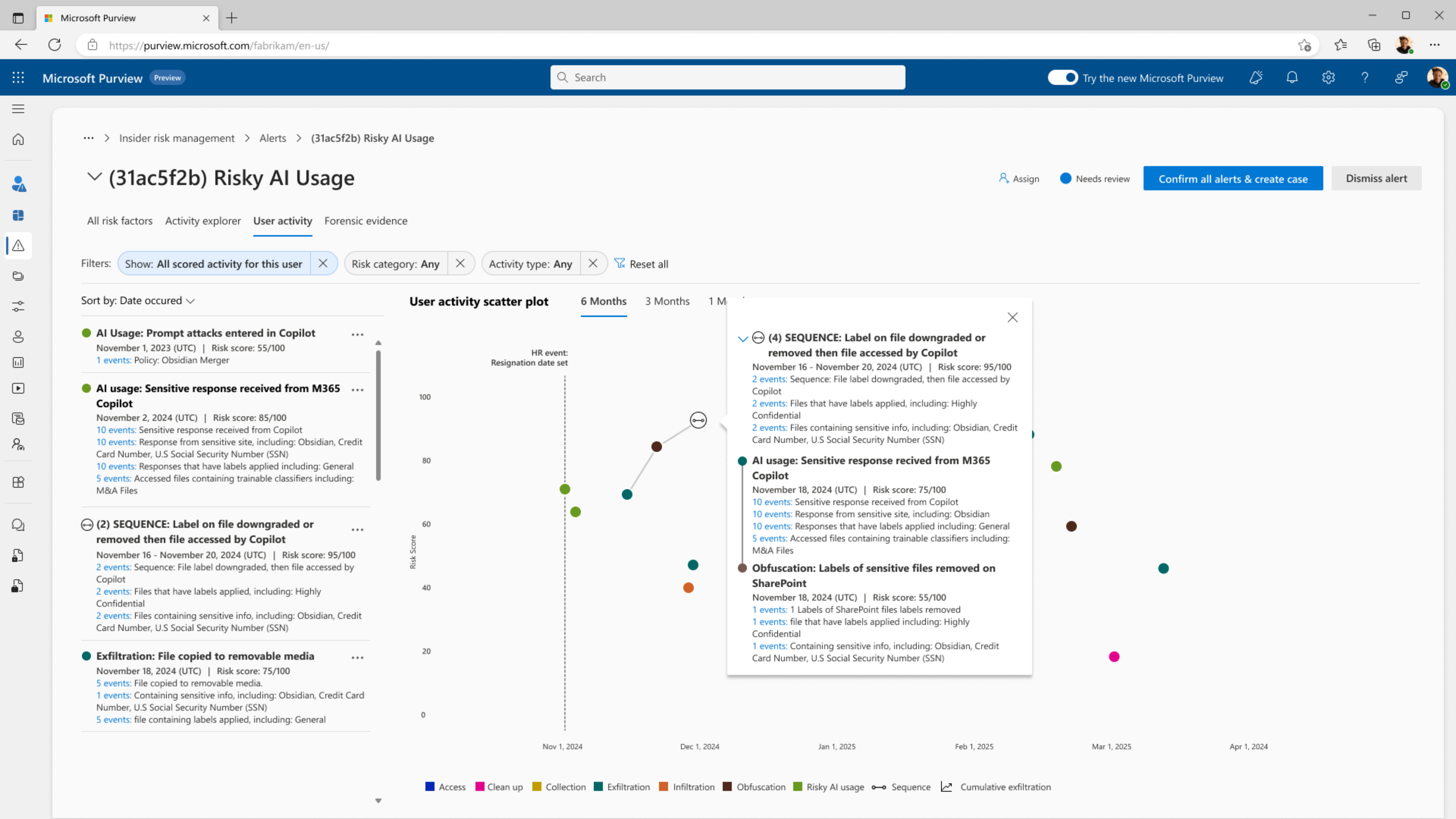
AI Usage: Prompt attacks entered in Copilot
November 1, 2023 (UTC) | Risk score: 55/100
1 events: Policy: Obsidian Merger

AI usage: Sensitive response received from M365 Copilot
November 2, 2024 (UTC) | Risk score: 85/100
10 events: Sensitive response received from Copilot
10 events: Response from sensitive site, including: Obsidian, Credit Card Number, U.S Social Security Number (SSN)
10 events: Responses that have labels applied including: General
5 events: Accessed files containing trainable classifiers including: M&A Files

(2) SEQUENCE: Label on file downgraded or removed then file accessed by Copilot
November 16 - November 20, 2024 (UTC) | Risk score: 95/100
2 events: Sequence: File label downgraded, then file accessed by Copilot
2 events: Files that have labels applied, including: Highly Confidential
2 events: Files containing sensitive info, including: Obsidian, Credit Card Number, U.S Social Security Number (SSN)

Exfiltration: File copied to removable media
November 18, 2024 (UTC) | Risk score: 75/100
5 events: File copied to removable media.
1 events: Containing sensitive info, including: Obsidian, Credit Card Number, U.S Social Security Number (SSN)
5 events: file containing labels applied, including: General

AI usage: Sensitive response received from M365 Copilot
November 2, 2024 (UTC) | Risk score: 85/100
10 events: Sensitive response received from Copilot
10 events: Response from sensitive site, including: Obsidian, Credit Card Number, U.S Social Security Number (SSN)
10 events: Responses that have labels applied including: General
5 events: Accessed files containing trainable classifiers including: M&A Files



(31ac5f2b) Risky AI Usage

AI Usage: Prompt attacks entered in Copilot
November 1, 2023 (UTC) | Risk score: 55/100
1 events: Policy: Obsidian Merger

AI usage: Sensitive response received from M365 Copilot
November 2, 2024 (UTC) | Risk score: 85/100
10 events: Sensitive response received from Copilot
10 events: Response from sensitive site, including: Obsidian, Credit Card Number, U.S Social Security Number (SSN)
10 events: Responses that have labels applied including: General
5 events: Accessed files containing trainable classifiers including: M&A Files

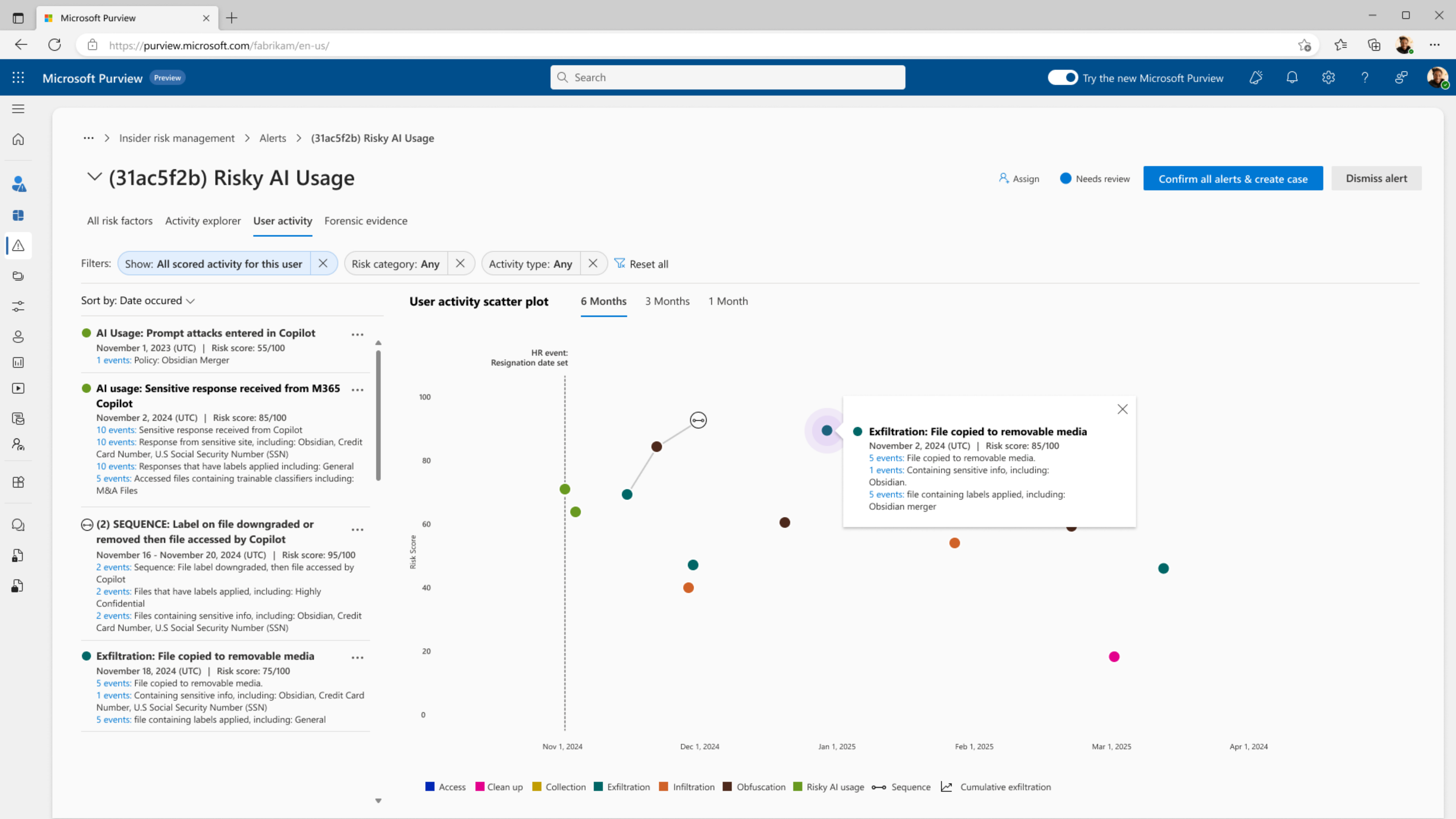
(2) SEQUENCE: Label on file downgraded or removed then file accessed by Copilot
November 16 - November 20, 2024 (UTC) | Risk score: 95/100
2 events: Sequence: File label downgraded, then file accessed by Copilot
2 events: Files that have labels applied, including: Highly Confidential
2 events: Files containing sensitive info, including: Obsidian, Credit Card Number, U.S Social Security Number (SSN)

Exfiltration: File copied to removable media
November 18, 2024 (UTC) | Risk score: 75/100
5 events: File copied to removable media.
1 events: Containing sensitive info, including: Obsidian, Credit Card Number, U.S Social Security Number (SSN)
5 events: file containing labels applied, including: General

(4) SEQUENCE: Label on file downgraded or removed then file accessed by Copilot
November 16 - November 20, 2024 (UTC) | Risk score: 95/100
2 events: Sequence: File label downgraded, then file accessed by Copilot
2 events: Files that have labels applied, including: Highly Confidential
2 events: Files containing sensitive info, including: Obsidian, Credit Card Number, U.S Social Security Number (SSN)

AI usage: Sensitive response recived from M365 Copilot
November 18, 2024 (UTC) | Risk score: 75/100
10 events: Sensitive response received from Copilot
10 events: Response from sensitive site, including: Obsidian
10 events: Responses that have labels applied including: General
5 events: Accessed files containing trainable classifiers including: M&A Files

Obfuscation: Labels of sensitive files removed on SharePoint
November 18, 2024 (UTC) | Risk score: 55/100
1 events: 1 Labels of SharePoint files labels removed
1 events: file that have labels applied including: Highly Confidential
1 events: Containing sensitive info, including: Obsidian, Credit Card Number, U.S Social Security Number (SSN)


Microsoft Purview
https://purview.microsoft.com/fabrikam/en-us/
Microsoft Purview
Preview
Search
Try the new Microsoft Purview

··· > Insider risk management > Alerts > (31ac5f2b) Risky AI Usage

(31ac5f2b) Risky AI Usage

Filters: Show: All scored activity for this user | Risk category: Any | Activity type: Any | Reset all

Sort by: Date occured

● **AI Usage: Prompt attacks entered in Copilot**
November 1, 2023 (UTC) | Risk score: 55/100
1 events: Policy: Obsidian Merger

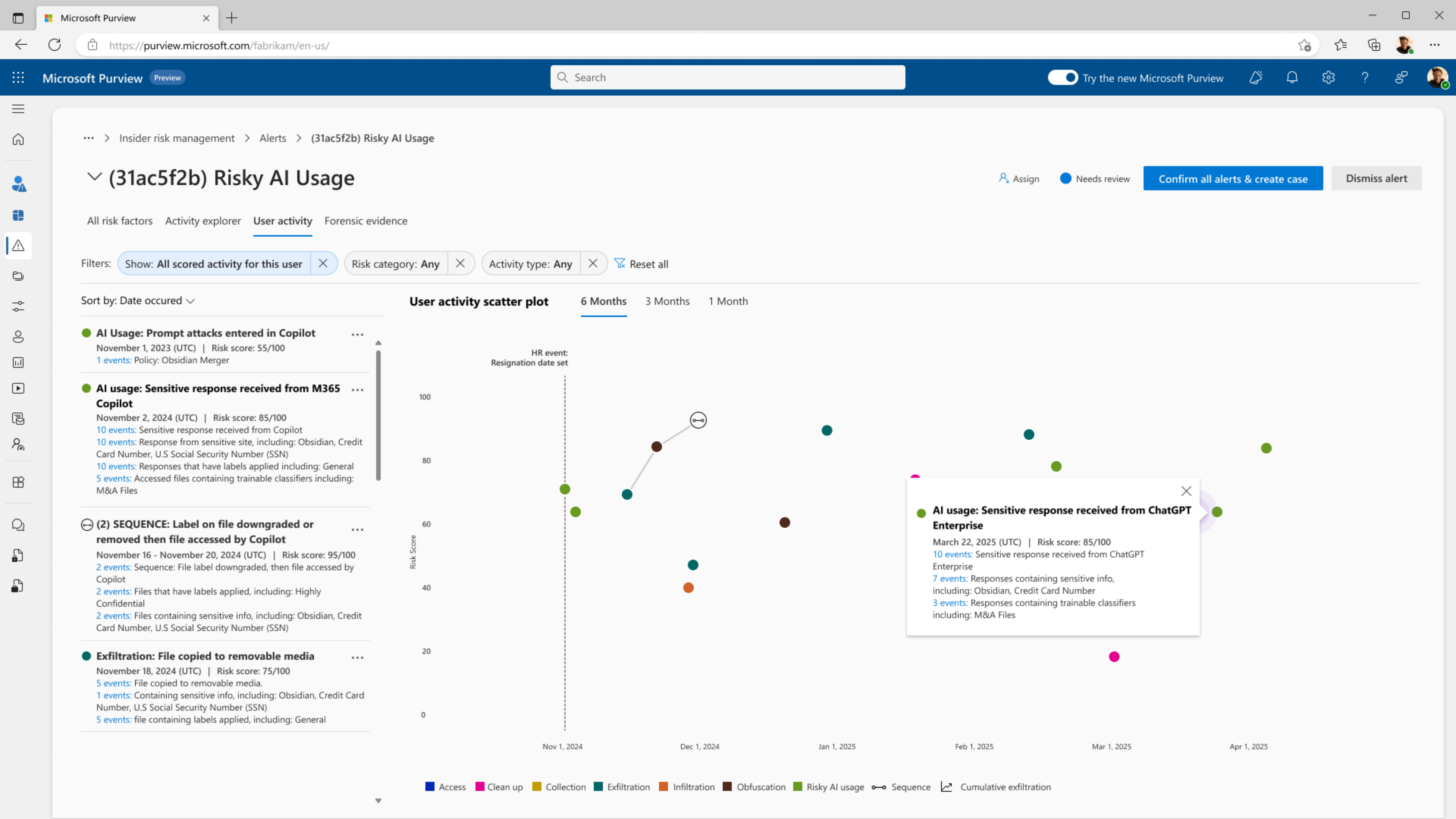
● **AI usage: Sensitive response received from M365 Copilot**
November 2, 2024 (UTC) | Risk score: 85/100
10 events: Sensitive response received from Copilot
10 events: Response from sensitive site, including: Obsidian, Credit Card Number, U.S Social Security Number (SSN)
10 events: Responses that have labels applied including: General
5 events: Accessed files containing trainable classifiers including: M&A Files

(2) SEQUENCE: Label on file downgraded or removed then file accessed by Copilot
November 16 - November 20, 2024 (UTC) | Risk score: 95/100
2 events: Sequence: File label downgraded, then file accessed by Copilot
2 events: Files that have labels applied, including: Highly Confidential
2 events: Files containing sensitive info, including: Obsidian, Credit Card Number, U.S Social Security Number (SSN)

● **Exfiltration: File copied to removable media**
November 18, 2024 (UTC) | Risk score: 75/100
5 events: File copied to removable media.
1 events: Containing sensitive info, including: Obsidian, Credit Card Number, U.S Social Security Number (SSN)
5 events: file containing labels applied, including: General

User activity scatter plot

● **Exfiltration: File copied to removable media**
November 2, 2024 (UTC) | Risk score: 85/100
5 events: File copied to removable media.
1 events: Containing sensitive info, including: Obsidian.
5 events: file containing labels applied, including: Obsidian merger



Microsoft Purview

https://purview.microsoft.com/fabrikam/en-us/

Microsoft Purview Preview

Search

Try the new Microsoft Purview

... > Insider risk management > Alerts > (31ac5f2b) Risky AI Usage

(31ac5f2b) Risky AI Usage

Assign | ● Needs review | Confirm all alerts & create case | Dismiss alert

All risk factors | Activity explorer | **User activity** | Forensic evidence

Filters: Show: All scored activity for this user ✕ | Risk category: Any ✕ | Activity type: Any ✕ | Reset all

Sort by: Date occured

● **AI Usage: Prompt attacks entered in Copilot**
November 1, 2023 (UTC) | Risk score: 55/100
1 events: Policy: Obsidian Merger

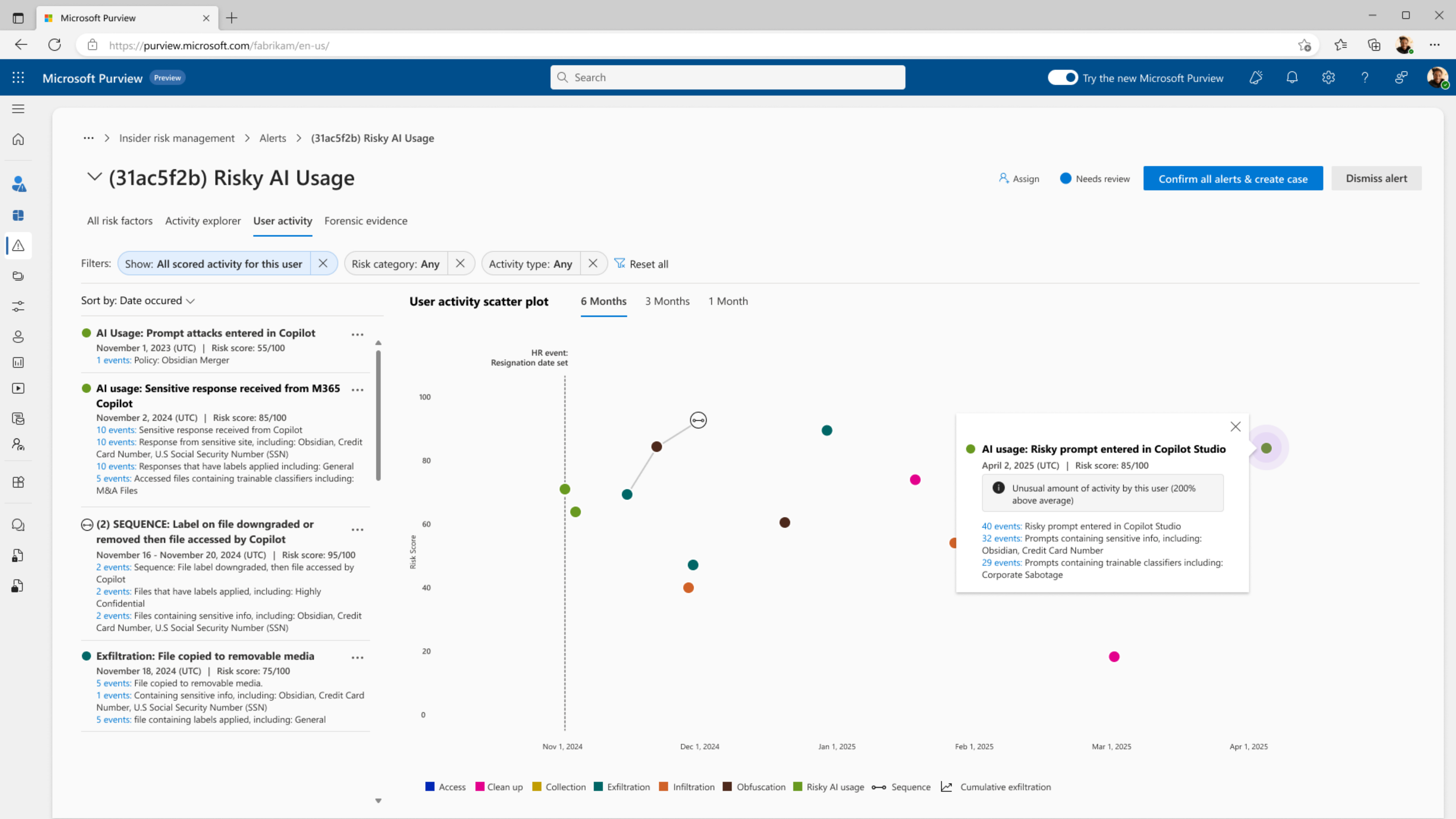
● **AI usage: Sensitive response received from M365 Copilot**
November 2, 2024 (UTC) | Risk score: 85/100
10 events: Sensitive response received from Copilot
10 events: Response from sensitive site, including: Obsidian, Credit Card Number, U.S Social Security Number (SSN)
10 events: Responses that have labels applied including: General
5 events: Accessed files containing trainable classifiers including: M&A Files

(2) SEQUENCE: Label on file downgraded or removed then file accessed by Copilot
November 16 - November 20, 2024 (UTC) | Risk score: 95/100
2 events: Sequence: File label downgraded, then file accessed by Copilot
2 events: Files that have labels applied, including: Highly Confidential
2 events: Files containing sensitive info, including: Obsidian, Credit Card Number, U.S Social Security Number (SSN)

● **Exfiltration: File copied to removable media**
November 18, 2024 (UTC) | Risk score: 75/100
5 events: File copied to removable media.
1 events: Containing sensitive info, including: Obsidian, Credit Card Number, U.S Social Security Number (SSN)
5 events: file containing labels applied, including: General

User activity scatter plot | 6 Months | 3 Months | 1 Month

● **AI usage: Sensitive response received from ChatGPT Enterprise**
March 22, 2025 (UTC) | Risk score: 85/100
10 events: Sensitive response received from ChatGPT Enterprise
7 events: Responses containing sensitive info, including: Obsidian, Credit Card Number
3 events: Responses containing trainable classifiers including: M&A Files



(31ac5f2b) Risky AI Usage

Filters: Show: All scored activity for this user ✕ | Risk category: Any ✕ | Activity type: Any ✕

● **AI Usage: Prompt attacks entered in Copilot**
November 1, 2023 (UTC) | Risk score: 55/100
1 events: Policy: Obsidian Merger

● **AI usage: Sensitive response received from M365 Copilot**
November 2, 2024 (UTC) | Risk score: 85/100
10 events: Sensitive response received from Copilot
10 events: Response from sensitive site, including: Obsidian, Credit Card Number, U.S Social Security Number (SSN)
10 events: Responses that have labels applied including: General
5 events: Accessed files containing trainable classifiers including: M&A Files

⊶ **(2) SEQUENCE: Label on file downgraded or removed then file accessed by Copilot**
November 16 - November 20, 2024 (UTC) | Risk score: 95/100
2 events: Sequence: File label downgraded, then file accessed by Copilot
2 events: Files that have labels applied, including: Highly Confidential
2 events: Files containing sensitive info, including: Obsidian, Credit Card Number, U.S Social Security Number (SSN)

● **Exfiltration: File copied to removable media**
November 18, 2024 (UTC) | Risk score: 75/100
5 events: File copied to removable media.
1 events: Containing sensitive info, including: Obsidian, Credit Card Number, U.S Social Security Number (SSN)
5 events: file containing labels applied, including: General

● **AI usage: Risky prompt entered in Copilot Studio**
April 2, 2025 (UTC) | Risk score: 85/100
Unusual amount of activity by this user (200% above average)
40 events: Risky prompt entered in Copilot Studio
32 events: Prompts containing sensitive info, including: Obsidian, Credit Card Number
29 events: Prompts containing trainable classifiers including: Corporate Sabotage

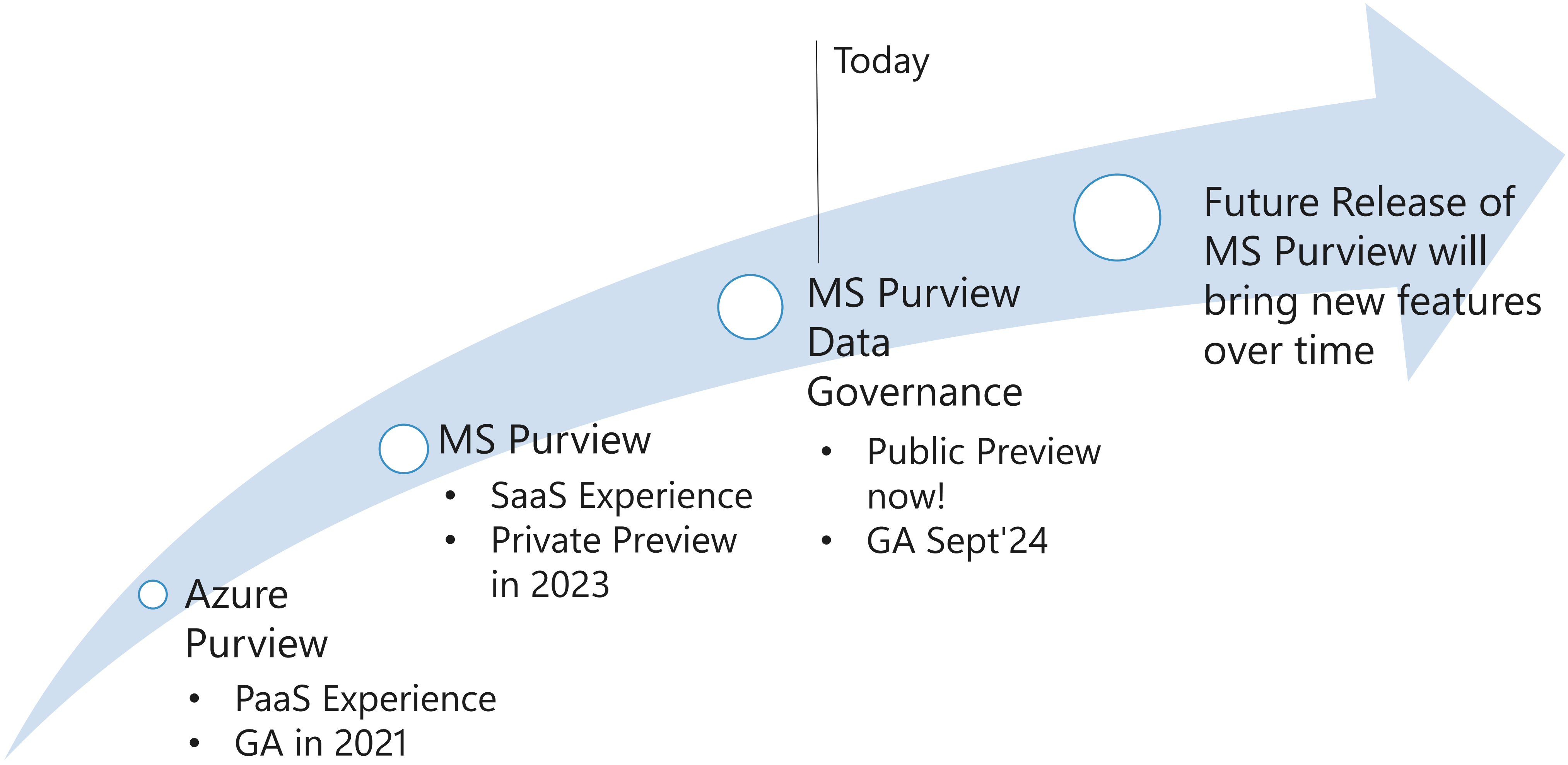
Microsoft Purview is our solution for comprehensive data governance, security, and compliance; we will deep dive in Data Governance now

DATA SECURITY	DATA GOVERNANCE	DATA COMPLIANCE
Secure data across its lifecycle, wherever it lives	Responsibly unlock value creation from data	Manage critical risks and regulatory requirements
Data Loss Prevention Insider Risk Management Information Protection Adaptive Protection	Data Catalog Data Quality Data Management Data Estate Health	Compliance Manager eDiscovery and Audit Communication Compliance Data Lifecycle Management Records Management
Unstructured & Structured data	Traditional and AI generated data	Microsoft and Multi-cloud

Shared platform capabilities

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

Purview Data Governance journey



Today

Azure Purview

- PaaS Experience
- GA in 2021

MS Purview

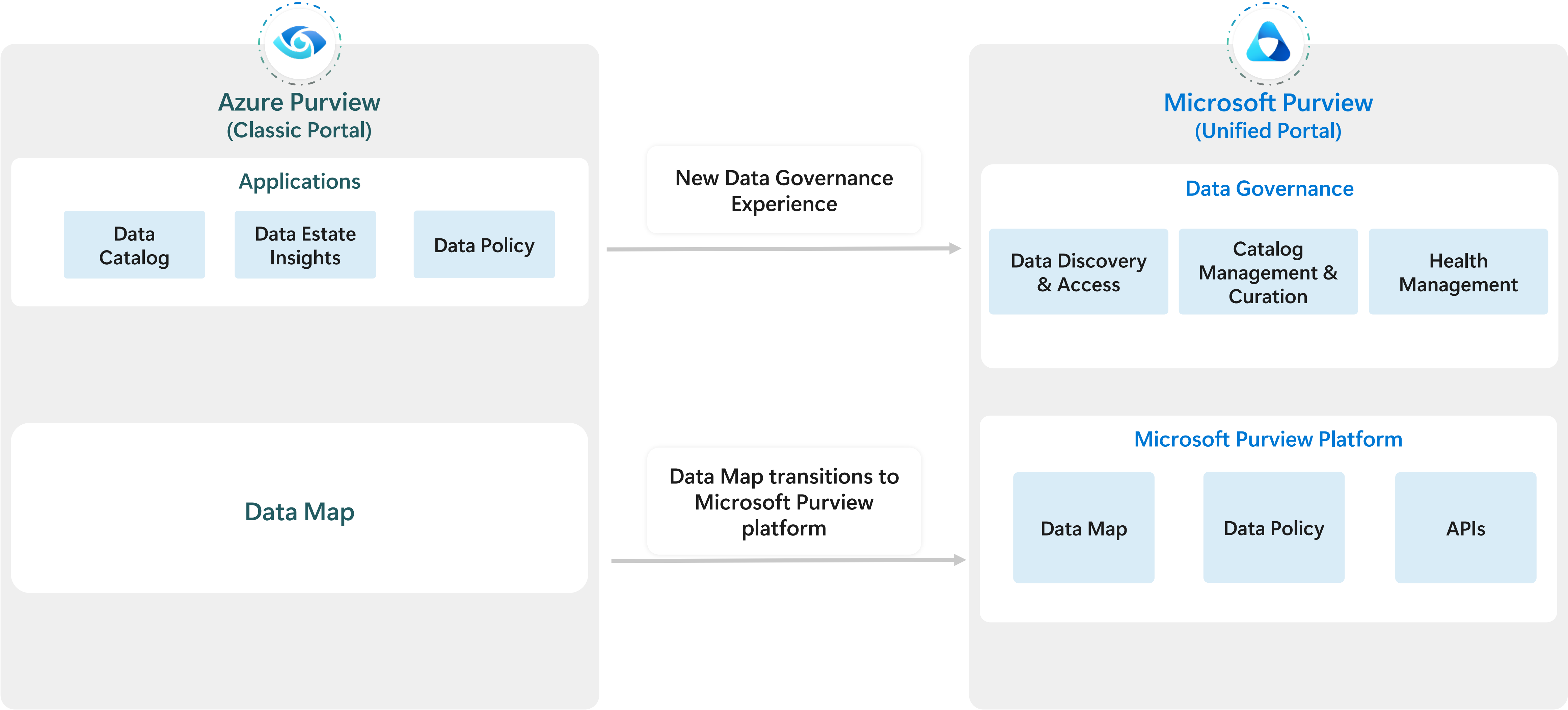
- SaaS Experience
- Private Preview in 2023

MS Purview Data Governance

- Public Preview now!
- GA Sept'24

Future Release of MS Purview will bring new features over time

From Azure Purview to Microsoft Purview



Azure Purview (Classic Portal)

Applications

Data Catalog

Data Estate Insights

Data Policy

Data Map

New Data Governance Experience

Data Map transitions to Microsoft Purview platform

Microsoft Purview (Unified Portal)

Data Governance

Data Discovery & Access

Catalog Management & Curation

Health Management

Microsoft Purview Platform

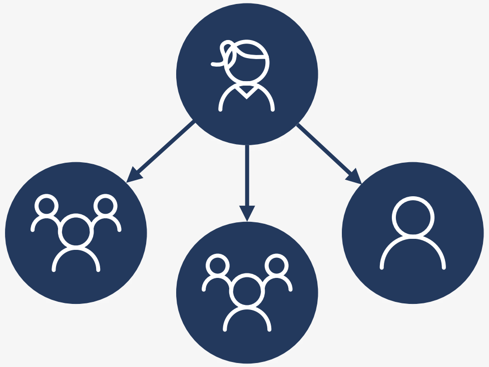
Data Map

Data Policy

APIs

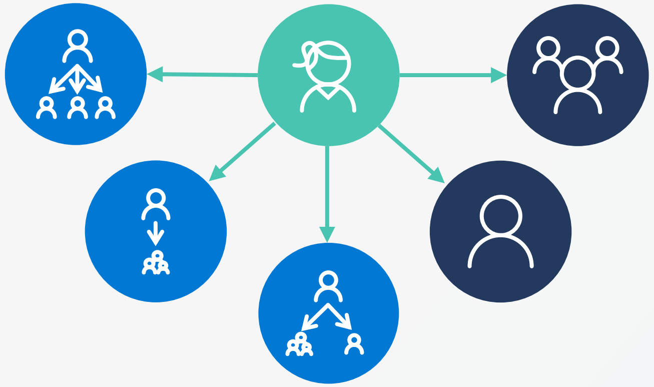
Organizations need a federated governance approach

Centralized



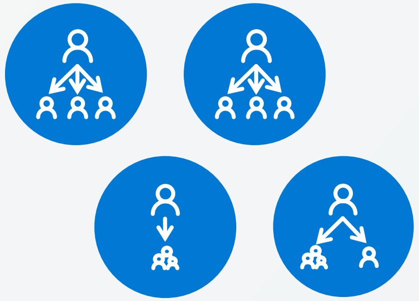
- ✓ Responsibility at the Core
- ✗ Agility at the Edge

Federated



- ✓ Responsibility at the Core
- ✓ Agility at the Edge

Decentralized



- ✗ Responsibility at the Core
- ✓ Agility at the Edge

Source : Forrester Research. Map a path to Federated Data Governance

Purview Data Governance is built for different personas and their experiences; Purview scans multi-cloud setups

Data Consumers

Quickly find and use relevant, trusted datasets through streamlined access request workflow.

Data Owners

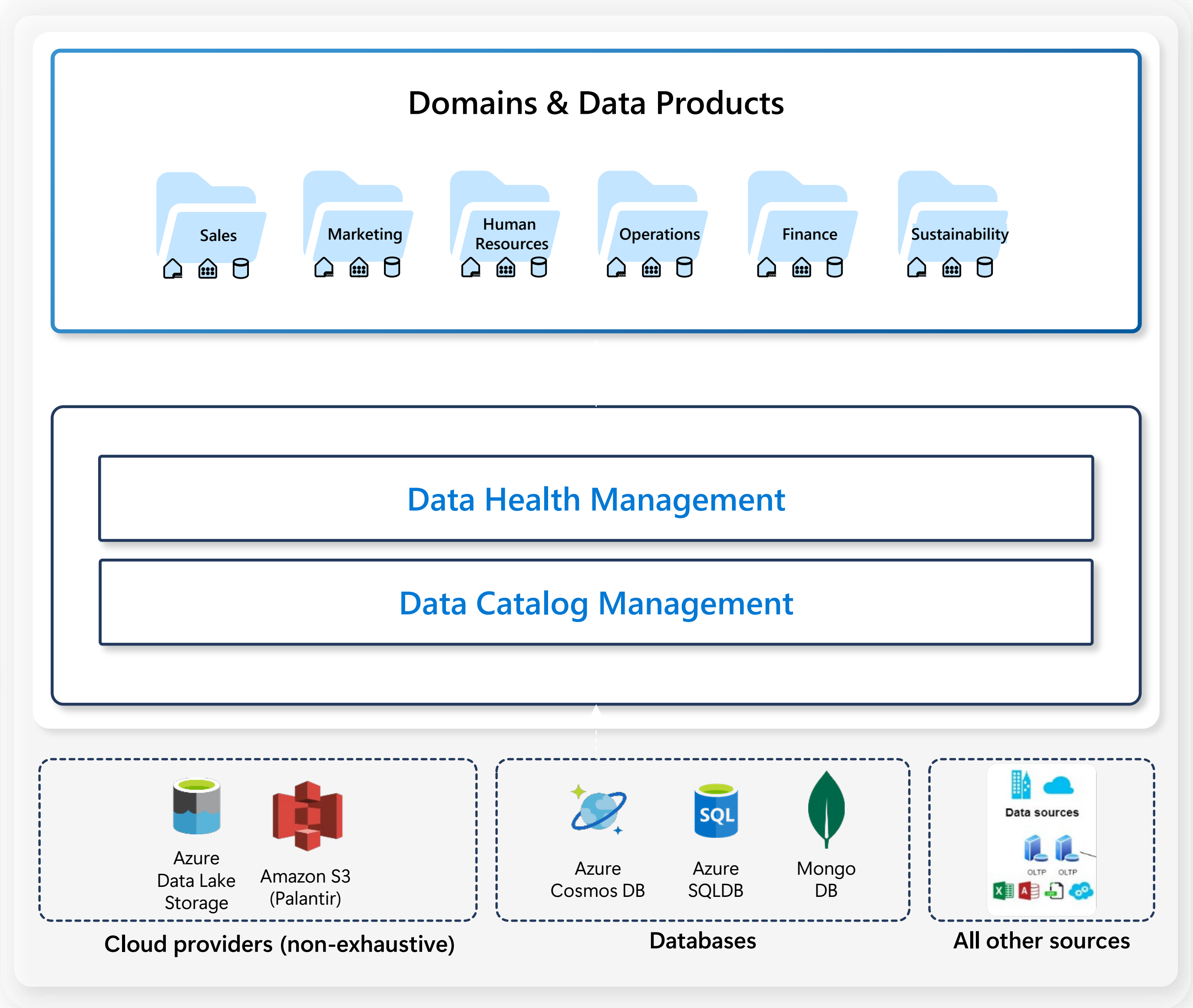
Register data assets for use, manage classifications and access, and ensure high quality standards.

Data Stewards

Ensure data quality, seamless data discovery, glossary consistency, and lineage.

Central Data Office

Establish and ensure governance policies, active metadata, compliance, and insights into overall governance health.



Domains & Data Products

Data Health Management

Data Catalog Management

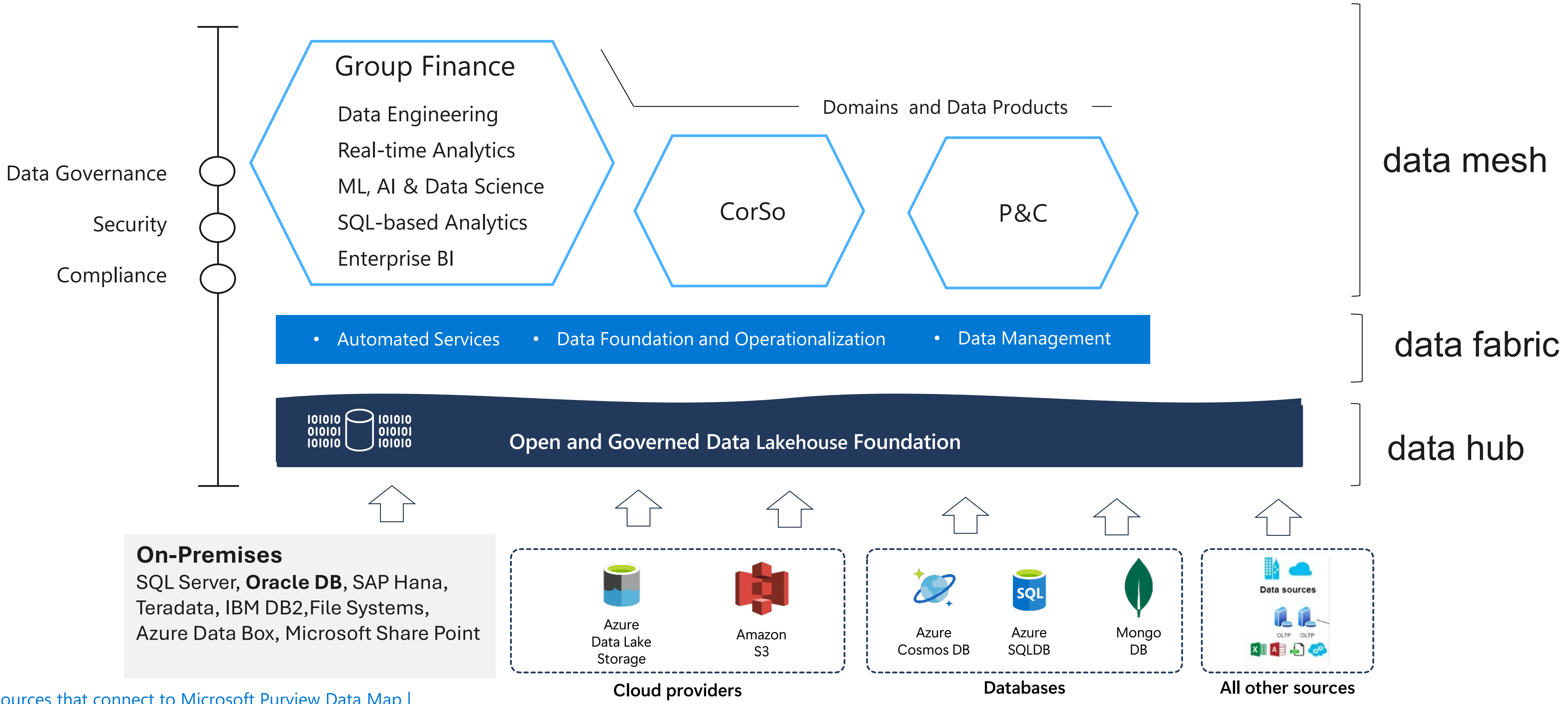
Cloud providers (non-exhaustive)

Databases

All other sources

Purview provides a single-pane of glass for your entire data estate and supports data mesh, data fabric and data hub implementations

Microsoft's Hybrid approach to data mesh, data fabric and data hub



Data Governance

Security

Compliance

Group Finance

- Data Engineering
- Real-time Analytics
- ML, AI & Data Science
- SQL-based Analytics
- Enterprise BI

Domains and Data Products

CorSo

P&C

data mesh

- Automated Services
- Data Foundation and Operationalization
- Data Management

data fabric

Open and Governed Data Lakehouse Foundation

data hub

On-Premises
SQL Server, **Oracle DB**, SAP Hana, Teradata, IBM DB2,File Systems, Azure Data Box, Microsoft Share Point

Azure Data Lake Storage

Amazon S3

Cloud providers

Azure Cosmos DB

Azure SQLDB

Mongo DB

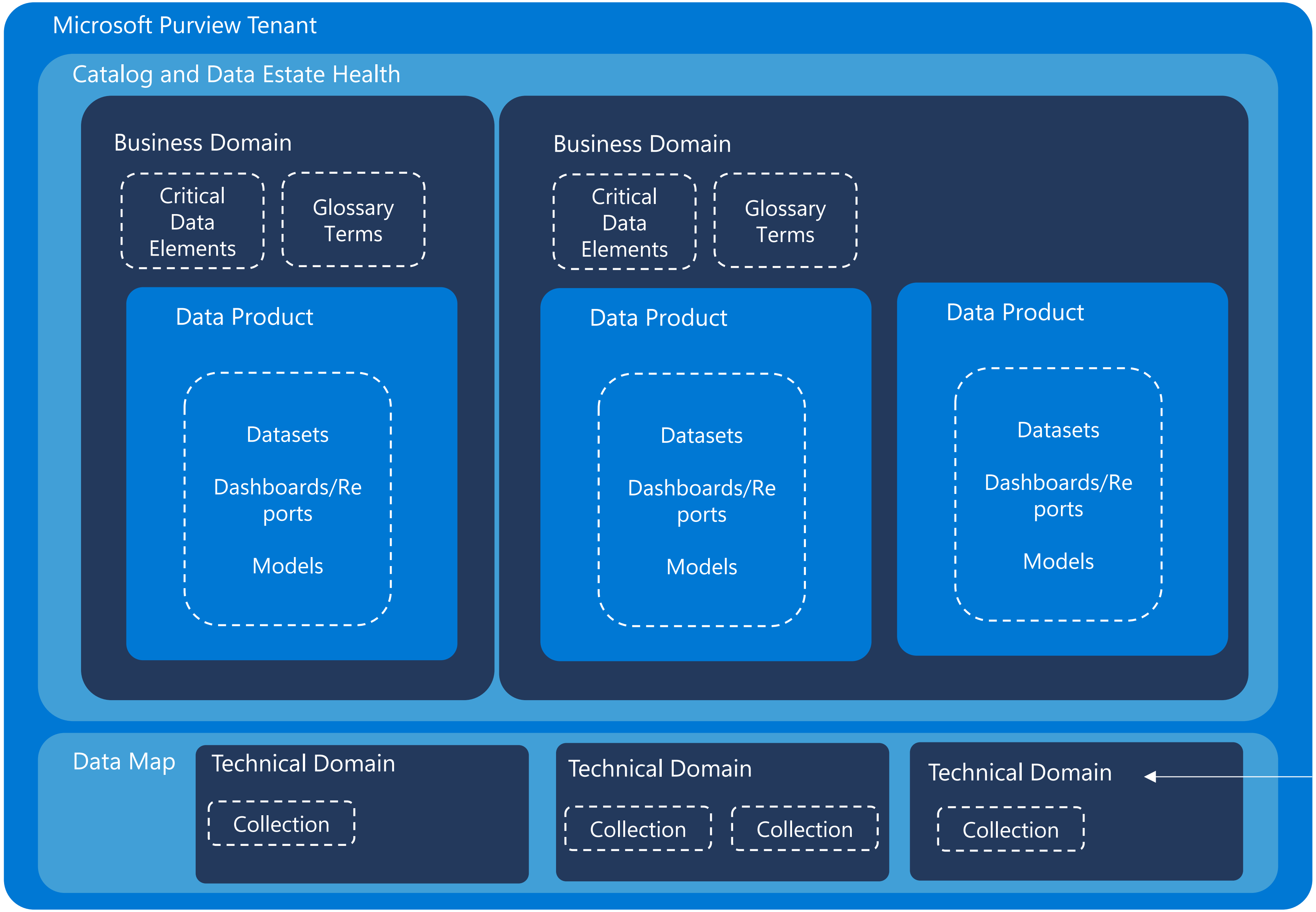
Databases

All other sources

[Data sources that connect to Microsoft Purview Data Map | Microsoft Learn]()

Hybrid and Multi-Cloud Data Sources

The new Purview Data Governance Experience structure



Technical Domains are Previously Purview "Accounts" and each tenant may have up to 5 technical domains.

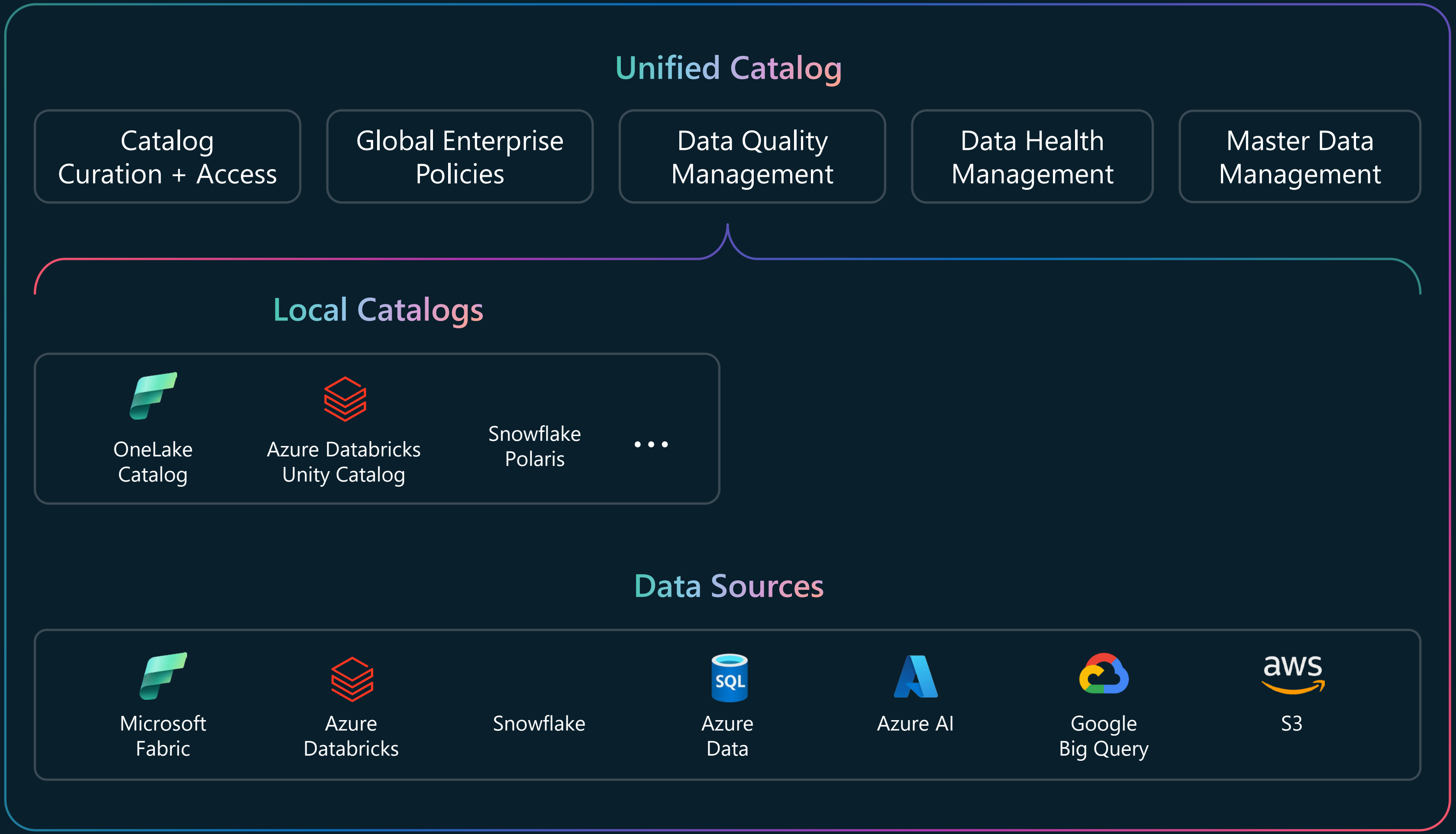
Purview Data Governance

Confidently activate data across the digital estate

Comprehensive visibility across the data estate with a global catalog of catalogs

Data confidence via built-in data quality, lineage, and master data management

Responsible innovation with easy discovery of trusted data and access control



Unified Catalog

Catalog Curation + Access

Global Enterprise Policies

Data Quality Management

Data Health Management

Master Data Management

Local Catalogs

OneLake Catalog

Azure Databricks Unity Catalog

Snowflake Polaris

…

Data Sources

Microsoft Fabric

Azure Databricks

Snowflake

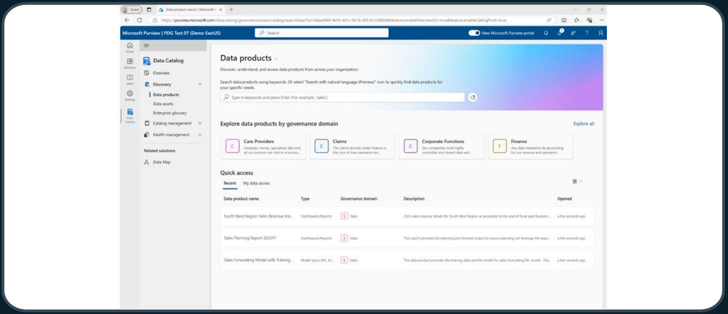
Azure Data

Azure AI

Google Big Query

S3

Govern and Activate your Multi-cloud Data Estate with Purview Data Governance



Data products

Discover, understand, and access data products from across your organization.

Search data products using keywords. Or select "Search with natural language (Preview)" icon to quickly find data products for your specific needs.

Type in keywords and press Enter (For example, 'sales')

Explore data products by governance domain

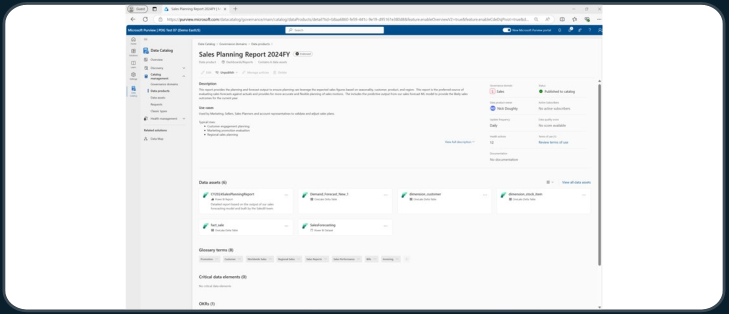
- Care Providers: Hospitals, nurses, specialists, labs and all our partners are vital to ensuring...
- Claims: The claims domain under finance is the core of how payments are...
- Corporate Functions: Our companies most highly controlled and shared data and...
- Finance: Any data needed to do accounting for our revenue and payments. ...

Quick access

Data product name	Type	Governance domain	Description	Opened
South West Region Sales Revenue Insi...	Dashboards/Reports	Sales	2023 sales revenue details for South West Region as presented at the end of fiscal year Business ...	a few seconds ago
Sales Planning Report 2023FY	Dashboards/Reports	Sales	This report provides the planning and forecast output to ensure planning can leverage the expe...	a few seconds ago
Sales Forecasting Model with Training ...	Model types (ML, AI,...	Sales	This data product provides the training data and the model for sales forecasting ML model. The...	a few seconds ago

Data Discovery

Discover, understand, and request access to data containing Fabric data and non-Fabric data in the Purview Unified catalog; leverage built-in Security Copilots to get work done faster.



Data Catalog > Governance domains > Data products >

Sales Planning Report 2024FY

Endorsed

Data product · Dashboards/Reports · Contains 6 data assets

Description

This report provides the planning and forecast output to ensure planning can leverage the expected sales figures based on seasonality, customer, product, and region. This report is the preferred source of evaluating sales forecasts against actuals and provides for more accurate and flexible planning of sales motions. The includes the predictive output from our sales forecast ML model to provide the likely sales outcomes for the current year.

Use cases

Used by Marketing, Sellers, Sales Planners and account representatives to validate and adjust sales plans.

Typical Uses:

- Customer engagement planning
- Marketing promotion evaluation
- Regional sales planning

Governance domain: Sales · Status: Published to catalog · Data product owner: Nick Doughty · Active Subscribers: No active subscribers · Update frequency: Daily · Data quality score: No score available · Health actions: 12 · Terms of use (1): Review terms of use · Documentation: No documentation

Data assets (6)

- CY2024SalesPlanningReport · Power BI Report · Detailed report based on the output of our sales forecasting model and built by the SalesBI team.
- Demand_Forecast_New_1 · OneLake Delta Table
- dimension_customer · OneLake Delta Table
- dimension_stock_item · OneLake Delta Table
- fact_sale · OneLake Delta Table
- SalesForecasting · Power BI Dataset

Glossary terms (8)

Promotion · Customer · Worldwide Sales · Regional Sales · Sales Reports · Sales Performance · Bills · Invoicing

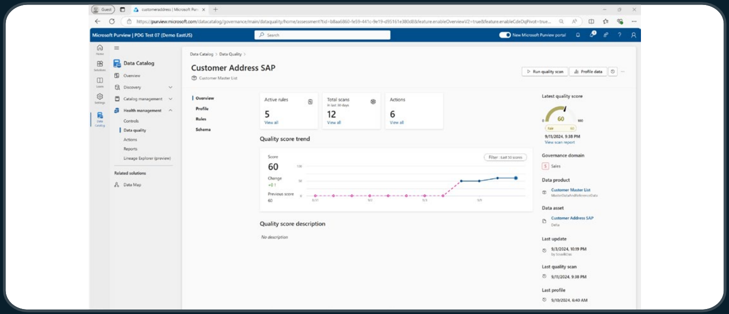
Critical data elements (0)

No critical data elements

OKRs (1)

Catalog Management

Organize, curate, and manage access to your entire data estate (including Fabric data) using logical, business-friendly vernacular your business stakeholders will understand; integrate your Master data management entities into your managed data estate (via 3rd party plug-ins).



Data Catalog > Data Quality >

Customer Address SAP

Customer Master List

Active rules: 5 · Total scans in last 30 days: 12 · Actions: 6

Quality score trend

Score 60 · Change +0.1 · Previous score 60

Quality score description

No description

Latest quality score: 60 · 9/11/2024, 9:38 PM

Governance domain: Sales

Data product: Customer Master List · MasterDataAndReferenceData

Data asset: Customer Address SAP · Delta

Last update: 9/3/2024, 10:19 PM

Last quality scan: 9/11/2024, 9:38 PM

Last profile: 9/10/2024, 6:40 AM

Health Management (Data Quality)

Manage, monitor, and improve data quality and overall data health across your enterprise, multi-cloud data estate (including Fabric data); develop your own Purview reports and/or activate estate cleanup actions using BYOC Fabric integration.

Demo of Purview Unified Catalog

Manage, govern, and secure data in era of AI

Go further by integrating Fabric with Microsoft Purview

Microsoft Fabric

Microsoft Purview

Manage, govern, and secure your data locally in Microsoft Fabric with built-in capabilities

Employ advanced governance and security to Microsoft Fabric

Data ownership | Simplified administration | Unified governance

Purpose-built to support different personas

Go further by integrating Fabric with Microsoft Purview

Microsoft Fabric

Data engineers & data scientists

Data analysts

Data admins

Business users

Microsoft Purview

Security & compliance officers

Data stewards & LoB data owners

Central data office

Data consumers

Designed for data workers

Designed for security, governance & compliance offices

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
- Universal security model*
- Certificates & standards
- Data residency
- Purview sensitivity labeling**
- Purview Data Loss Prevention policies**
- Purview Audit**

Encourage data discovery, trust, and use

- OneLake catalog (Explore tab)
- Endorsements
- Data lineage & impact analysis
- External data sharing
- Metadata curation
- Discover & Reuse

Monitor, uncover insights, and act

- OneLake catalog (Govern tab)
- Monitoring hub
- Workspace monitoring
- Capacity metrics
- Admin monitoring
- Purview Hub

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 (Data Quality)

Risk & compliance posture

- Purview Audit

Fabric natively integrated with Microsoft Purview

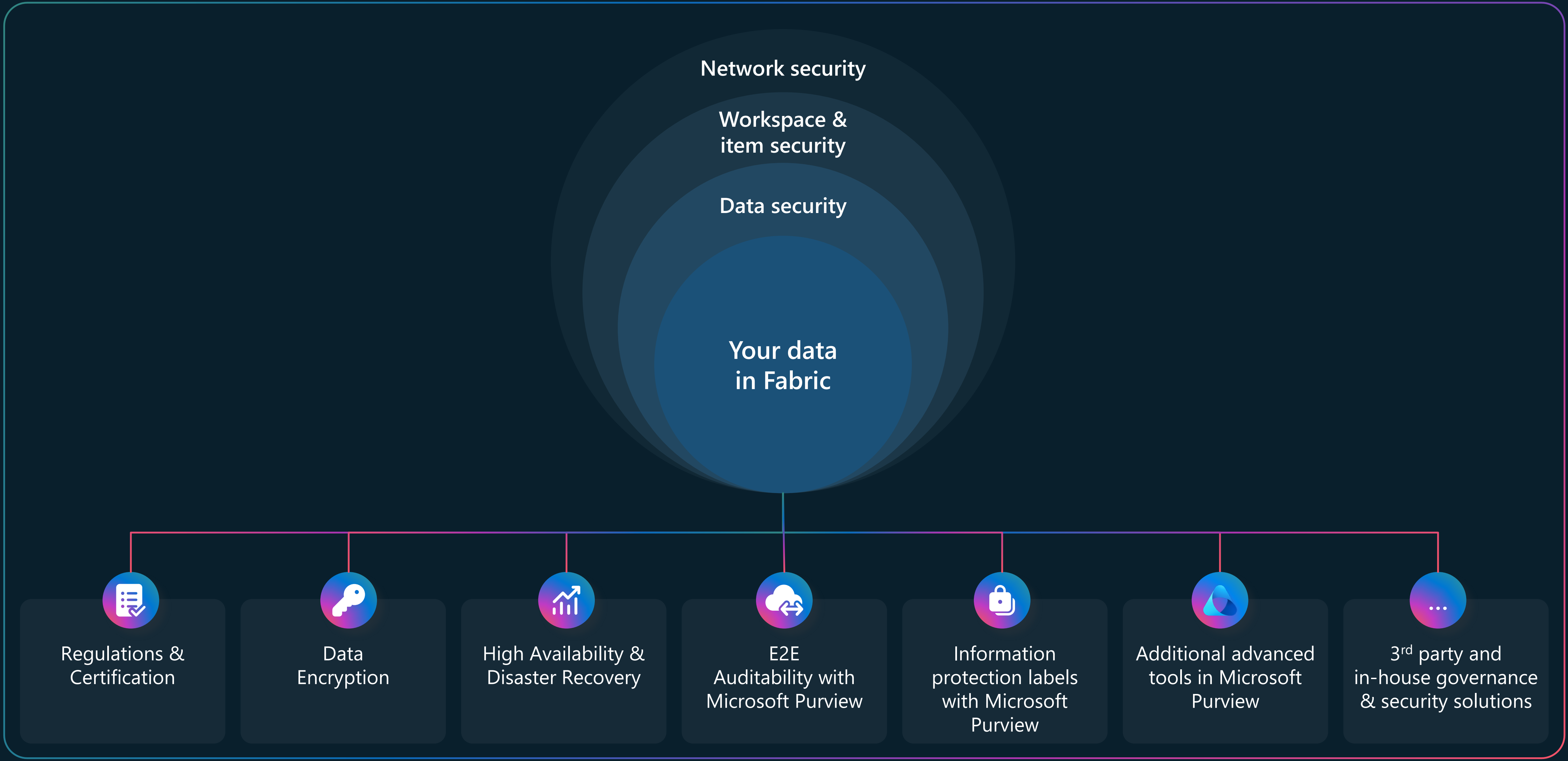
***Additional Microsoft Purview purchase required*

The foundation for responsible data innovation

Seamlessly secure

Confidently activate

Security layers in Microsoft Fabric



Network security

Workspace & item security

Data security

Your data in Fabric

Regulations & Certification

Data Encryption

High Availability & Disaster Recovery

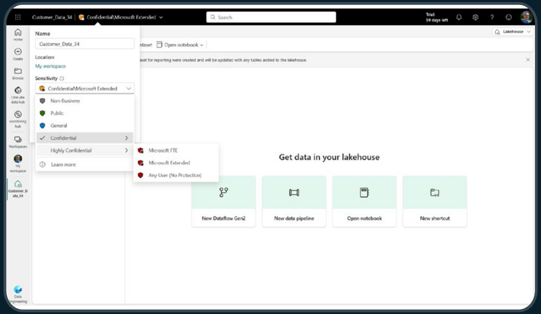
E2E Auditability with Microsoft Purview

Information protection labels with Microsoft Purview

Additional advanced tools in Microsoft Purview

3rd party and in-house governance & security solutions

Purview Data Security & Compliance integration with Fabric


Customer_Data_34 | Confidential\Microsoft Extended

Search

Trial
59 days left

Name: Customer_Data_34

Location: My workspace

Sensitivity: Confidential\Microsoft Extended

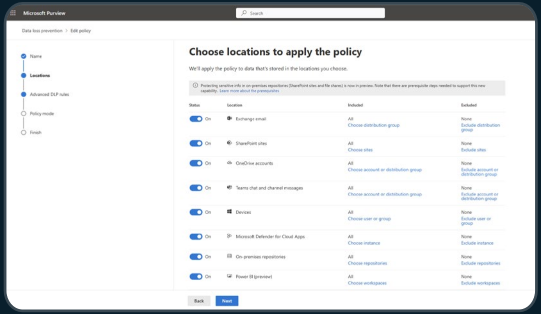
- Non-Business
- Public
- General
- ✓ Confidential
- Highly Confidential
- Learn more

- Microsoft FTE
- Microsoft Extended
- Any User (No Protection)

Get data in your lakehouse

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.


Microsoft Purview

Data loss prevention > Edit policy

Name – Locations – Advanced DLP rules – Policy mode – Finish

Choose locations to apply the policy

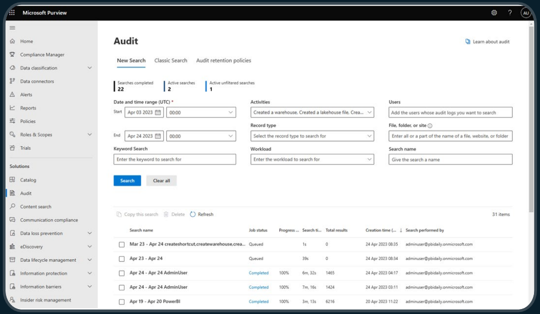
We'll apply the policy to data that's stored in the locations you choose.

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

Status	Location	Included	Excluded
On	Exchange email	All Choose distribution group	None Exclude distribution group
On	SharePoint sites	All Choose sites	None Exclude sites
On	OneDrive accounts	All Choose account or distribution group	None Exclude account or distribution group
On	Teams chat and channel messages	All Choose account or distribution group	None Exclude account or distribution group
On	Devices	All Choose user or group	None Exclude user or group
On	Microsoft Defender for Cloud Apps	All Choose instance	None Exclude instance
On	On-premises repositories	All Choose repositories	None Exclude repositories
On	Power BI (preview)	All Choose workspaces	None Exclude workspaces

Data loss prevention policies

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


Microsoft Purview

Audit

New Search | Classic Search | Audit retention policies

Searches completed: 22 | Active searches: 2 | Active unfiltered searches: 1

Date and time range (UTC) *: Start Apr 03 2023 00:00; End Apr 24 2023 00:00

Activities: Created a warehouse, Created a lakehouse file, Crea...

Users: Add the users whose audit logs you want to search

Record type: Select the record type to search for

File, folder, or site: Enter all or a part of the name of a file, website, or folder

Keyword Search: Enter the keyword to search for

Workload: Enter the workload to search for

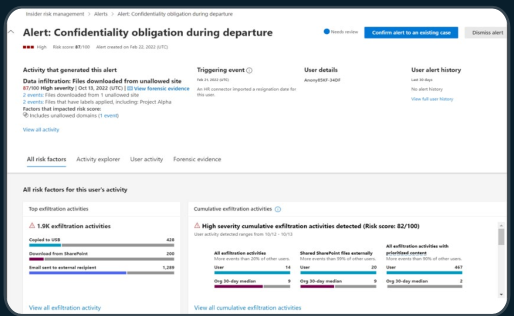
Search name: Give the search a name

31 items

Search name	Job status	Progress ...	Search ti...	Total results	Creation time (...	Search performed by
Mar 23 - Apr 24 createshortcut,createwarehouse,crea...	Queued		1s	0	24 Apr 2023 08:35	adminuser@pbidaily.onmicrosoft.com
Apr 23 - Apr 24	Queued		39s	0	24 Apr 2023 08:34	adminuser@pbidaily.onmicrosoft.com
Apr 24 - Apr 24 AdminUser	Completed	100%	6m, 32s	1465	24 Apr 2023 04:17	adminuser@pbidaily.onmicrosoft.com
Apr 24 - Apr 24 AdminUser	Completed	100%	7m, 16s	1424	24 Apr 2023 03:11	adminuser@pbidaily.onmicrosoft.com
Apr 19 - Apr 20 PowerBI	Completed	100%	3m, 13s	6216	20 Apr 2023 11:22	adminuser@pbidaily.onmicrosoft.com

Audit

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


Insider risk management > Alerts > Alert: Confidentiality obligation during departure

Alert: Confidentiality obligation during departure

High | Risk score: 87/100 | Alert created on Feb 22, 2022 (UTC) | Needs review

Activity that generated this alert

Data infiltration: Files downloaded from unallowed site

87/100 High severity | Oct 13, 2022 (UTC) | View forensic evidence

2 events: Files downloaded from 1 unallowed site

2 events: Files that have labels applied, including: Project Alpha

Factors that impacted risk score:

Includes unallowed domains (1 event)

View all activity

Triggering event: Feb 21, 2022 (UTC). An HR connector imported a resignation date for this user.

User details: Anony85KF-34DF

User alert history: Last 30 days. No alert history. View full user history

All risk factors | Activity explorer | User activity | Forensic evidence

All risk factors for this user's activity

Top exfiltration activities

1.9K exfiltration activities

Copied to USB	428
Download from SharePoint	200
Email sent to external recipient	1,289

View all exfiltration activity

Cumulative exfiltration activities

High severity cumulative exfiltration activities detected (Risk score: 82/100)

User activity detected ranges from 10/12 - 10/13

	All exfiltration activities	Shared SharePoint files externally	All exfiltration activities with prioritized content
	More events than 20% of other users.	More events than 99% of other users.	More events than 90% of other users.
User	14	20	467
Org 30-day median	9	9	2

View all cumulative exfiltration activities

Insider Risk Management

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

Additional Microsoft Purview purchase required

Microsoft Purview Information Protection Policies

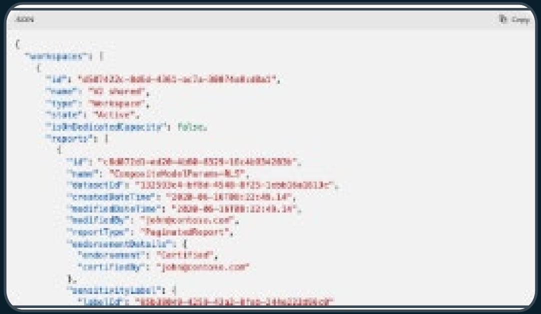
Data Loss Prevention policies for Lakehouse

The foundation for responsible data innovation

Seamlessly secure

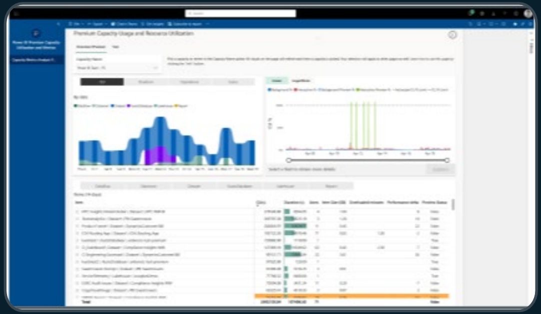
Confidently activate

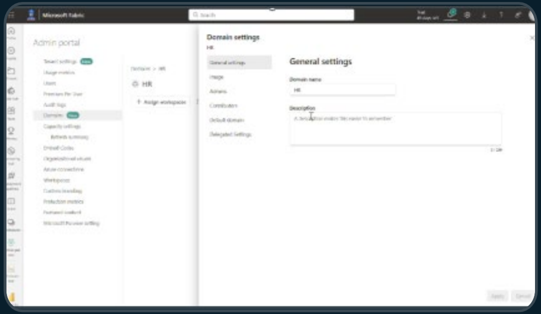
Manage an org-wide data mesh in Fabric with central & delegated settings



JSON Copy

```
{
  "workspaces": [
    {
      "id": "[illegible]",
      "name": "V2 shared",
      "type": "Workspace",
      "state": "Active",
      "isOnDedicatedCapacity": false,
      "reports": [
        {
          "id": "[illegible]",
          "name": "CompositeModelParams-NLS",
          "datasetId": "[illegible]",
          "createdDateTime": "2020-06-16T00:22:48.14",
          "modifiedDateTime": "2020-06-16T00:22:48.14",
          "modifiedBy": "john@contoso.com",
          "reportType": "PaginatedReport",
          "endorsementDetails": {
            "endorsement": "Certified",
            "certifiedBy": "john@contoso.com"
          },
          "sensitivityLabel": {
            "labelId": "[illegible]"
```





Tenant-wide and granular control in Admin Portal

Fabric admins can manage Fabric in one central location with fine-grained control while also gain end-to-end visibility with tenant-wide reports.

Tenant metadata scanning

Easily extract information incl. inventory, item metadata & lineage for all items across Fabric, and connect to 3rd party or homegrown tools.

Manage capacities

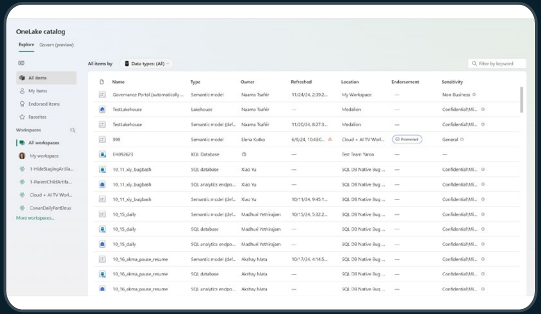
Manage multiple capacities, each with a distinct pool of resources to manage cost at a granular level and get visibility into capacity utilization and usage trends.

Domains, subdomains, workspaces, & folders

Implement a data mesh pattern by grouping your items in folders and workspaces and then in domains to achieve granular control & optimized consumption.

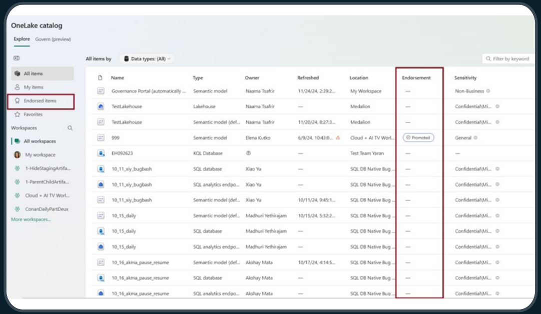
Governance and compliance in Microsoft Fabric

Easily discover, manage, and collaborate on org data



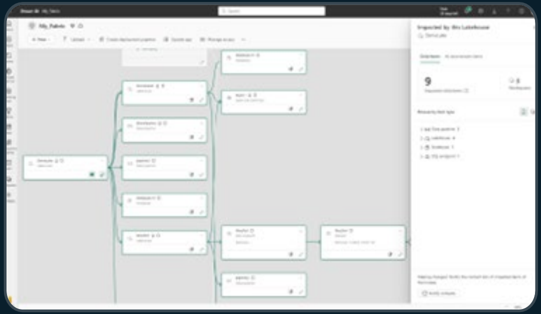
OneLake catalog

Centrally Find, explore, and use relevant Fabric data items in your organization. Data hub Pervasive across Fabric as well as in Teams, Excel and more.



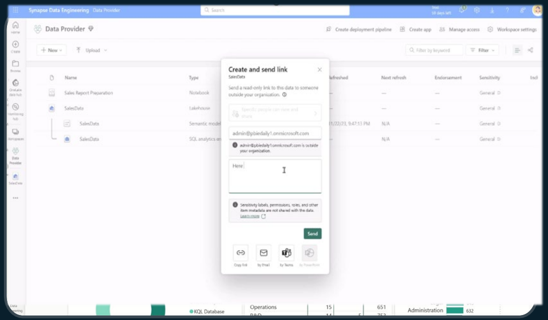
Endorsements & tags

Endorse trusted high-quality items in Fabric and apply relevant tags to create curated sources of truth and increase discoverability and reuse.



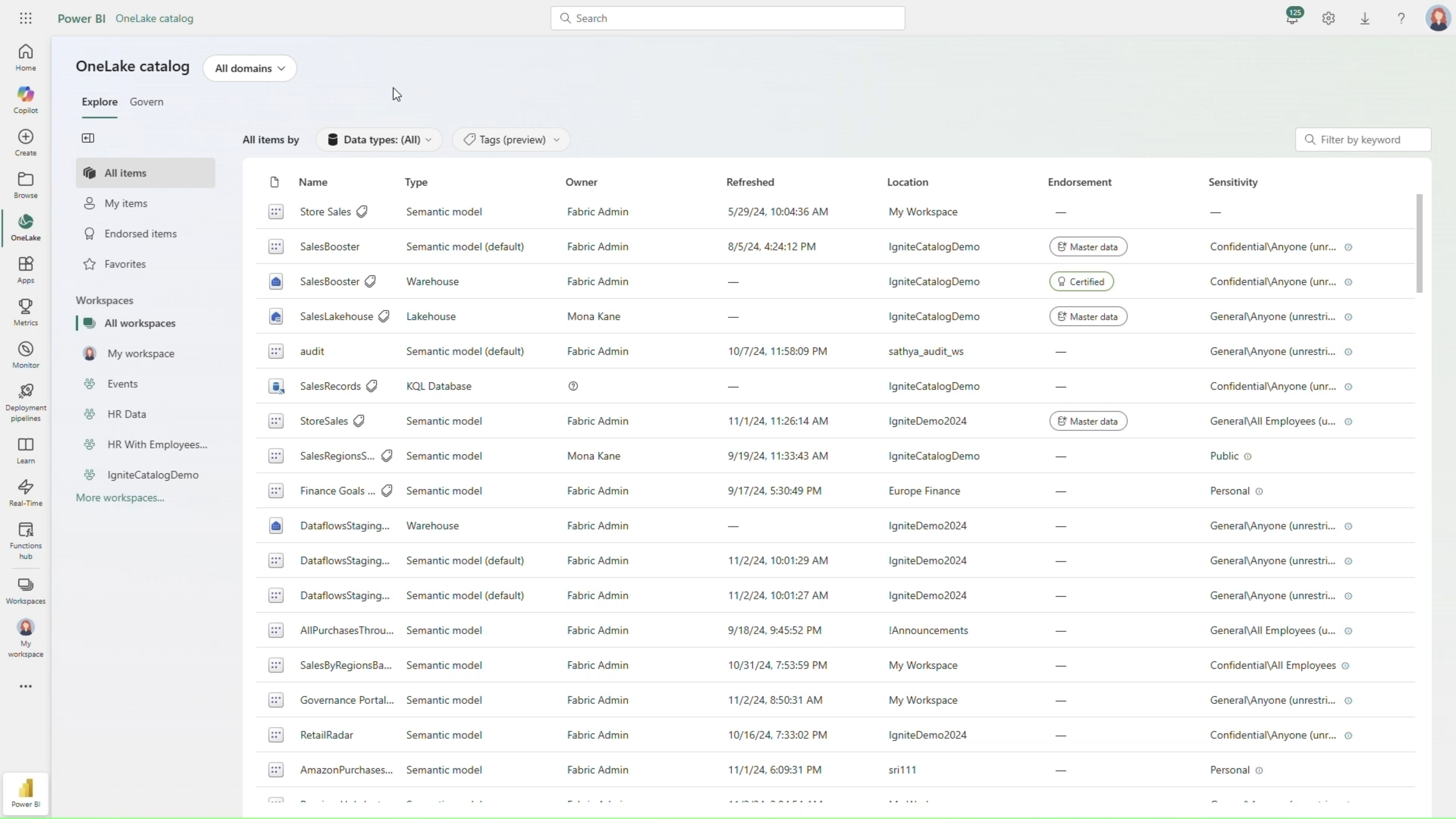
Lineage & impact analysis

Track data lineage of your analytical projects to see how data flows through items and perform impact analysis to assess impact of changes.



External data sharing

Share data and assets with external organizations from OneLake storage locations without copying the data.



OneLake catalog   All domains

Explore   Govern

- All items
- My items
- Endorsed items
- Favorites

Workspaces

- All workspaces
- My workspace
- Events
- HR Data
- HR With Employees...
- IgniteCatalogDemo

More workspaces...

All items by   Data types: (All)   Tags (preview)   Filter by keyword

Name	Type	Owner	Refreshed	Location	Endorsement	Sensitivity
Store Sales	Semantic model	Fabric Admin	5/29/24, 10:04:36 AM	My Workspace	—	—
SalesBooster	Semantic model (default)	Fabric Admin	8/5/24, 4:24:12 PM	IgniteCatalogDemo	Master data	Confidential\Anyone (unr...
SalesBooster	Warehouse	Fabric Admin	—	IgniteCatalogDemo	Certified	Confidential\Anyone (unr...
SalesLakehouse	Lakehouse	Mona Kane	—	IgniteCatalogDemo	Master data	General\Anyone (unrestri...
audit	Semantic model (default)	Fabric Admin	10/7/24, 11:58:09 PM	sathya_audit_ws	—	General\Anyone (unrestri...
SalesRecords	KQL Database	?	—	IgniteCatalogDemo	—	Confidential\Anyone (unr...
StoreSales	Semantic model	Fabric Admin	11/1/24, 11:26:14 AM	IgniteDemo2024	Master data	General\All Employees (u...
SalesRegionsS...	Semantic model	Mona Kane	9/19/24, 11:33:43 AM	IgniteCatalogDemo	—	Public
Finance Goals ...	Semantic model	Fabric Admin	9/17/24, 5:30:49 PM	Europe Finance	—	Personal
DataflowsStaging...	Warehouse	Fabric Admin	—	IgniteDemo2024	—	General\Anyone (unrestri...
DataflowsStaging...	Semantic model (default)	Fabric Admin	11/2/24, 10:01:29 AM	IgniteDemo2024	—	General\Anyone (unrestri...
DataflowsStaging...	Semantic model (default)	Fabric Admin	11/2/24, 10:01:27 AM	IgniteDemo2024	—	General\Anyone (unrestri...
AllPurchasesThrou...	Semantic model	Fabric Admin	9/18/24, 9:45:52 PM	!Announcements	—	General\All Employees (u...
SalesByRegionsBa...	Semantic model	Fabric Admin	10/31/24, 7:53:59 PM	My Workspace	—	Confidential\All Employees
Governance Portal...	Semantic model	Fabric Admin	11/2/24, 8:50:31 AM	My Workspace	—	General\Anyone (unrestri...
RetailRadar	Semantic model	Fabric Admin	10/16/24, 7:33:02 PM	IgniteDemo2024	—	Confidential\Anyone (unr...
AmazonPurchases...	Semantic model	Fabric Admin	11/1/24, 6:09:31 PM	sri111	—	Personal

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

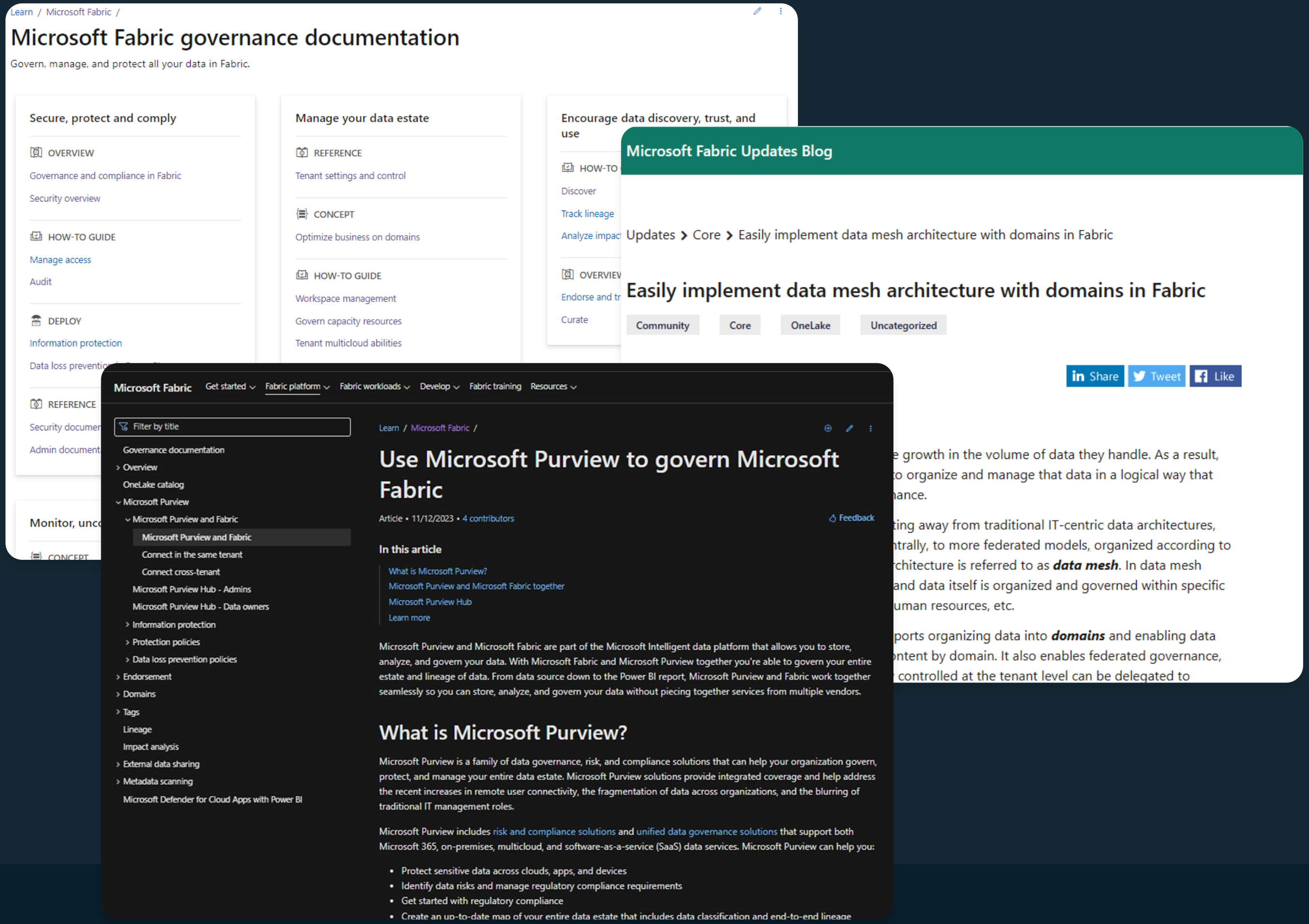
Fabric and Purview resources available

Microsoft Learn Documentation:

- Use Microsoft Purview to govern Microsoft Fabric
- Governance and compliance in Microsoft Fabric
- Security in Microsoft Fabric
- Administration overview in Microsoft Fabric

Blogs:

- Exploring the Relationship Between Fabric and Microsoft Purview: What You Need to Know
- Introducing the new OneLake catalog: Your central hub for discovery, management, and governance
- Easily implement data mesh architecture with domains in Fabric
- Introducing modern data governance for the era of AI | Microsoft Azure Blog



Learn / Microsoft Fabric /

Microsoft Fabric governance documentation

Govern, manage, and protect all your data in Fabric.

Secure, protect and comply

OVERVIEW
Governance and compliance in Fabric
Security overview

HOW-TO GUIDE
Manage access
Audit

DEPLOY
Information protection
Data loss preventio

REFERENCE
Security documen
Admin document

Manage your data estate

REFERENCE
Tenant settings and control

CONCEPT
Optimize business on domains

HOW-TO GUIDE
Workspace management
Govern capacity resources
Tenant multicloud abilities

Encourage data discovery, trust, and use

HOW-TO
Discover
Track lineage
Analyze impac

OVERVIEW
Endorse and tr
Curate

Monitor, unc

CONCEPT

Microsoft Fabric Updates Blog

Updates › Core › Easily implement data mesh architecture with domains in Fabric

Easily implement data mesh architecture with domains in Fabric

Community | Core | OneLake | Uncategorized

in Share | Tweet | Like

e growth in the volume of data they handle. As a result, o organize and manage that data in a logical way that ance.

ting away from traditional IT-centric data architectures, ntrally, to more federated models, organized according to chitecture is referred to as ***data mesh***. In data mesh and data itself is organized and governed within specific uman resources, etc.

ports organizing data into ***domains*** and enabling data ontent by domain. It also enables federated governance, controlled at the tenant level can be delegated to

Microsoft Fabric | Get started | Fabric platform | Fabric workloads | Develop | Fabric training | Resources

Filter by title

- Governance documentation
- › Overview
- OneLake catalog
- ⌄ Microsoft Purview
  - ⌄ Microsoft Purview and Fabric
    - Microsoft Purview and Fabric
    - Connect in the same tenant
    - Connect cross-tenant
  - Microsoft Purview Hub - Admins
  - Microsoft Purview Hub - Data owners
  - › Information protection
  - › Protection policies
  - › Data loss prevention policies
- › Endorsement
- › Domains
- › Tags
- Lineage
- Impact analysis
- › External data sharing
- › Metadata scanning
- Microsoft Defender for Cloud Apps with Power BI

Learn / Microsoft Fabric /

Use Microsoft Purview to govern Microsoft Fabric

Article • 11/12/2023 • 4 contributors

Feedback

In this article

What is Microsoft Purview?
Microsoft Purview and Microsoft Fabric together
Microsoft Purview Hub
Learn more

Microsoft Purview and Microsoft Fabric are part of the Microsoft Intelligent data platform that allows you to store, analyze, and govern your data. With Microsoft Fabric and Microsoft Purview together you're able to govern your entire estate and lineage of data. From data source down to the Power BI report, Microsoft Purview and Fabric work together seamlessly so you can store, analyze, and govern your data without piecing together services from multiple vendors.

What is Microsoft Purview?

Microsoft Purview is a family of data governance, risk, and compliance solutions that can help your organization govern, protect, and manage your entire data estate. Microsoft Purview solutions provide integrated coverage and help address the recent increases in remote user connectivity, the fragmentation of data across organizations, and the blurring of traditional IT management roles.

Microsoft Purview includes risk and compliance solutions and unified data governance solutions that support both Microsoft 365, on-premises, multicloud, and software-as-a-service (SaaS) data services. Microsoft Purview can help you:

- Protect sensitive data across clouds, apps, and devices
- Identify data risks and manage regulatory compliance requirements
- Get started with regulatory compliance
- Create an up-to-date map of your entire data estate that includes data classification and end-to-end lineage

Purview data governance : click-through demos

Click-through demos:

- Overview - https://purviewdatagovernance.storylane.io/share/kfdnjhua9hlh
- Set up roles and permissions https://purviewdatagovernance.storylane.io/share/dwuqjygdm0zi
- Set up governance domains- https://purviewdatagovernance.storylane.io/share/ymmxfeakupij
- Set up and register your data- https://purviewdatagovernance.storylane.io/share/8ubzzhh1npwl
- Publish data products- https://purviewdatagovernance.storylane.io/share/7xjutjocwcyz
- Set up data quality- https://purviewdatagovernance.storylane.io/share/3ltoiwe8eiev
- Manage data health - https://purviewdatagovernance.storylane.io/share/qqysnfkfarvd
- Democratize data - https://purviewdatagovernance.storylane.io/share/asstzxddztgf

Purview Data Security, risk & compliance resources available

Microsoft Learn Documentation:

Microsoft 365 Copilot blueprint for oversharing | Microsoft Learn

Secure AI: Purview for M365 Copilot Training & Resources

Supported AI sites by Microsoft Purview for data security and compliance protections | Microsoft Learn

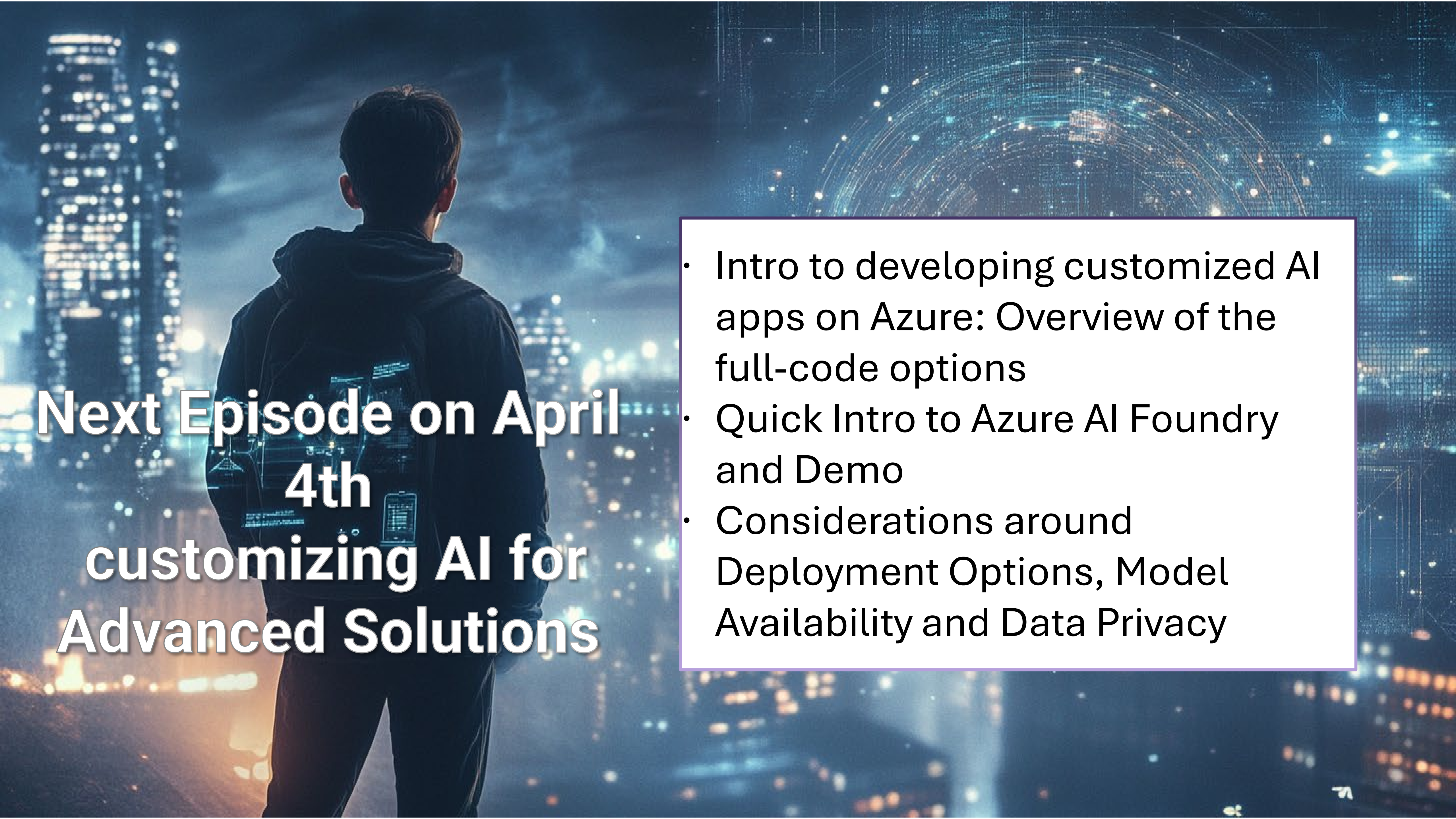
Help dynamically mitigate risks with Adaptive Protection | Microsoft Learn

Learn about Data Security Posture Management (preview) | Microsoft Learn

Learn about data loss prevention | Microsoft Learn

Insider risk management | Microsoft Learn

Microsoft Purview Information Protection | Microsoft Learn



Next Episode on April 4th customizing AI for Advanced Solutions

- Intro to developing customized AI apps on Azure: Overview of the full-code options
- Quick Intro to Azure AI Foundry and Demo
- Considerations around Deployment Options, Model Availability and Data Privacy

Thank You

Erjola Lekaj

Technical Specialist
Security

Lisa Wolffhugel

Partner Solution Architect
Data, AI & Sustainability

Avi Melwani

Technical Specialist
Data & AI