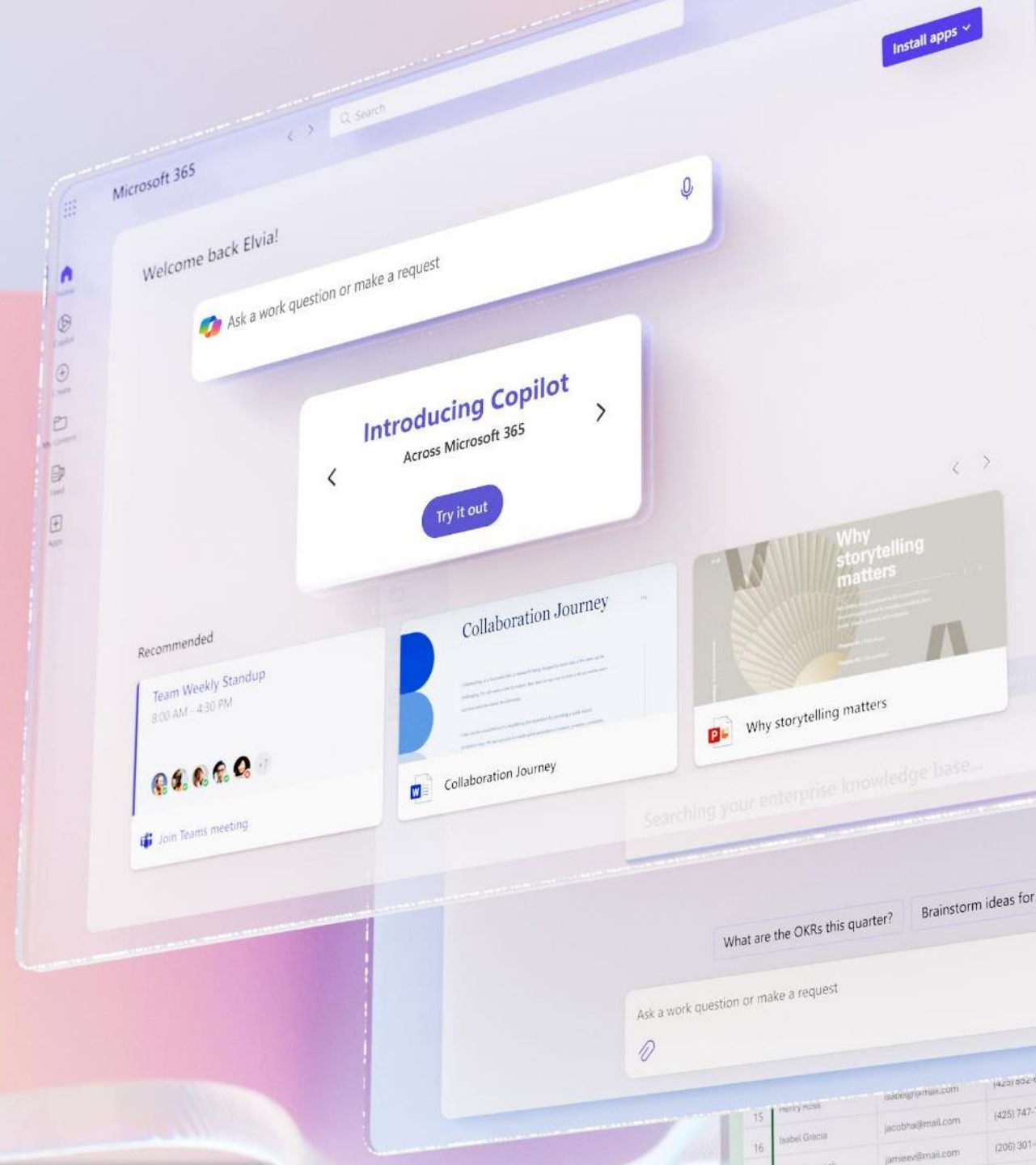
Microsoft 365

Secure and govern data in the age of AI

Overview of Copilot for Microsoft 365

21 May 2024

Erfan Setork | Principal Technical Specialist, Compliance
Natalie Noonan | Global Black Belt, Compliance



Welcome + Introductions

Erfan Setork

Principal Technical Specialist, Compliance

erfansetork@microsoft.com | Linkedin

- Leads data protection and data governance strategies for prominent US healthcare providers and payers
- 10+ years as a former IT, cybersecurity and compliance analyst within enterprise software companies

Natalie Noonan

Global Black Belt, Compliance

CIPM (IAPP), IGP (ARMA), CSM, PMP

nanoonan@microsoft.com | Linkedin

- Works with Microsoft's customers, partners, and engineering teams to bring customer insights and enhancements into the risk and compliance solutions
- Point of escalation for customers assessing and deploying Microsoft Purview to meet legal, risk, and compliance obligations
- 20+ years as a former program leader, practitioner, and consultant specializing in information governance, ediscovery, and privacy

Agenda

Overview

→ What is Copilot for M365? What are top information governance problems and risks?
→ How do we deploy Copilot securely? Where do we start?

Readiness

1. How do we get ready for Copilot for M365? >>"plan on a page"
2. Planning your Copilot rollout – enabling data clean-up and governance by design

Demo

Administrator – Risk and Compliance Controls

1. Applying retention and deletion controls (e.g., Copilot interactions, recordings and transcripts)
2. Monitoring for ethical and appropriate use
3. Gathering evidence and audit for data investigations and litigation
4. Using specialized tools for data clean-up and data governance

End User – Prompts and Responses

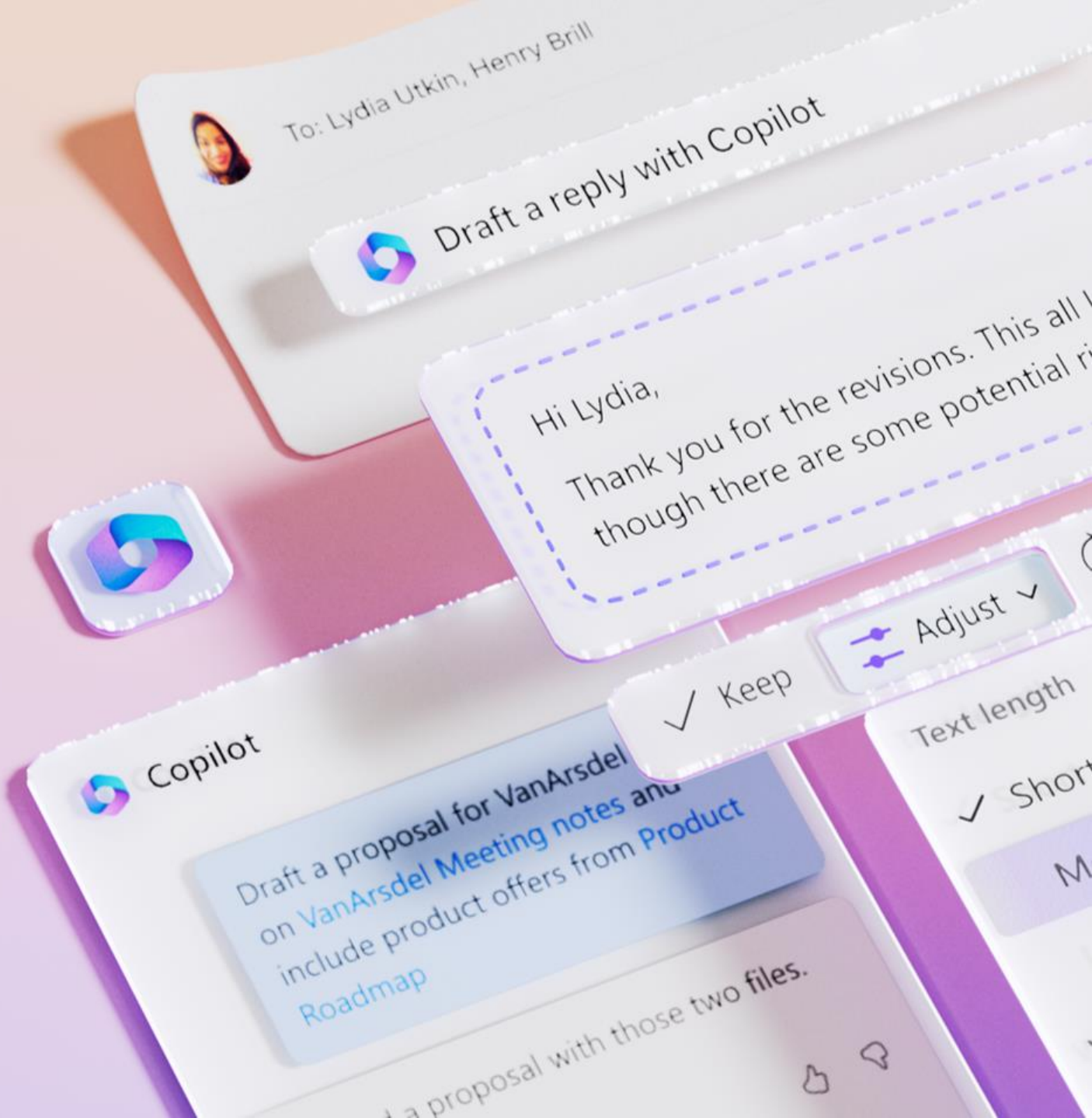
1. Sensitivity labels – applying and enforcing protection (content markings, encryption, privacy, access controls)
2. Label citations – guiding awareness of data sources and classification
3. Label inheritance – driving labels to content created by Copilot
4. Permissions adherence – performing only authorized activities (least privilege access)

Closing

Q&A

Overview

Copilot for Microsoft 365

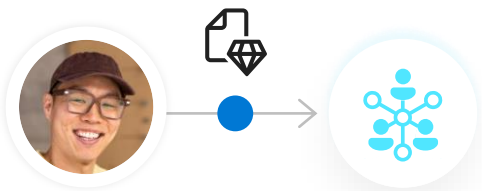


Security and compliance concerns with AI usage

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

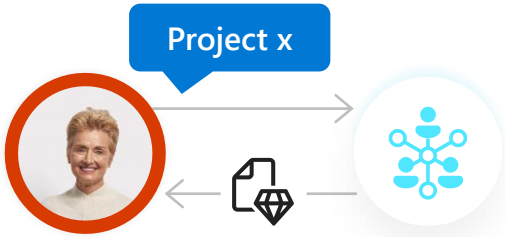
1

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



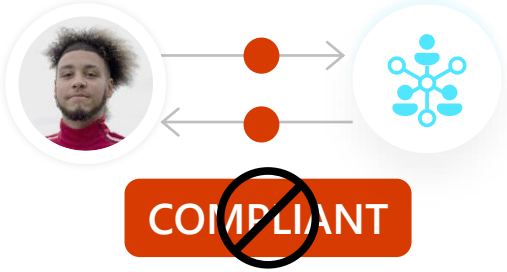
2

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



3

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



What is Microsoft Copilot?

[Microsoft Copilot | Microsoft AI]

Copilot (Edge)

Better interaction with web content

Microsoft 365

Word

Better reading and writing assistance

Outlook

Better e-mail management

Excel

Better data analysis

PowerPoint

Better presentations

Teams

Better meetings

M365 Chat

Your AI assistant

Viva

Drive adoption

Windows

Better interaction with OS, apps, and files

Copilot for Web

Copilot for Productivity

Enhance Copilot for Everyday

Dynamics

Better sales and customer support

Fabric

Better data analytics and business intelligence

Security

Better threat detection, identification, and mitigation

GitHub

Better code development

Copilot Studio

Better creation of apps, workflows, and agents

Copilots for Business

Copilots for Analytics

Copilot for Security

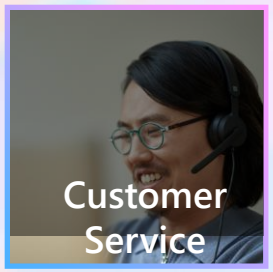
Copilot for Development

Copilot for Low/No Code Development

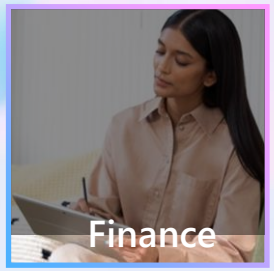
What are common use cases?

Jumpstart the creative process and generate ideas while writing

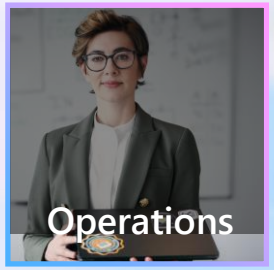
Stay focused on closing deals with an AI assistant for email



Stay coordinated as a team to resolve more customer issues



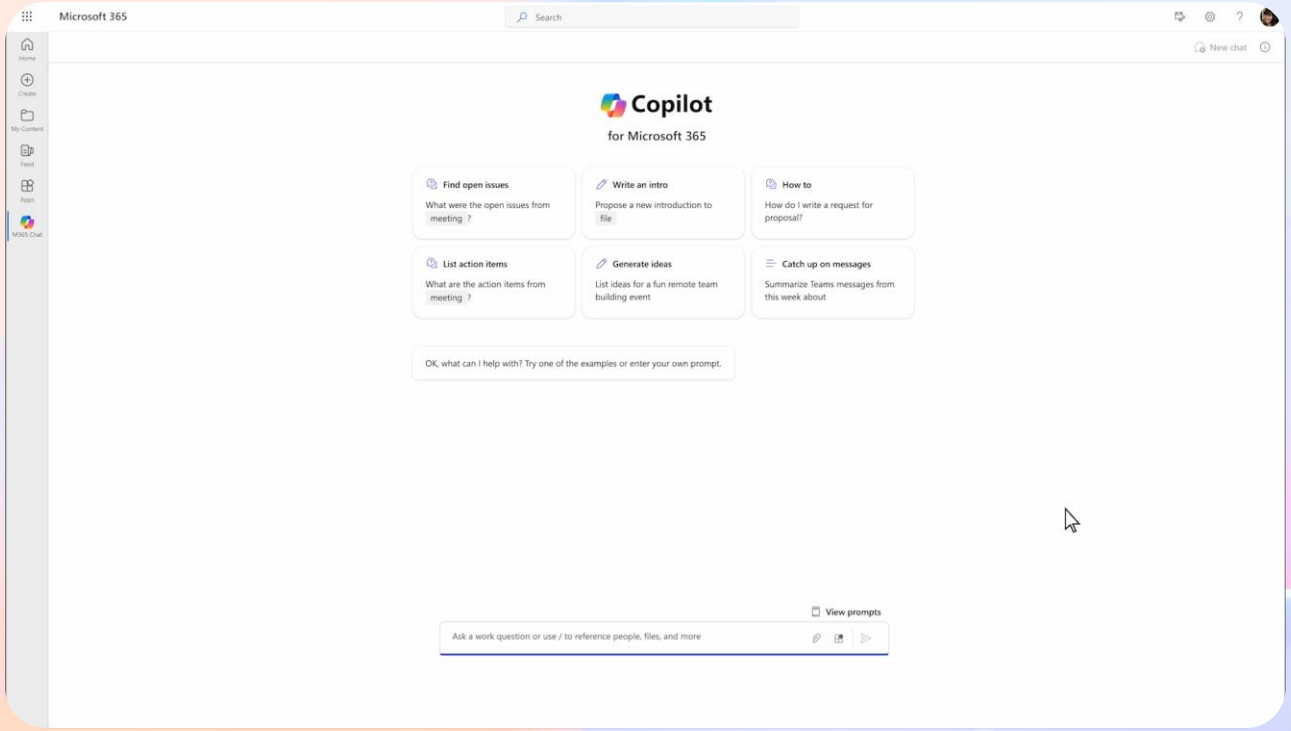
Quickly search data to solve your most complex problems



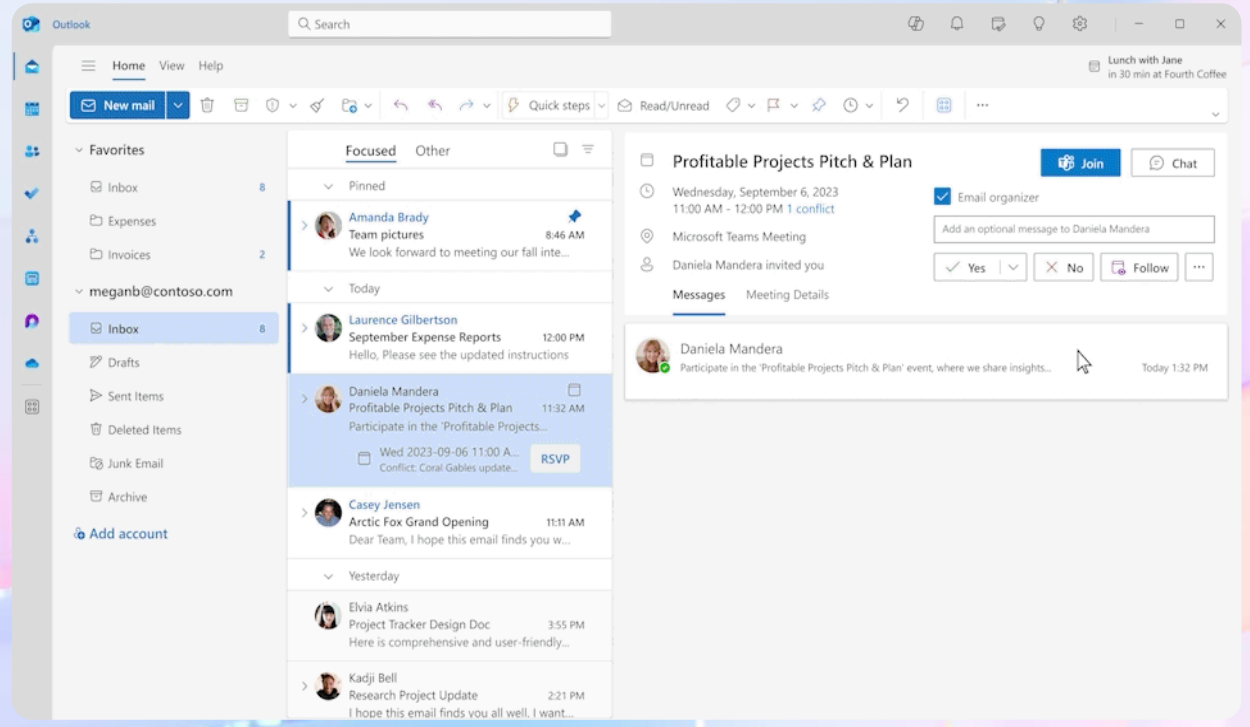
Simplify quality reporting and data validation

Effectively manage shared projects and track progress

Store, access, and prioritize notes in a fraction of the time



Copilot for Microsoft 365



Copilot in Outlook

Comparing Personal, Work and Copilot for M365

	Copilot	Copilot	Copilot for Microsoft 365
	Personal (consumer)	**Web** (enterprise/web)	**Work** (enterprise/tenant)
GPT Large Language Model	●	●	●
AI-Powered Web Search, Answers & Content Generation	●	●	●
Commercial Data Protection		●	●
Enterprise Security, Privacy & Compliance			●
Microsoft 365 Graph (content & context)			●
Microsoft 365 Apps			●
Prompts retained	●		●
Prompts potentially used to tune LLM	●		

Technical Readiness

How do we get ready for Copilot for M365?

"Plan on a page" - Envision your data security, privacy, and governance processes and requirements

Identify high value improvement actions to strengthen security and privacy controls and readiness for Copilot for Microsoft 365	1 **Limit use of consumer generative AI** to protect your corporate data, avoid data leakage, and benefit from Microsoft Responsible AI standards and Copilot Copyright Commitments. 2 **Plan your Copilot rollout by controlling who gets access first**, allowing for data clean-up, least-privilege access controls, and supporting communications and training. Zero Trust Model 3 **Strengthen data access controls** to drive awareness, review, and remediation actions (i.e., manage overprivileged and risky users and devices) Microsoft Entra ID Access Reviews | SharePoint admin center | Microsoft Intune 4 **Prioritize deployment of data security and compliance controls** - identify and label sensitive, personal, and business critical data for appropriate Copilot usage. Microsoft Purview | Microsoft Purview data security and compliance protections for Copilot 5 **Use specialized tools for data clean-up** to accelerate the remediation of data oversharing at scale via data governance reports, restricted access controls, and more. SharePoint Premium | Microsoft Graph Data Connect
Identify those who can help	**Work with your Microsoft customer enablement teams and partners** on top priority actions, readiness assessments, and deployment plans. Copilot for Microsoft 365 – Microsoft Adoption | Microsoft Copilot for Microsoft 365 setup guide

How do we get ready for Copilot for M365?

"Plan on a page" - Envision your data security, privacy, and governance processes and requirements

1

Identify high value improvement actions to strengthen security and privacy controls and readiness for Copilot for Microsoft 365

1. **Limit use of consumer generative AI** to protect your corporate data, avoid data leakage, and benefit from Microsoft Responsible AI standards and Copilot Copyright Commitments.
2. **Plan your Copilot rollout by controlling who gets access first**, allowing for data clean-up, least-privilege access controls, and supporting communications and training.
   Zero Trust Model
3. **Strengthen data access controls** to drive awareness, review, and remediation actions (i.e., manage overprivileged and risky users and devices)
   Microsoft Entra ID Access Reviews | SharePoint admin center | Microsoft Intune
4. **Prioritize deployment of data security and compliance controls** - identify and label sensitive, personal, and business critical data for appropriate Copilot usage.
   Microsoft Purview | Microsoft Purview data security and compliance protections for Copilot
5. **Use specialized tools for data clean-up** to accelerate the remediation of data oversharing at scale via data governance reports, restricted access controls, and more.
   SharePoint Premium | Microsoft Graph Data Connect

Identify those who can help

- **Work with your Microsoft customer enablement teams and partners** on top priority actions, readiness assessments, and deployment plans.
  Copilot for Microsoft 365 – Microsoft Adoption | Microsoft Copilot for Microsoft 365 setup guide

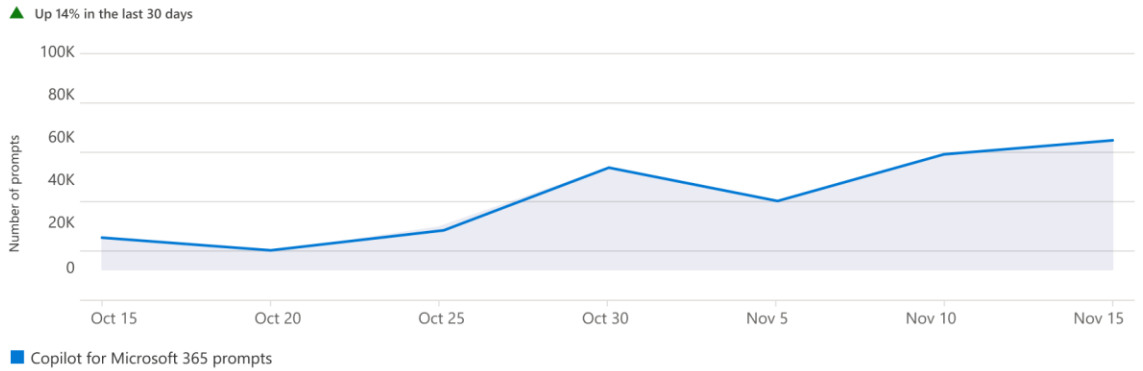
AI hub (preview)

1

Analytics Policies Activity explorer

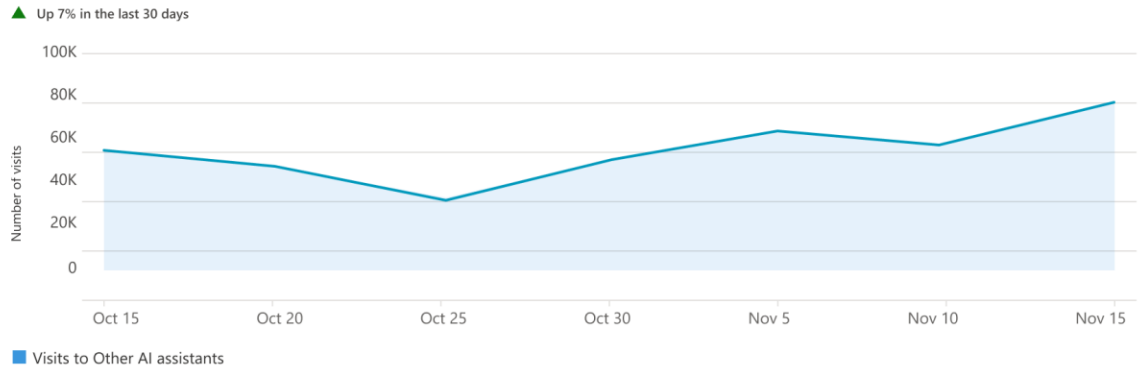
AI hub in Microsoft Purview provides insights to help security teams gain comprehensive visibility into data security risks (e.g., prompts containing sensitive data in consumer generative AI).

Total prompts over time (Microsoft Copilot)



View details

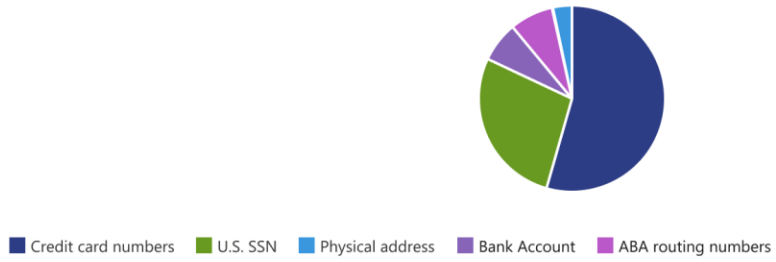
Total visits (Other AI assistants)



View details

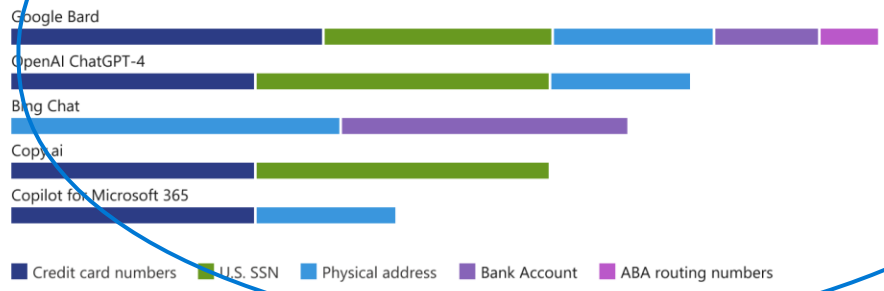
Sensitive data in prompts

Sensitive data shared with all AI assistants grouped by sensitive information type.



Total prompts with sensitive data

Total number of prompts containing sensitive data shared with all AI assistants.



Public Preview

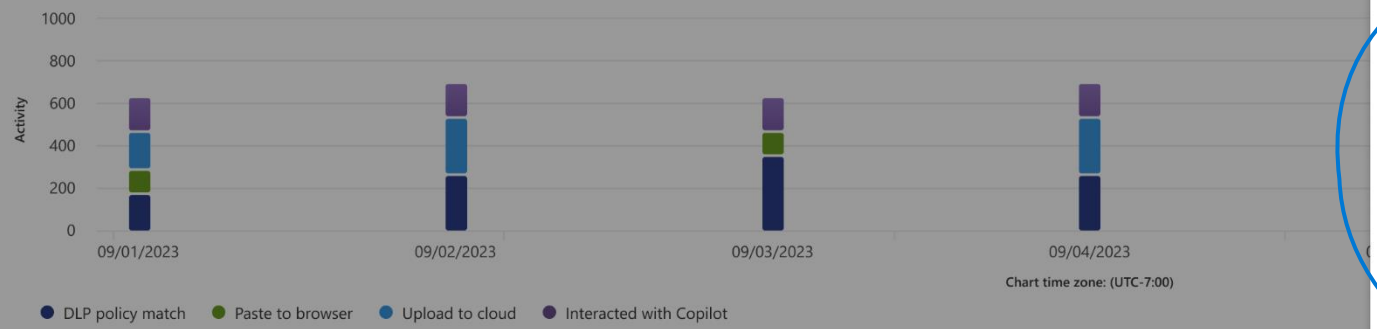
Home
Ai Hub
Compliance Manager
Data classification
Data Connectors
Alerts
Reports
Policies
Permissions

Solutions
Catalog
Audit
Content search
Communication compliance
Data loss prevention
eDiscovery
Data lifecycle management
Information protection
Insider risk management
Records management

AI hub (preview)

Analytics | Policies | Activity explorer

Activity: All values | User: All values | DLP policy matched: All values | Sensitive info type: All values | Add filter | Reset all



Activity	User	Time happened	Device full name	Enforcement mode	Sensitive info type	File sensitiv
File upload to cloud	Mona Kane	Sep 01, 2023 3:54 PM	Desktop-3453HD	Audit	Credit card number	Confidentia
Paste to browser	Dean Renzo	Sep 01, 2023 3:54 PM	Desktop-363345HD	Audit	Social security number	
File upload to cloud	Edison GII	Sep 02, 2023 3:54 PM	Desktop-53544EF	Audit	Physical address	Confidentia
Interacted with Copilot	Sarah Terry	Sep 03, 2023 3:54 PM		Audit	Credit card number	
File upload to cloud	Posie Par	Sep 03, 2023 3:54 PM	Desktop-53544EF	Audit	Physical address	Confidentia
Interacted with Copilot	Dean Renzo	Sep 05, 2023 3:54 PM		Audit	Social security number	
Paste to browser	Sarah Terry	Sep 06, 2023 3:54 PM	Desktop-3534345-LD	Audit	Bank account	
Interacted with Copilot	Sarah Terry	Sep 06, 2023 3:54 PM	Desktop-3534345-LD	Audit	Bank account	
Paste to browser	Mona Kane	Sep 13, 2023 3:54 PM	Desktop-ASFD213	Audit	Credit card number	

File upload to cloud

1

Activity details

Activity
File upload to cloud

Happened
Sep 13, 2023 3:54 PM

Client IP
131.109.147.63

Enforcement mode
Audit

Target domain
bard.google.com

JIT triggered
False

About this item

User
Mona.Kane@contoso.com

Sensitve info type
Credit card number

Policy
AI hub – Data Protection

Rule
Audit-UploadToCloud

Location details

Source location type
Unknown

Destination location type
Unknown

Platform
Windows

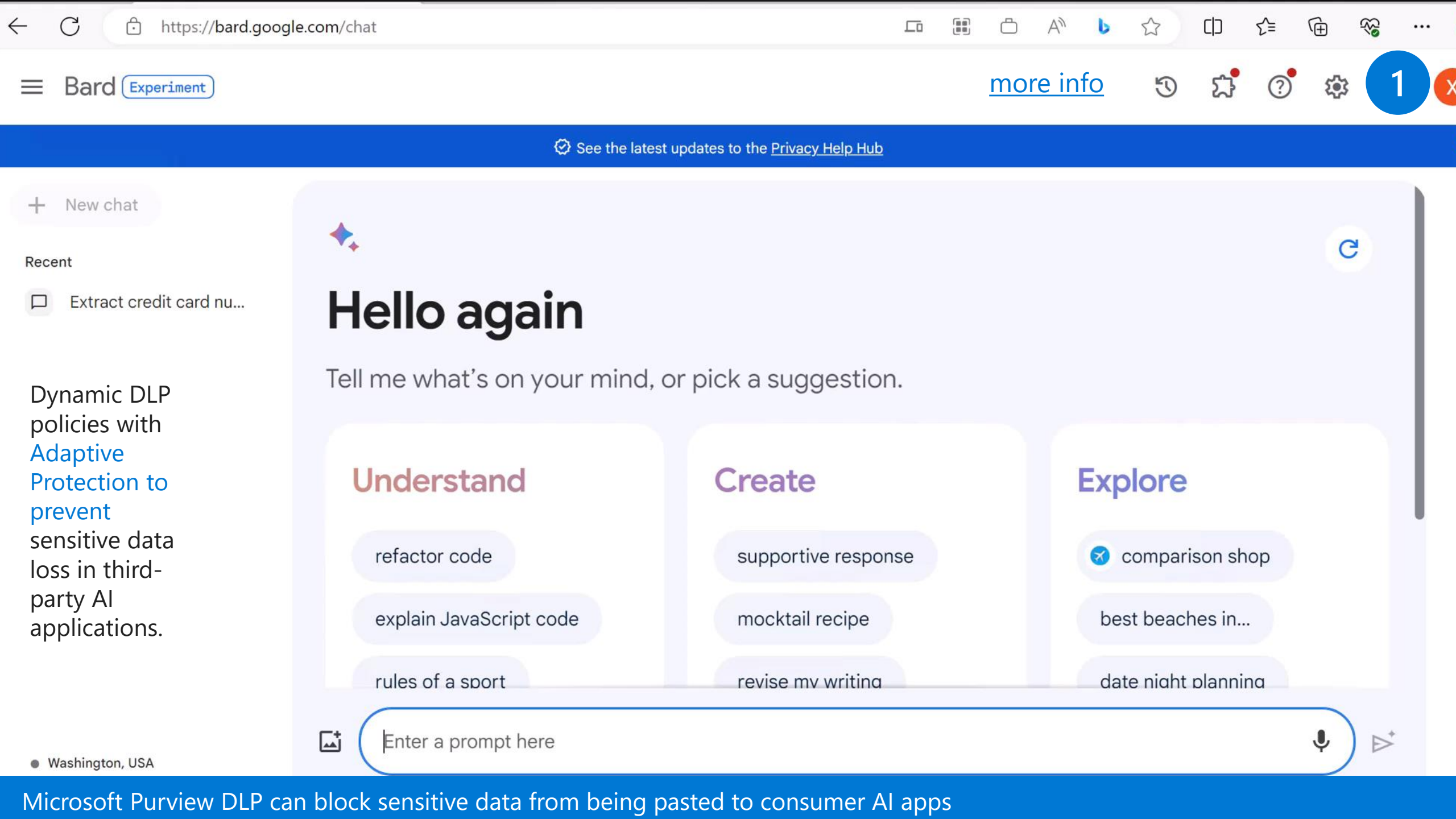
Application
msedge.exe

Application
Desktop-3453HD
View device details

MDAIP device ID
33oe9ca0778b9ec2ab7933ac9f7ehsd1987bacd8

Done

Public Preview



Dynamic DLP policies with Adaptive Protection to prevent sensitive data loss in third-party AI applications.

Microsoft Purview DLP can block sensitive data from being pasted to consumer AI apps

How do we get ready for Copilot for M365?

"Plan on a page" - Envision your data security, privacy, and governance processes and requirements

2

Identify high value improvement actions to strengthen security and privacy controls and readiness for Copilot for Microsoft 365

1 **Limit use of consumer generative AI** to protect your corporate data, avoid data leakage, and benefit from Microsoft Responsible AI standards and Copilot Copyright Commitments.

2 **Plan your Copilot rollout by controlling who gets access first**, allowing for data clean-up, least-privilege access controls, and supporting communications and training.
Zero Trust Model

3 **Strengthen data access controls** to drive awareness, review, and remediation actions (i.e., manage overprivileged and risky users and devices)
Microsoft Entra ID Access Reviews | SharePoint admin center | Microsoft Intune

4 **Prioritize deployment of data security and compliance controls** - identify and label sensitive, personal, and business critical data for appropriate Copilot usage.
Microsoft Purview | Microsoft Purview data security and compliance protections for Copilot

5 **Use specialized tools for data clean-up** to accelerate the remediation of data oversharing at scale via data governance reports, restricted access controls, and more.
SharePoint Premium | Microsoft Graph Data Connect

Identify those who can help

✓ **Work with your Microsoft customer enablement teams and partners** on top priority actions, readiness assessments, and deployment plans.
Copilot for Microsoft 365 – Microsoft Adoption | Microsoft Copilot for Microsoft 365 setup guide

Perform data discovery

Optional tasks and tools to aid as part of a data discovery risk assessment depending on licensing and skills

2

We must discover and classify data to understand how it is being used, stored, and shared to implement appropriate safeguards.

Why does this matter?

Purpose: To uncover and report on potential risks of overexposed sensitive data, oversharing of sites and content, and to aid in the preparation of remediation activities

Procedure: Run manual procedures, tools, scripts, and building of visual assets to help uncover and present existing risks of data, permissions, and other security, privacy, and information technology concerns to help plan for the remediation activities ahead

Results: To obtain knowledge of exposed risks, required activities of remediation, assignment and alignment of resources required, and estimations of time required to implement the necessary controls

Areas of focus

Uncover Risks

Data discovery

- Permissions
- Sensitive and personal data
- Privacy levels
- Data overexposure
- Obsolete data

- Levels of sensitivity
- Application of retention
- Access request procedures
- Data loss procedures
- On/Offboarding procedures

Optional actions

E3	E5	Add-on
Review existing permissions of Teams and Sites	Use content search to discover sensitive information	Run PowerShell scripts to generate reports
Use Content Explorer to identify sensitive content	Identify data exposition with Defender for Cloud Apps	Use eDiscovery Premium to identify sensitive content
Identify overshared personally identifiable information with Microsoft Priva	Identify sensitive or overexposed content with SharePoint Premium	Microsoft Purview Advanced Rich Reporting

Compliance Manager
Data classification
Data connectors
Alerts
Reports
Policies
Permissions
Trials

Solutions
Catalog
App governance
Audit
Content search
Communication compliance
Data loss prevention
eDiscovery
Data lifecycle management
Information protection
Records management

Data classification

Overview | Trainable classifiers | Sensitive info types | EDM classifiers | Content explorer | Activity explorer

Explore the email and docs in your organization that contain sensitive info or have labels applied. You drill down further by reviewing the source content that's currently stored in Exchange, SharePoint, and OneDrive. Support for more locations is coming soon. Learn more

Filter on labels, info types, or categories

All locations > SharePoint > https://m365x10870916.sharepoint.com/sites/Retail

Lab Test Terms 1

Sensitivity labels

Highly Confidential/Merger and Acquisition 1

Retention labels

Retain 5yrs and Delete 8

PII Data - United States 1

Trainable Classifiers

Finance 23

Agreements 17

Legal Affairs 16

M&A Files 15

Non disclosure agreement 1

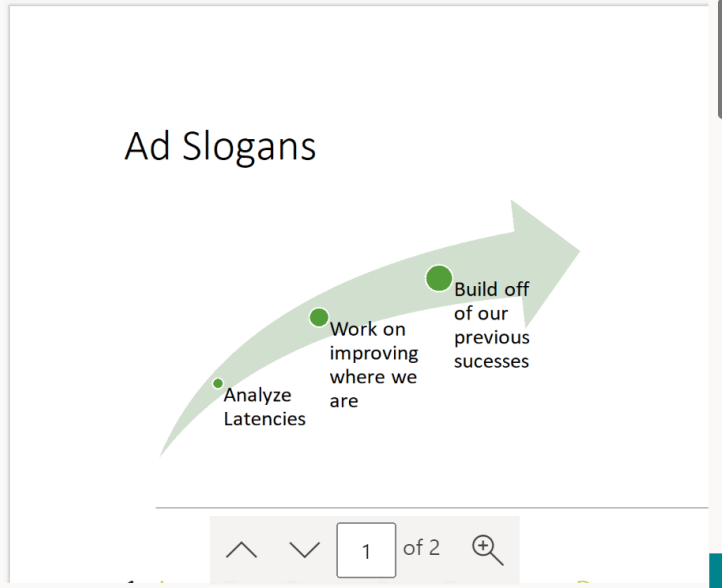
The actual number of items in this site/folder might be different from the calculated number that's displayed on the left

Export | Search

Name	Sensitive info type	Tra
Contoso Electronic...	All Full Names	Fina
Electronics Store Tr...	All Full Names	Fina
Ad Slogans.docx		Fina
CE Annual Report.d...	All Full Names	Fina
letter of intent_8.pdf	Types Of M... +1 more	Agr
term sheet_4.pdf	Australian C... +5 more	Agr
letter of intent_9.pdf	All Full Na... +2 more	Agr
term sheet_1.pdf	All Full Na... +2 more	M8

Ad Slogans.docx

Source | Details

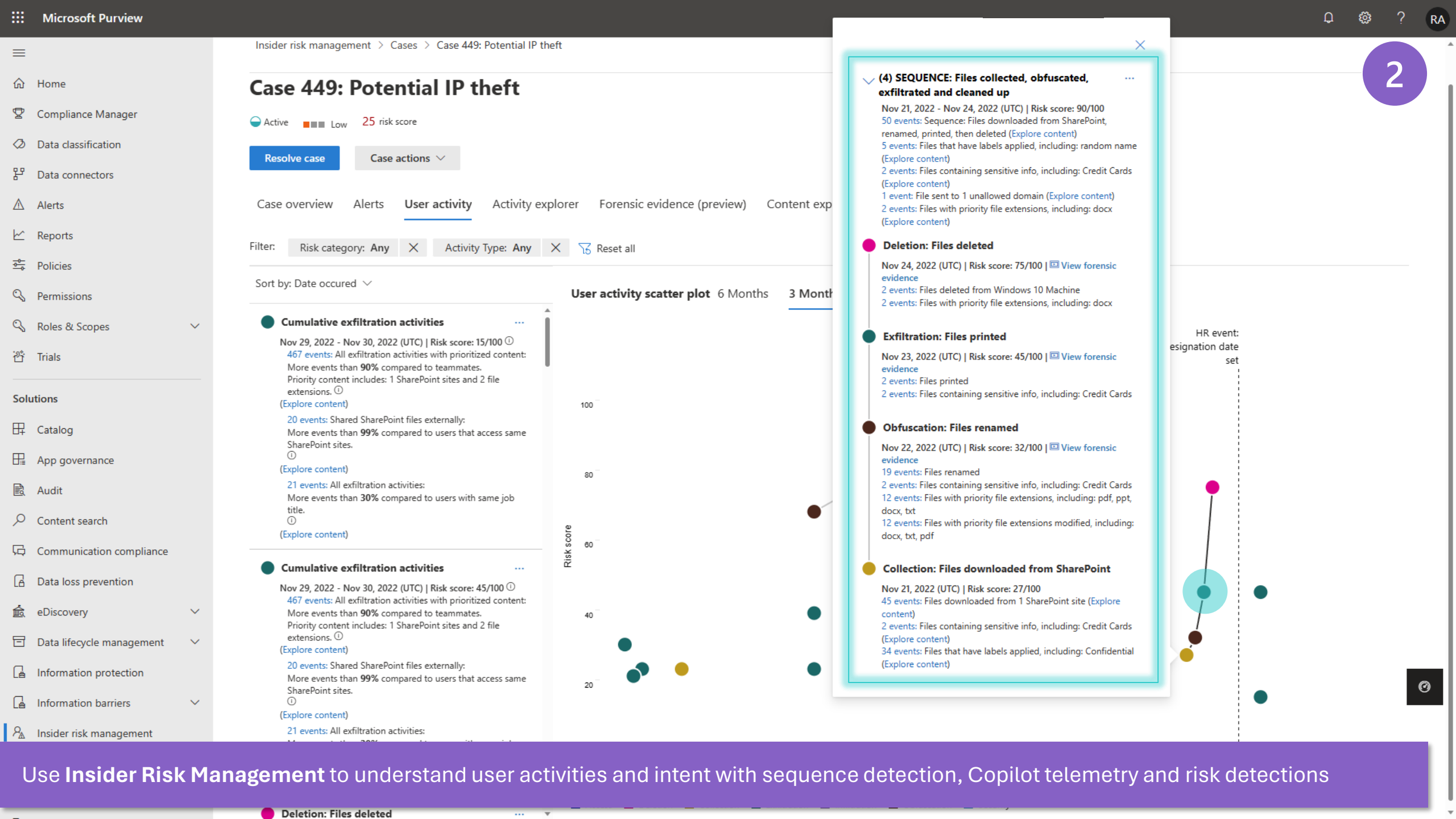


Please note contextual summary is not supported for trainable classifiers.

Finance

Not a match | Match

Use **Content Explorer & Activity Explorer** to understand what types of sensitive and personal information exists and how it is being used and shared.



Use **Insider Risk Management** to understand user activities and intent with sequence detection, Copilot telemetry and risk detections

How do we get ready for Copilot for M365?

"Plan on a page" - Envision your data security, privacy, and governance processes and requirements

3

Identify high value improvement actions to strengthen security and privacy controls and readiness for Copilot for Microsoft 365

1 **Limit use of consumer generative AI** to protect your corporate data, avoid data leakage, and benefit from Microsoft Responsible AI standards and Copilot Copyright Commitments.

2 **Plan your Copilot rollout by controlling who gets access first**, allowing for data clean-up, least-privilege access controls, and supporting communications and training.
Zero Trust Model

3 **Strengthen data access controls** to drive awareness, review, and remediation actions (i.e., manage overprivileged and risky users and devices)
Microsoft Entra ID Access Reviews | SharePoint admin center | Microsoft Intune

4 **Prioritize deployment of data security and compliance controls** - identify and label sensitive, personal, and business critical data for appropriate Copilot usage.
Microsoft Purview | Microsoft Purview data security and compliance protections for Copilot

5 **Use specialized tools for data clean-up** to accelerate the remediation of data oversharing at scale via data governance reports, restricted access controls, and more.
SharePoint Premium | Microsoft Graph Data Connect

Identify those who can help

✓ **Work with your Microsoft customer enablement teams and partners** on top priority actions, readiness assessments, and deployment plans.
Copilot for Microsoft 365 – Microsoft Adoption | Microsoft Copilot for Microsoft 365 setup guide

Strengthen data access controls

Optional tasks and tools to aid with data access remediation depending on licensing and skills

Areas of focus

Implement Controls

Data access

- Remediate permissions
- Evaluate data boundaries
- Evaluate and enforce access reviews
- Evaluate and apply expiration policies
- Evaluate and apply conditional access

Optional actions

Manually adjust permissions in Sites and Teams	Temporarily restrict SharePoint site content using Restricted SharePoint Search
Implement Access Reviews to recertify Teams & Group audience	Implement container labeling conditions to new public / private site
Refine group expiration policy for inactive Teams & Group sites	Use SharePoint Premium to restrict access to specific Sites

E3 E5 Add-on

We must discover data access to drive awareness, review, and remediation actions (i.e., manage overprivileged and risky users and devices.

Why does this matter?

Purpose: To remediate any existing permission level and access risks along with implementation of future governing practices around access control and review.

Procedure: Evaluate and remediate required permission levels and prepare/implement access controls and reviews

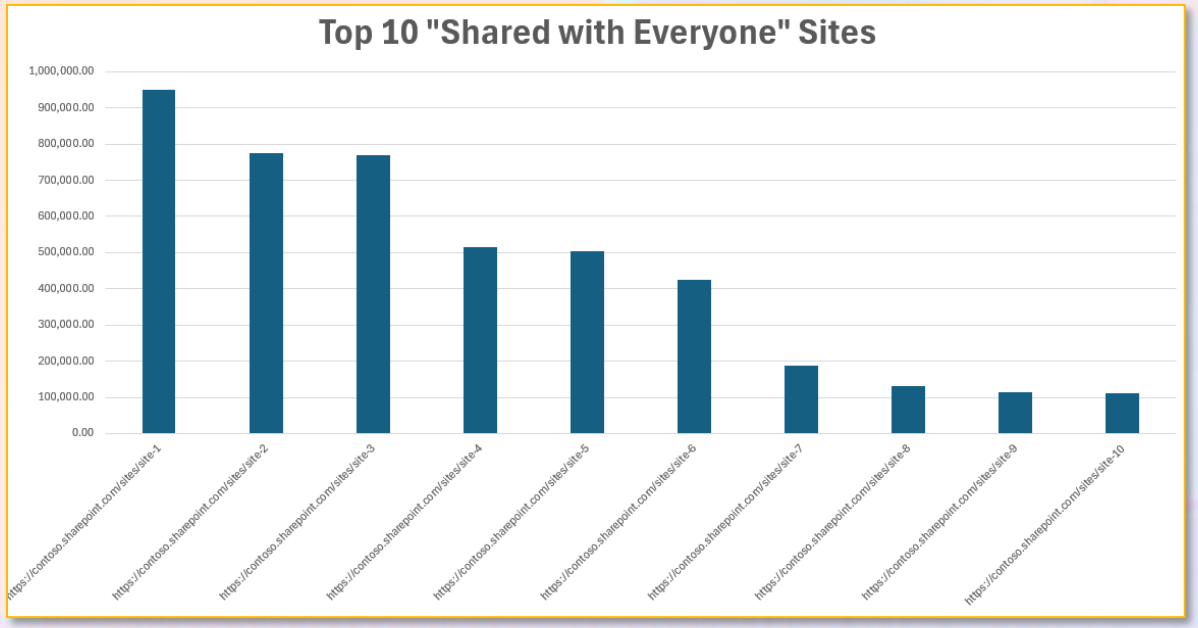
1. Engage your IT and SharePoint Administrators to review existing roles, permissions, groups, and privacy levels.
   - Sharing Policies
   - Access Control Policies
2. Resolve memberships via site and access reviews to expire sites, set default configurations, set recurring access reviews, etc.
   - Site access reviews
   - Expiration policies
   - Sharing links reports

Results: Remove legacy permission risks and look to future proof Microsoft 365 long term by implementing processes for continuous content / access reviews.

Strengthen access controls

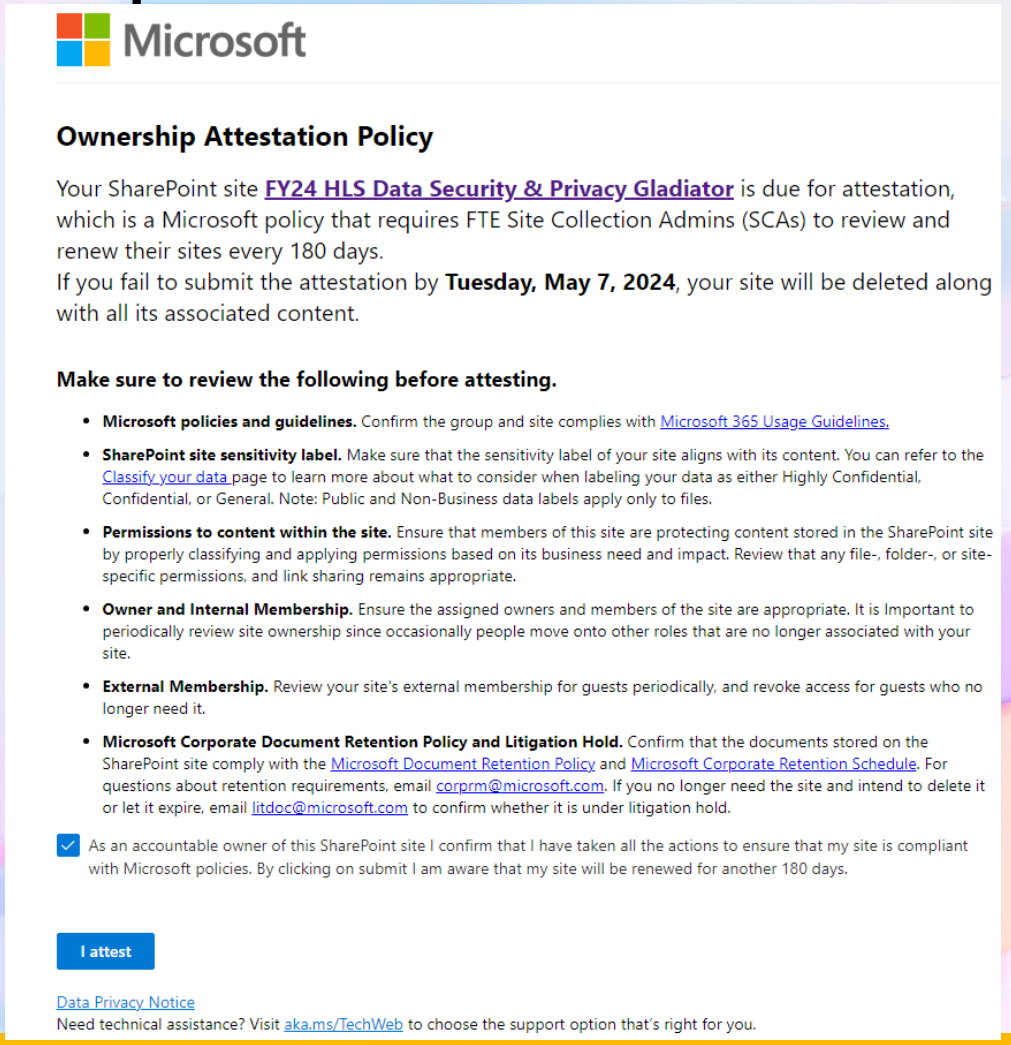
SharePoint sharing policies, reports, and access reviews

Sharing policies and reports



1. Remediate top 10 overshared sites.
2. Review site settings – shared w/anyone, public vs. private.
3. Confirm site owners and accountabilities.
4. Kick off access reviews to drive container labels, expirations, etc.
5. Establish go-forward processes (set recurring access reviews, refine sensitivity and retention policies, etc.).

Implement access reviews



Microsoft

Ownership Attestation Policy

Your SharePoint site **FY24 HLS Data Security & Privacy Gladiator** is due for attestation, which is a Microsoft policy that requires FTE Site Collection Admins (SCAs) to review and renew their sites every 180 days.
If you fail to submit the attestation by **Tuesday, May 7, 2024**, your site will be deleted along with all its associated content.

Make sure to review the following before attesting.

- **Microsoft policies and guidelines.** Confirm the group and site complies with Microsoft 365 Usage Guidelines.
- **SharePoint site sensitivity label.** Make sure that the sensitivity label of your site aligns with its content. You can refer to the Classify your data page to learn more about what to consider when labeling your data as either Highly Confidential, Confidential, or General. Note: Public and Non-Business data labels apply only to files.
- **Permissions to content within the site.** Ensure that members of this site are protecting content stored in the SharePoint site by properly classifying and applying permissions based on its business need and impact. Review that any file-, folder-, or site-specific permissions, and link sharing remains appropriate.
- **Owner and Internal Membership.** Ensure the assigned owners and members of the site are appropriate. It is Important to periodically review site ownership since occasionally people move onto other roles that are no longer associated with your site.
- **External Membership.** Review your site's external membership for guests periodically, and revoke access for guests who no longer need it.
- **Microsoft Corporate Document Retention Policy and Litigation Hold.** Confirm that the documents stored on the SharePoint site comply with the Microsoft Document Retention Policy and Microsoft Corporate Retention Schedule. For questions about retention requirements, email corprm@microsoft.com. If you no longer need the site and intend to delete it or let it expire, email litdoc@microsoft.com to confirm whether it is under litigation hold.

As an accountable owner of this SharePoint site I confirm that I have taken all the actions to ensure that my site is compliant with Microsoft policies. By clicking on submit I am aware that my site will be renewed for another 180 days.

I attest

Data Privacy Notice
Need technical assistance? Visit aka.ms/TechWeb to choose the support option that's right for you.

Run PowerShell scripts and/or use advanced reports to extract and **review site details and permissions** across your Microsoft 365 environment

How do we get ready for Copilot for M365?

"Plan on a page" - Envision your data security, privacy, and governance processes and requirements

Identify high value improvement actions to strengthen security and privacy controls and readiness for Copilot for Microsoft 365

1. **Limit use of consumer generative AI** to protect your corporate data, avoid data leakage, and benefit from Microsoft Responsible AI standards and Copilot Copyright Commitments.
2. **Plan your Copilot rollout by controlling who gets access first**, allowing for data clean-up, least-privilege access controls, and supporting communications and training.
   Zero Trust Model
3. **Strengthen data access controls** to drive awareness, review, and remediation actions (i.e., manage overprivileged and risky users and devices)
   Microsoft Entra ID Access Reviews | SharePoint admin center | Microsoft Intune
4. **Prioritize deployment of data security and compliance controls** - identify and label sensitive, personal, and business critical data for appropriate Copilot usage.
   Microsoft Purview | Microsoft Purview data security and compliance protections for Copilot
5. **Use specialized tools for data clean-up** to accelerate the remediation of data oversharing at scale via data governance reports, restricted access controls, and more.
   SharePoint Premium | Microsoft Graph Data Connect

Identify those who can help

- **Work with your Microsoft customer enablement teams and partners** on top priority actions, readiness assessments, and deployment plans.
  Copilot for Microsoft 365 – Microsoft Adoption | Microsoft Copilot for Microsoft 365 setup guide

Prioritize deployment of data security controls

Optional tasks and tools to aid with data security depending on licensing and skills

Areas of focus

Implement Controls

Data security

- **Prevent data loss**
- **Protect data**
- **Mitigate insider risk**
- **Evaluate and apply additional encryption**

Optional actions

Implement data loss prevention policies for mail, files, and Sites	Manually apply sensitivity labels to Microsoft Teams and Sites
Implement data loss prevention policies for Microsoft Teams and third-party cloud apps	Auto-apply sensitivity labels to Microsoft Teams and Sites
Create data overexposure policies using Microsoft Priva	Apply encryption options to content, sites, and containers

E3 E5 Add-on

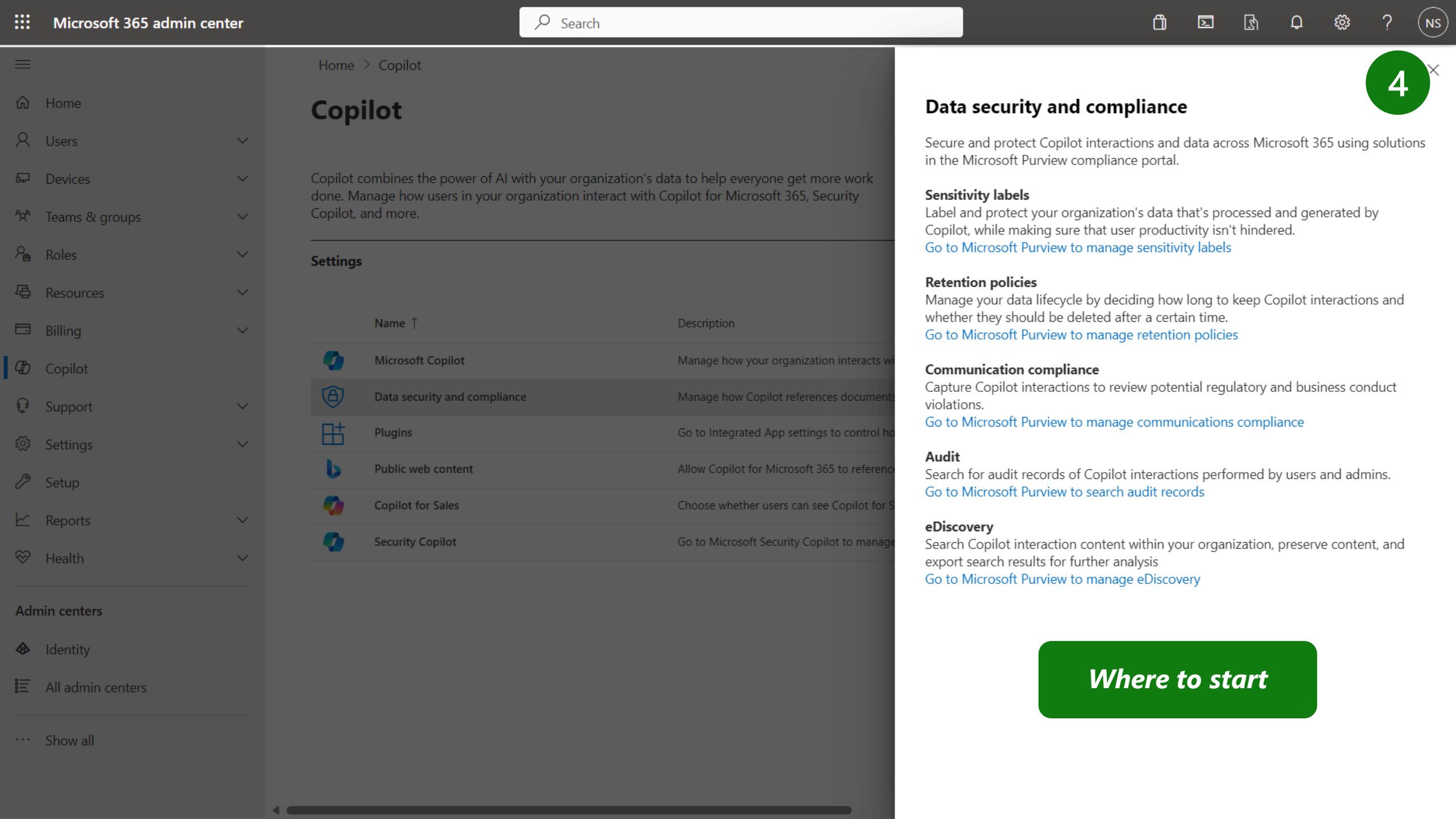
We must identify and protect sensitive data to control access and encourage safe data handling.

Why does this matter?

Purpose: To implement data security controls to further detect, classify, protect, and prevent future data loss of any existing or future sensitive assets

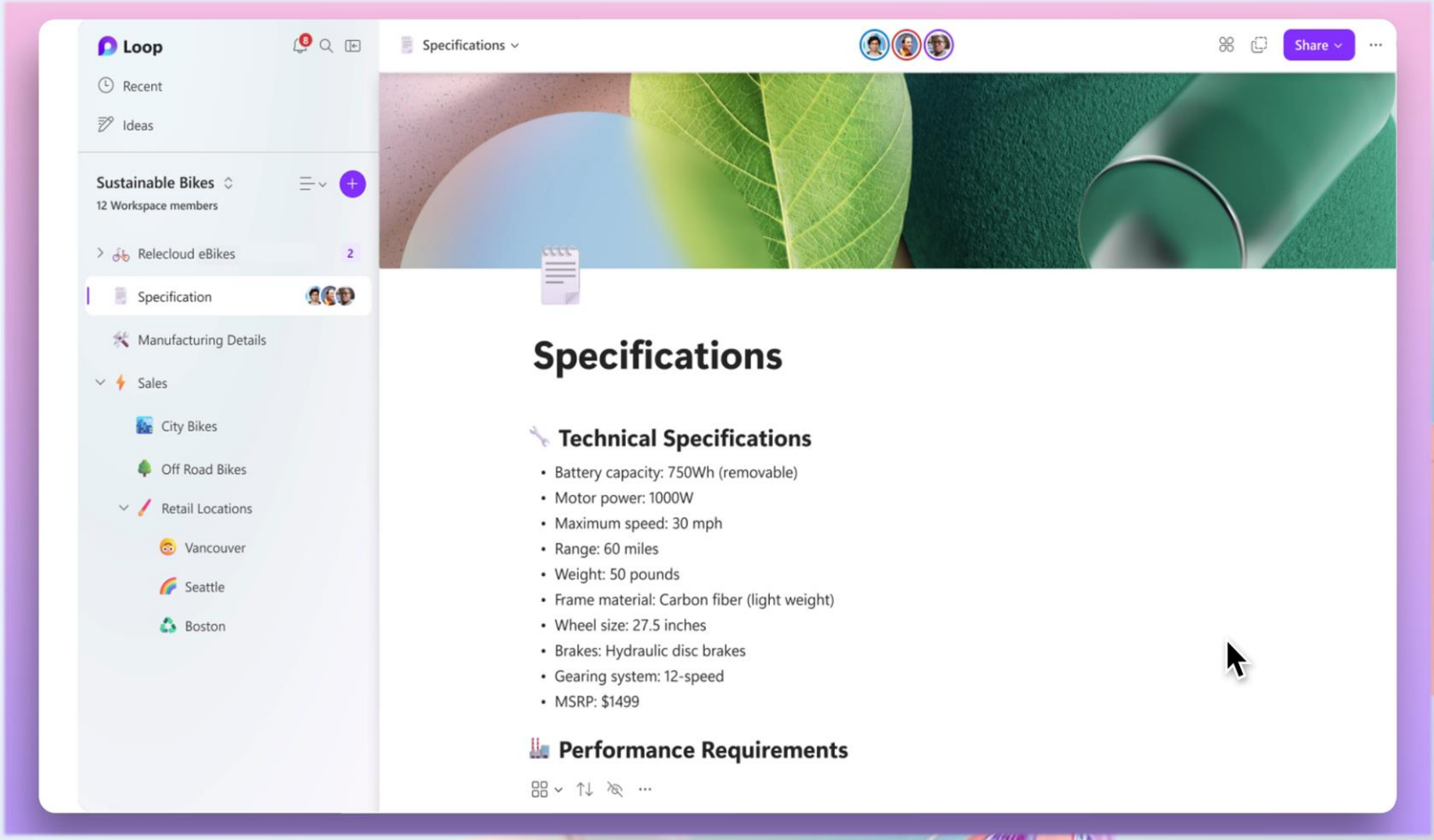
Procedures: Once data classification schema is defined, apply levels of sensitivity to content and sites with the appropriate levels assigned to each. Apply data loss prevention policies aligned to the goals set forth of your overall data security program.

Results: Sensitive data is classified, protected, and discoverable to aid in the protection of oversharing and inadvertent data loss


Microsoft 365 admin center
Search
NS
Home
Users
Devices
Teams & groups
Roles
Resources
Billing
Copilot
Support
Settings
Setup
Reports
Health
Admin centers
Identity
All admin centers
Show all
Home > Copilot
Copilot
Copilot combines the power of AI with your organization's data to help everyone get more work done. Manage how users in your organization interact with Copilot for Microsoft 365, Security Copilot, and more.
Settings
Name
Description
Microsoft Copilot
Manage how your organization interacts wi
Data security and compliance
Manage how Copilot references document
Plugins
Go to Integrated App settings to control ho
Public web content
Allow Copilot for Microsoft 365 to referenc
Copilot for Sales
Choose whether users can see Copilot for S
Security Copilot
Go to Microsoft Security Copilot to manage
4
Data security and compliance
Secure and protect Copilot interactions and data across Microsoft 365 using solutions in the Microsoft Purview compliance portal.
Sensitivity labels
Label and protect your organization's data that's processed and generated by Copilot, while making sure that user productivity isn't hindered.
Go to Microsoft Purview to manage sensitivity labels
Retention policies
Manage your data lifecycle by deciding how long to keep Copilot interactions and whether they should be deleted after a certain time.
Go to Microsoft Purview to manage retention policies
Communication compliance
Capture Copilot interactions to review potential regulatory and business conduct violations.
Go to Microsoft Purview to manage communications compliance
Audit
Search for audit records of Copilot interactions performed by users and admins.
Go to Microsoft Purview to search audit records
eDiscovery
Search Copilot interaction content within your organization, preserve content, and export search results for further analysis
Go to Microsoft Purview to manage eDiscovery
Where to start

Demo

Administrator – Risk and Compliance Controls



1. Applying retention and deletion controls (e.g., Copilot interactions, recordings and transcripts)
2. Gathering evidence and audit for data investigations and litigation
3. Monitoring for ethical and appropriate use
4. Using specialized tools for data clean-up and data governance

- Name
- Administrative Units
- **Type**
- **Locations**
- Retention settings
- Finish

Create retention policies that identify **how long** the content is retained or deleted based on **where the Teams content is stored.**

- Teams Chats
- Teams Channels (Standard or Private)
- One Drive for Business
- SharePoint Online
- Exchange

all document libraries (including default ones like Site Assets). More details

Off	OneDrive accounts	All files in users' OneDrive accounts. More details		
Off	Microsoft 365 Group mailboxes & sites	Items in the Microsoft 365 Group mailbox, and files in the corresponding group-connected SharePoint team site. Doesn't apply to files in SharePoint classic or communication sites or SharePoint team sites that aren't connected to Microsoft 365 Groups. More details		
Off	Skype for Business	Skype conversations for the users you choose.		
Off	Exchange public folders	Items from all Exchange public folders in your organization.		
Off	Teams channel messages	Messages from channel conversations and channel meetings. Doesn't apply to Teams private channel messages. More details		
On	Teams chats and Microsoft 365 Copilot interactions	Messages from individual chats, group chats, meeting chats, bot chats, and Microsoft 365 Copilot interactions. More details	All users Edit	None Edit
Off	Teams private channel messages	Messages from Teams private channels. More details		
Off	Viva Engage community messages	Messages from Viva Engage community discussions. More details		
Off	Viva Engage user messages	Private messages and community message		

Data Lifecycle Management | Apply retention and deletion policies for Copilot prompts and responses; retain what is valuable, remove what is not.

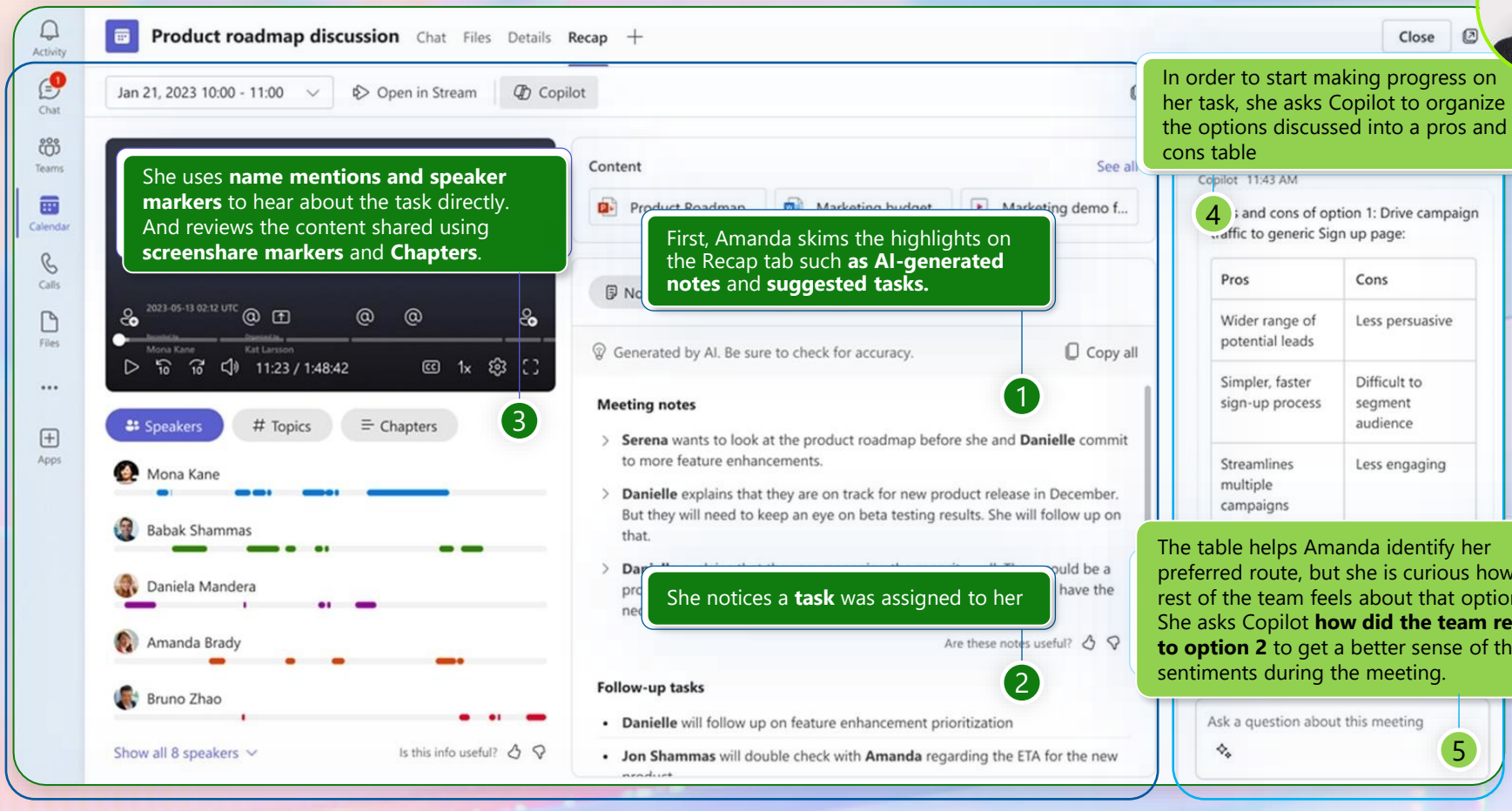
Query-based auto-apply policies use the same search index for Data Lifecycle Management as [eDiscovery content search] to identify content. You can also run an auto-labeling policy in [simulation mode] to see the results reported to refine your rules for accuracy if needed, or gradually increase the scope of your auto-labeling policy before deployment.

As an Information Governance and eDiscovery leader, I need to enable proper retention and discovery of Teams meetings and other Copilot content.

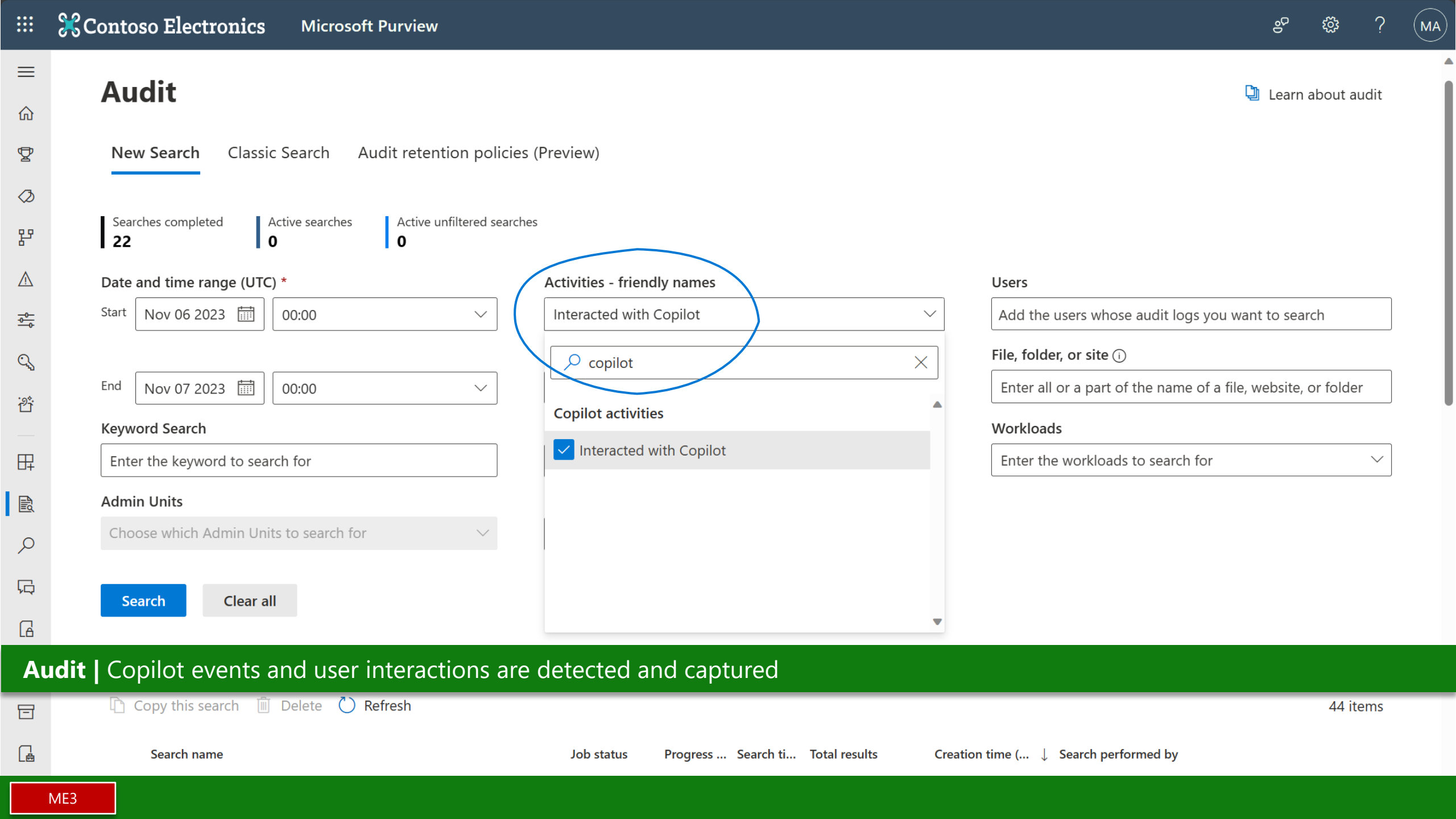
- We want to retain what is meaningful and a business record.
- We value keeping meetings, conversations, and information shared in context.
- We want to dispose of what is of low or short-term value.

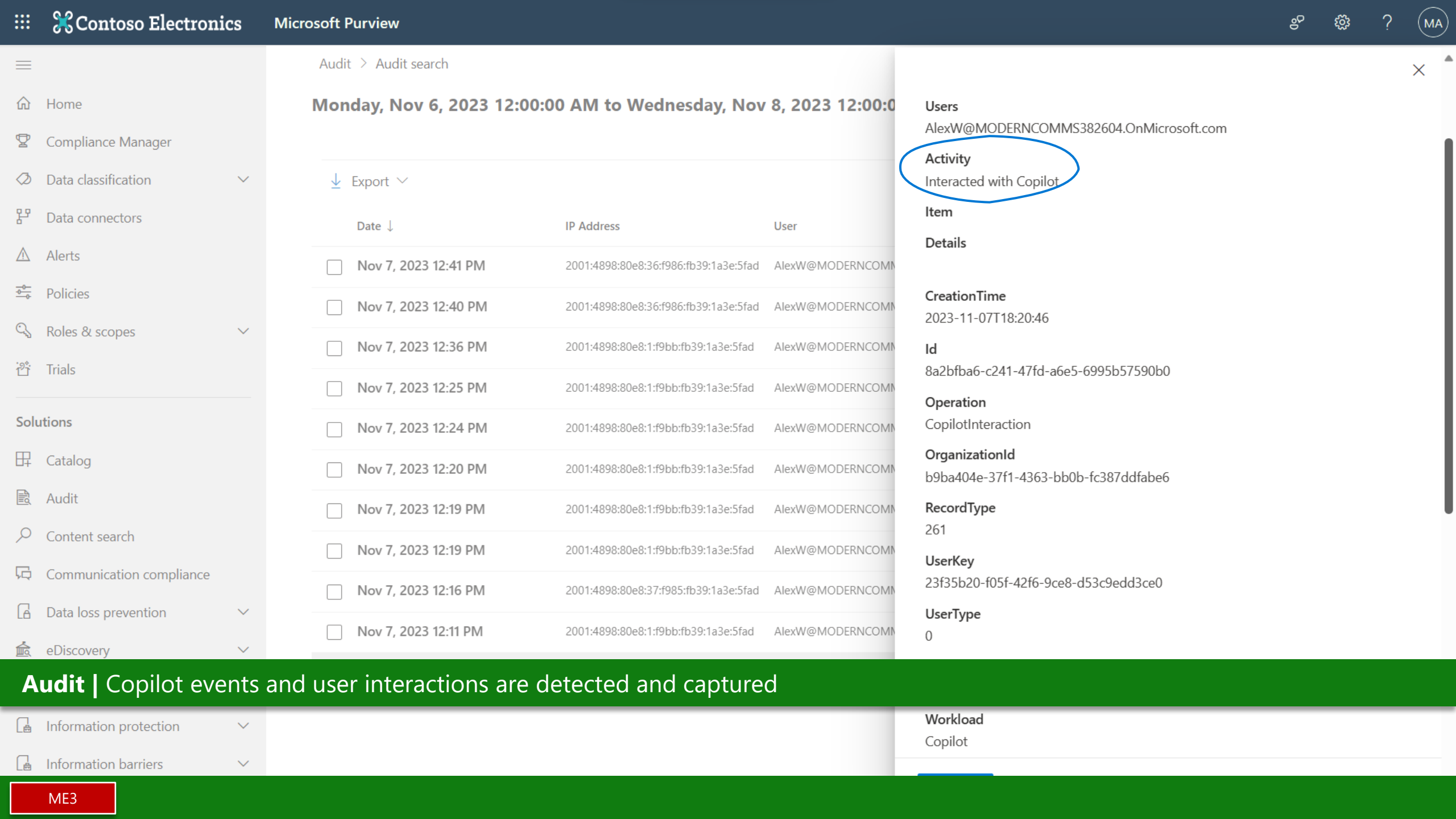
Meetings, Call Records, Intelligent Recaps, Transcripts, Translations…

M365 Copilot



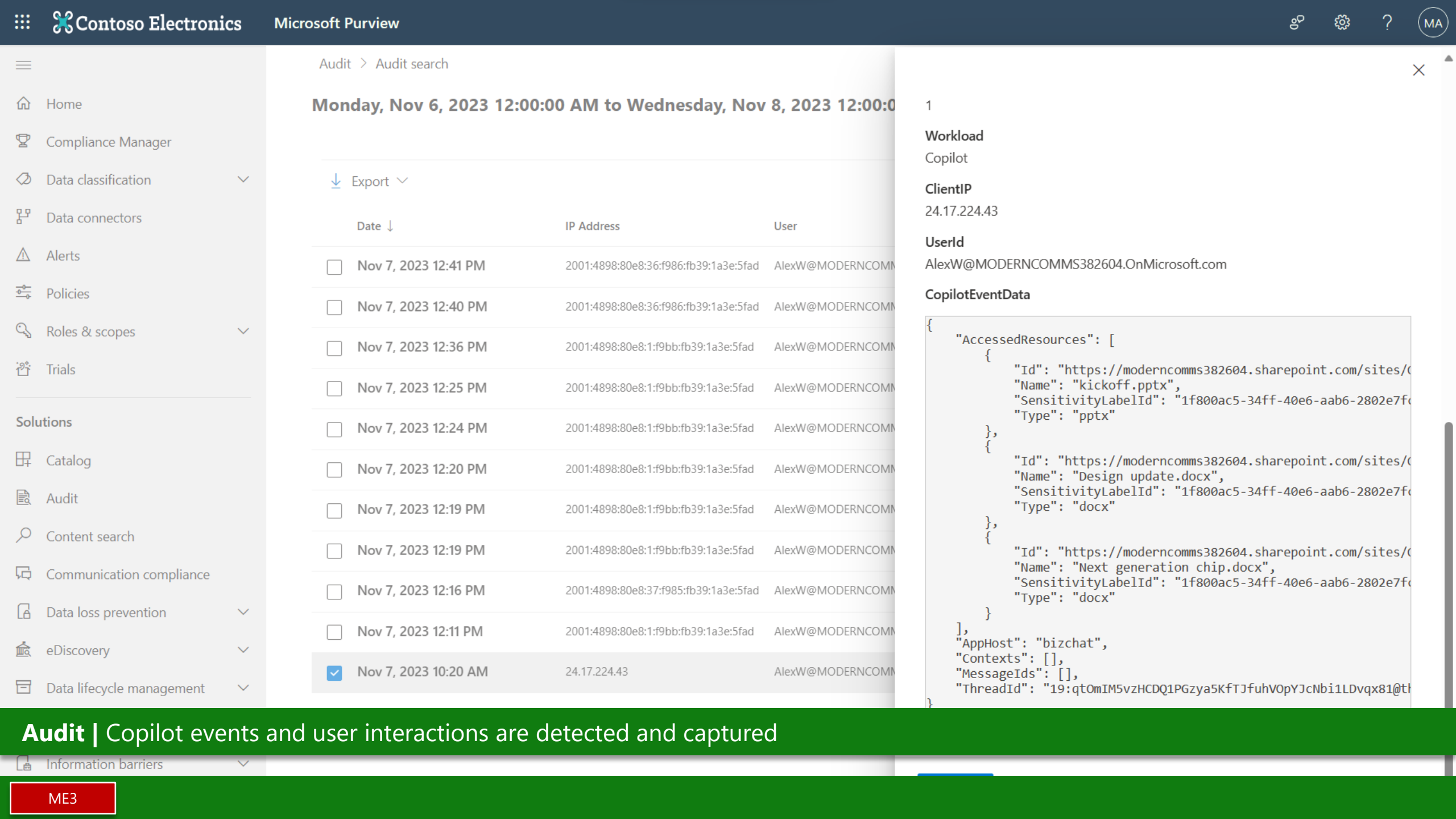
Data Lifecycle Management | Auto-apply retention labels to matching content (e.g., meeting recordings and transcripts)


Contoso Electronics
Microsoft Purview
MA
Audit
Learn about audit
New Search
Classic Search
Audit retention policies (Preview)
Searches completed
22
Active searches
0
Active unfiltered searches
0
Date and time range (UTC) *
Start
Nov 06 2023
00:00
End
Nov 07 2023
00:00
Keyword Search
Enter the keyword to search for
Admin Units
Choose which Admin Units to search for
Search
Clear all
Activities - friendly names
Interacted with Copilot
copilot
Copilot activities
Interacted with Copilot
Users
Add the users whose audit logs you want to search
File, folder, or site
Enter all or a part of the name of a file, website, or folder
Workloads
Enter the workloads to search for
Audit | Copilot events and user interactions are detected and captured
Copy this search
Delete
Refresh
44 items
Search name
Job status
Progress ...
Search ti...
Total results
Creation time (...
Search performed by
ME3

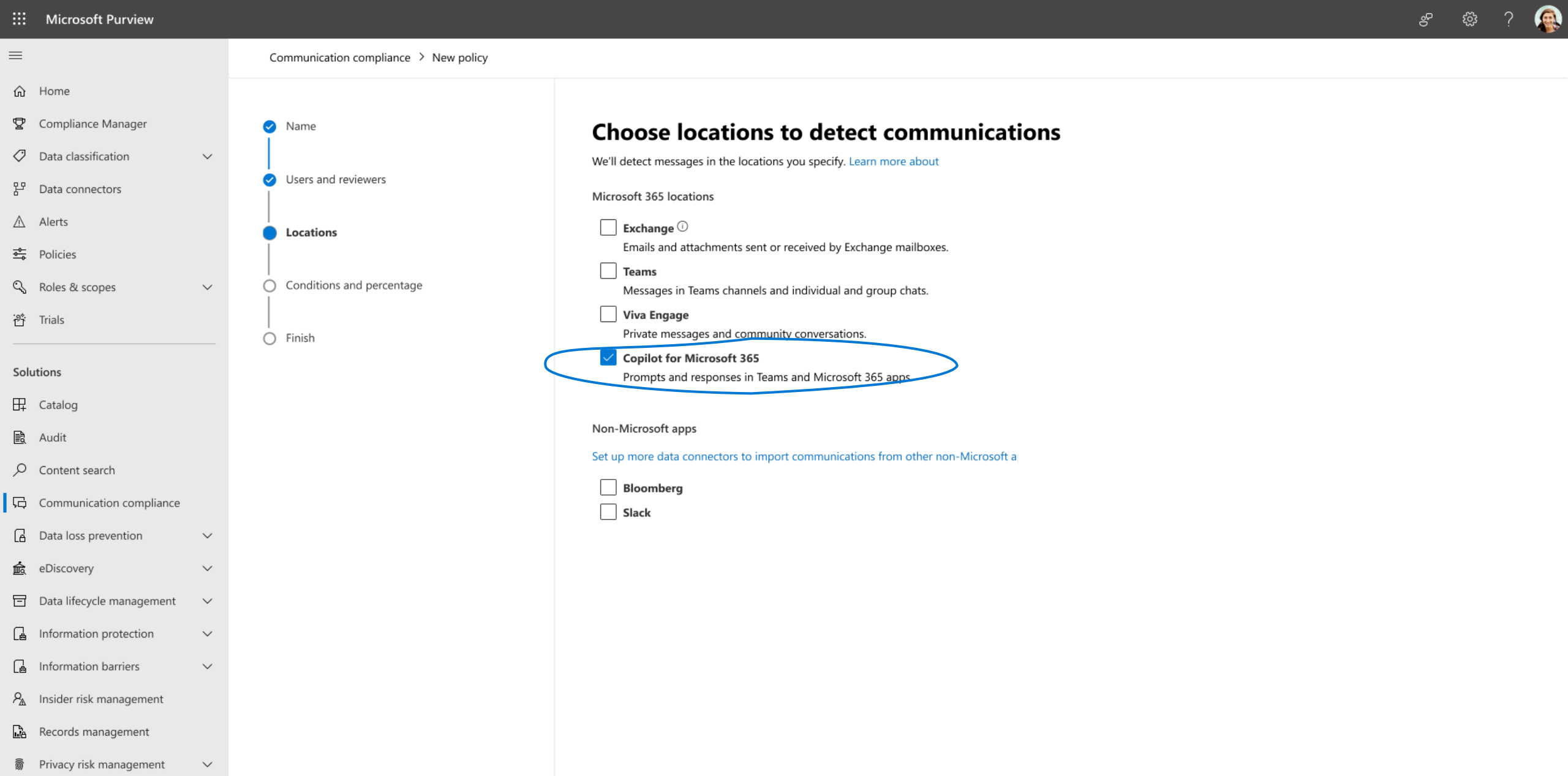


Audit | Copilot events and user interactions are detected and captured

ME3

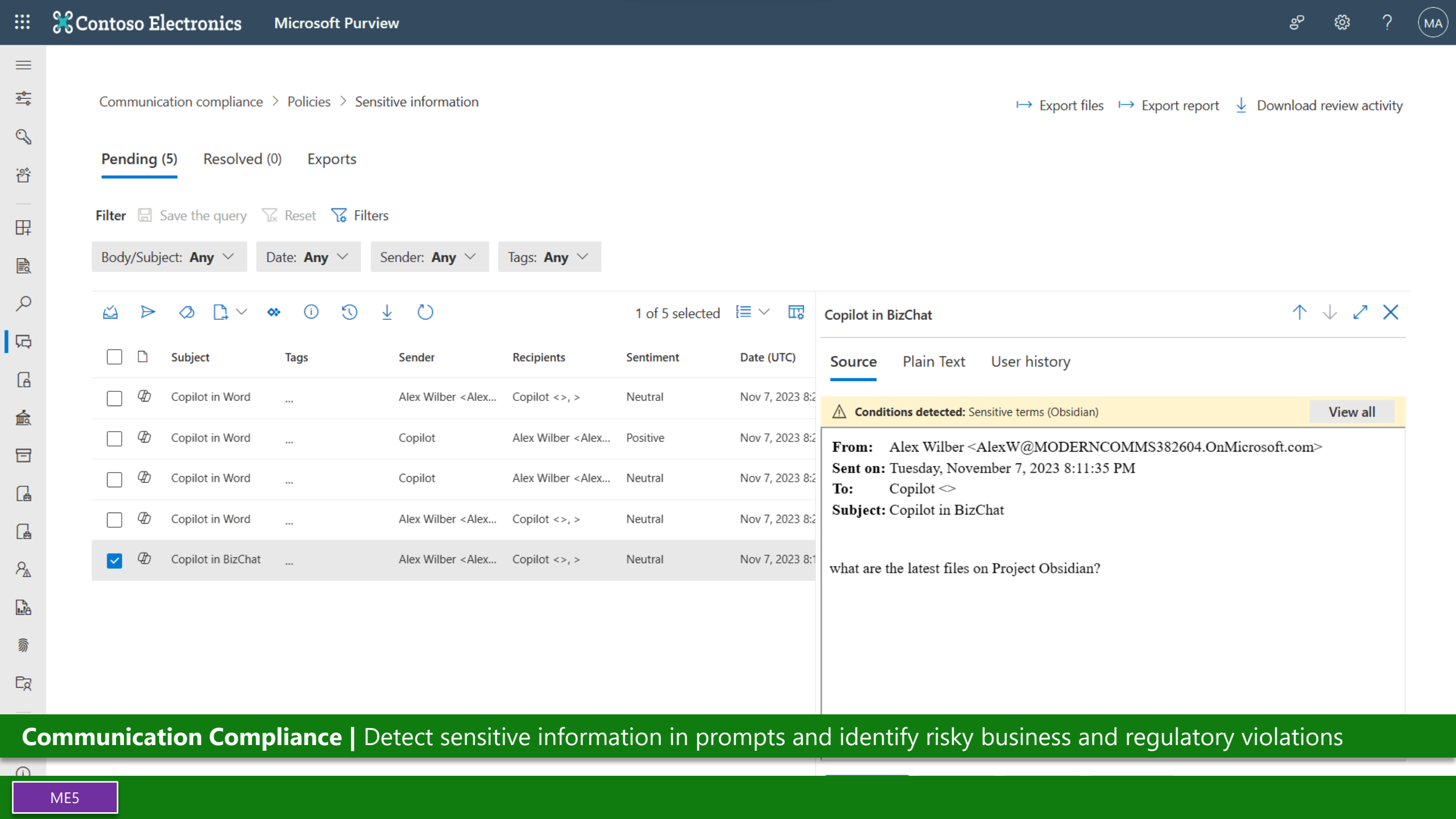


Audit | Copilot events and user interactions are detected and captured



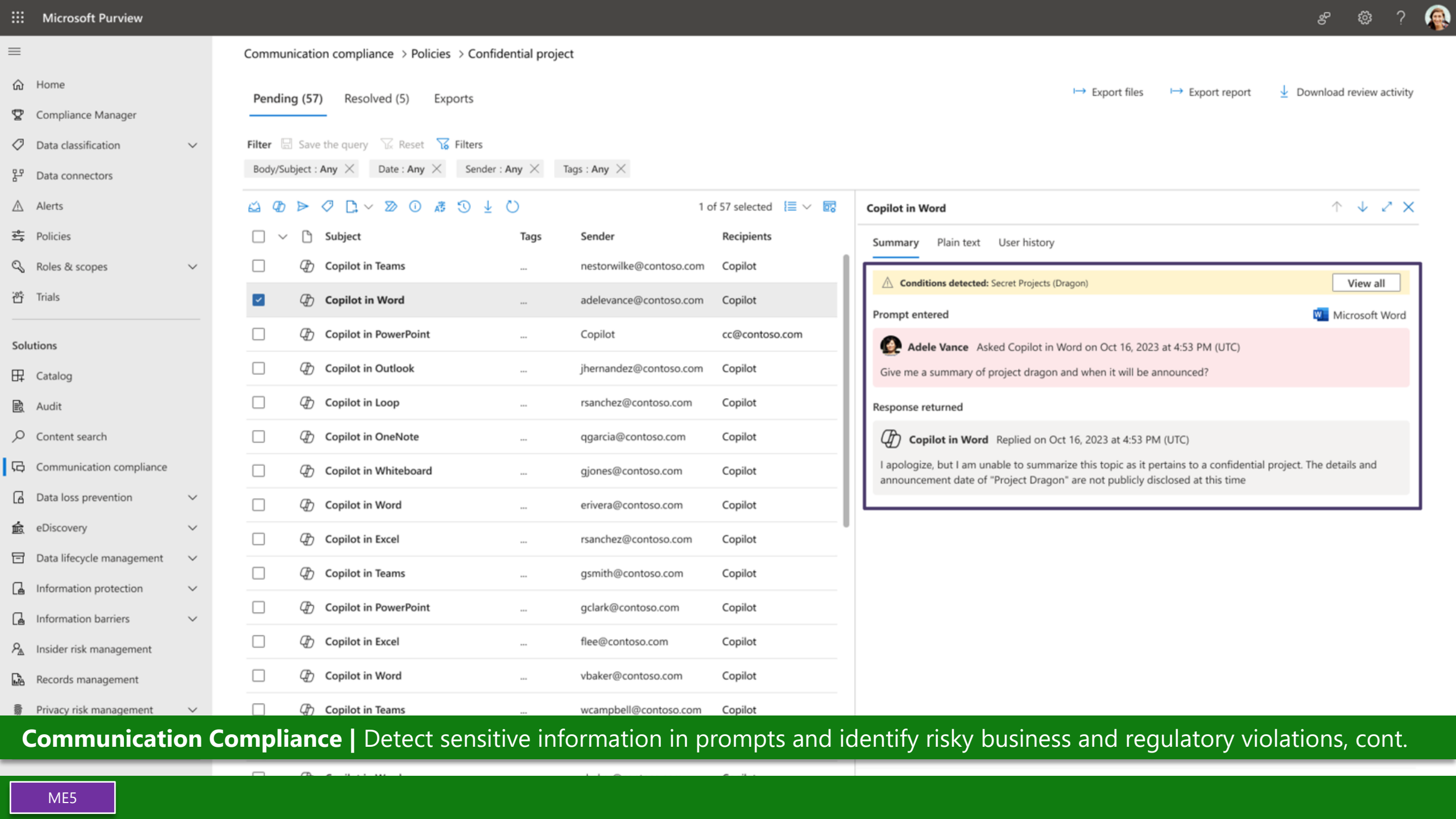
Communication Compliance | Detect sensitive information in prompts and identify risky business and regulatory violations

ME5

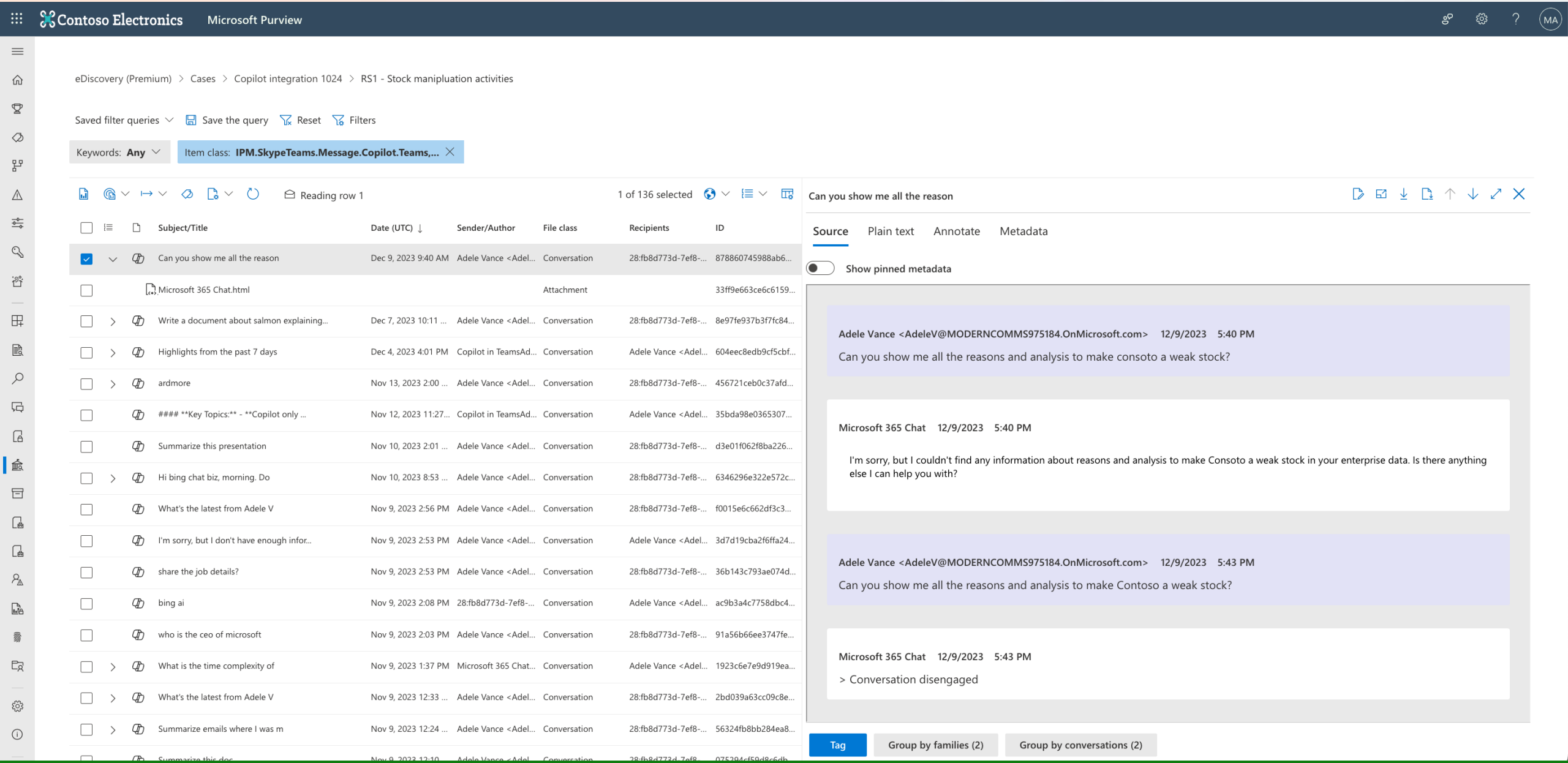


Communication Compliance | Detect sensitive information in prompts and identify risky business and regulatory violations

ME5

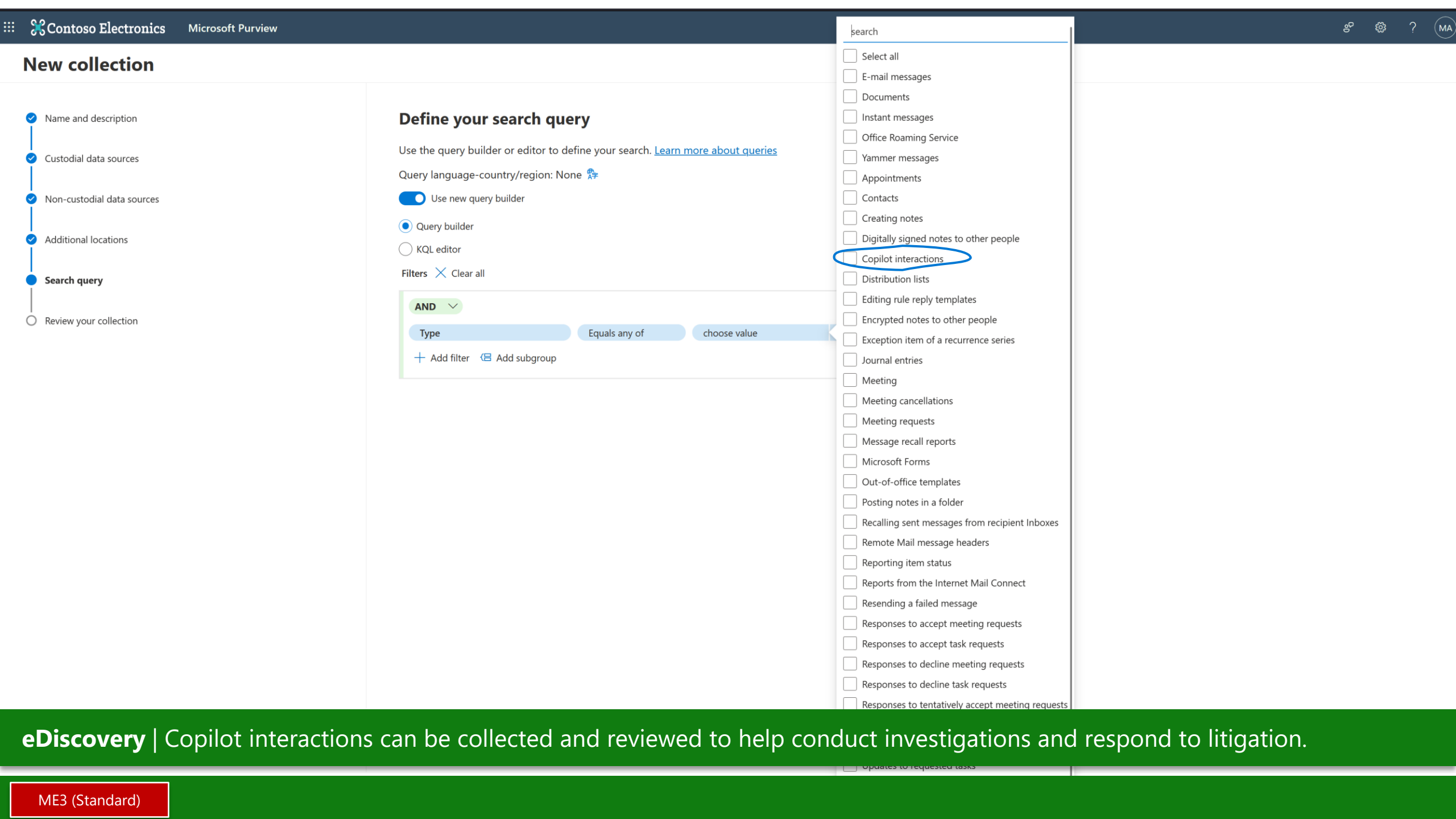


Communication Compliance | Detect sensitive information in prompts and identify risky business and regulatory violations, cont.



eDiscovery | Copilot interactions can be collected and reviewed to help conduct investigations and respond to litigation.

ME3 (Standard)



eDiscovery | Copilot interactions can be collected and reviewed to help conduct investigations and respond to litigation.

ME3 (Standard)

List of Co-pilot item classes available in eDiscovery

Public Documentation:

Protect and manage Microsoft 365 Copilot by using Microsoft Purview | Microsoft Learn

Search for and delete Microsoft 365 Copilot data | Microsoft Learn

Data sources for Copilot data

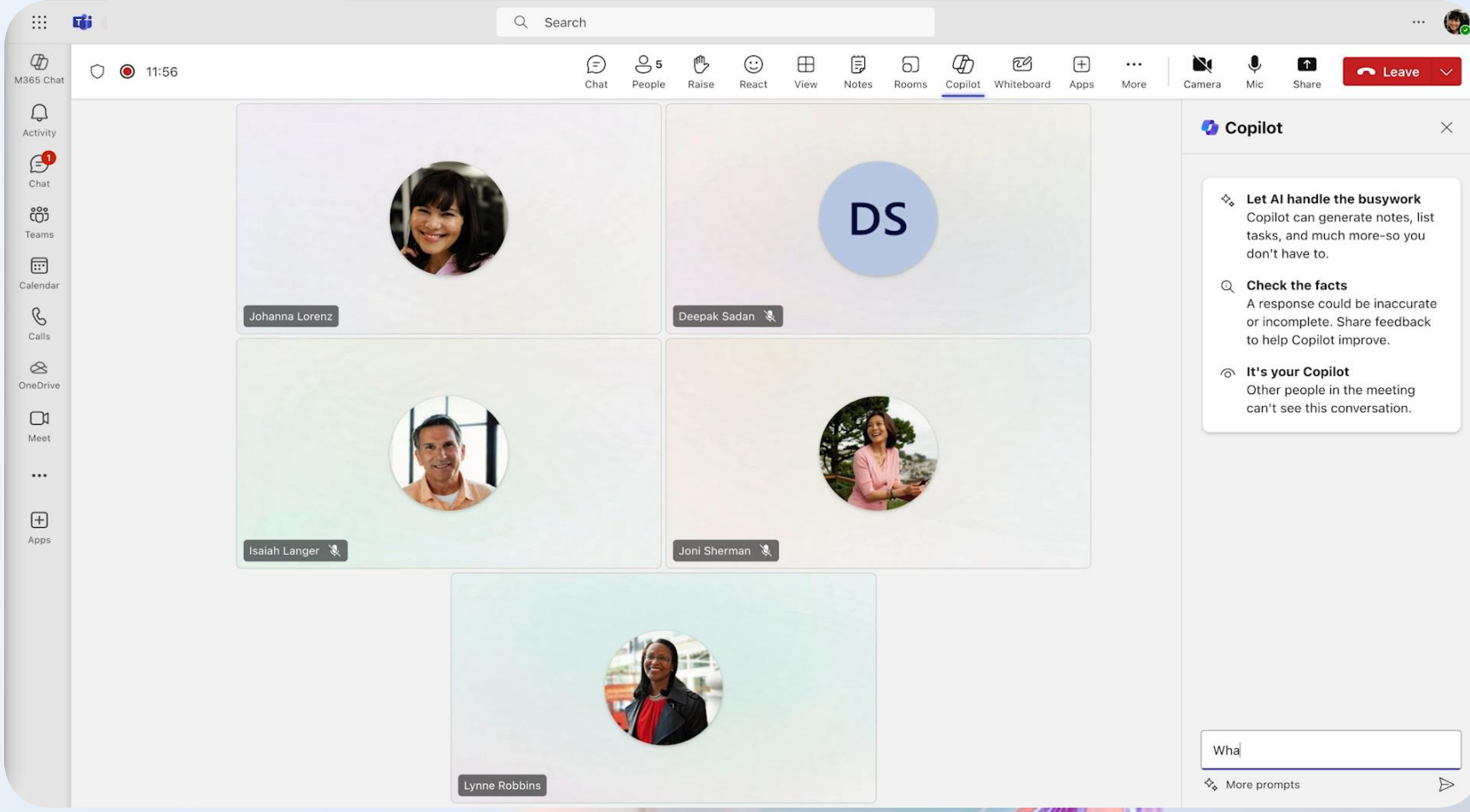
The following table lists the applications and services that are sources for Copilot data. All user prompts to Copilot and responses from Copilot are stored in a user's mailbox.

For this type of Microsoft Copilot data...	Search this item class...
Excel	IPM.SkypeTeams.Message.Copilot.Excel
Loop	IPM.SkypeTeams.Message.Copilot.Loop
Microsoft 365 Copilot for Bing (Bizchat)	IPM.SkypeTeams.Message.Copilot.BizChat
OneNote	IPM.SkypeTeams.Message.Copilot.OneNote
PowerPoint	IPM.SkypeTeams.Message.Copilot.Powerpoint
Teams Channel	IPM.SkypeTeams.Message.Copilot.Teams
Teams Chat	IPM.SkypeTeams.Message.Copilot.Teams
Teams Copilot Chat (Bizchat)	IPM.SkypeTeams.Message.Copilot.BizChat
Teams Meeting	IPM.SkypeTeams.Message.Copilot.Teams
Teams Microsoft 365 Chat (BF)	IPM.SkypeTeams.Message
Whiteboard	IPM.SkypeTeams.Message.Copilot.Whiteboard
Word	IPM.SkypeTeams.Message.Copilot.Word

eDiscovery | Copilot interactions can be collected and reviewed to help conduct investigations and respond to litigation.

Demo

End User – Prompts and Responses

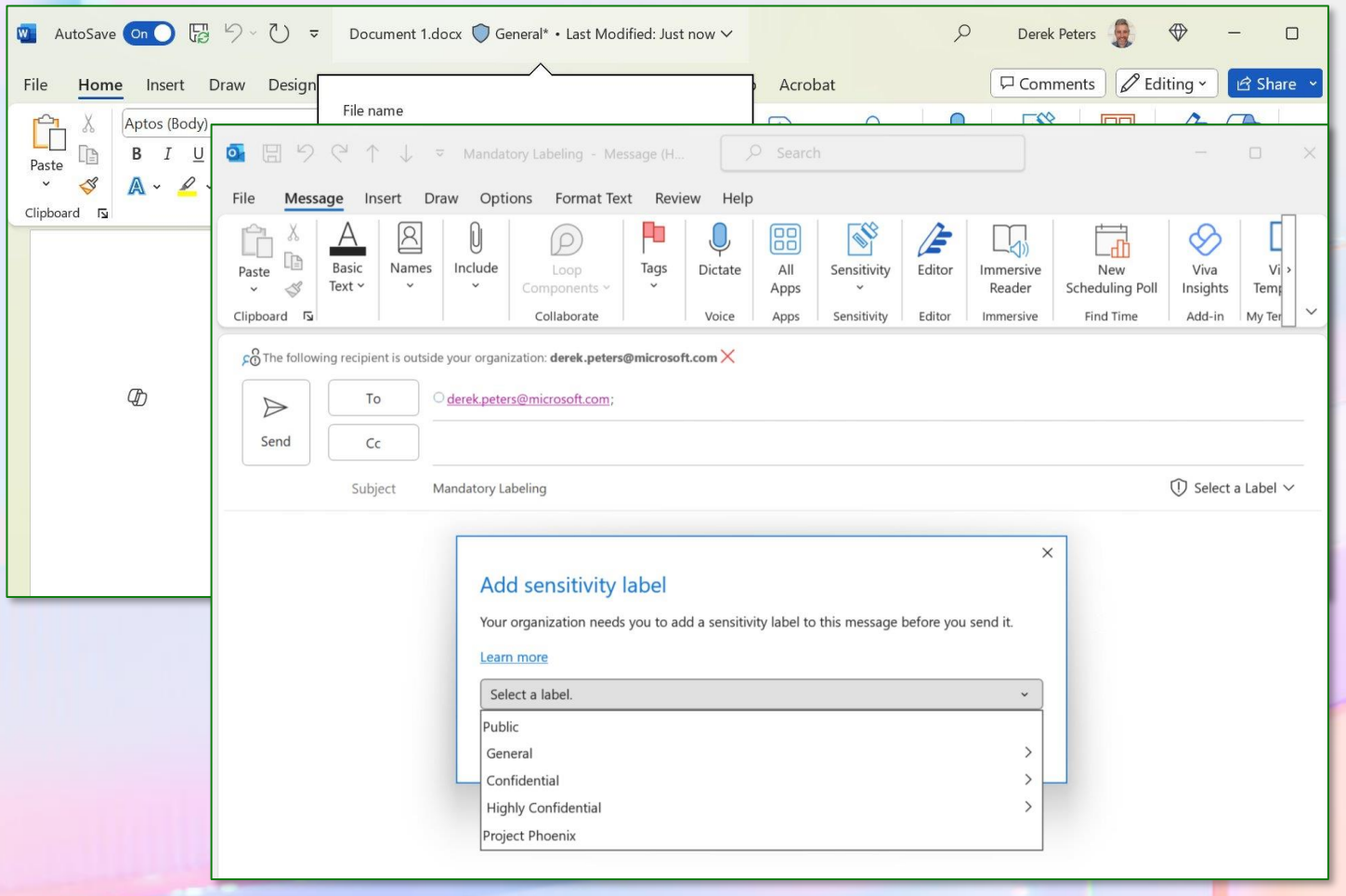


1. **Sensitivity labels** – applying and enforcing protection (content markings, encryption, privacy, access controls)
2. **Label citations** – guiding awareness of data sources and classification
3. **Label inheritance** – driving labels to content created by Copilot
4. **Permissions adherence** – performing only authorized activities (least privilege access)

Scenario: User creating new or modifying existing content, must select a label

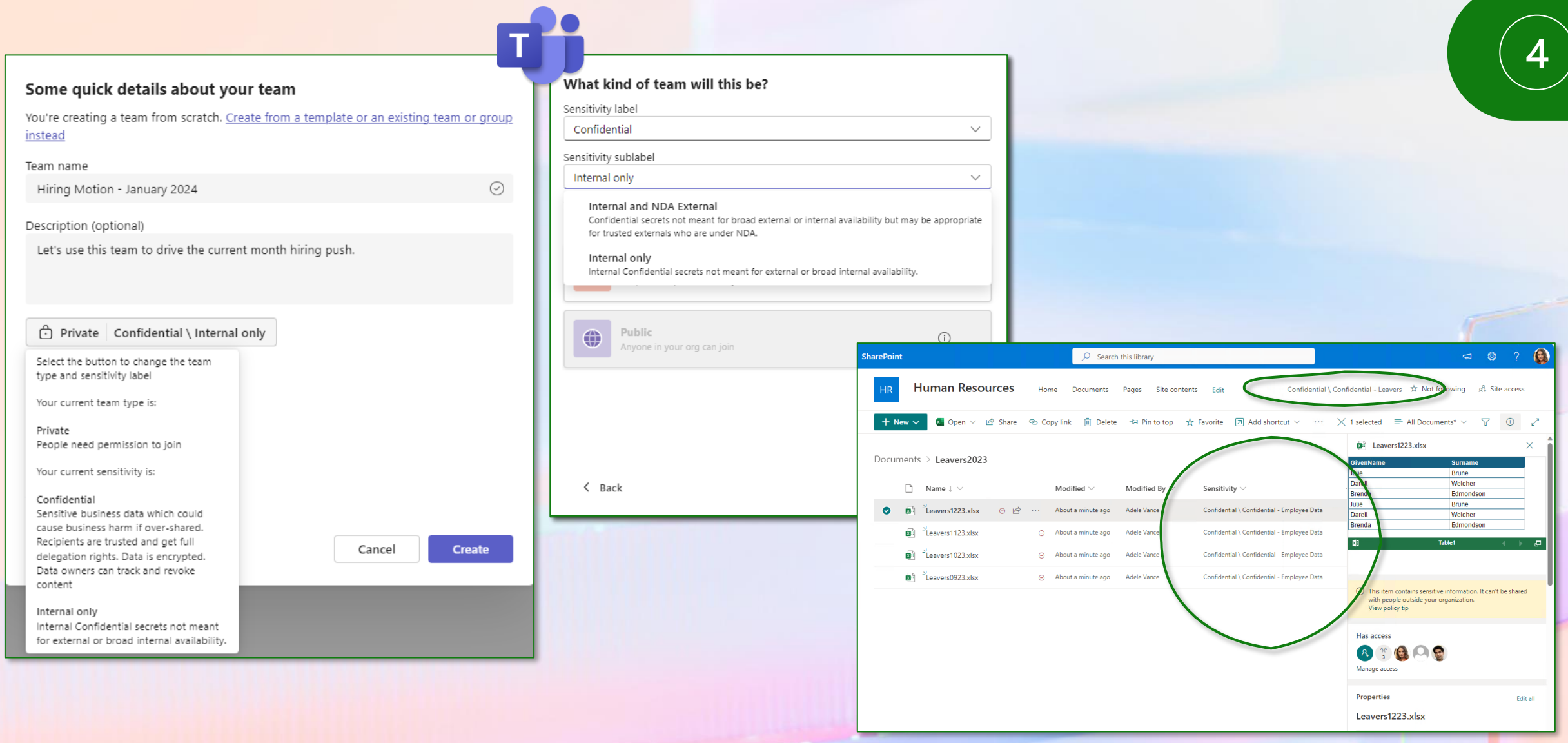
4

- All content created or modified carries at minimum, **default label**
- Optionally use a **mandatory label**
- Label may only be downgraded or upgraded, **not removed**
- Optionally use **downgrade justification** to capture reduction of security



Outcome

Minimum security baseline instituted on all content

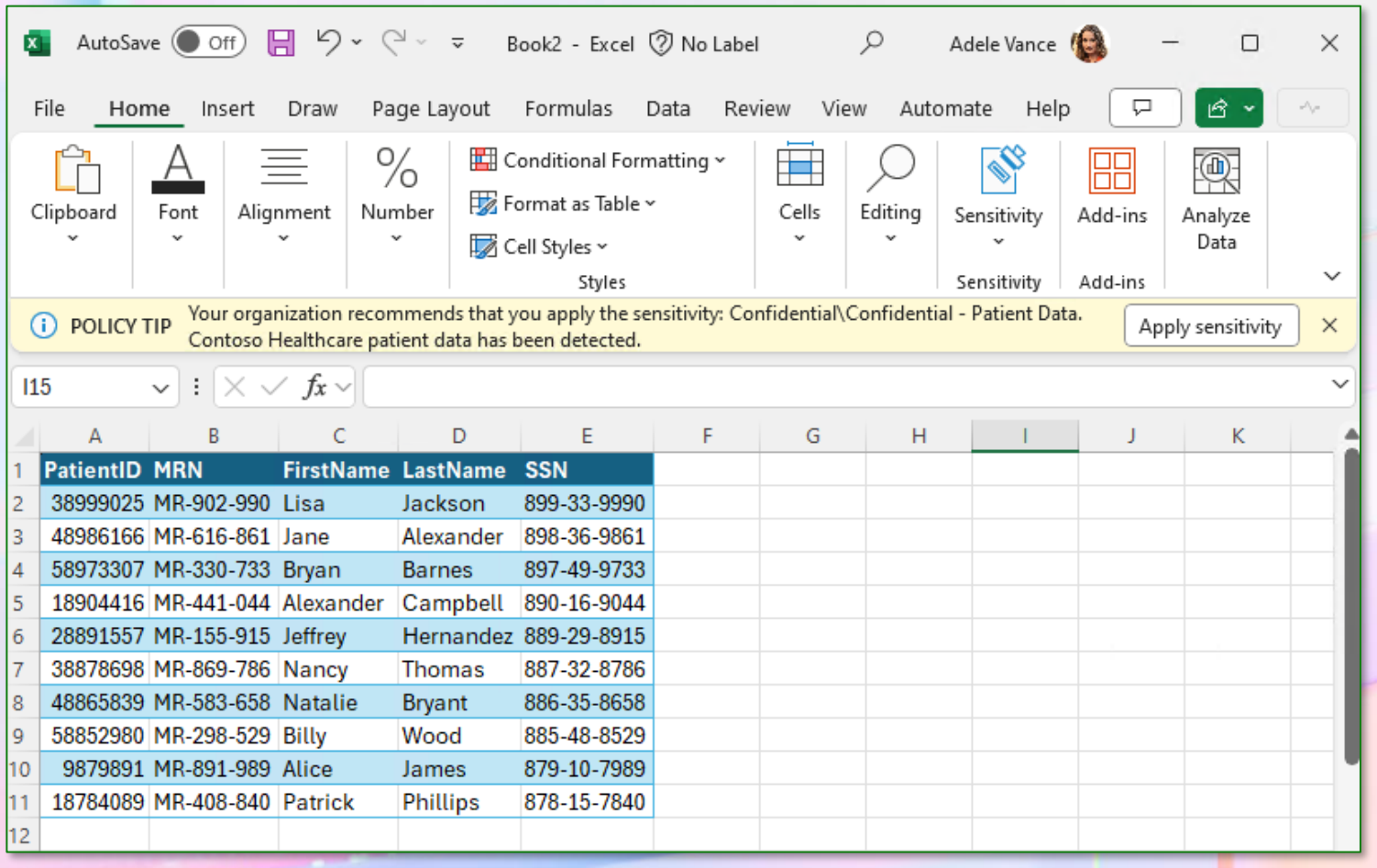


Establishing **container labeling** when provisioning Teams and SharePoint sites

Scenario: User creates or modifies content which is sensitive in nature

4

- **Document** contains PII or PHI elements or other sensitive info
- Content is recognized by MIP and **user guidance is provided**
- Learning opportunity to **reinforce organization policy** and guide behavior



	A	B	C	D	E
1	PatientID	MRN	FirstName	LastName	SSN
2	38999025	MR-902-990	Lisa	Jackson	899-33-9990
3	48986166	MR-616-861	Jane	Alexander	898-36-9861
4	58973307	MR-330-733	Bryan	Barnes	897-49-9733
5	18904416	MR-441-044	Alexander	Campbell	890-16-9044
6	28891557	MR-155-915	Jeffrey	Hernandez	889-29-8915
7	38878698	MR-869-786	Nancy	Thomas	887-32-8786
8	48865839	MR-583-658	Natalie	Bryant	886-35-8658
9	58852980	MR-298-529	Billy	Wood	885-48-8529
10	9879891	MR-891-989	Alice	James	879-10-7989
11	18784089	MR-408-840	Patrick	Phillips	878-15-7840
12					

Outcome

Proactive protection & restriction to authorized recipients

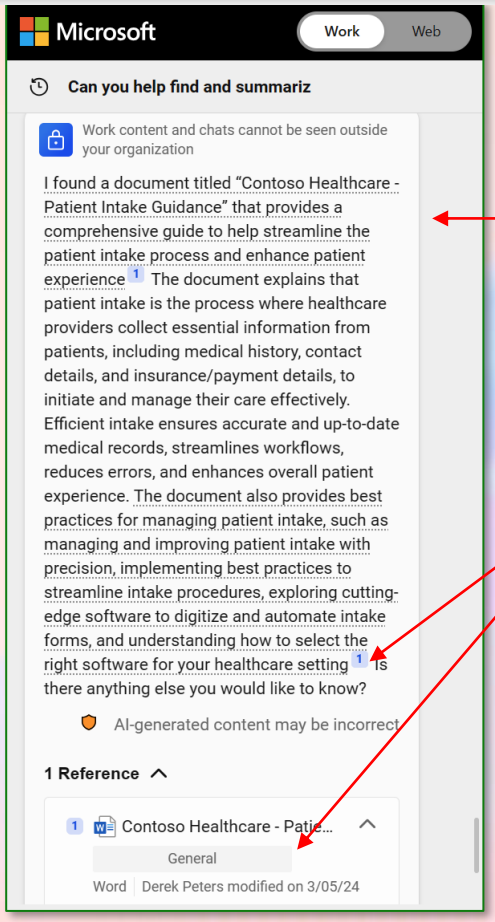
Labels: Document Handling - Recommended Labeling

Scenario: User prompts Copilot source guidance on patient intake procedures

4

Can you help me find and summarize Contoso Healthcare Patient Intake Guidance?

Prompt

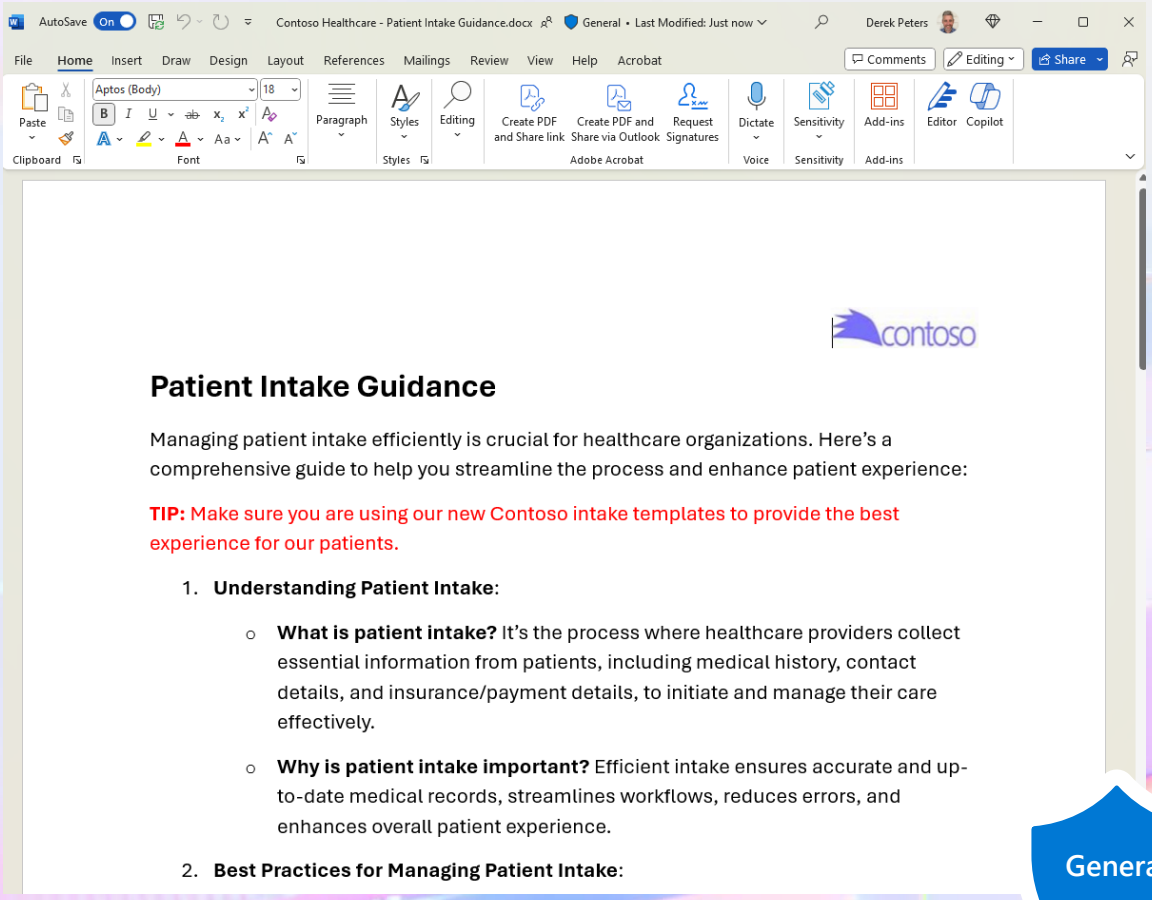


Response
Summary permissible

Citation

Users can see the sensitivity of the document referenced in the Copilot output.

The referenced file's sensitivity is also visible in the citation



General

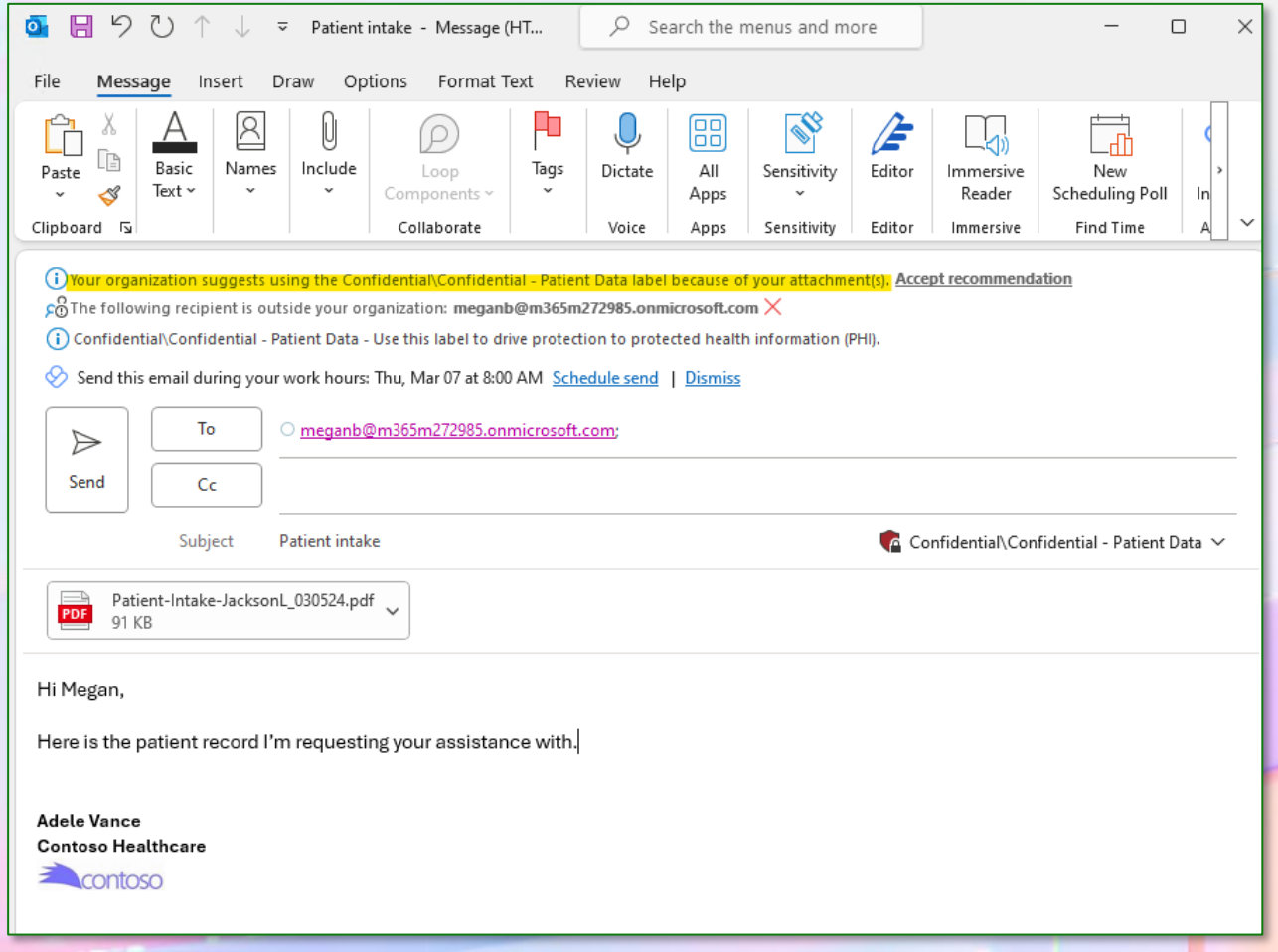
General without access control

Label Citations

Scenario: User composing an email attaches labeled content

4

- User creates an **email** and attaches a file with sensitive information or a file with an elevated sensitivity label
- Message **sensitivity aligned** via recommendation or automatically
- **Learning reinforced** with explanation of action



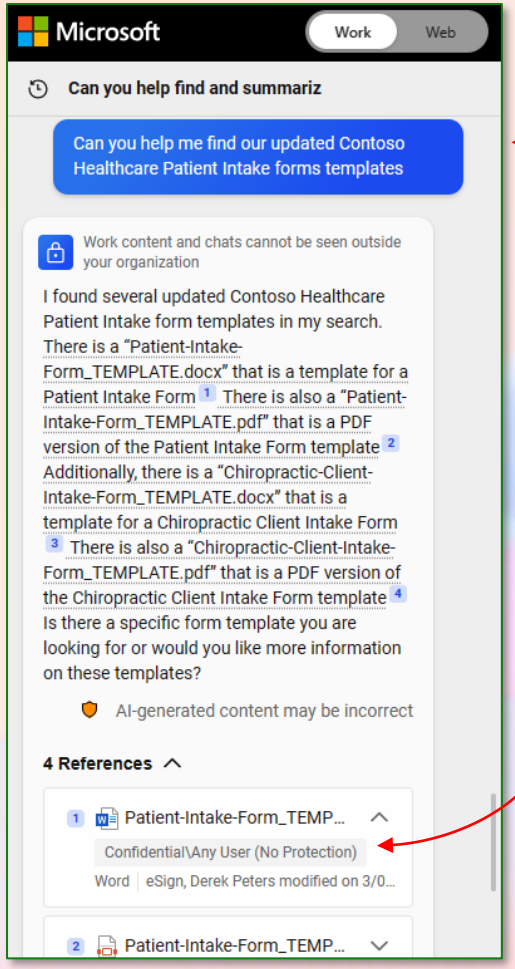
Outcome

Proactive Protection and restriction to authorized recipients

Labels: Email Handing Recommended Labeling

Scenario: User prompts Copilot to source patient intake forms

4

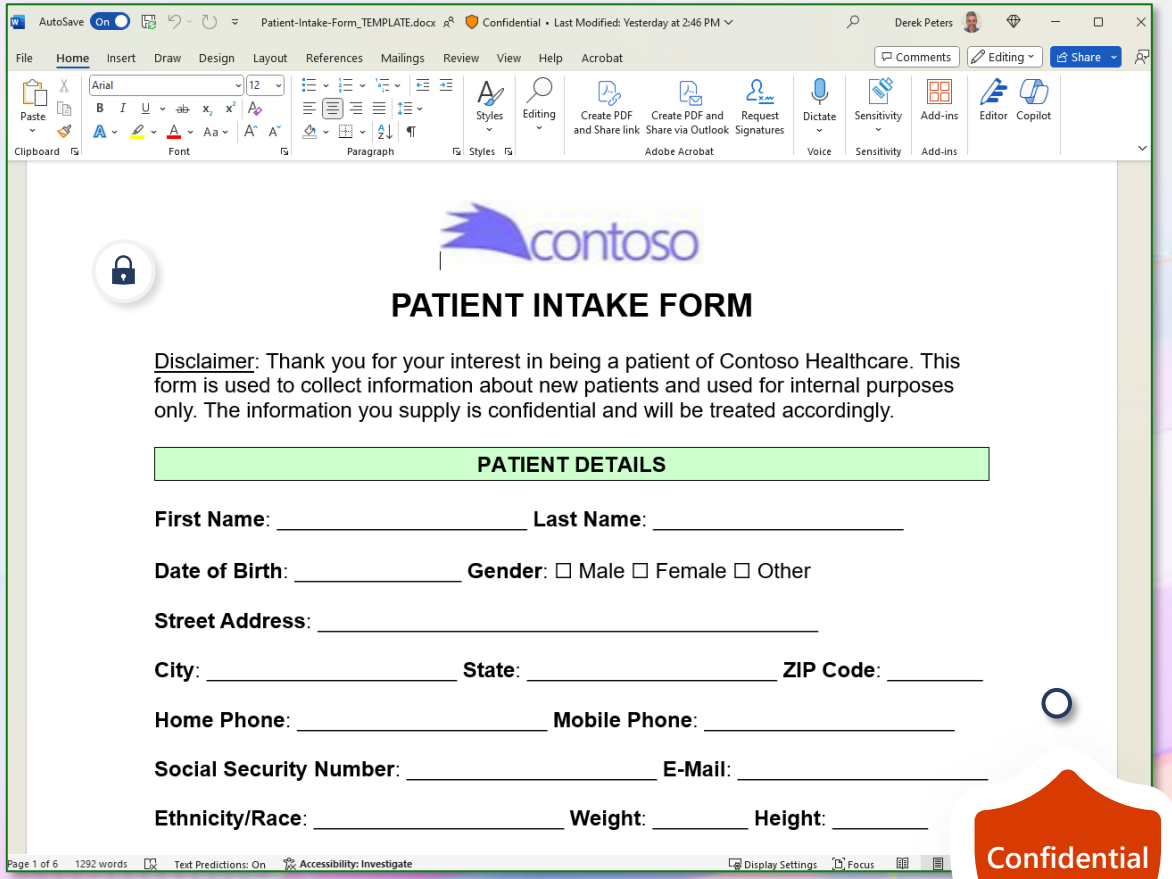


Prompt

Response
Summary permissible

Label Citation

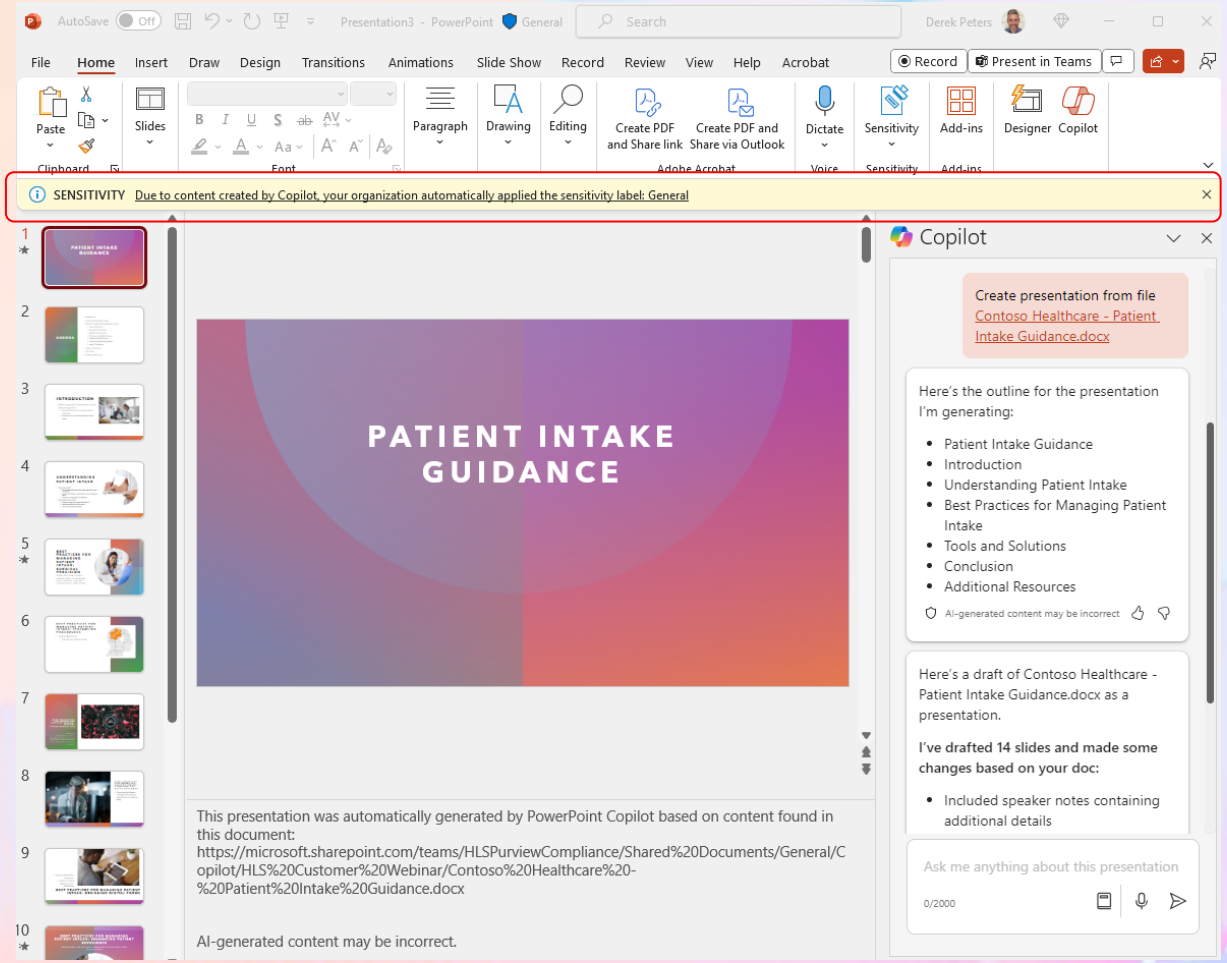
- Users can see the sensitivity of the document referenced in the Copilot output.
- The referenced file's sensitivity is also visible in the citation



Confidential without access control

Label Citations

Scenario: User prompts Copilot to create a presentation from a sourced document



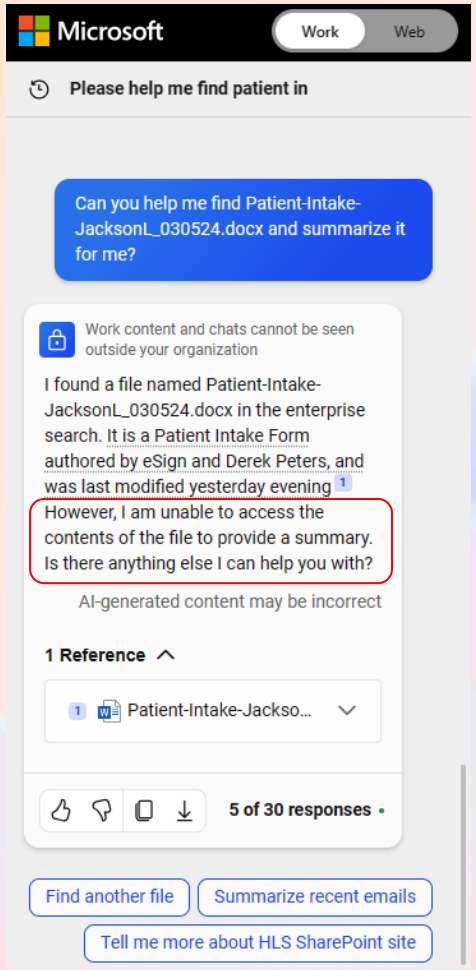
Label inherited from source

Prompt

- The source file's sensitivity is applied to the **new content created by Copilot**.
- **User guidance** is provided on this activity to reinforce protection
- **Copilot citation** in speaker notes

Scenario: User prompts Copilot to summarize a protected document

4

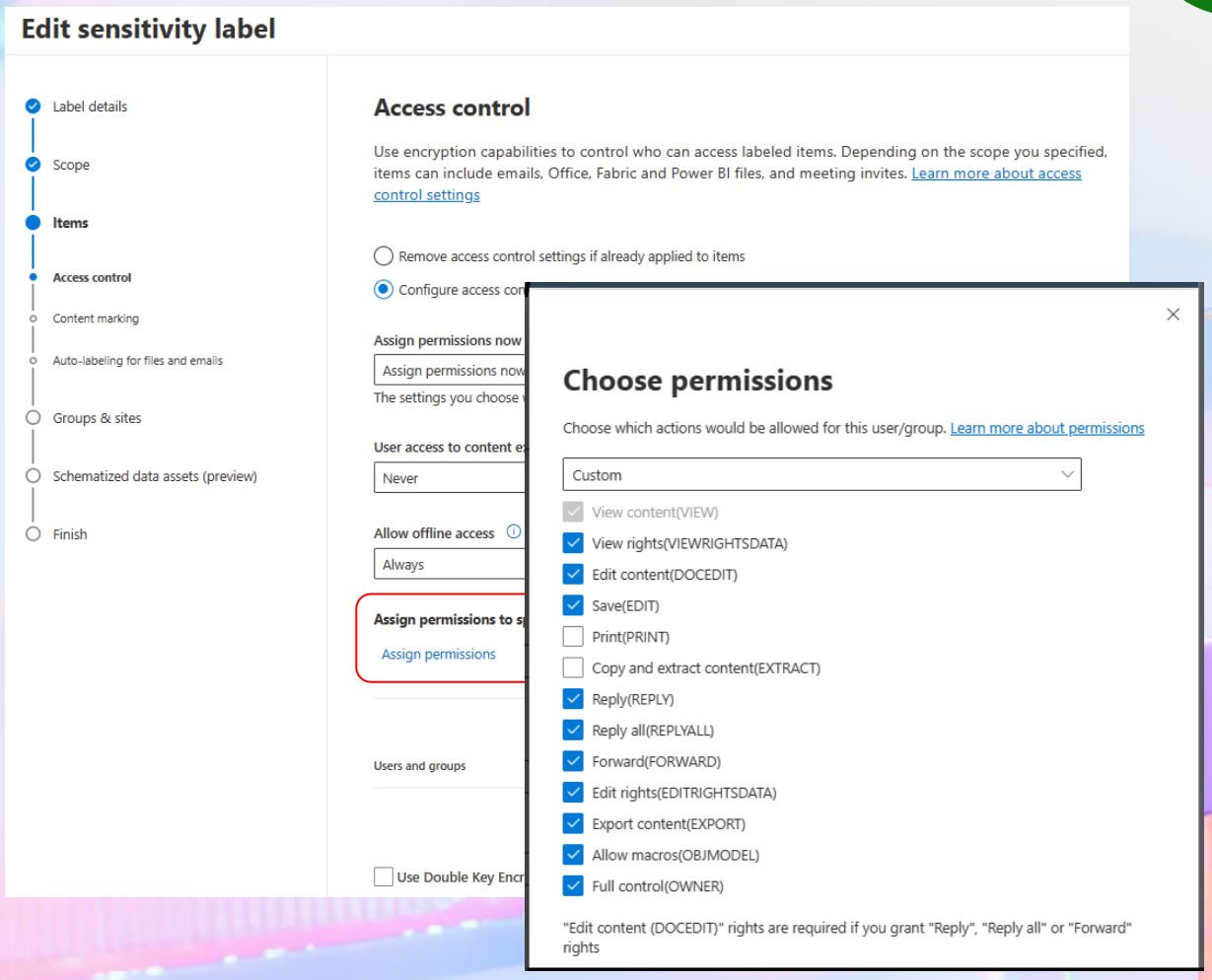


Prompt

Response

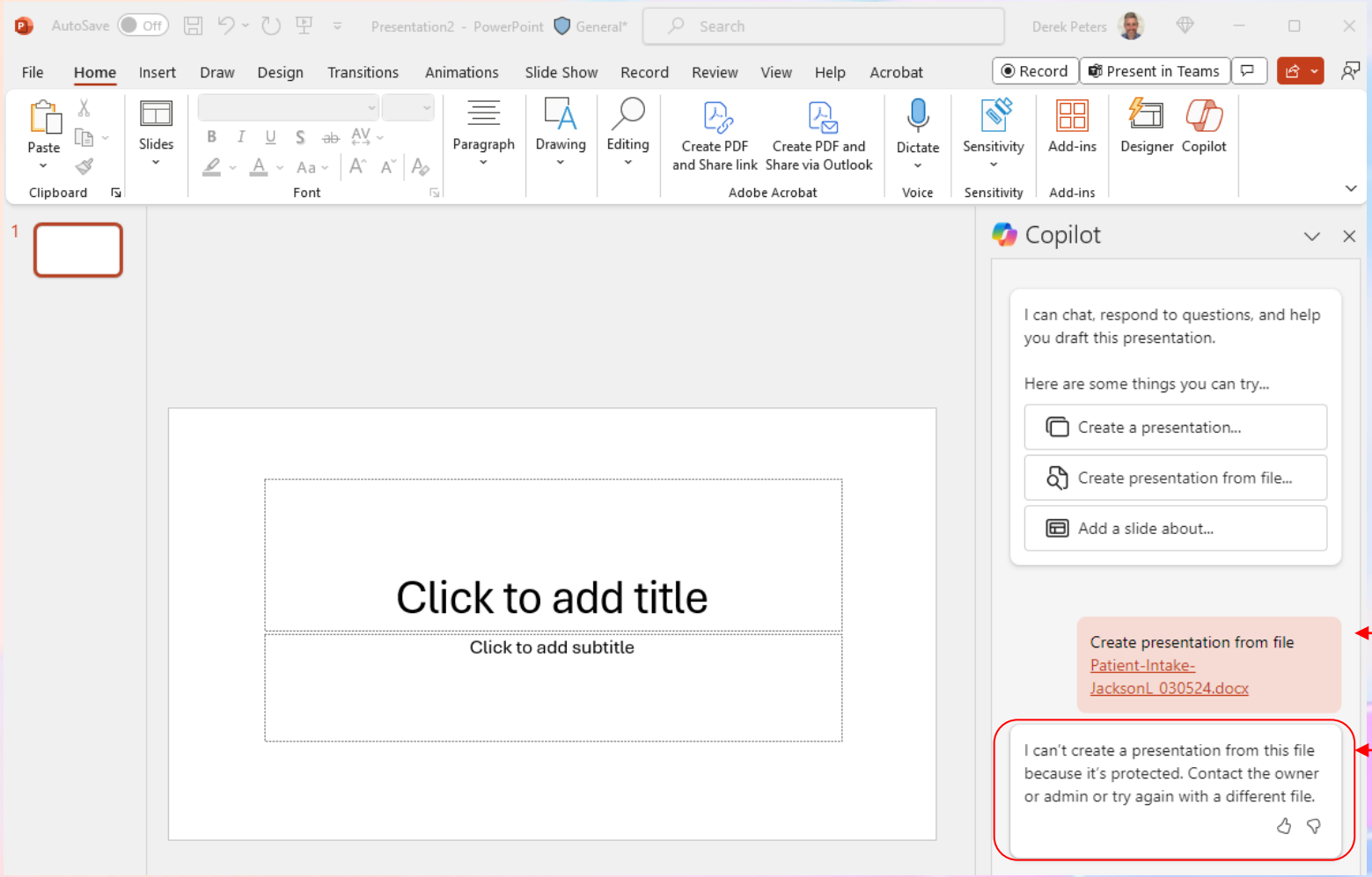
NO summary given

- ❑ Copilot cannot extract content from source
- ❑ Protection maintained



Scenario: User prompts Copilot to create new content from protected source

4



Prompt

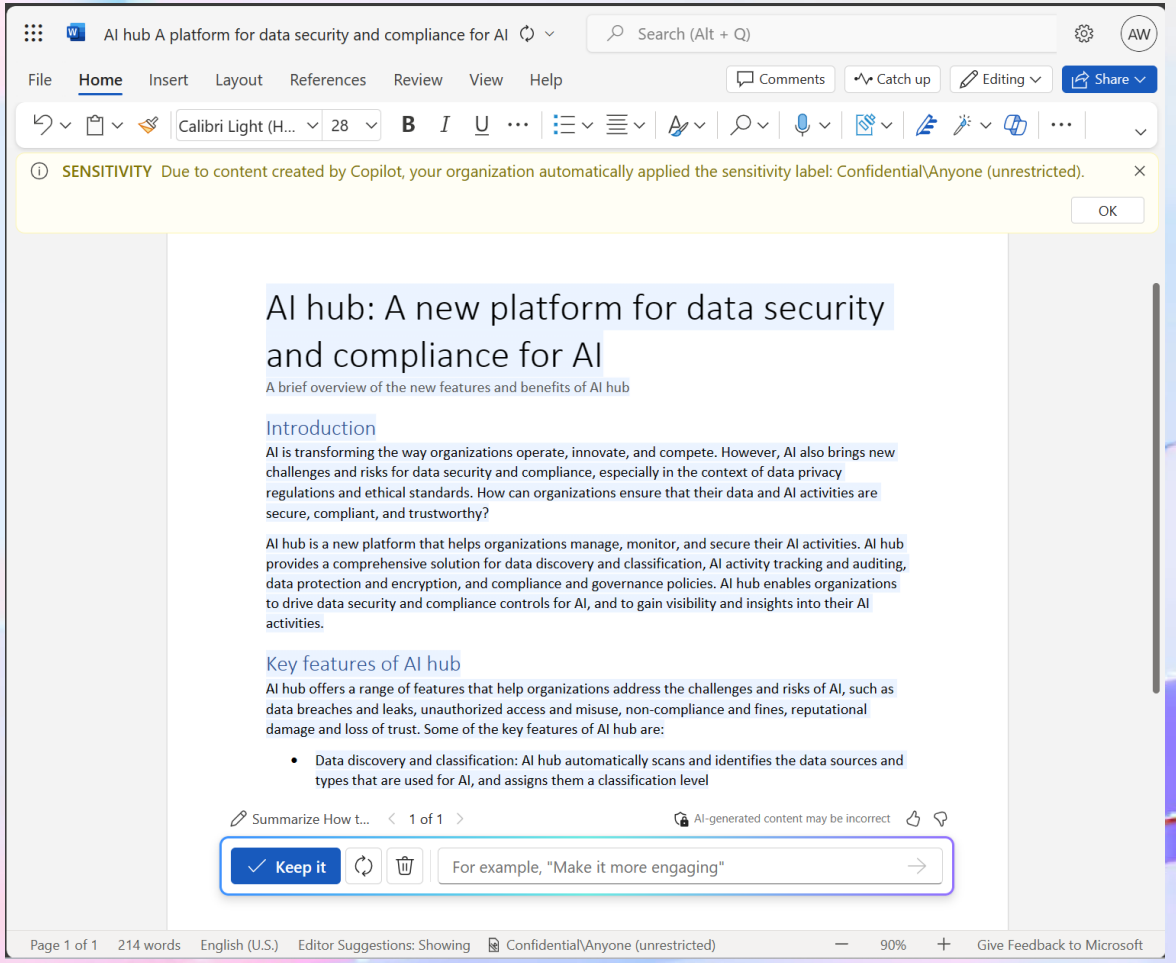
Response

- ❑ Copilot cannot extract content from source
- ❑ Protection maintained

Scenario: User prompts Copilot to create new content from an unlabeled source

4

Copilot generated output will be automatically labeled if sensitive content is detected and auto labeling policies are set up.



How do we get ready for Copilot for M365?

"Plan on a page" - Envision your data security, privacy, and governance processes and requirements

Identify high value improvement actions to strengthen security and privacy controls and readiness for Copilot for Microsoft 365

1 **Limit use of consumer generative AI** to protect your corporate data, avoid data leakage, and benefit from Microsoft Responsible AI standards and Copilot Copyright Commitments.

2 **Plan your Copilot rollout by controlling who gets access first**, allowing for data clean-up, least-privilege access controls, and supporting communications and training.
Zero Trust Model

3 **Strengthen data access controls** to drive awareness, review, and remediation actions (i.e., manage overprivileged and risky users and devices)
Microsoft Entra ID Access Reviews | SharePoint admin center | Microsoft Intune

4 **Prioritize deployment of data security and compliance controls** - identify and label sensitive, personal, and business critical data for appropriate Copilot usage.
Microsoft Purview | Microsoft Purview data security and compliance protections for Copilot

5 **Use specialized tools for data clean-up** to accelerate the remediation of data oversharing at scale via data governance reports, restricted access controls, and more.
SharePoint Premium | Microsoft Graph Data Connect

Identify those who can help

✓ **Work with your Microsoft customer enablement teams and partners** on top priority actions, readiness assessments, and deployment plans.
Copilot for Microsoft 365 – Microsoft Adoption | Microsoft Copilot for Microsoft 365 setup guide

Use specialized tools for data clean-up

Several **options** available to aid with overall Microsoft 365 data security, governance, and compliance *

5

Areas of focus

Uncover Risks

Data discovery

- Permissions
- Sensitive and personal data
- Privacy levels
- Data overexposure
- Obsolete data

- Levels of sensitivity
- Application of retention
- Access request procedures
- Data loss procedures
- On/Offboarding procedures

Implement Controls

Data access

- Remediate permissions
- Evaluate data boundaries
- Evaluate and enforce access reviews
- Evaluate and apply expiration policies
- Evaluate and apply conditional access

Data security

- Prevent data loss
- Protect data
- Mitigate insider risk
- Evaluate and apply additional encryption

Risk and compliance

- Evaluate and enforce retention policies
- Evaluate and implement records keeping
- Understand discovery and audit
- Implement communication surveillance
- Evaluate disposition and archiving needs

Optional actions

Data discovery			Data access	Data security		Risk and compliance	
Review existing permissions of Teams and Sites	Use content search to discover sensitive information	Run PowerShell scripts to generate reports	Manually adjust permissions in Sites and Teams	Temporarily restrict SharePoint site content using Restricted SharePoint Search	Implement data loss prevention policies for mail, files, and Sites	Manually apply sensitivity labels to Microsoft Teams and Sites	Implement location-wide retention and deletion policies	Use Audit Standard to review any Copilot activities
Use Content Explorer to identify sensitive content	Identify data exposition with Defender for Cloud Apps	Use eDiscovery Premium to identify sensitive content	Implement Access Reviews to recertify Teams & Group audience	Implement container labeling conditions to new public / private site	Implement data loss prevention policies for Microsoft Teams and third-party cloud apps	Auto-apply sensitivity labels to Microsoft Teams and Sites	Implement adaptive retention and deletion policies (scoped retention)	Implement disposition reviews before deleting or archiving content/sites
Identify overshared personally identifiable information with Microsoft Priva	Identify sensitive or overexposed content with SharePoint Premium	Microsoft Purview Advanced Rich Reporting	Refine group expiration policy for inactive Teams & Group sites	Use SharePoint Premium to restrict access to specific Sites	Create data overexposure policies using Microsoft Priva	Apply encryption options to content, sites, and containers	Use Microsoft Priva to introduce data minimization policies	Use SharePoint Premium to manage Site lifecycle policies

E3 E5 Add-on

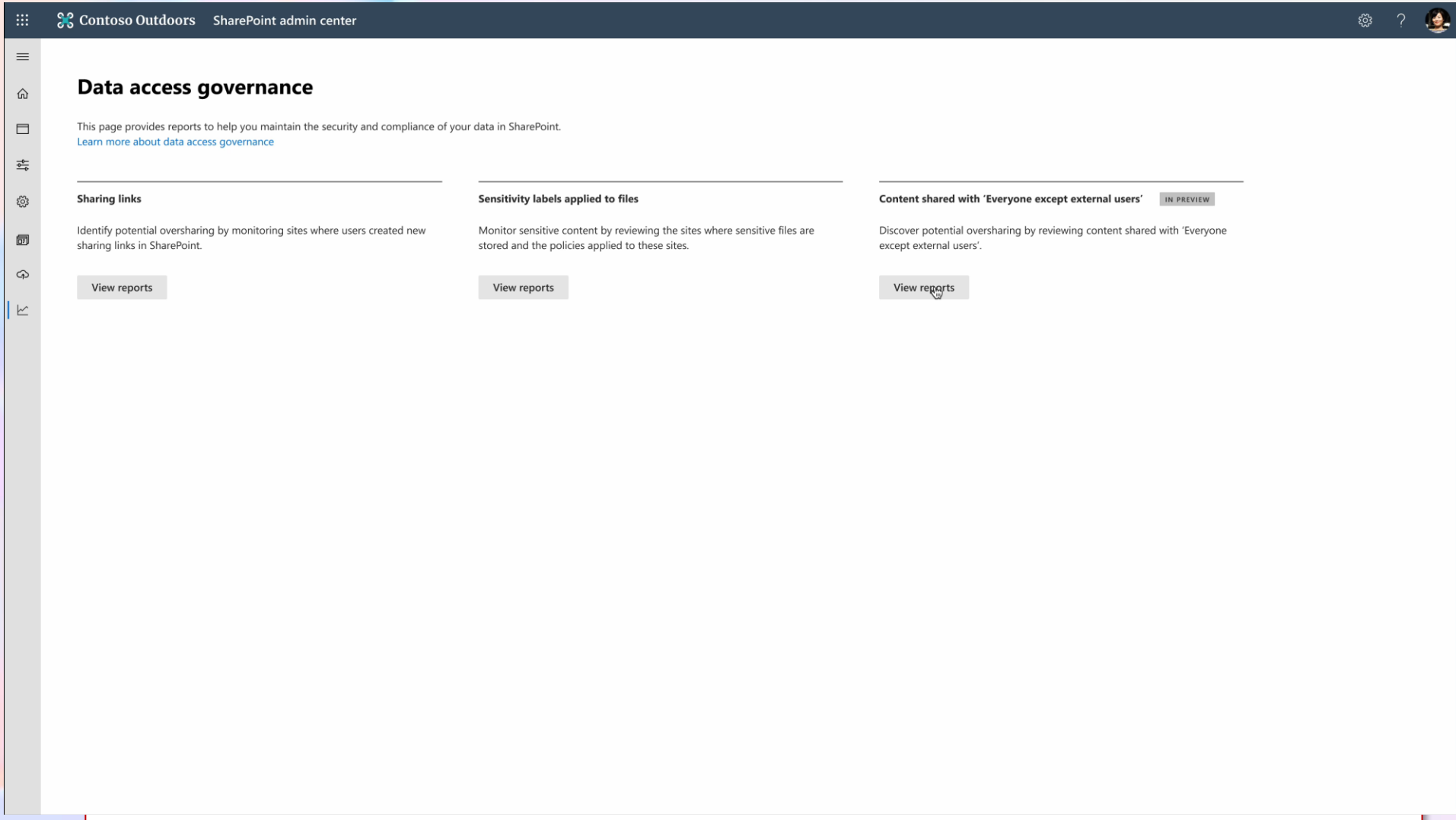
*** NOTE: These activities are purely optional and NOT a requirement for Copilot for Microsoft 365 nor in any particular order of precedence**

Use specialized tools for data clean-up

Long-term options to aid with continual overall data governance

5

- SharePoint Advanced Management
- Microsoft Priva | Privacy Rights Management
- SharePoint Premium| Backup and Archive
- SharePoint Premium | "Project Archimedes"
- Microsoft Graph | Microsoft Graph Data Connect
- Microsoft Fabric | Azure Synapse Analytics
- Power BI | to build visualizations and reports
- Microsoft Purview APIs | extensibility
- PowerShell Scripts | custom scripts
- Microsoft Purview Advanced Rich Reports



Data access governance | Shows the top sites that have the most oversharing links by sensitivity, external sharing, RAC, unmanaged devices, dates, and more. Enables forcing a **site access review** (one-time/recurring) to remediate oversharing.

Optimizing your Copilot for Microsoft 365 rollout

Optimize your data security, privacy, and governance processes and requirements

Identify high value improvement actions to strengthen security and privacy controls and readiness for Copilot for Microsoft 365

1. **Limit use of consumer generative AI** to protect your corporate data, avoid data leakage, and benefit from Microsoft Responsible AI standards and Copilot Copyright Commitments.
2. **Plan your Copilot rollout by controlling who gets access first**, allowing for data clean-up, least-privilege access controls, and supporting communications and training.
   Zero Trust Model
3. **Strengthen data access controls** to drive awareness, review, and remediation actions (i.e., manage overprivileged and risky users and devices)
   Microsoft Entra ID Access Reviews | SharePoint admin center | Microsoft Intune
4. **Prioritize deployment of data security and compliance controls** - identify and label sensitive, personal, and business critical data for appropriate Copilot usage.
   Microsoft Purview | Microsoft Purview data security and compliance protections for Copilot
5. **Use specialized tools for data clean-up** to accelerate the remediation of data oversharing at scale via data governance reports, restricted access controls, and more.
   SharePoint Premium | Microsoft Graph Data Connect

Identify those who can help

Work with your Microsoft customer enablement teams and partners on top priority actions, readiness assessments, and deployment plans.
Copilot for Microsoft 365 – Microsoft Adoption | Microsoft Copilot for Microsoft 365 setup guide

Appendix

- Explore support options through Microsoft Unified Support and FastTrack
- Get end to end assistance through Partner offers
- Delve into security, privacy and compliance
- Learn how AI is creating a whole new way of working
- Leverage the Resources for Adoption

Meet the Microsoft Purview Family

Integrated solutions to secure and govern your entire data estate

DATA SECURITY	DATA GOVERNANCE	RISK & COMPLIANCE POSTURE
Secure data across its lifecycle, wherever it lives	Responsibly democratize value creation from data	Manage critical risks and regulatory requirements
Data Loss Prevention Insider Risk Management Information Protection Adaptive Protection	Data Catalog Data Curation Data Management Data Discoverability Data Understanding Responsible Access and Use	Compliance Manager eDiscovery & Audit Communication Compliance Data Lifecycle Management Records Management

Secure ⟷ Compliant

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

Shared Platform

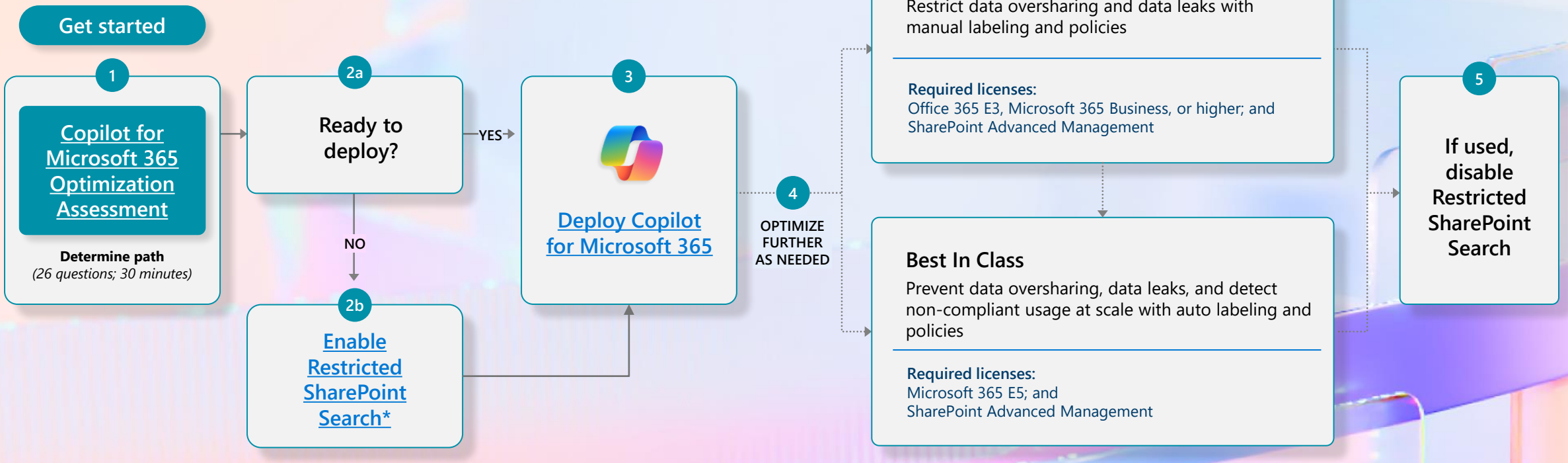
Data Map, Data Classification, Data Labels, Audit, Data Connectors

On-prem and multi-cloud | **Unstructured & structured data** | **Across IaaS and SaaS**

Planning your Copilot for Microsoft 365 rollout

Get started quickly and continue to optimize along the way

2



- *Restricted SharePoint Search will limit Copilot for Microsoft 365 experiences and organization-wide search.*
- *It is a temporary option which gives you time to address oversharing concerns while getting started on your Copilot journey.*

Use specialized tools for data clean-up

Restricted SharePoint Search

2

This is intended as a temporary solution to give you time to review and audit site permissions, while implementing robust data security solutions from Microsoft Purview and content management with SharePoint Advanced Management.

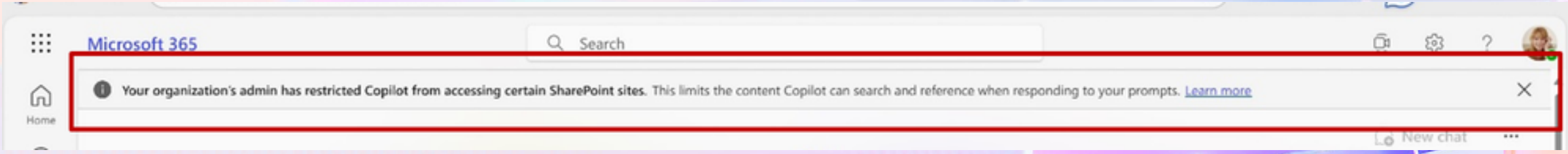
- **Restricted SharePoint Search** is designed for organizations particularly concerned about unintentional oversharing of content
- When enabled, Copilot experiences and organization-wide search are limited to a select set of SharePoint sites, as well as the individual user's files and content

IMPACT

Restricted SharePoint Search disables organization-wide search, while allowing you to select sites that you trust. This means users in your organization can use Copilot to reason over:

- An allowed list of curated SharePoint sites set up by admins (up to 100 SharePoint sites), honoring existing permissions on a site
- Users' OneDrive for Business, chats they are part of, emails they send and receive, calendars to which they have access, etc.
- Files that are shared with, and accessed by users
- Content from users' frequently visited sites

Access this blog for more info.



PREREQUISITES

- Available to tenants with Copilot for Microsoft 365 subscriptions
- Activation requires Global/Tenant/SharePoint admin rights

Data discovery and planning

Optional preparation tasks to perform before conducting a data discovery risk assessment

Assistance availability

Internal resources

- Assess current skill levels and availability
- Helps with knowledge of existing environment

Technical specialists

- Tools and product knowledge
- Helps to understand what is technically available

FastTrack

- Guided assistance only
- Does not perform hands-on or advisory activities

Unified support

- Designate engineers with hands-on experience
- Leverages existing support hours to engage

Assistance required

Internal hiring

- Assess current skill gaps and necessary ways to fulfill those people needs
- Evaluate potential hiring needs ahead of planning and rollout

External consultants

- Leveraged for advisory services such as legal counsel and adoption
- Aids with independent analysis of the requirements ahead

Microsoft Partner

- Subject matter expertise of technologies and requirements
- Aids with technical and advisory services by applying past best practices experiences

Data definitions

Sensitive Content

- Define what patterns and content would be deemed as sensitive in nature
- Used to help scan and report on locations of sensitive materials

Personal Data

- Define what patterns and content would be deemed as personally identifiable in nature
- Used to help scan and report on locations of personally identifiable materials

Data security, privacy and handling policies

- Review and update any required policies or procedures related to the proper use of organizational data
- Understand the methods for auditing and discovery of use
- Helps to guide and prepare for the use and resilience of the rollout

Data classification

Levels of sensitivity

- Define an agreed upon corporate data classification schema to be used for data security
- Used throughout the process of discovery and remediation of data security

Classification awareness

- Prepare for end user knowledge and awareness
- Helps drive end user adoption and importance of data security

Environment preparation

Tools and environment

- Determine hardware and/or software required
- Aids in cost analysis and timing for preparation

Security

- Determine what minimal permissions are required
- Helps in defining technical roles and responsibilities

Copilot for Microsoft 365

- Procure and activate Copilot for implementation team
- Aids in overall learning

Reporting

- Determine who and methods for reporting results
- Helps communicate risks