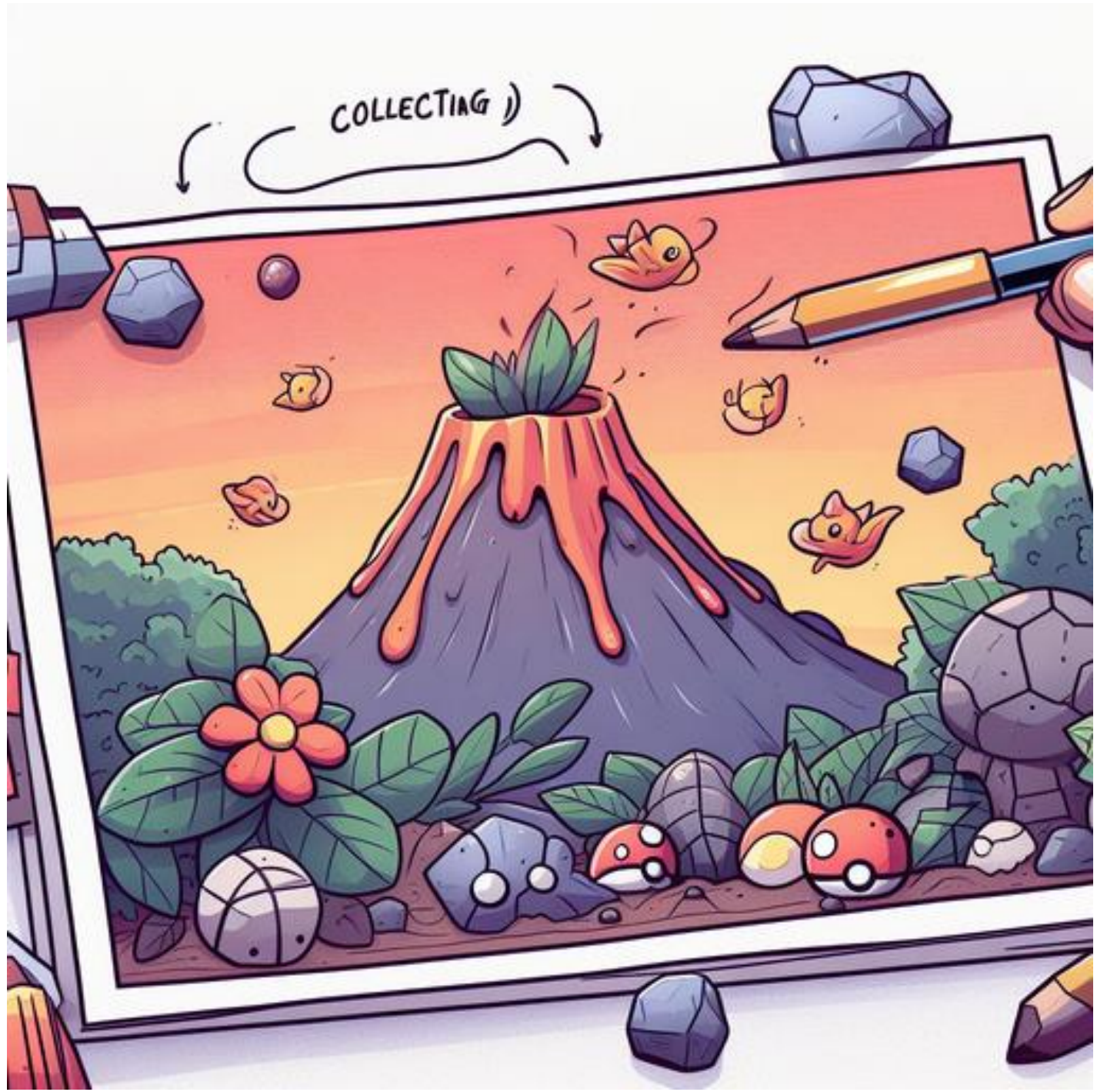
All we hear is Copilot, but how to make it (Data) Secure

Microsoft Security

Tim Hermie

Technical Specialist Data Security
Former Microsoft MVP Enterprise Mobility
Former Windows Insider MVP
Microsoft Most Valuable Mentor
Microsoft Certified Trainer
Founding Board Member MC2MC
@_Cloud_boy
Drums – World Explorer – Volcano Addict – Foodie


COLLECTING

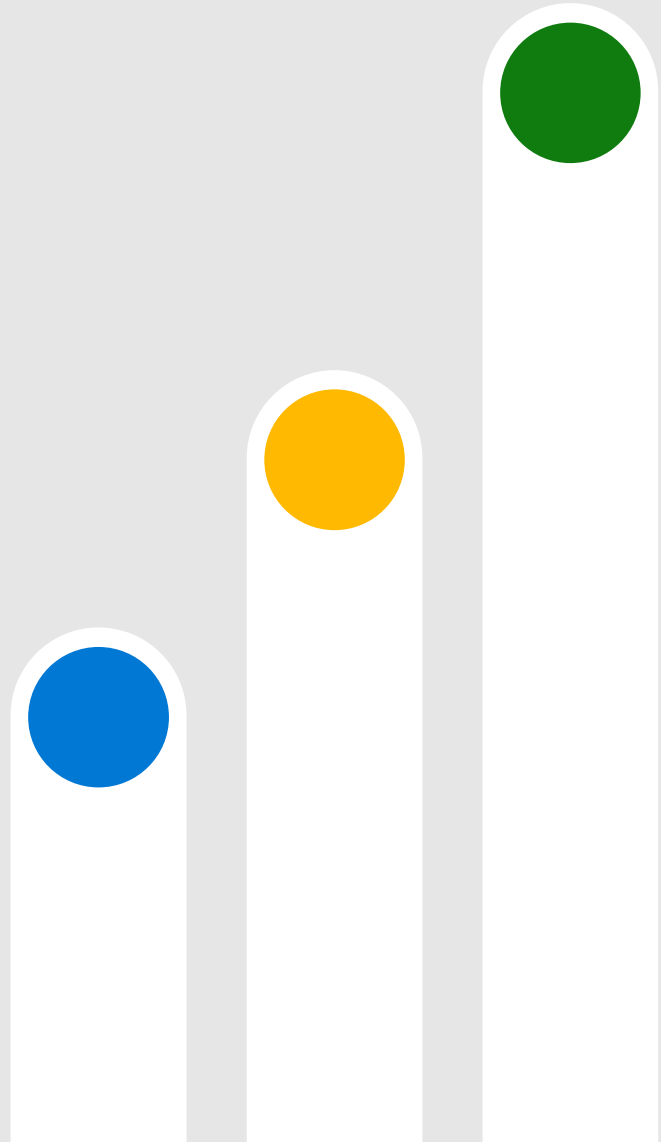
Agenda

Securing generative AI
growing usage

Copilot for Microsoft 365
with **Microsoft Purview**

Copilot for Security
for/in **Microsoft Purview**

A glimpse into the future
& **secure 3rd party GenAI**



Agenda

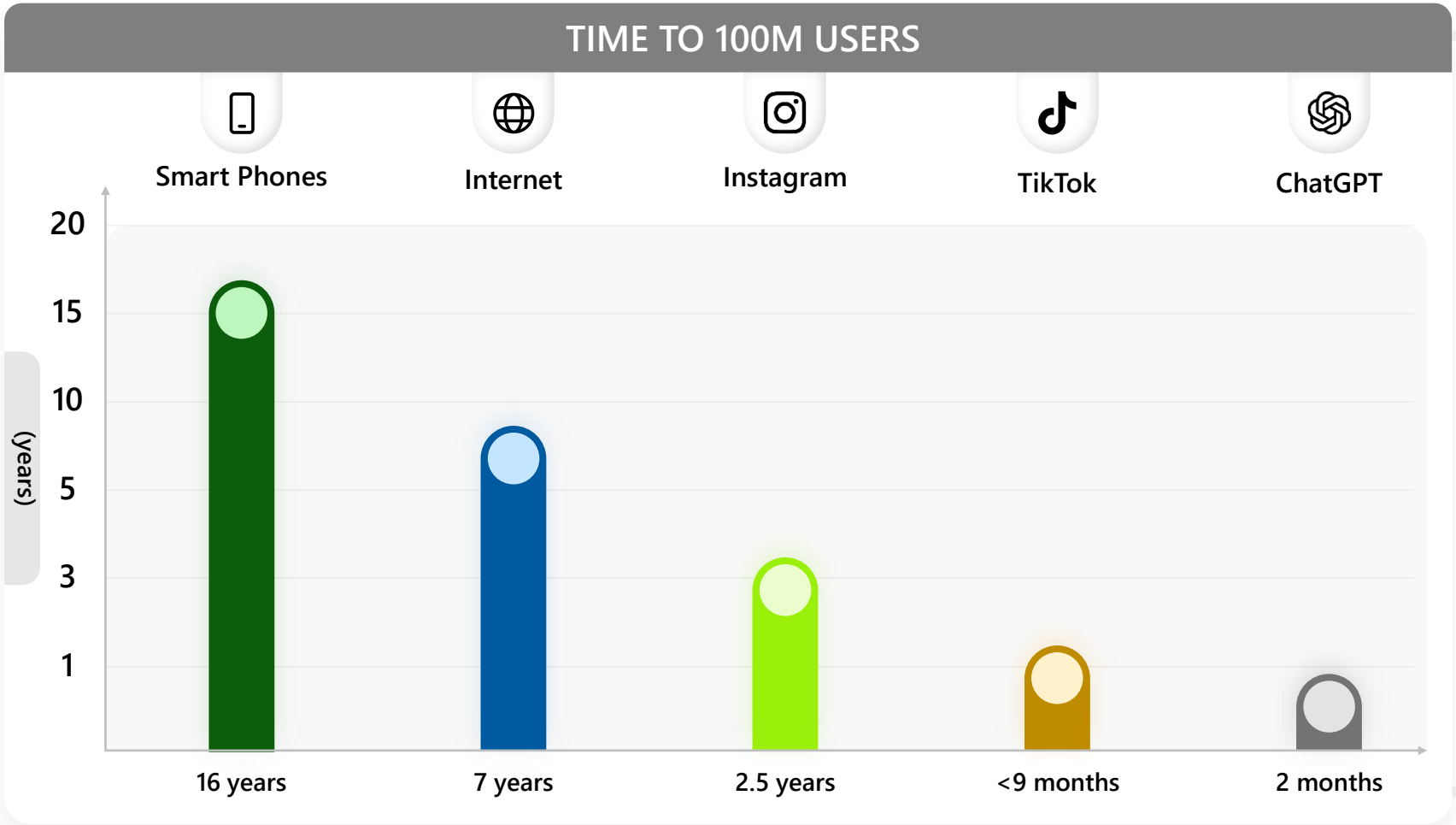
Securing generative AI
growing usage

Copilot for Microsoft 365
with **Microsoft Purview**

Copilot for Security
for/in **Microsoft Purview**

A glimpse into the future
& **secure 3rd party GenAI**

Generative AI technology is here!



And can help...

- Unleash creativity
- Unlock productivity
- Uplevel skills

But there are associated risks

Lack of controls to protect data shared in AI

of business and cybersecurity leaders cited leakage of sensitive data as their main concern[1]

Lack of controls to govern data shared in AI

of business leaders worry about AI bias and ethical concerns[1]

Increased regulatory pressure

at least one global company will see its AI deployment banned by a regulator for noncompliance with data protection or AI governance legislation.[3]

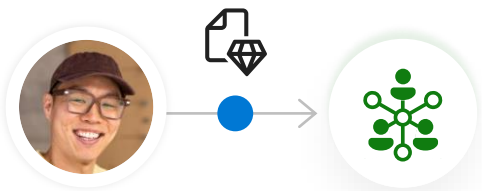
1. First Annual Generative AI study: Business Rewards vs. Security Risks, , Q3 2023, ISMG, N=400
2. Survey of 658 data security professions, Mar 2023, commissioned by Microsoft
3. Gartner Security Leader's Guide to Data Security, Sep 2023

Security concerns associated with AI usage

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

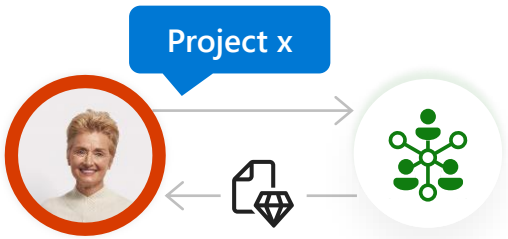
1

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



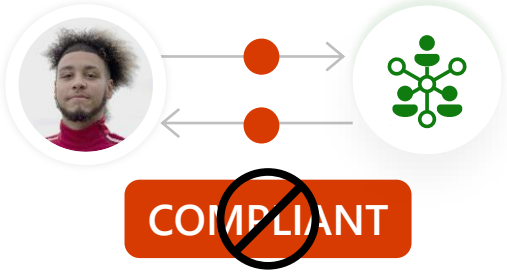
2

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



Shared responsibilities of security for AI usage for Microsoft Copilot for Microsoft 365

Privacy & Compliance

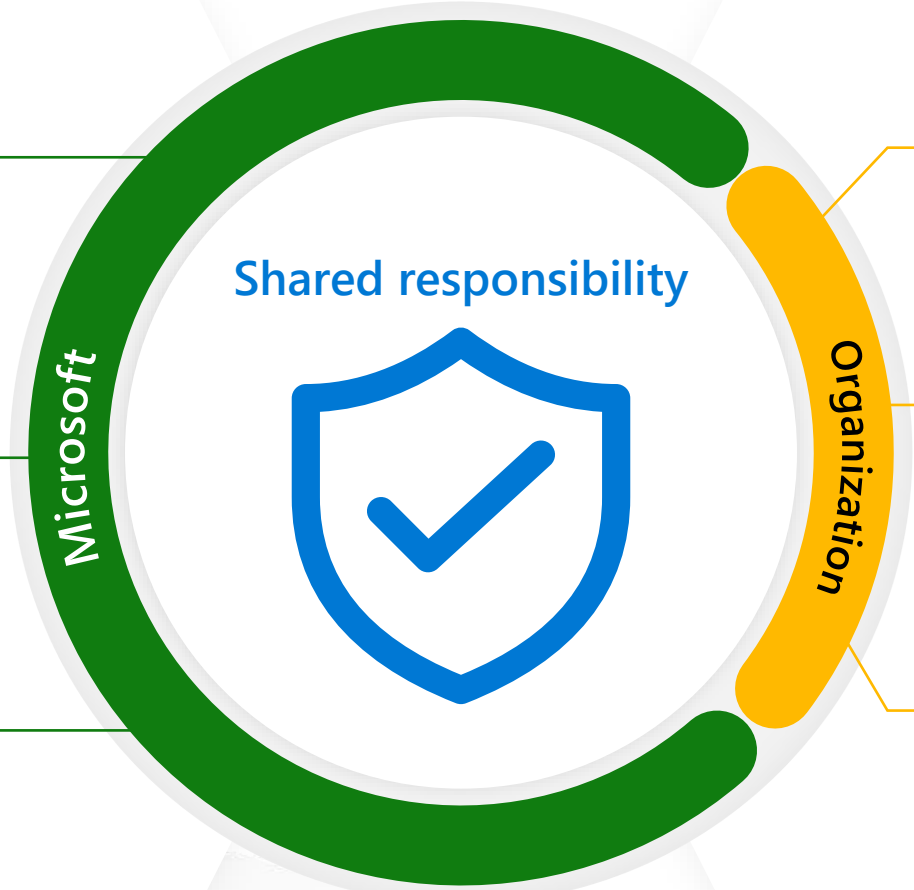
Compliance with our existing privacy, security, and compliance commitments to Microsoft 365 commercial customers, including the General Data Protection Regulation (GDPR) and European Union (EU) Data Boundary.

Service boundary

Prompts, responses, and data accessed through Microsoft Graph aren't used to train foundation LLMs, including those used by Microsoft Copilot for Microsoft 365.

Responsible AI

At Microsoft, we are guided by our AI principles and Responsible AI Standard – fairness, reliability and safety, privacy and security, inclusiveness, transparency, and accountability



Access to AI apps

Set up access control policy, leveraging identity and access management solutions

Protect and govern data entered and created by AI apps

Apply data security and compliance controls on data in AI interactions.

User accountability of AI use

Implement and operate organization-wide AI security training

Microsoft Purview

Comprehensive solution to secure and govern AI

Microsoft Purview – High Level Overview

Microsoft

Data Map and Data Catalog
Maximize the business value of data for your consumers by creating a unified map to automate and manage metadata from hybrid sources. Helps you manage and govern your on-premises, multi-cloud, and software-as-a-service (SaaS) data.

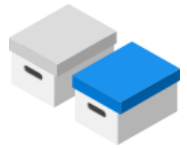
Compliance Manager
Reduce risk by translating complex regulatory requirements into specific improvement actions that help you raise your score and track progress. (ISO, NIST, GDPR, TISAX, ...)

Information protection
Discover, identify, classify, and protect sensitive data that is business critical, then manage and protect it across your environment.

Privacy management
Generates actionable insights on enterprise personal data to help you spot issues and reduce risks and to respond to data subject requests for GDPR.

Data loss prevention
Automatically protect sensitive information from risky and unauthorized access across apps, services, endpoints, and on-premises files.

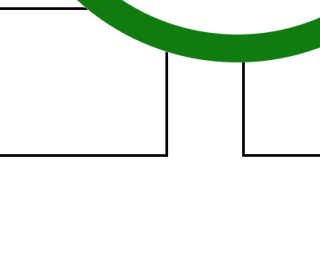
Audit (Premium)
Records user and admin activity from your organization so you can search the audit log and investigate a comprehensive list of activities across all locations and services.



Data Lifecycle Management
Classify and govern data at scale to meet your legal, business, privacy, and regulatory content obligations.

eDiscovery (Premium)
Discover and manage your data in-place with end-to-end workflows for internal or legal investigations.

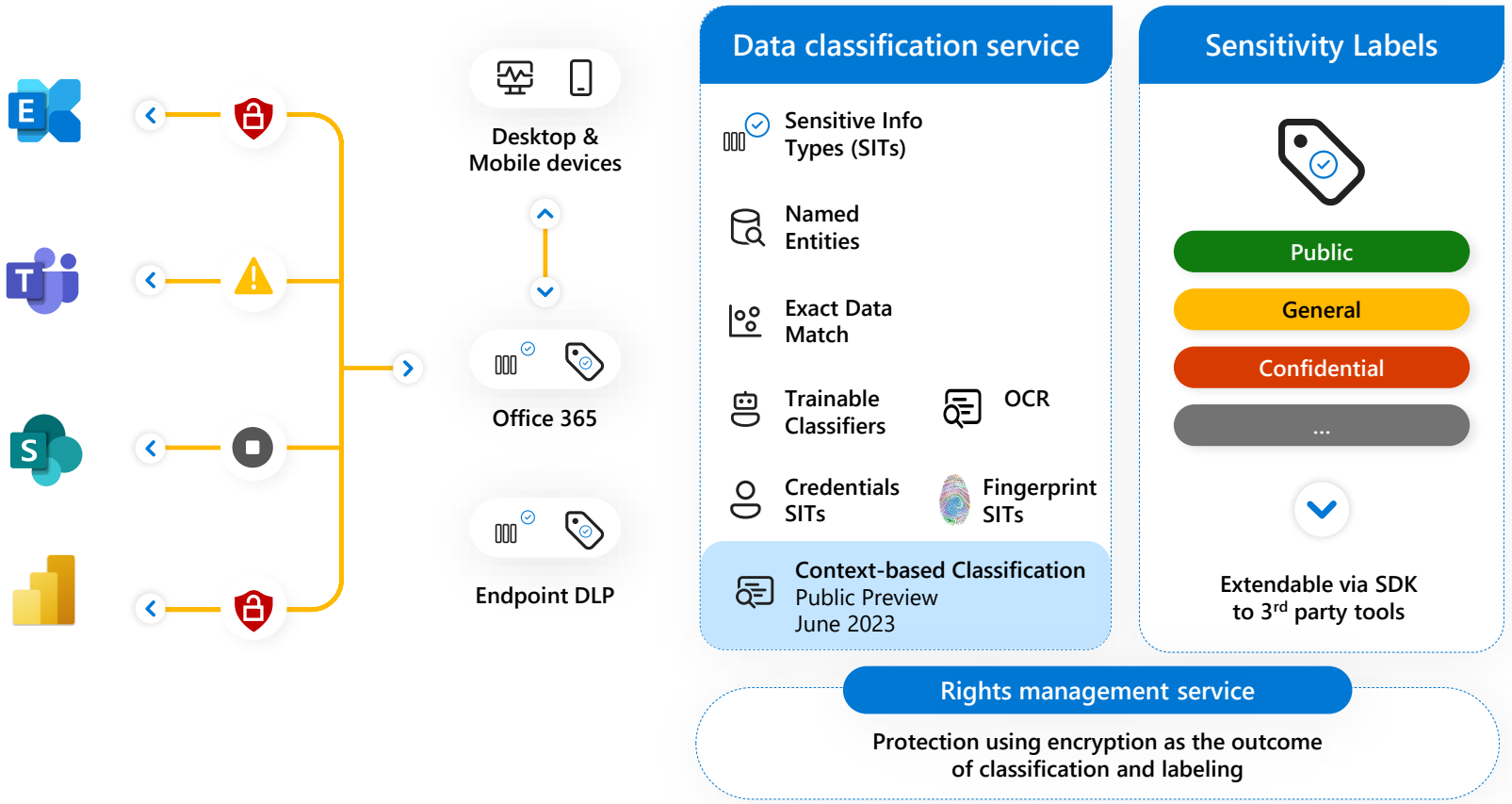
Records management
Uses intelligent classification to automate and simplify the retention schedule for regulatory, legal and business-critical records in your organization.



Communication compliance
Reduce risk by translating complex regulatory requirements into specific improvement actions that help you raise your score and track progress.

Insider risk management
Detect, investigate, and take actions on critical risks in your organization, including data theft, data leaks, and security policy violations.

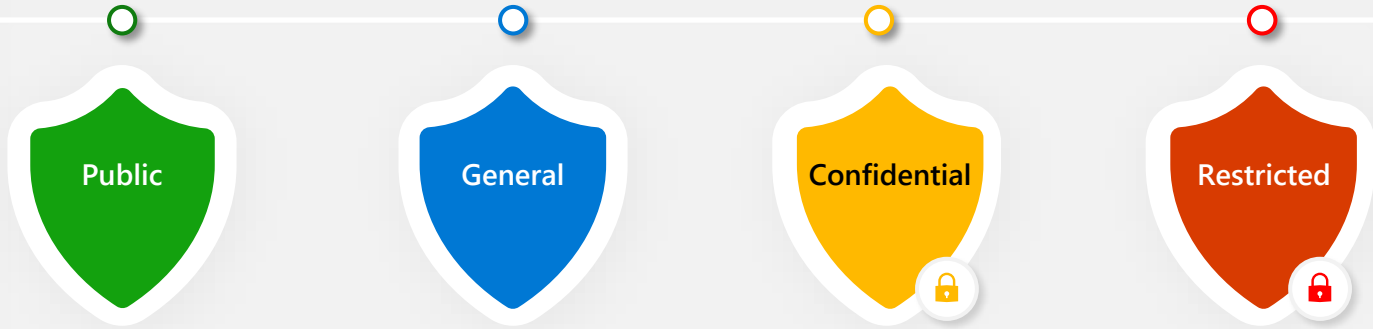
Microsoft Purview Information Protection



- Uniform content & context-based classification
- Native integration with Microsoft 365 apps and services
- Broad support with 3rd party solutions, data repositories, and LOB applications

Sensitivity labels span your entire data estate

- They are a representation of your information taxonomy.
- They describe the priority assigned to your categories of sensitive information.



Content labels

Applied To: Office apps, Power BI reports, Azure Data

Protections: Encryption and visual markings

Automation: Can be applied either manually by users or automatically based on classification

Container labels

Applied To: SharePoint sites, Teams channels, Microsoft 365 groups

Protections: Access control, privacy settings, conditional access

Automation: Can be applied manually by site/Team or group owners

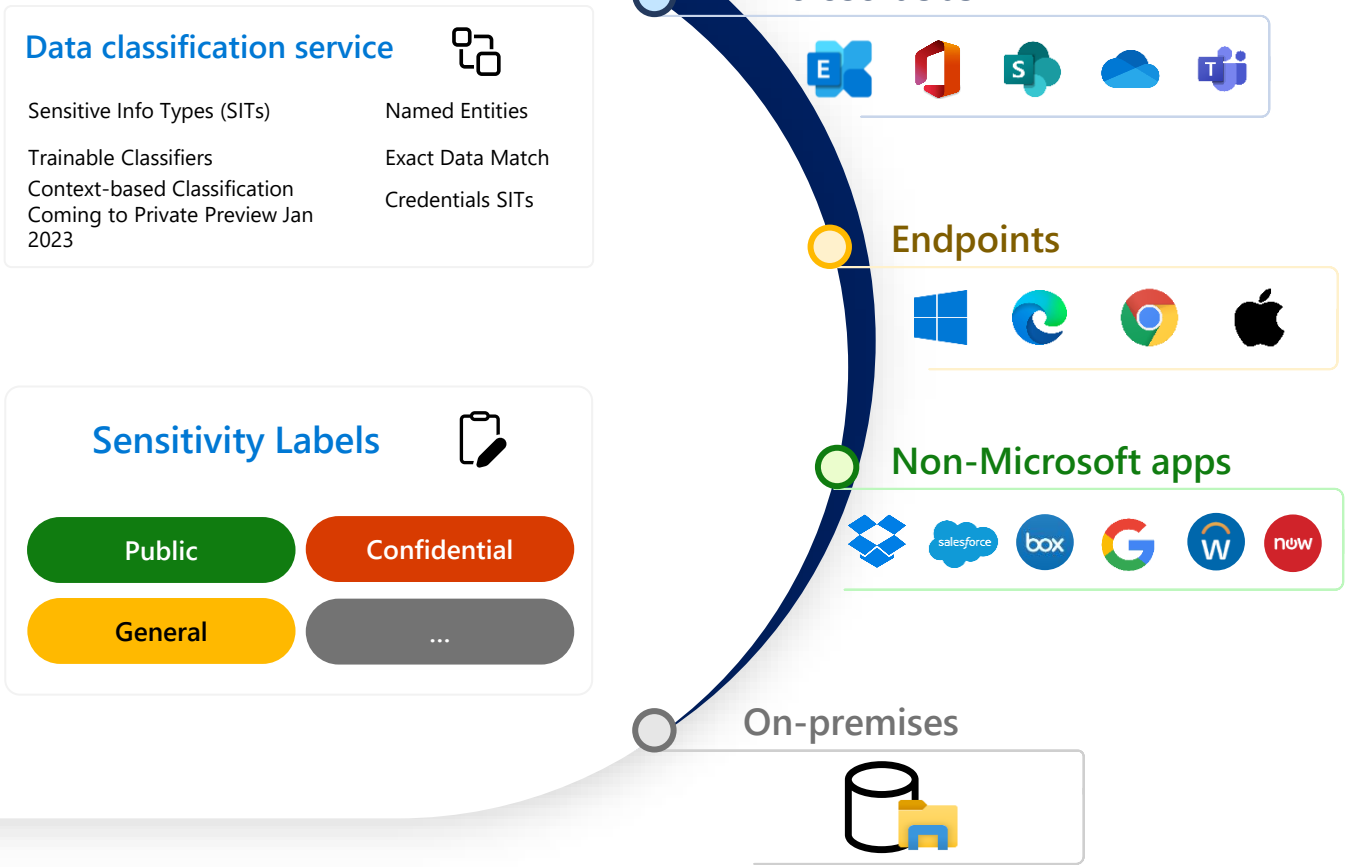
Powerful controls that ensure labels are applied where needed

Apply labels by default, make them mandatory, audit label downgrades

Cloud native with built-in protection

Save cost and scale effectively

- Cloud managed and delivered, no on-premise infrastructure or agents needed
- Built-in experiences in Microsoft 365 apps and services, Windows endpoints, On-premises
- Extend protection to non-Microsoft applications and platforms

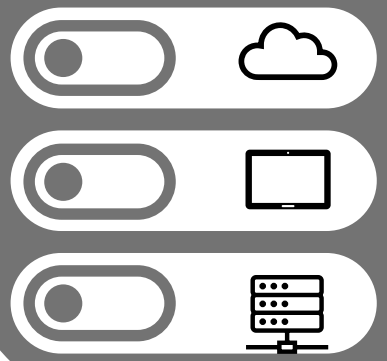


Unified and flexible policy management

Balance protection and productivity

Unified policy creation

Create and manage policies for all workloads from one location



Role-based access controls

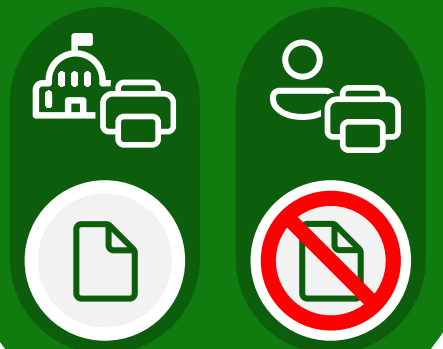
Only authorized admins can create policies and investigate alerts for scoped users

German admin

German users

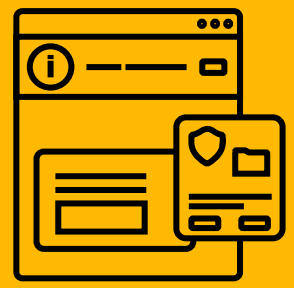
Granular policy control

Granular policy configuration controls for differentiated actions



Policy tips and user notifications

Educate users on security best practices through policy tips and notifications

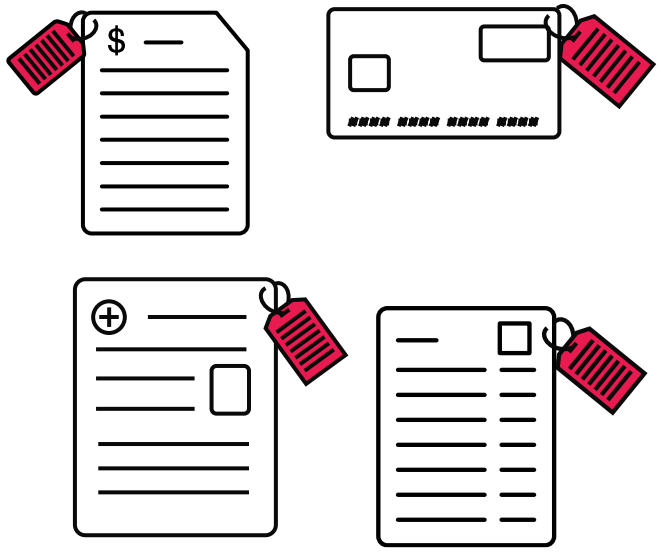


Integrated insights and alerting

Enrich policy and investigation with rich signals

Know the context

Leverage classification and labeling on sensitive data from Information Protection



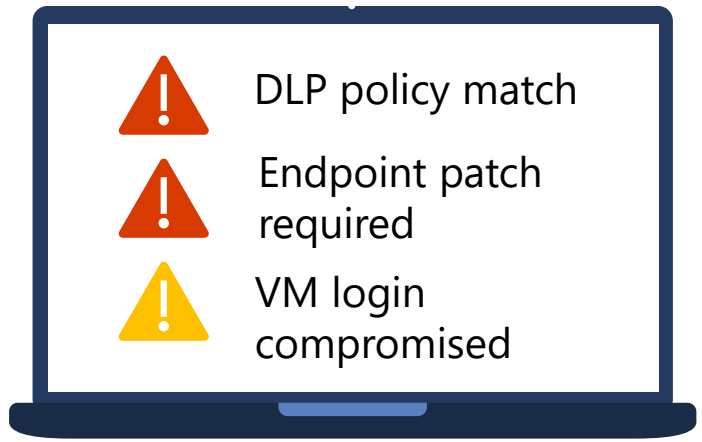
Understand the intent

Automatically apply risk insights from Insider Risk Management to DLP policies

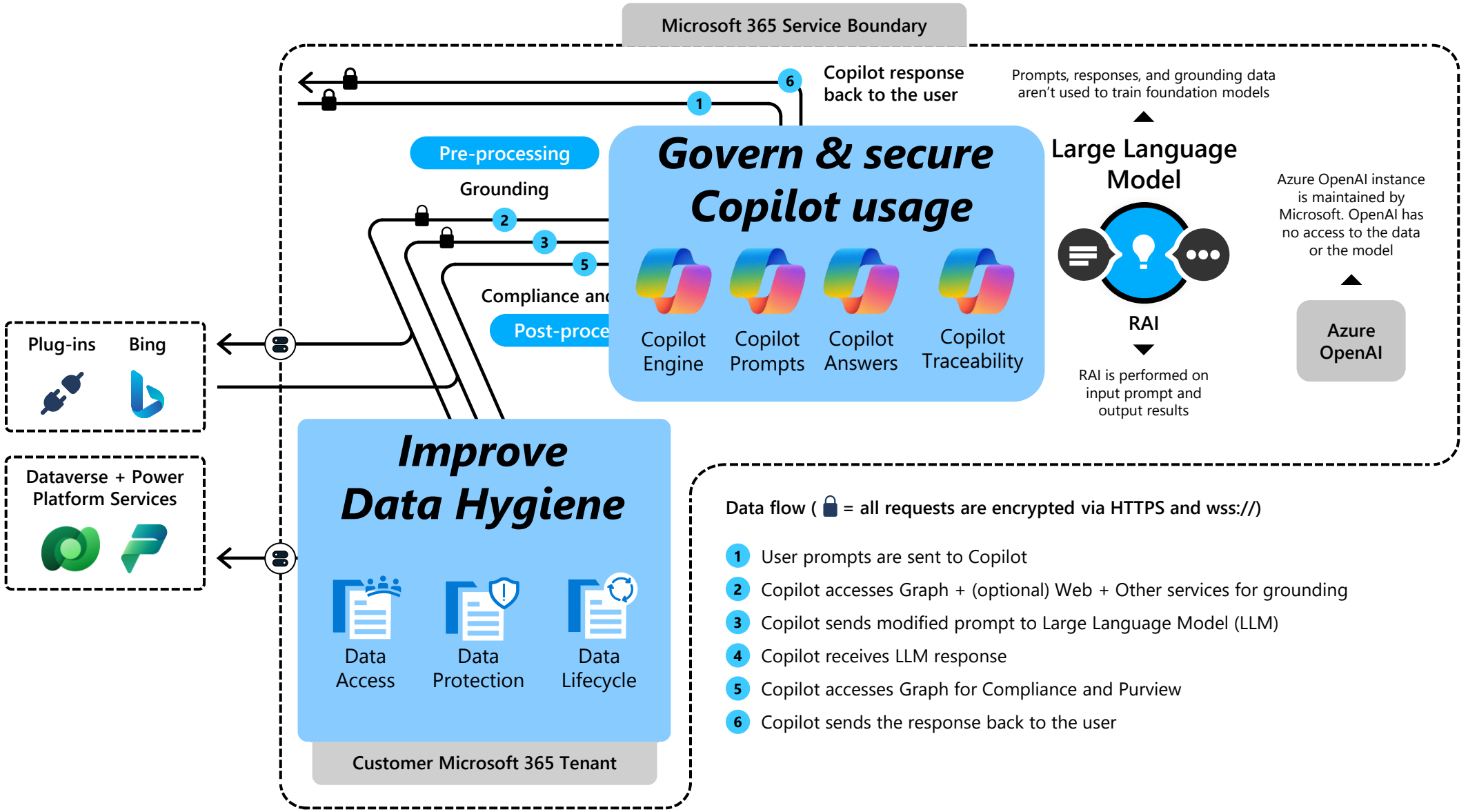
Elevated risk	→	DLP Policy 1	Block
Moderate risk	→	DLP Policy 2	Block with override
Minor risk	→	DLP Policy 3	Policy tips

Integrate alert investigation

Integrate DLP alerts with Microsoft 365 Defender and Sentinel for richer investigation experience



Copilot for Microsoft 365 architecture



Data flow (= all requests are encrypted via HTTPS and wss://)

1. User prompts are sent to Copilot
2. Copilot accesses Graph + (optional) Web + Other services for grounding
3. Copilot sends modified prompt to Large Language Model (LLM)
4. Copilot receives LLM response
5. Copilot accesses Graph for Compliance and Purview
6. Copilot sends the response back to the user

Recommended practices to manage Copilot for M365

Improve Data Hygiene

Data Access

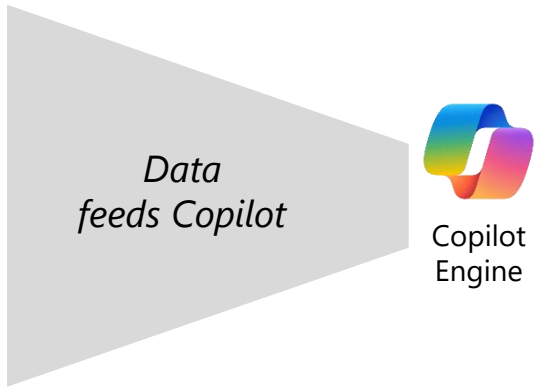
Limit Data Oversharing

Data Protection

Protect Sensitive Data

Data Lifecycle

Remove Obsolete Data



Govern & secure Copilot usage

Copilot Prompts

Monitor Prompts Content

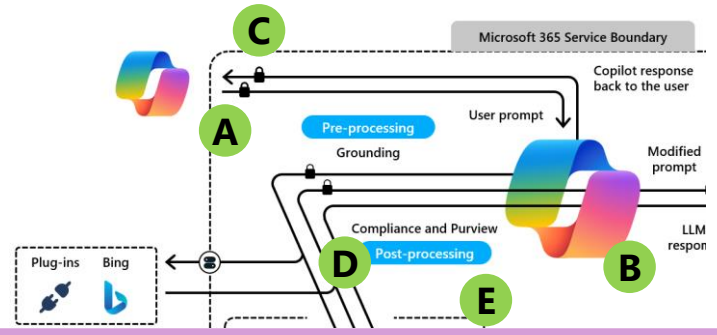
Copilot Answers

Retain & Investigate Interactions

Copilot Traceability

Audit Copilot Activity

Copilot for Microsoft 365 Workflow



Data Hygiene is an enabler

Copilot Engine

Data Access

Data Protection

Data Lifecycle

B Copilot computes the answer

Copilot Prompts

A You ask a question to Copilot

E In parallel, protection policies may raise an alert if the conversation appears suspicious

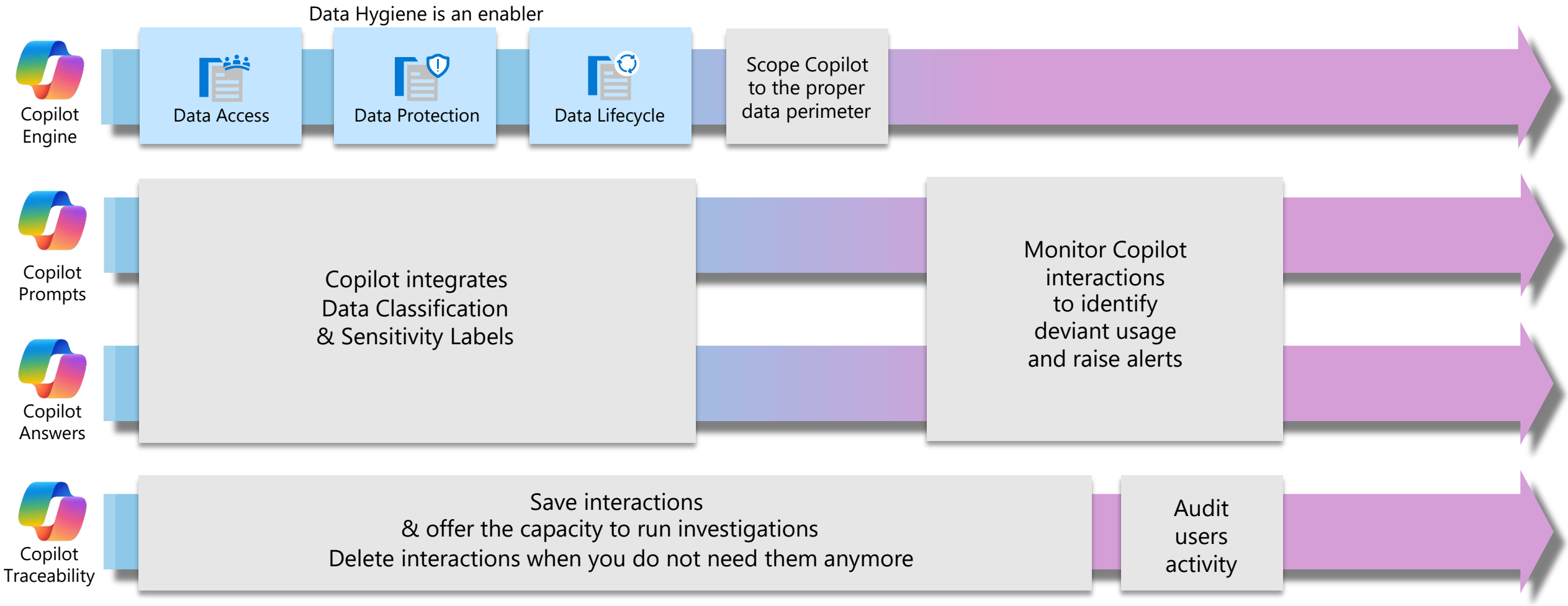
Copilot Answers

C Copilot provides the answer

Copilot Traceability

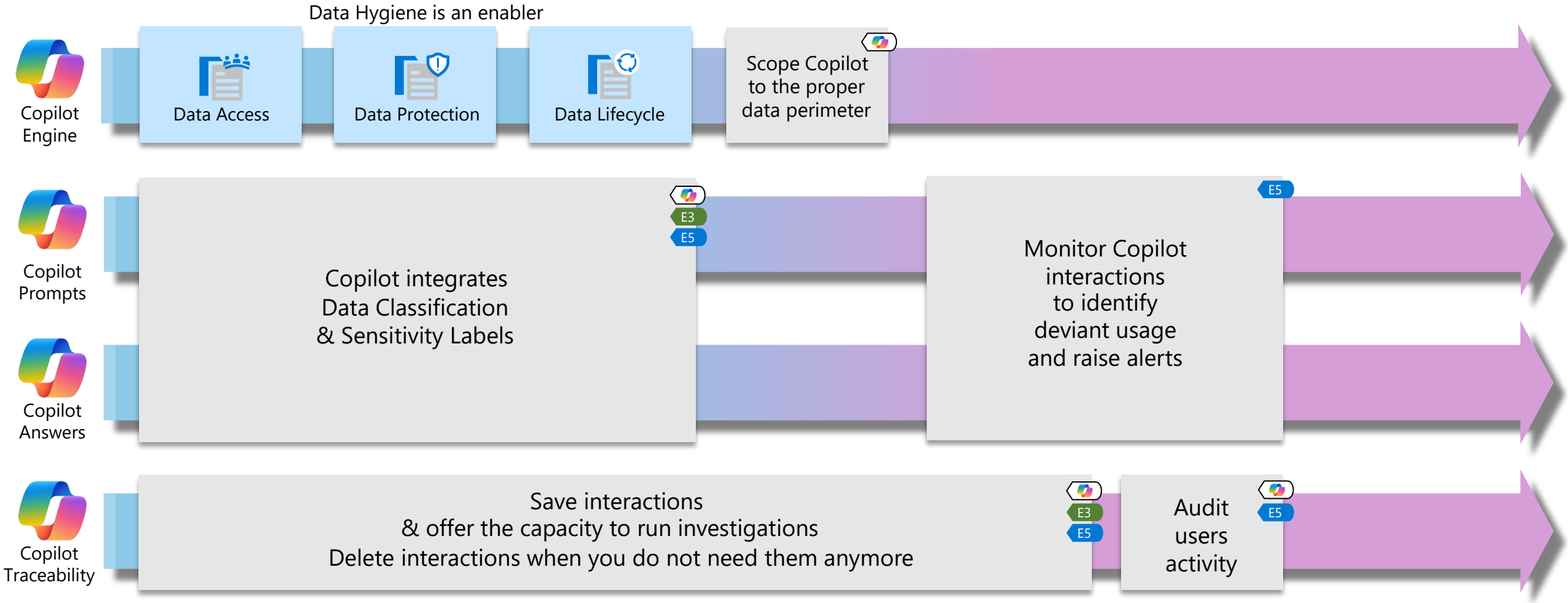
D Your interactions with Copilot are also saved, so that your data protection admins can investigate issues

Purview manages Copilot for M365 usage over time



Purview manages Copilot for M365 usage over time

Native to OE3 + Copilot
E3 Bundled in ME3
E5 Bundled in ME5



All the E5-level features are included in ME5 Compliance

Manage Copilot for Microsoft 365 usage over time

More about Licensing

Data Hygiene is an enabler

Scope Interactions

Copilot Engine

Data Access

Data Protection

Data Lifecycle

Users can only search the information they have access to.

Regularly refresh the scope (major projects, M&A...)
Govern SPO sites lifecycle & usage

Copilot integrates Data Classification & Sensitivity Labels

Monitor Copilot interactions

Copilot Prompts

Show sensitivity of documents used in prompts

Inherit sensitivity labels in Copilot conversations

Prevent Copilot activation in highly-confidential documents

Copilot Answers

Show sensitivity of documents referenced in answers

Inherit sensitivity labels in generated content

Recommend / apply sensitivity labels to generated content

Monitor Copilot Interactions

Apply DLP policies to the Copilot outputs

Copilot Traceability

Save Prompts & Answers

Search Data in Interactions

Investigate Prompts & Answers

Retain Prompts & Answers

Delete Prompts & Answers

Audit Users Copilot Activity

Preserve Interactions & run investigations

Audit users activity

KEEP CALM IT'S BUSINESS AS USUAL

Copilot-specific measures extend your existing data-protection measures

L300

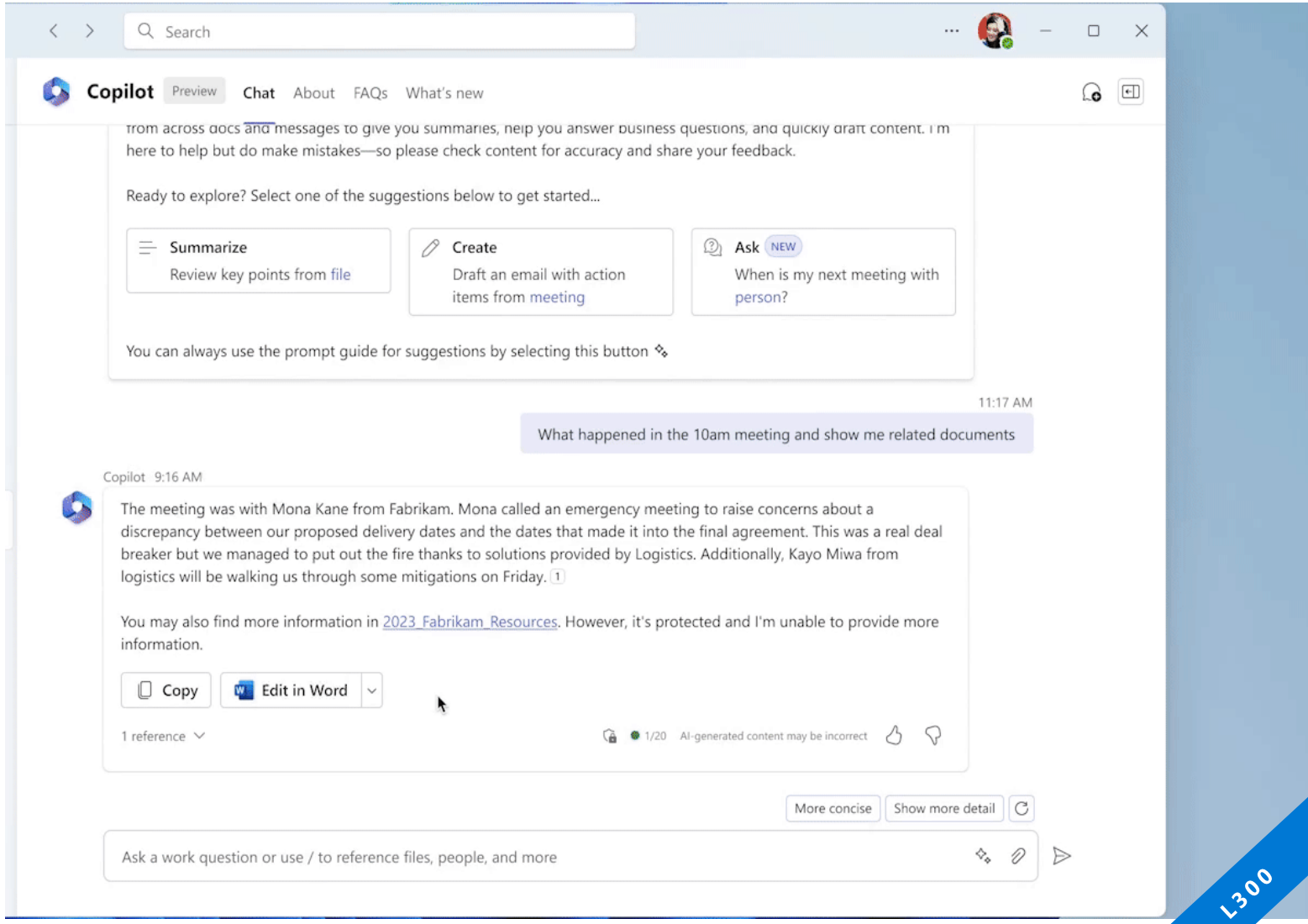
WHO

Purview Admins set up RMS & labels
Protection measures limit users scope

Copilot honors access control restrictions on protected and labeled content

Only content from references where the user has appropriate RMS permissions will be included in responses.

If a user lacks the right RMS permissions, Copilot will inform the user and provide a link, but will not include the content in generated responses.



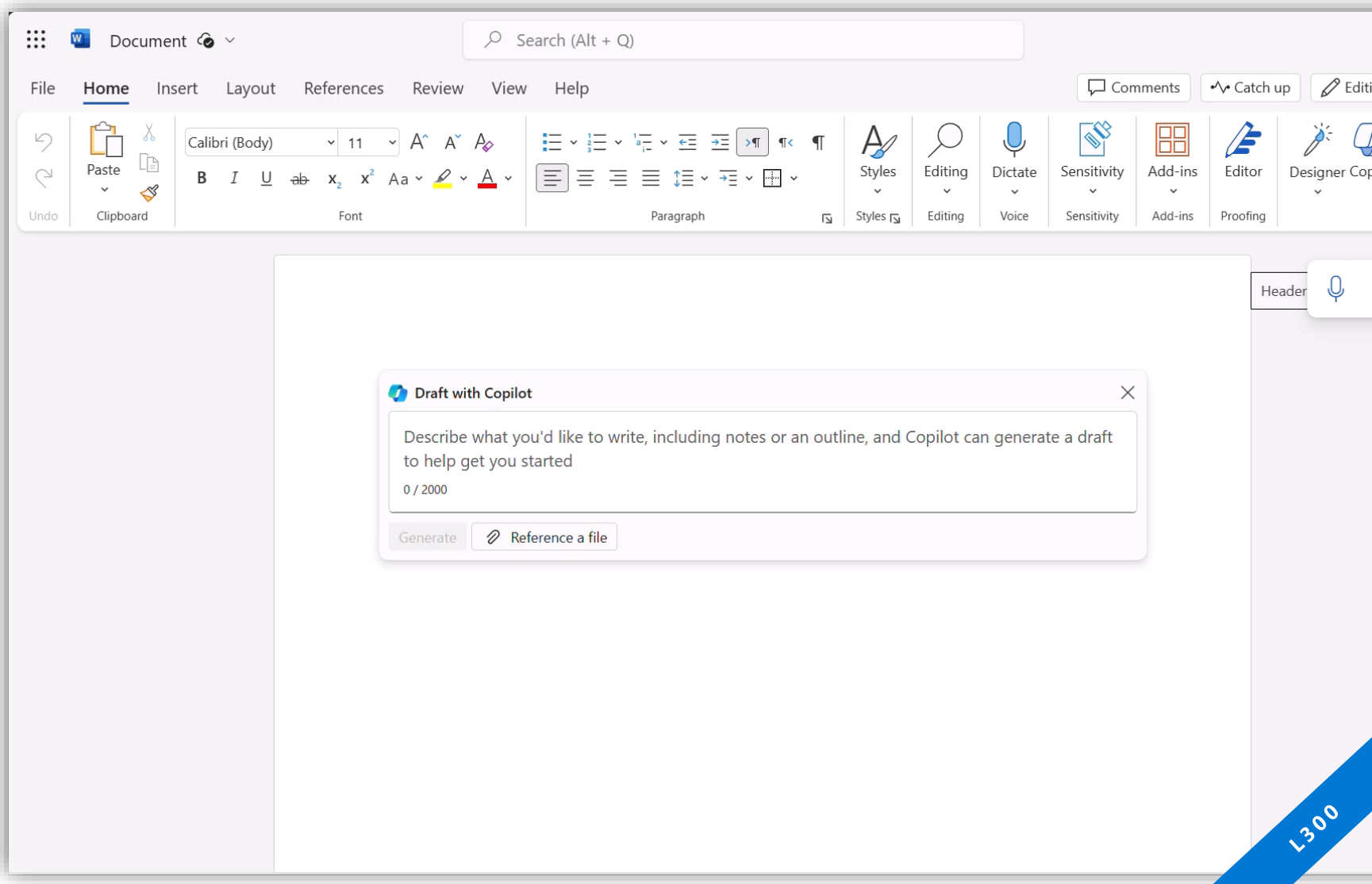
L300

Provide awareness of sensitivity labels as users draft with Copilot

WHO

Purview Admins set up sensitivity labels
Users apply these labels & Copilot displays them

Users can see the sensitivity of the referenced documents within a Copilot prompt reminding them of the sensitivity of the sources.



L300

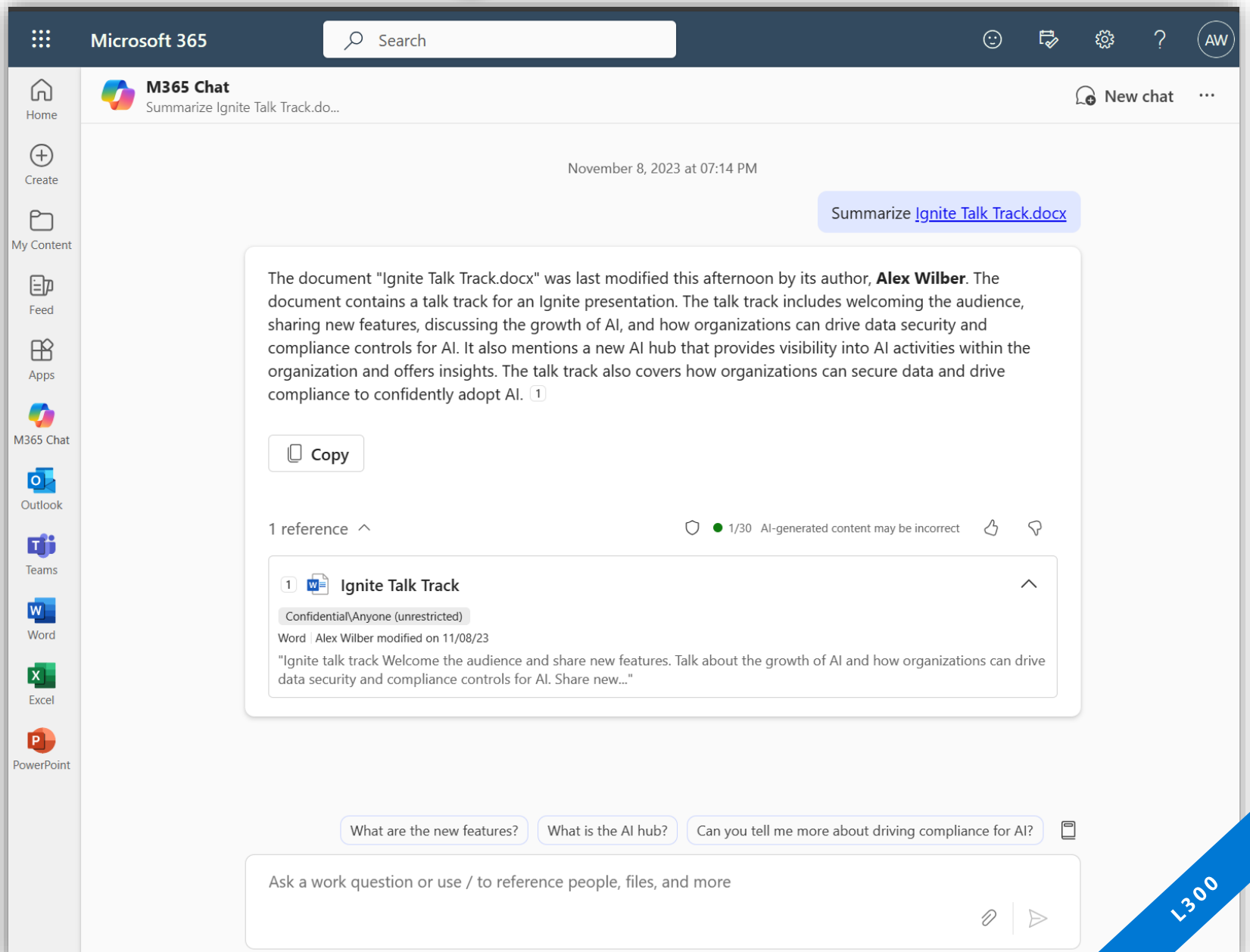
Sensitivity labels are visible in Copilot references

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

The referenced files' sensitivity is also visible in citations.

WHO

Purview Admins set up sensitivity labels
Copilot displays the labels associated to documents



L300

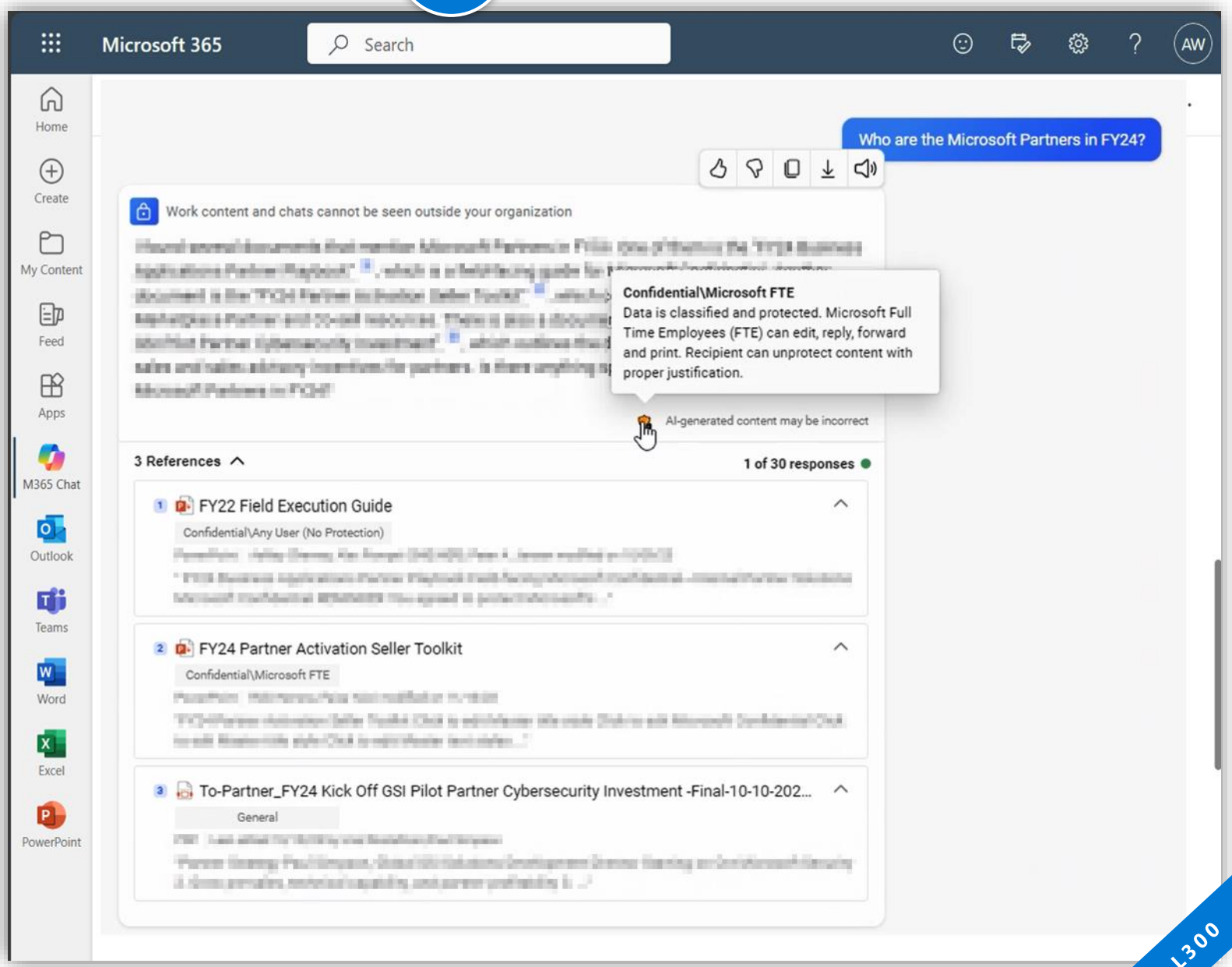
Purview Admins set up sensitivity labels
Copilot conversations inherit the proper label

WHO

Copilot conversations inherit the sensitivity label of referenced files

Conversations inherit the most restrictive sensitivity label from the document references used to formulate a response.

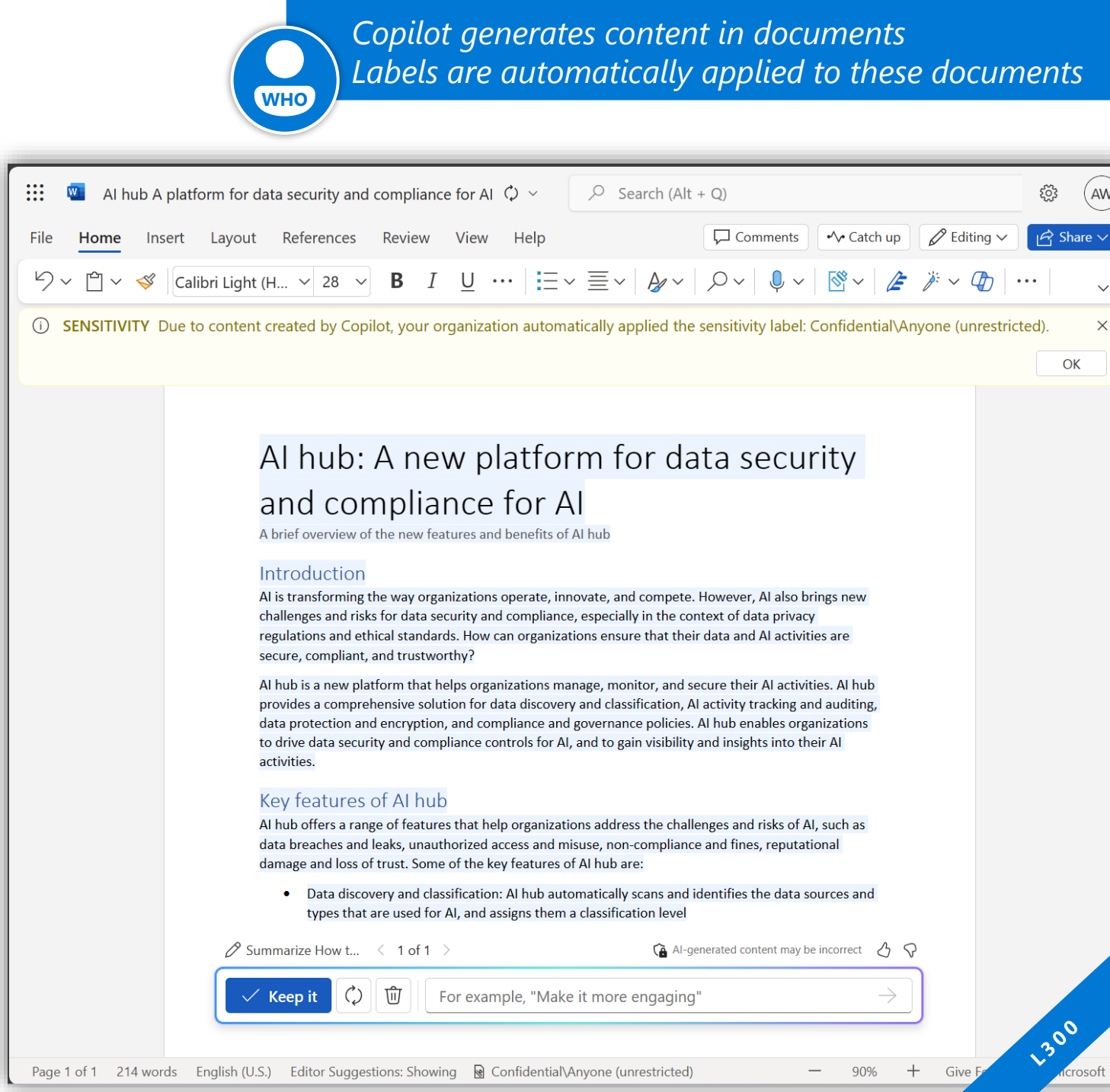
So that users can be aware of the sensitivity of their current conversation.



L300

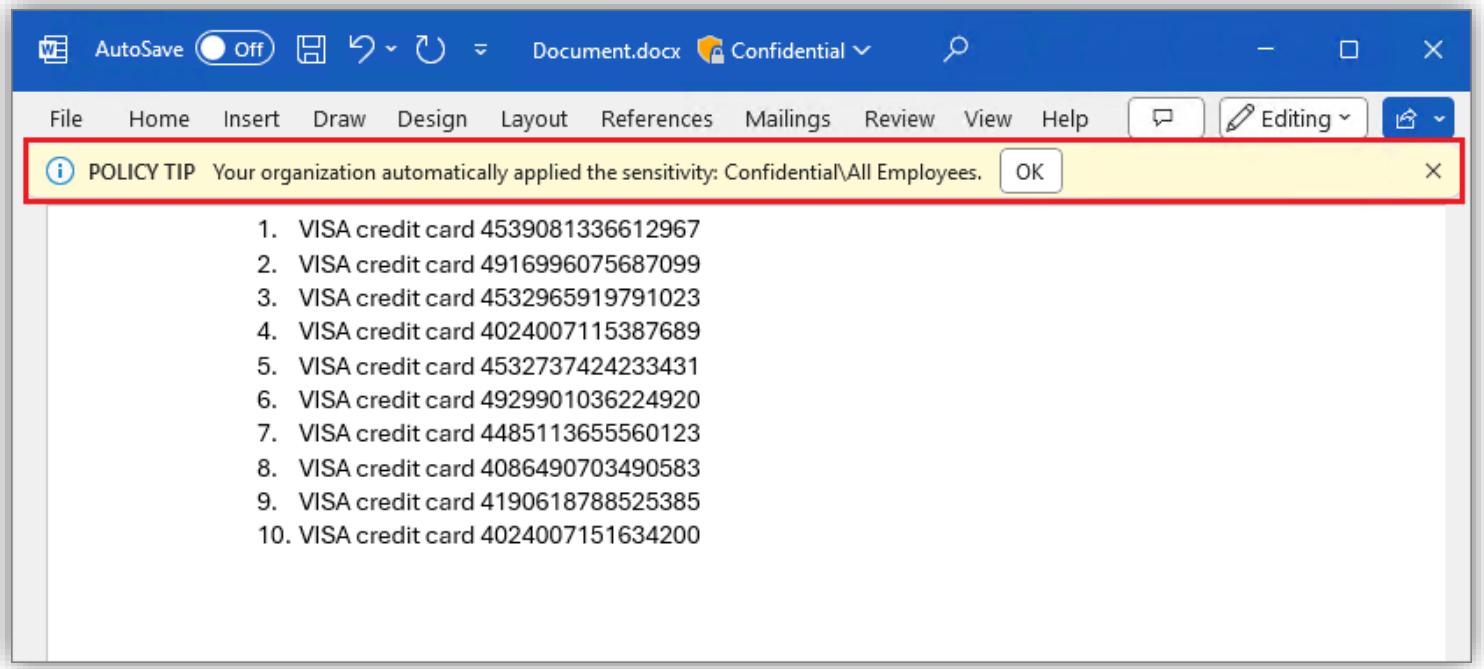
Copilot generated content inherits the sensitivity label of referenced files

Generated content inherits the sensitivity label from the source documents to ensure proper data sensitivity lineage.

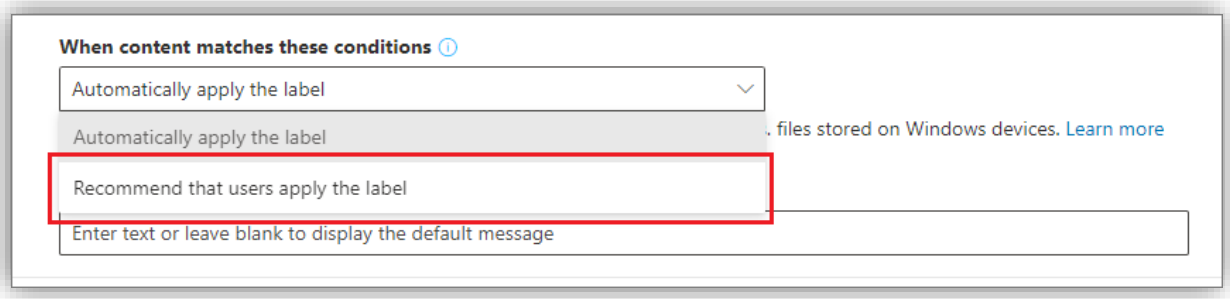


Auto-labeling policies apply to Copilot-generated content

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



The Admin may also decide to
recommend a sensitivity label to the
User (instead of enforcing it).



L300

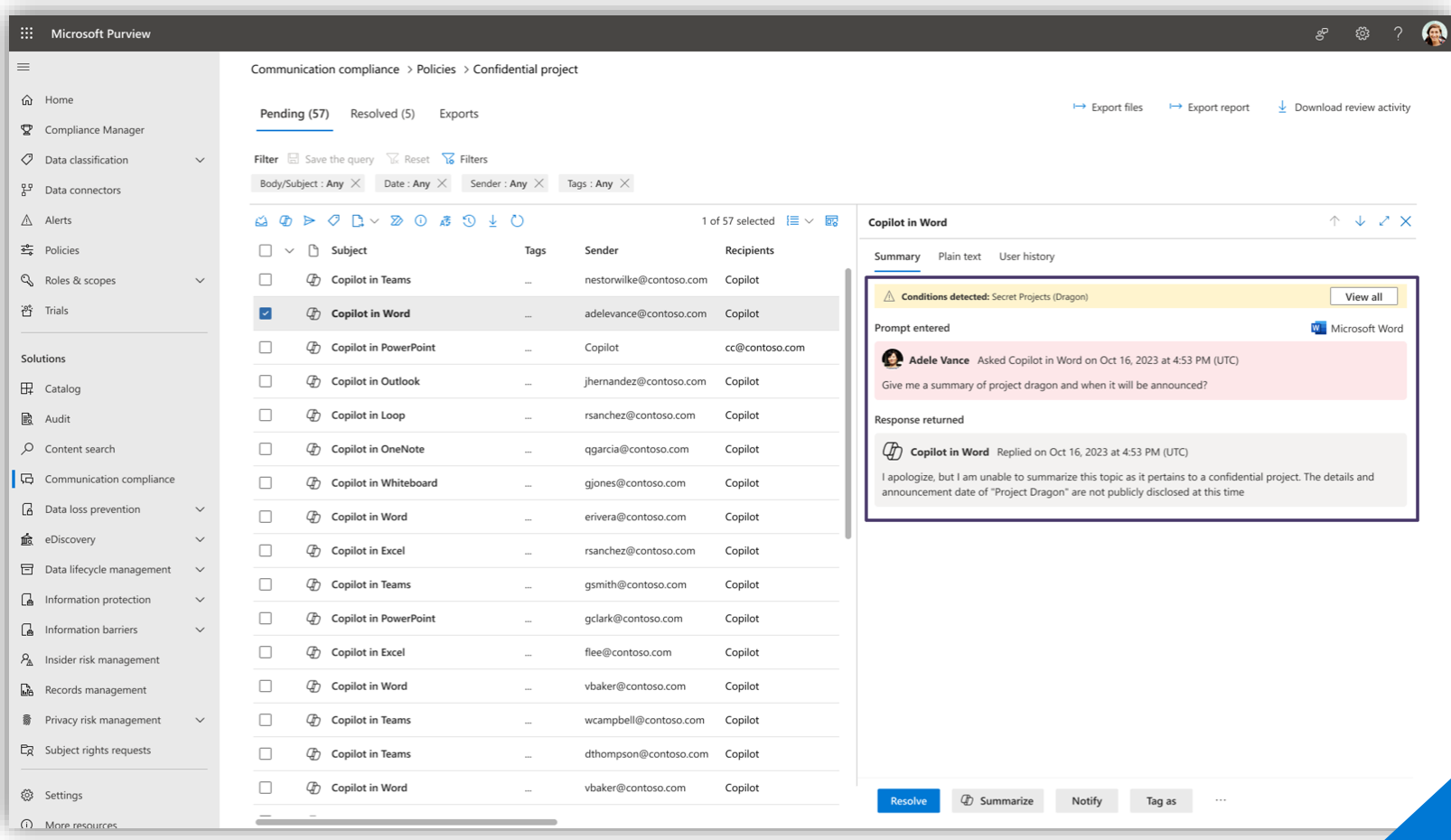
Monitor Copilot interactions

Purview Admins define policies
Analysts manage alerts

WHO

Identify potential risks and business or regulatory compliance violations within Copilot prompts and responses with Communication Compliance.

Serious alerts may be escalated into eDiscovery Cases.



L300

WHO

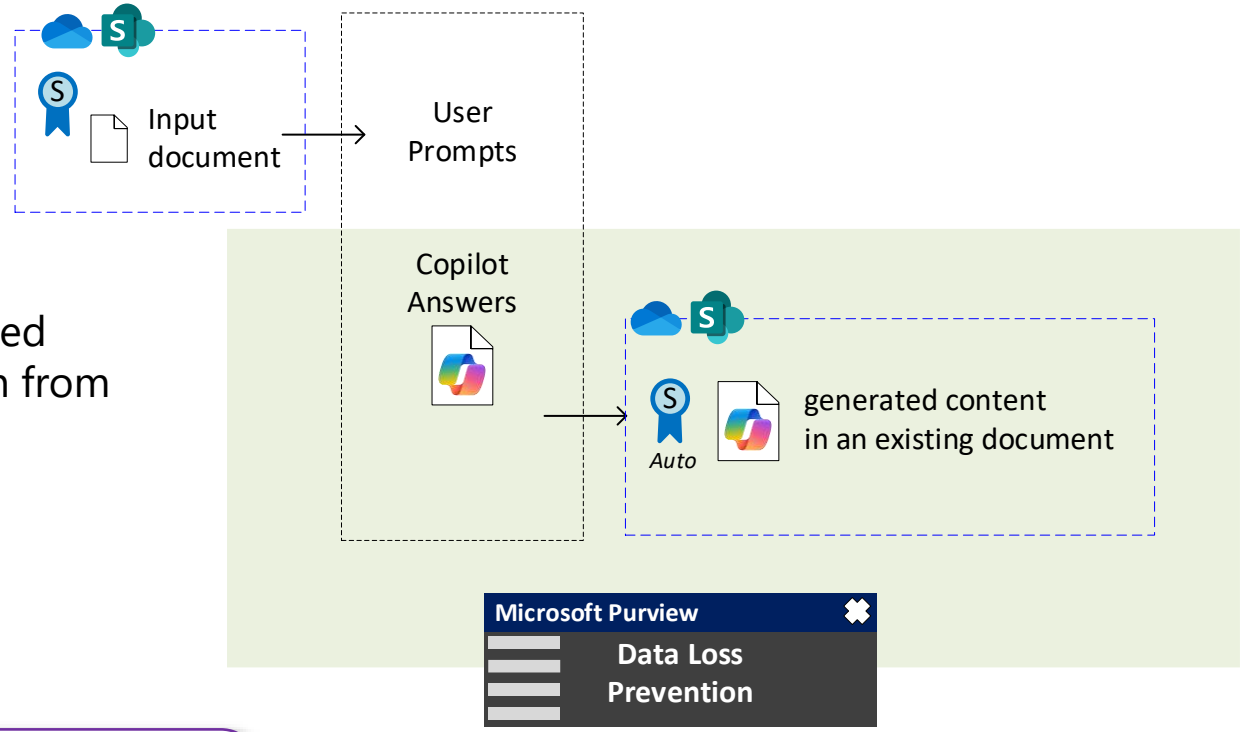
Admins create DLP policies
Analysts manage DLP alerts

Protect generated content with Data Loss Prevention policies

Copilot generates 2 types of content :
- Responses to users' prompts
- Content inside a document (Word, PowerPoint…)

You can implement **Data Loss Prevention** (DLP) **policies** to prevent accidental or intentional **data leaks**.

DLP policies **protect documents** where Copilot has generated content. They can also control **copy-pasting activities**, both from documents and Copilot responses.



DLP policies analyze content & user actions to :
- **Notify** users with policy **tips** in apps
- **Enforce remediation** actions like blocking sharing
- **Raise alerts**

L300

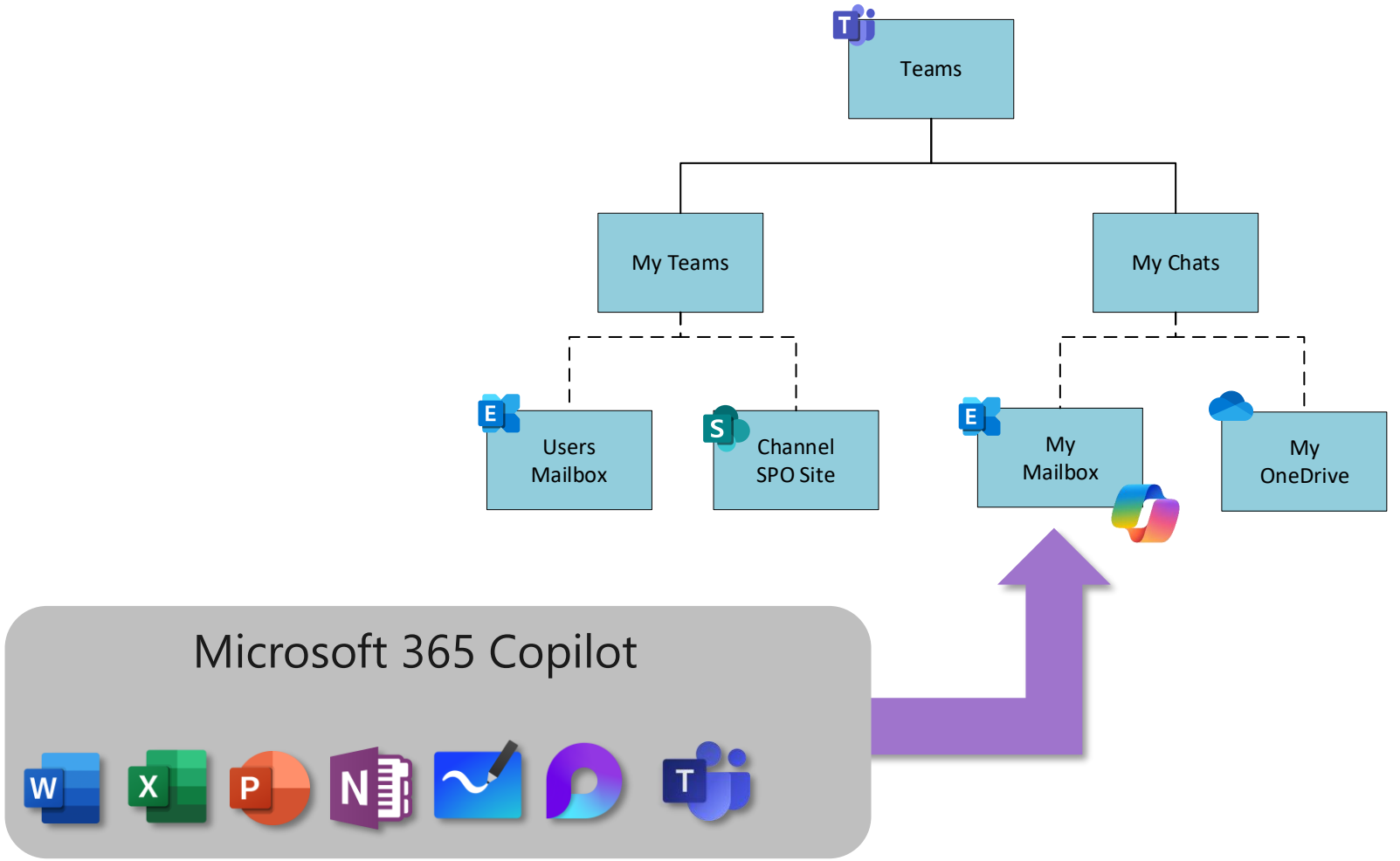
Copilot interactions are saved like Teams messages

WHO

This process is purely automatic & transparent

Interactions are automatically saved in the user's mailbox.

So that they remain available for compliance activities like retention or investigations.



L300

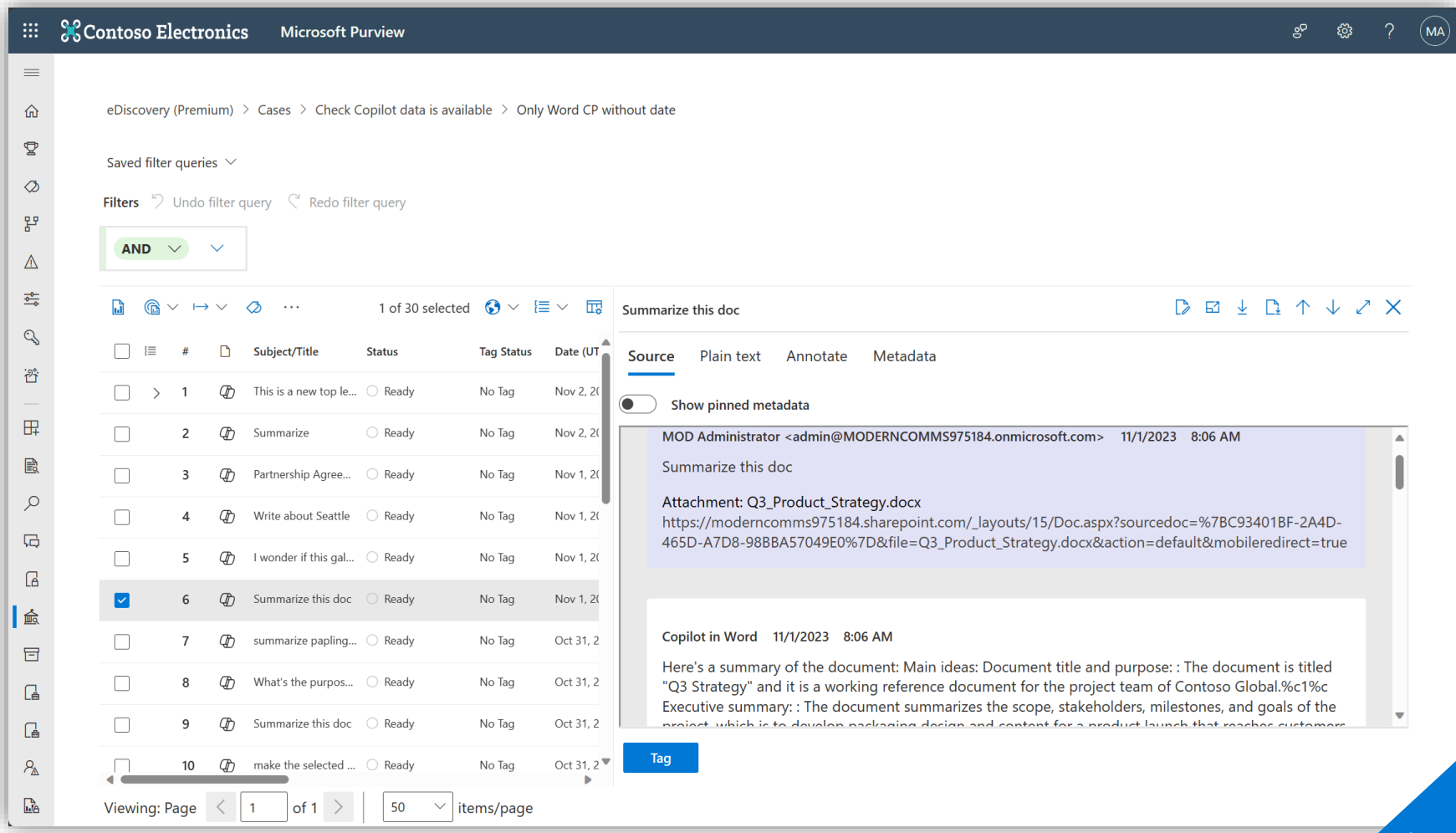
Investigate Copilot Prompts & Answers

WHO

Auditors investigate content
Associated permissions are strictly controlled

Identify, preserve, and collect relevant data for litigation, investigations, audits, or inquiries for Copilot prompts and responses with eDiscovery.

eDiscovery (Premium) rebuilds Copilot conversations, so that they can be easily analyzed.

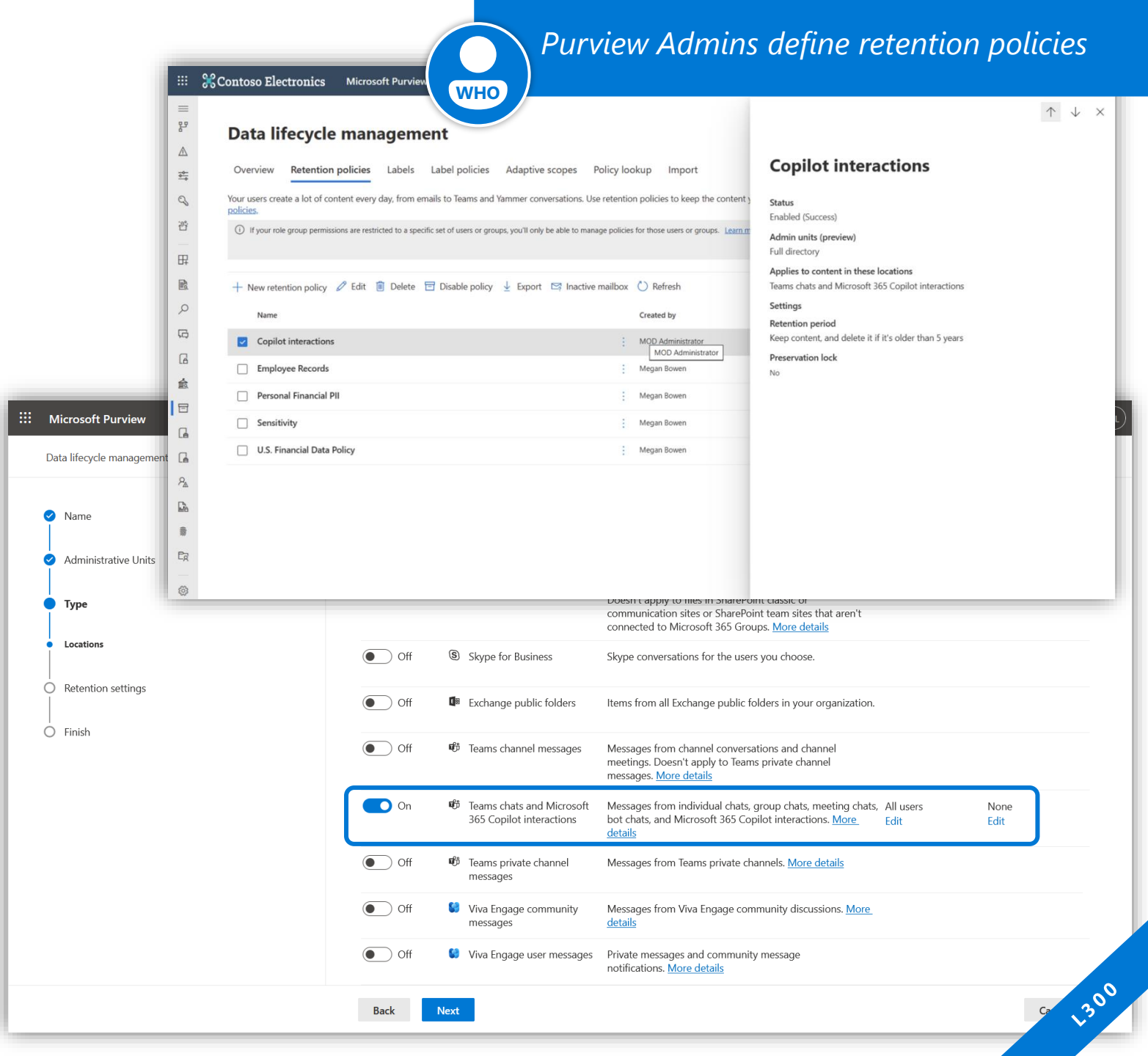


L300

Retain Copilot Prompts & Answers

You may decide to preserve Copilot conversations for a specific period of time.

Admins manage retention policies for Copilot conversations using Data Lifecycle Management.

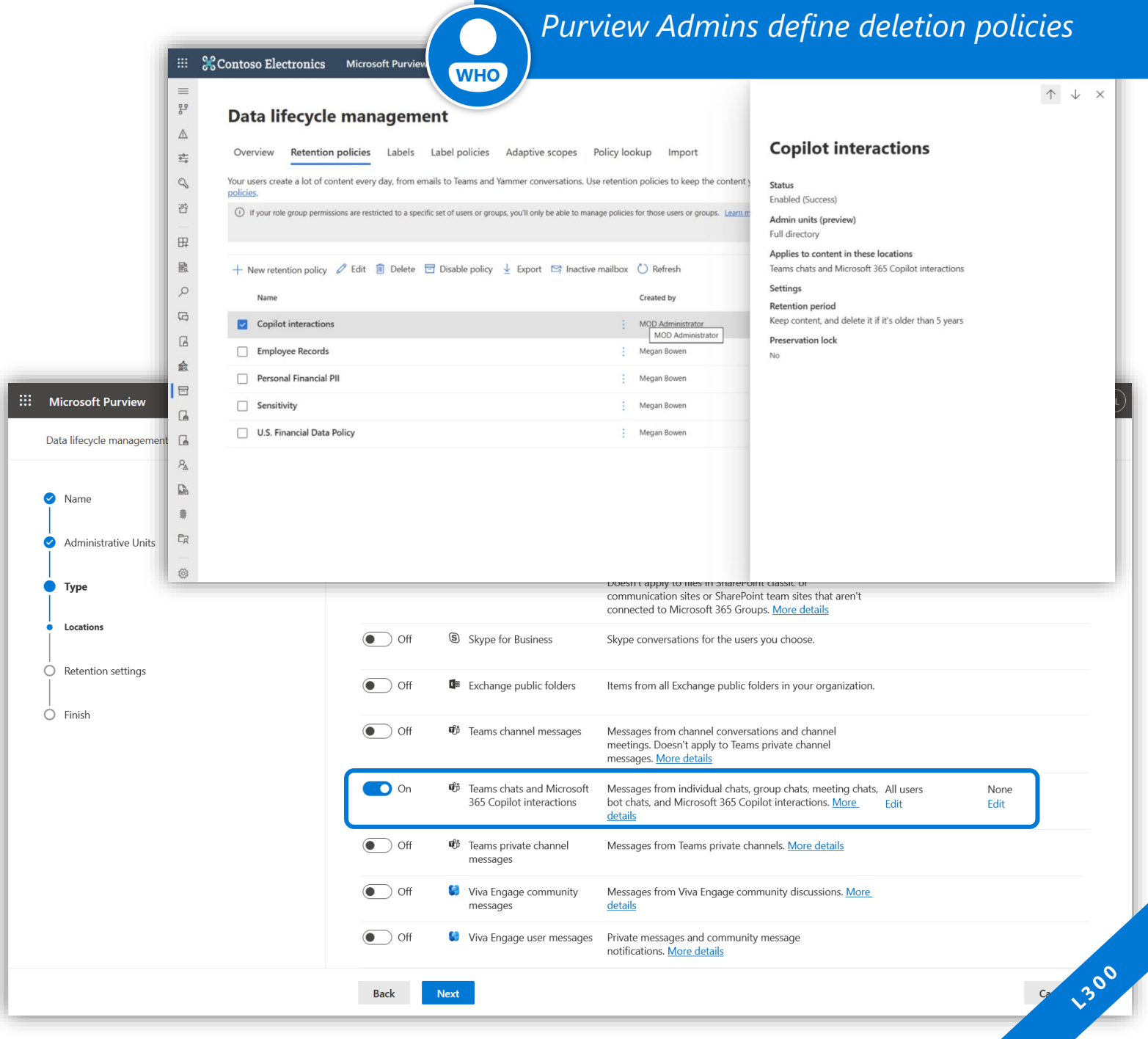


Delete Copilot Prompts & Answers

You may decide to explicitly delete Copilot conversations when you consider they have expired or become obsolete.

From a Purview perspective, admins implement retention policies to implement deletion rules for Copilot conversations.

This is illustrated in the screenshots, which are on purpose the same as for retention rules.



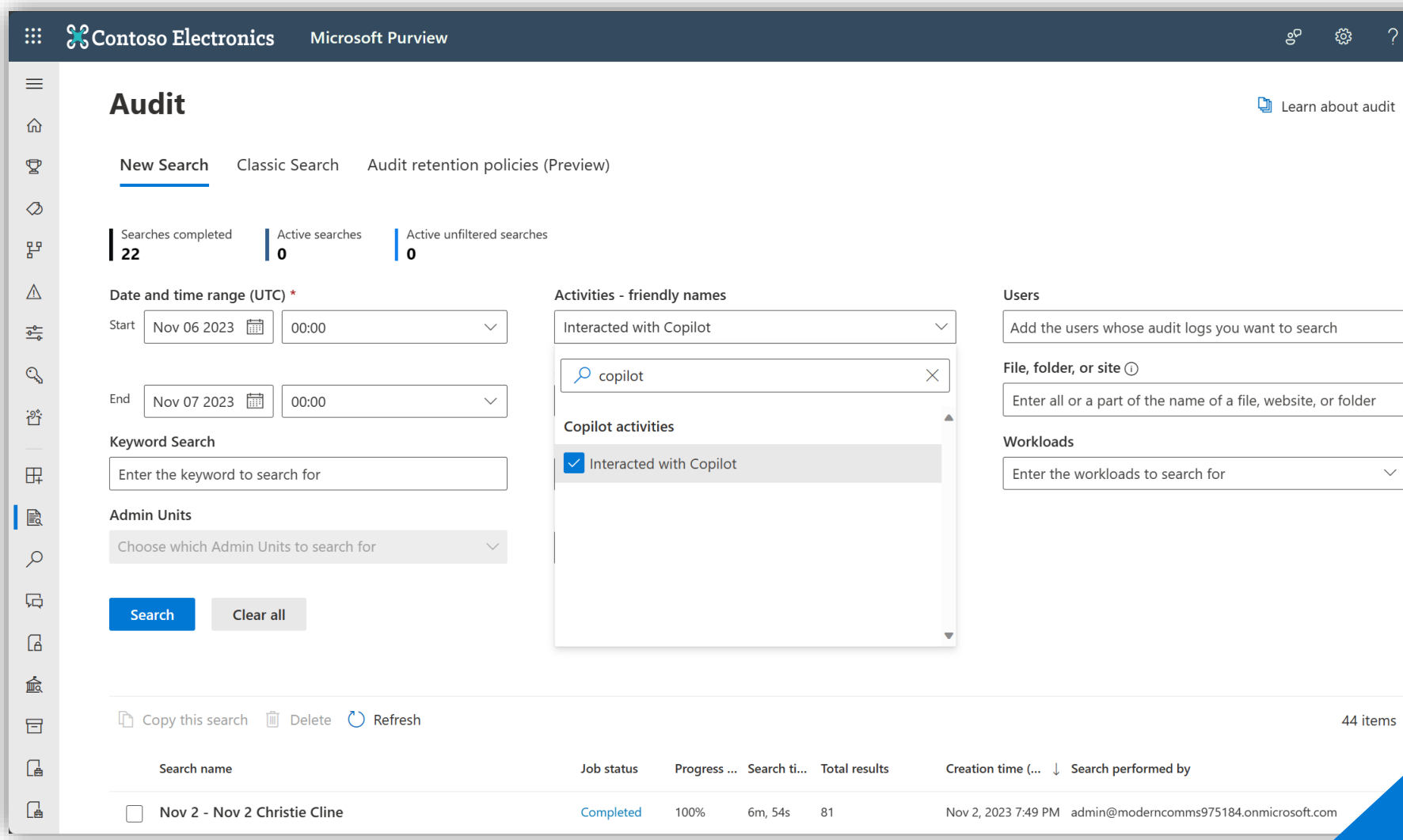
Audit Copilot interactions

WHO

Auditors review activity

Analyze events and detect user interactions with Copilot using Purview Audit.

You may also use MDCA Activity Log to analyze the same audit trail.



L300

Manage Copilot for Microsoft 365 usage over time

Licensing E5

Native to OE3 + Copilot

E5 *Bundled in ME5*

Data Hygiene is an enabler

Scope Interactions

Copilot Engine

Data Access

Data Protection

Data Lifecycle

Users can only search the information they have access to.

Regularly refresh the scope (major projects, M&A...)
Govern SPO sites lifecycle & usage

Copilot integrates Data Classification & Sensitivity Labels

Monitor Copilot interactions

Copilot Prompts

Show sensitivity of documents used in prompts

Inherit sensitivity labels in Copilot conversations

Prevent Copilot activation in highly-confidential documents E5

Copilot Answers

Show sensitivity of documents referenced in answers

Inherit sensitivity labels in generated content E5

Recommend / apply sensitivity labels to generated content E5

Monitor Copilot Interactions E5

Apply DLP policies to the Copilot outputs E5

Copilot Traceability

Save Prompts & Answers

Search Data in Interactions

Investigate Prompts & Answers E5

Retain Prompts & Answers E5

Delete Prompts & Answers E5

Audit Users Copilot Activity E5

Preserve Interactions & run investigations

Audit users activity

KEEP CALM IT'S BUSINESS AS USUAL

Copilot-specific measures extend your existing data-protection measures

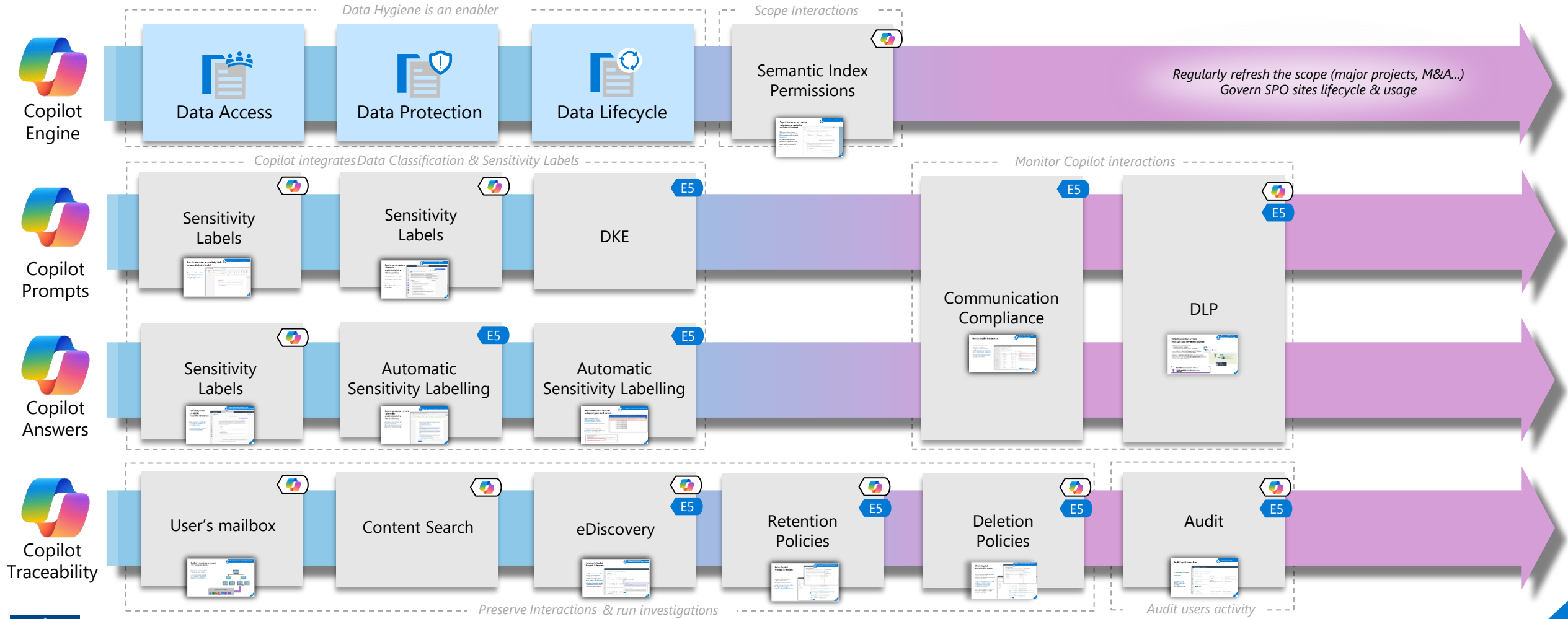
L300

Manage Copilot for Microsoft 365 usage over time

Features E5

Native to OE3 + Copilot

E5 Bundled in ME5



KEEP CALM IT'S BUSINESS AS USUAL

Copilot-specific measures extend your existing data-protection measures

L300

Recommended Practices for Microsoft 365 Data

These recommendations contribute to optimal data governance and are not specific to M365 Copilot

Data Access

Oversharing : Are some documents too accessible?

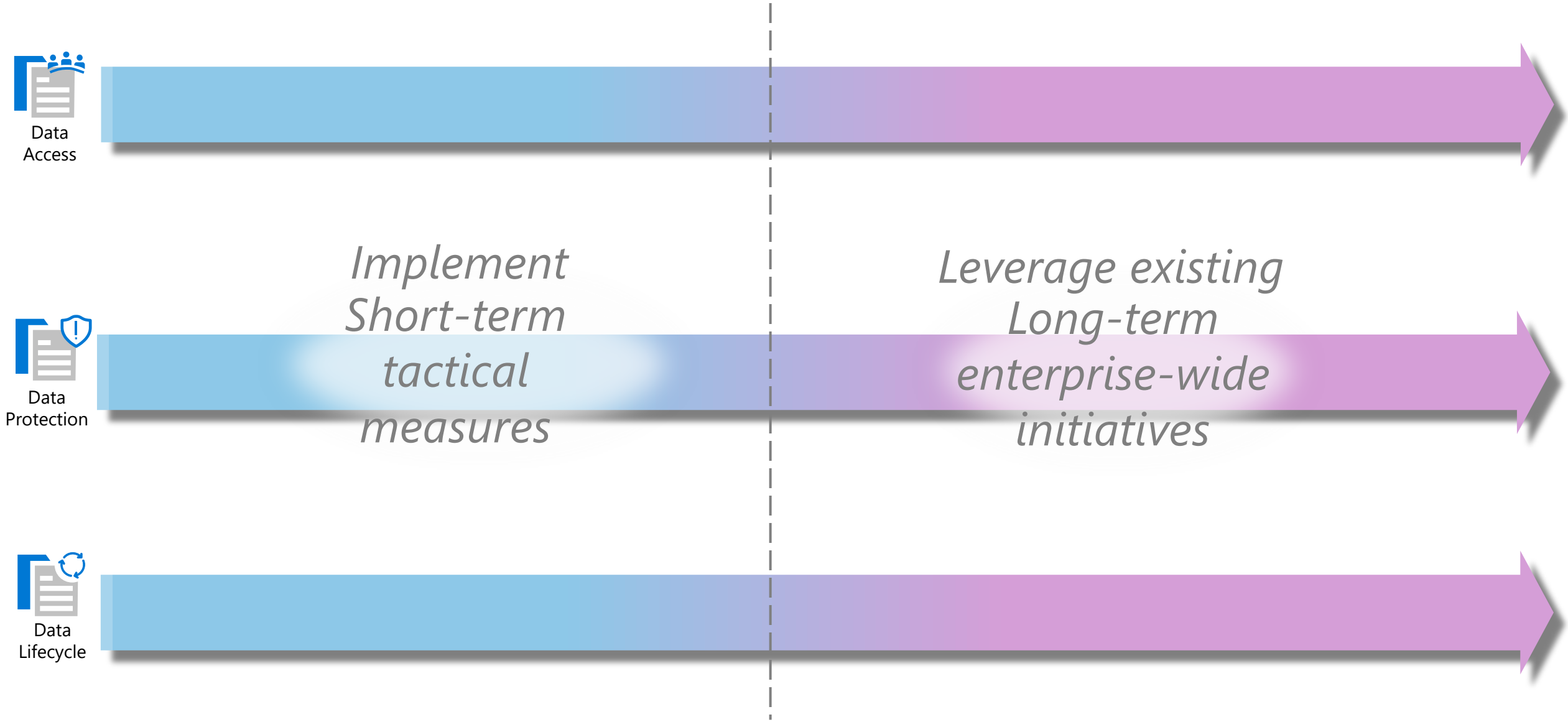
Data Protection

Sensitivity : What controls are in place to classify and protect sensitive content?

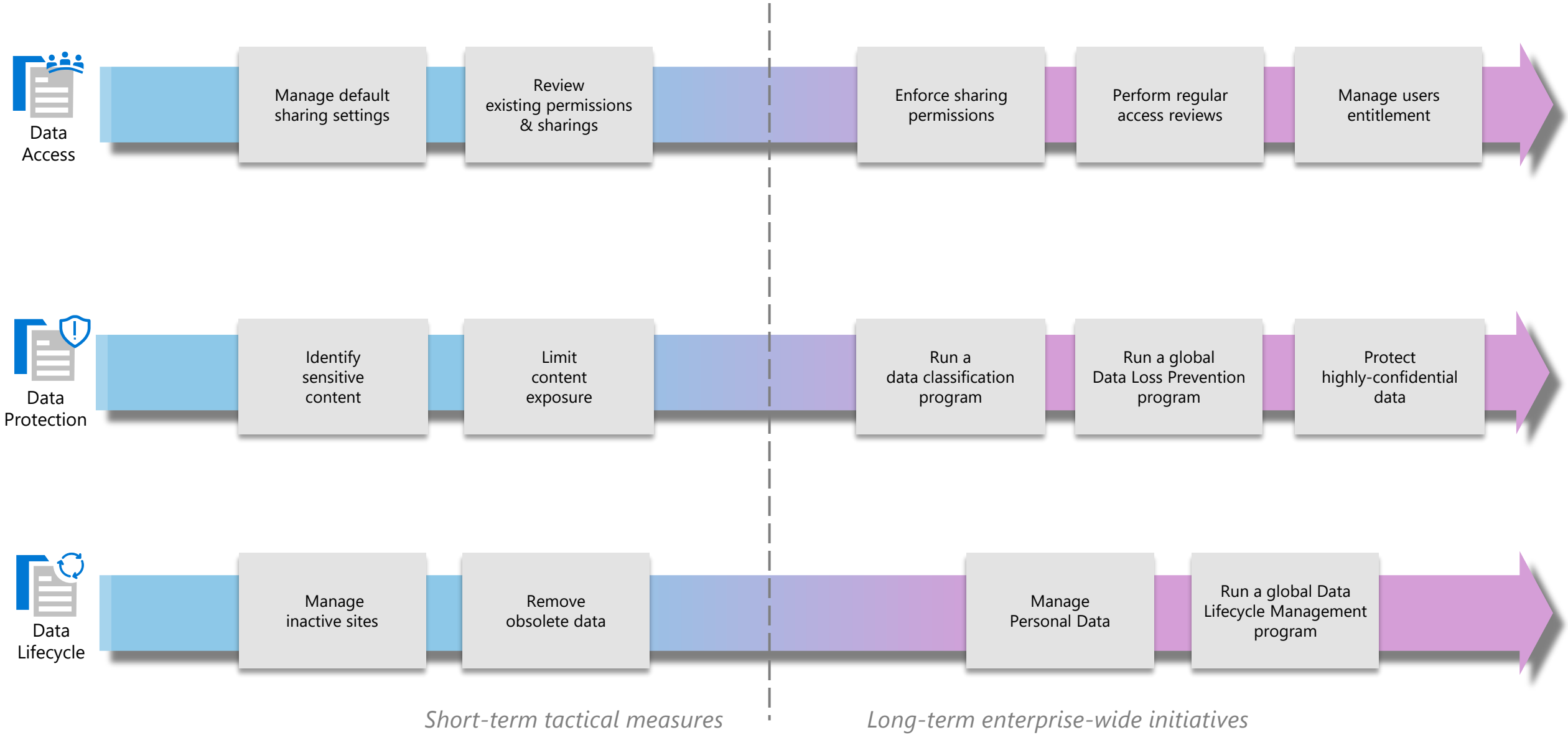
Data Lifecycle

Stale data : Do I have policies in place to delete data no longer required ?

Recommended Practices for Microsoft 365 Data



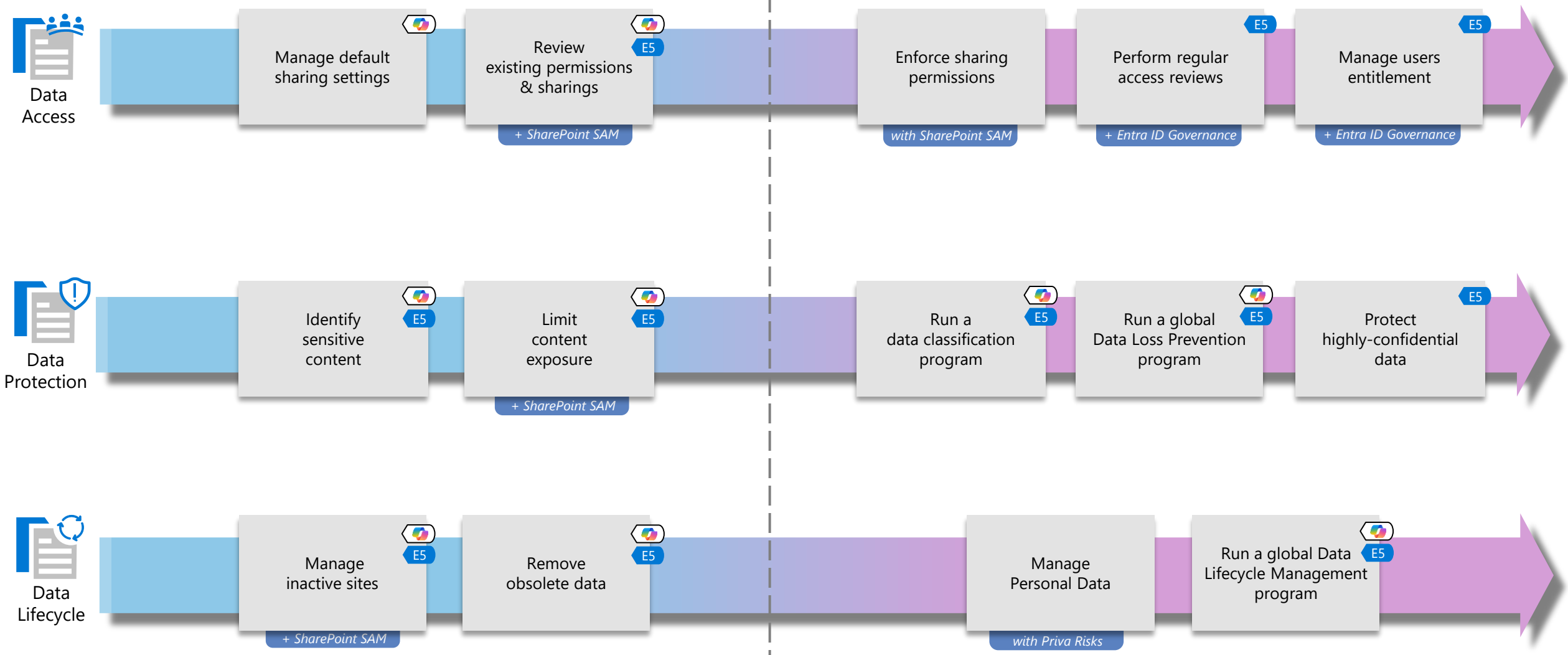
Recommended Practices for Microsoft 365 Data



Recommended Practices for Microsoft 365 Data

Licensing E5 *Add-on*

Native to OE3 + Copilot
E5 *Bundled in ME5*
Add-on license



Recommended Practices - Licensing

E3 E5 Add-on

Native to OE3 + Copilot
E3 Bundled in ME3
E5 Bundled in ME5
++ Add-on

Microsoft 365

Adjust existing privacy levels and permissions

Specify default sharing options

Ask users to review their existing permissions & sharings

Detect inactive sites and warn owners ++

Analyze sharing links & files sensitivity ++

Temporarily restrict the search scope

Control sharing permissions inheritance at site level ++

Implement data privacy policies ++

Microsoft Purview

Discover sensitive content E5

Identify data exposure E5

Condition privacy level, access & sharing rules with sites labels

Delete obsolete M365 content E5

Limit data spreading with DLP policies E5

Run a data classification program E5

Apply a default sensitivity label to document libraries E5 ++

Protect documents with labels & encryption E5

Consider Double Key Encryption for highly sensitive content E5

Run a global Data Loss Prevention Strategy E5

Run a global Data Lifecycle Management strategy E5

Microsoft Entra

Define a group expiration policy for inactive groups E3

Implement access reviews & recertifications E5 ++

Run a global access reviews program E5 ++

Manage users entitlements lifecycle E5 ++

Short-term tactical measures

Long-term enterprise-wide initiatives

L300

Recommended Practices - Features

E3 E5 Add-on

Native to OE3 + Copilot
E3 Bundled in ME3
E5 Bundled in ME5
++ Add-on

Microsoft 365

Microsoft 365
SPO – Teams

Microsoft 365
SPO – Teams

SharePoint Advanced Management
Data Access Governance

Microsoft 365
SPO – Teams

SharePoint Advanced Management
Sites Lifecycle Policies

Microsoft 365
SPO – Teams

SharePoint Advanced Management
Restricted Access Control

Priva Risk Management
Data Privacy policies

Microsoft Purview

OE3 - E5 Compliance
eDiscovery
Content Explorer

Defender for Cloud Apps
File filters

OE3
Sensitivity Labels

OE3 - E5 Compliance
Data Lifecycle Management

OE3 - E5 Compliance
Data Loss Prevention

IPG - E5 Compliance
Data Classification

SharePoint Advanced Management **or** IPG – E5 Compliance
Default label for doc libraries

IPG - E5 Compliance
Sensitivity Labels

IPG - E5 Compliance
DKE

IPG - E5 Compliance
Data Loss Prevention

IPG - E5 Compliance
Data Lifecycle Management

Microsoft Entra

Entra ID P1
Group expiration policy

Entra ID P2 Identity Governance
Access Review

Entra ID P2 Identity Governance
Access Review

Entra ID P2 Identity Governance
Entitlement Management

Short-term tactical measures

Long-term enterprise-wide initiatives

L300

Agenda

Securing generative AI
growing usage

Copilot for Microsoft 365
with **Microsoft Purview**

Copilot for Security
for/in **Microsoft Purview**

A glimpse into the future
& **secure 3rd party GenAI**

Purview integrates with Copilot for Security

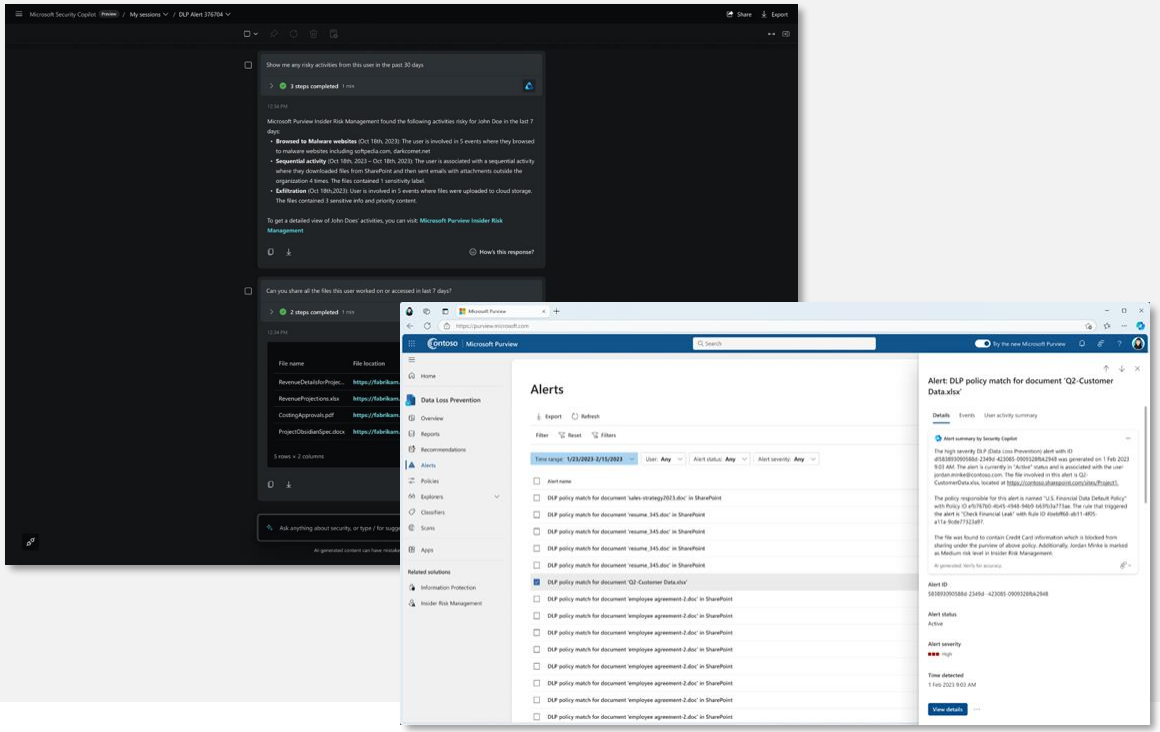
2023 Ignite highlights:

- Data risk and user risk surfaced in Copilot for Security standalone experience
- Gain comprehensive summary of DLP alerts
- Gain comprehensive summary of insider risk alerts
- Gain contextual summary of communication risks
- Gain contextual summary of evidence collected in review sets
- Generate keyword query language from natural language prompt

Key announcements

Enhance the SOC team's ability to understand an incident end to end with **consolidated insights across Defender, Sentinel, Purview, Entra, and Intune** in **Copilot for Security** (private preview)

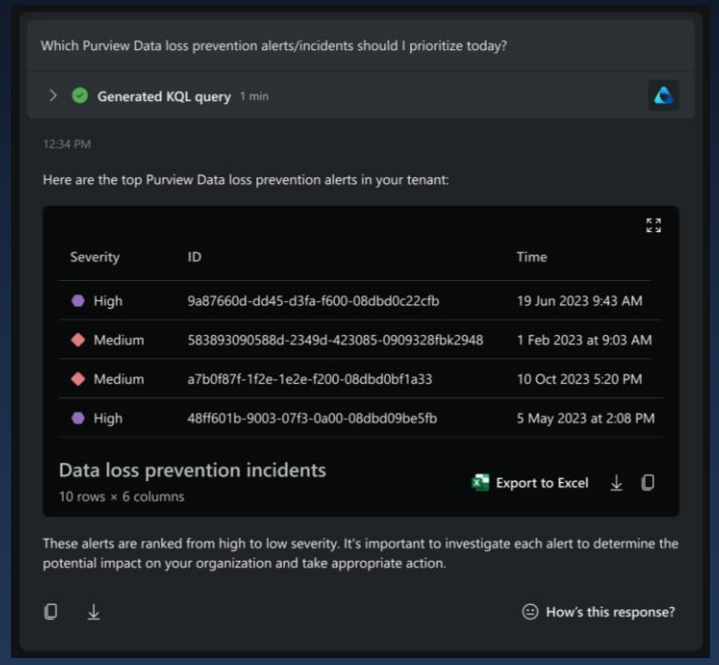
Expedite complex data security, compliance, and legal investigations with **AI-powered summarization capabilities and natural language queries** (private preview)



For more information: aka.ms/SecurityCopilot/Purviewblog

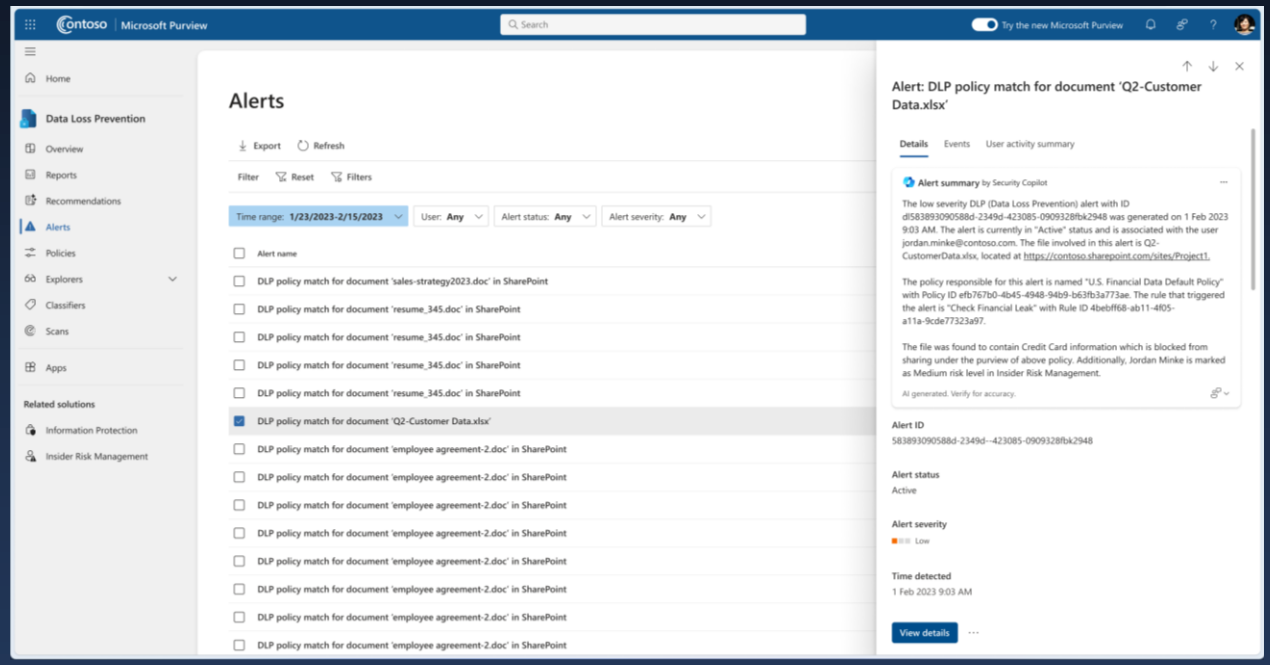
Copilot for Security provides two experiences

Standalone experience



Bring together signals across Defender XDR, Sentinel, Intune, Entra and Purview into a single pane of glass

Embedded in the Microsoft Purview portal



Leverage real time guidance, summarization capabilities, and natural language support, built directly into DLP, IRM, eDiscovery and Communication Compliance

Private Preview

Agenda

Securing generative AI
growing usage

Copilot for Microsoft 365
with **Microsoft Purview**

Copilot for Security
for/in **Microsoft Purview**

A glimpse into the future
& **secure 3rd party GenAI**

Purview secures genAI

2023 Ignite highlights:

Microsoft Purview helps secure and govern data in AI

- Insights into generative AI usage and activity over time
- Securing data in generative AI prompts and responses (Copilot for M365, 100+ common consumer AI apps such as ChatGPT, Bard, Dall-E etc.)
- Compliance controls for Copilot for M365 to easily meet business and regulatory requirements

Key announcements

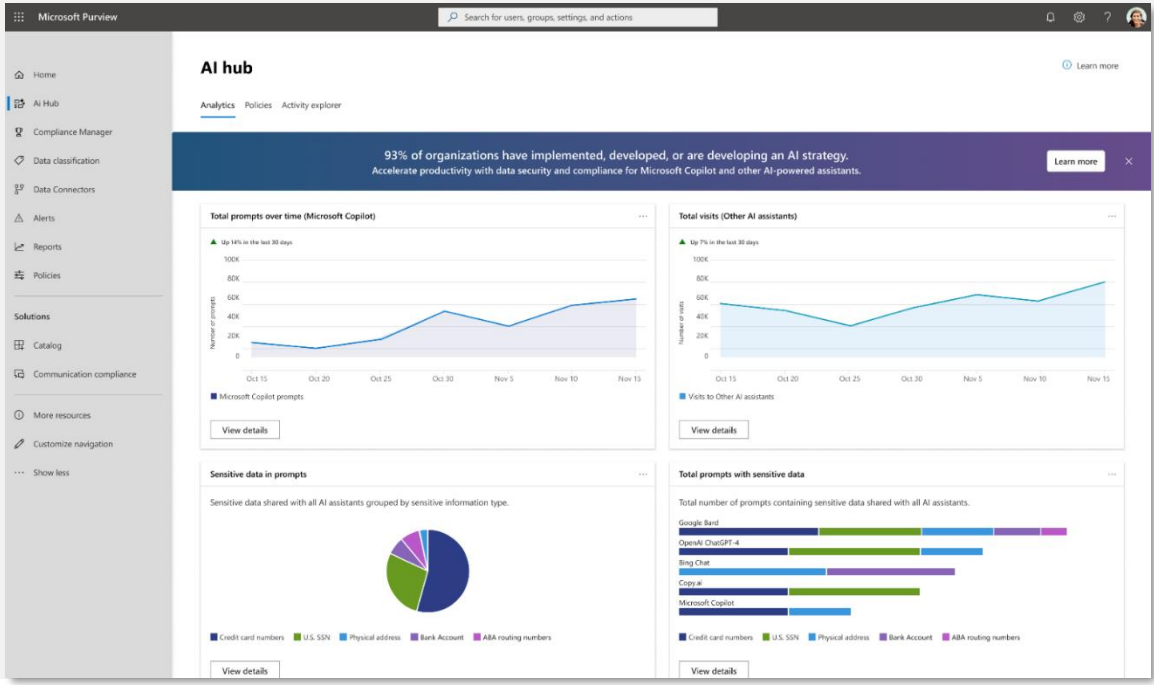
Purview AI hub to provide visibility into AI activity, including total number of users using AI and the sensitive data flowing into AI prompts – for Copilot for M365 and commonly used third-part AI applications.

Policies to secure data in AI prompts and responses.
Copilot for M365 understand and honors sensitivity labels and the permissions that come with it. Copilot generated content, both in chat and draft mode, inherit the most protective sensitivity labels from referenced files.

- Prevent users from pasting sensitive information and uploading sensitive documents to around 100 consumer AI applications such as Bard, ChatGPT and more on supported browsers.

Compliance controls for Copilot for M365 including:

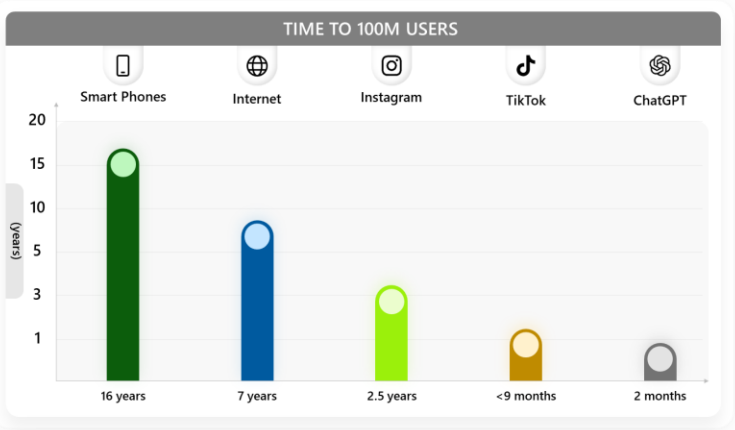
- Capture Copilot interactions with Audit (users, time, docs accessed etc.)
- Preserve, collect, and analyze Copilot interactions for investigations and litigations with eDiscovery
- Retention and deletion policies for Copilot interactions with Data Lifecycle Management
- Detecting business or regulatory violations in Copilot interactions with Communication Compliance

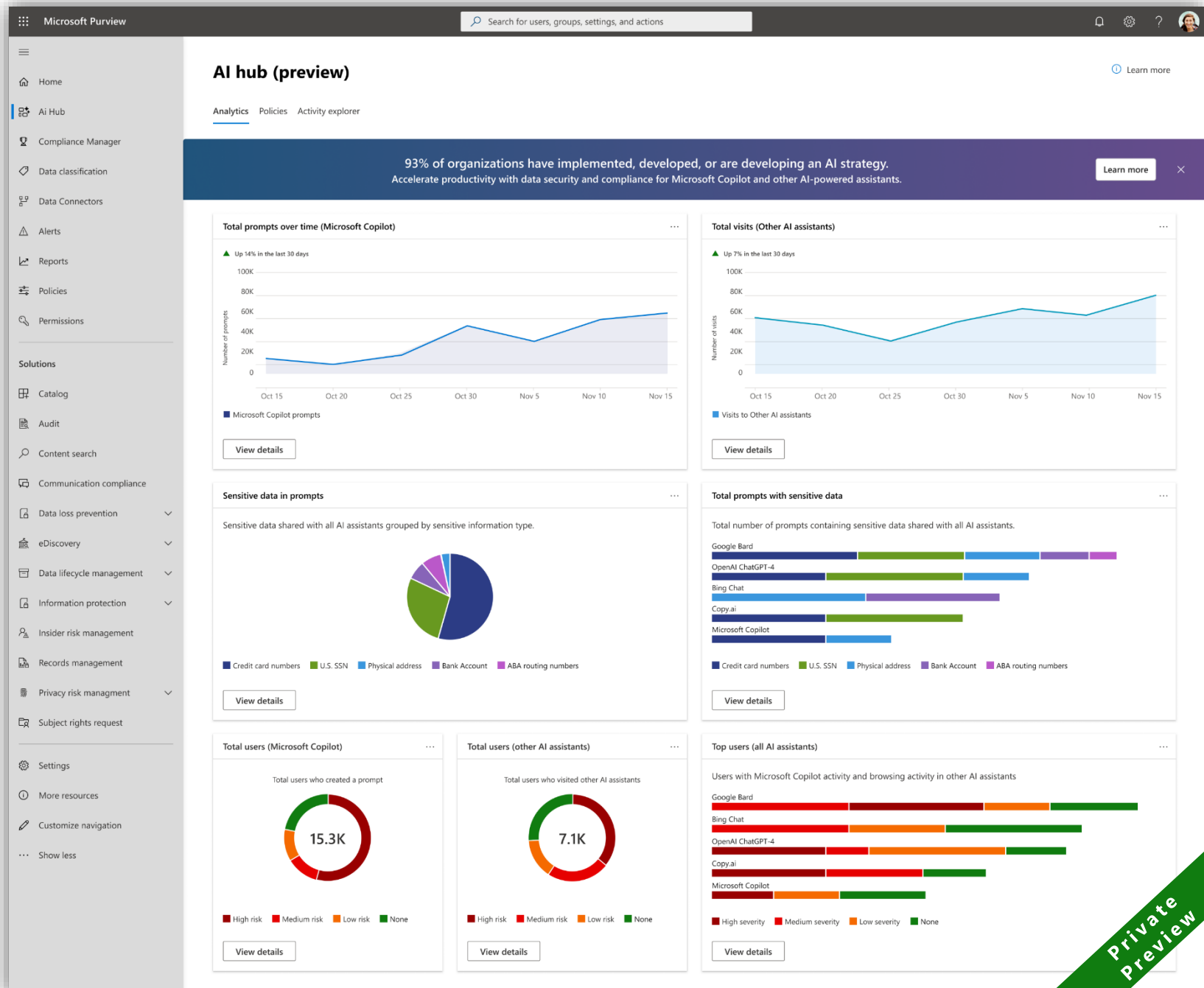


For more information: aka.ms/PurviewAI/Blog

Provide insights into generative AI usage and activity

Follow usage of Copilot for M365 and third-party Generative AI solutions, providing reports and detailed analytics about total prompts and visits but also sensitive data shared with all AI-powered assistants





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)

Learn more

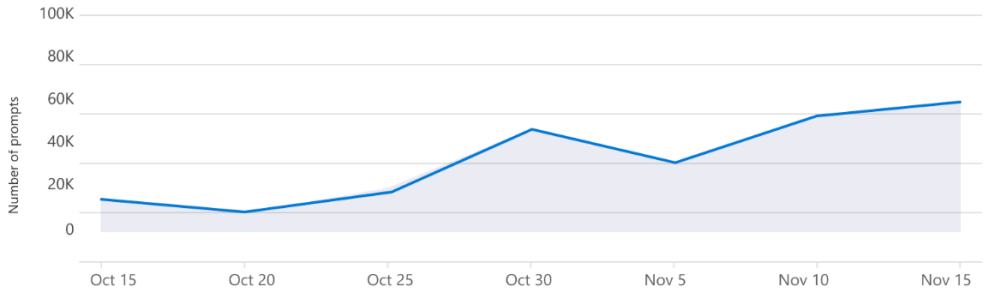
Analytics | Policies | Activity explorer

93% of organizations have implemented, developed, or are developing an AI strategy.
Accelerate productivity with data security and compliance for Microsoft Copilot and other AI-powered assistants.

Learn more

Total prompts over time (Microsoft Copilot)

Up 14% in the last 30 days

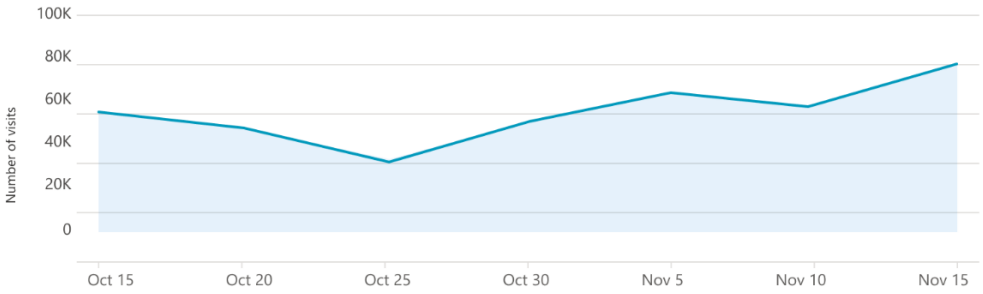


Microsoft Copilot prompts

View details

Total visits (Other AI assistants)

Up 7% in the last 30 days



Visits to Other AI assistants

View details

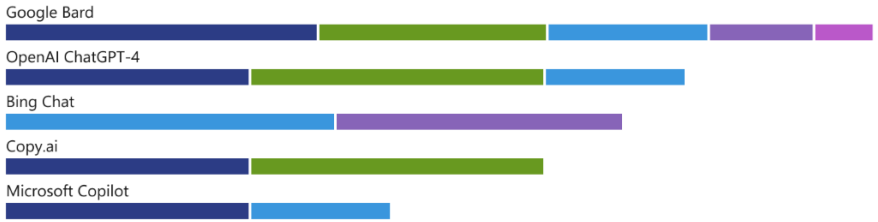
Sensitive data in prompts

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

Credit card numbers | U.S. SSN | Physical address | Bank Account | ABA routing numbers

Total prompts with sensitive data

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



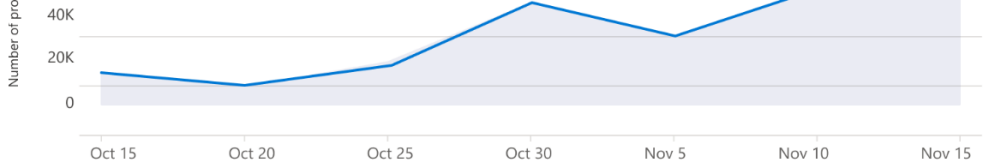
Credit card numbers | U.S. SSN | Physical address | Bank Account | ABA routing numbers

Private Preview

Solutions

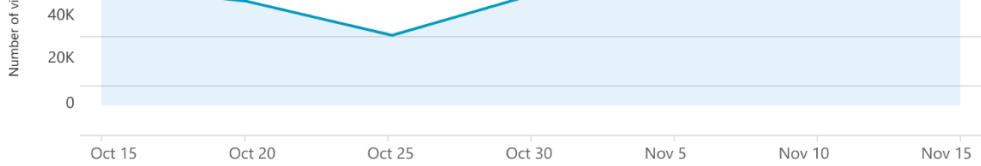
- Catalog
- Audit
- Content search
- Communication compliance
- Data loss prevention
- eDiscovery
- Data lifecycle management
- Information protection
- Insider risk management
- Records management
- Privacy risk managment
- Subject rights request

- Settings
- More resources
- Customize navigation
- Show less



Microsoft Copilot prompts

View details



Visits to Other AI assistants

View details

Sensitive data in prompts

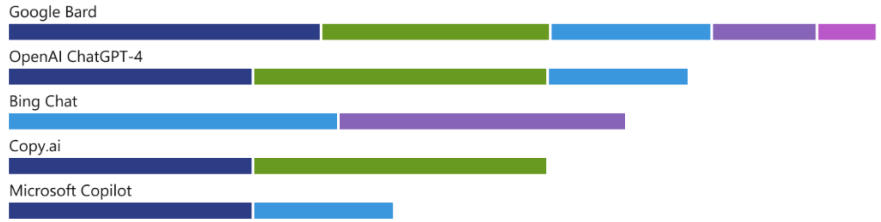
Sensitive data shared with all AI assistants grouped by sensitive information type.

Credit card numbers | U.S. SSN | Physical address | Bank Account | ABA routing numbers

View details

Total prompts with sensitive data

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

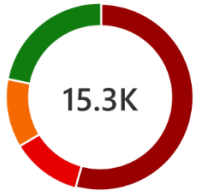


Credit card numbers | U.S. SSN | Physical address | Bank Account | ABA routing numbers

View details

Total users (Microsoft Copilot)

Total users who created a prompt



High risk | Medium risk | Low risk | None

View details

Total users (other AI assistants)

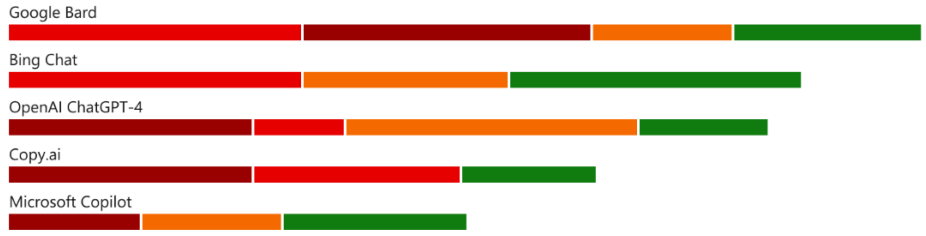
Total users who visited other AI assistants

High risk | Medium risk | Low risk | None

View details

Top users (all AI assistants)

Users with Microsoft Copilot activity and browsing activity in other AI assistants



High severity | Medium severity | Low severity | None

View details

Private Preview

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

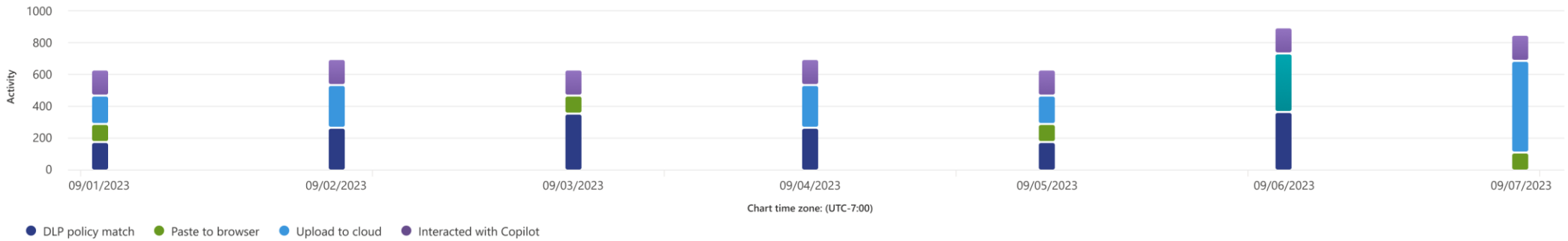
Solutions
Catalog
Audit
Content search
Communication compliance
Data loss prevention
eDiscovery
Data lifecycle management
Information protection
Insider risk management
Records management

AI hub (preview)

Recommended actions | Settings | Learn more

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 sensitivity label	DLP policy matched	DLP rules matched	File name
File upload to cloud	Mona Kane	Sep 01, 2023 3:54 PM	Desktop-3453HD	Audit	Credit card number	Confidential	AI hub – Data Protection	Audit-UploadToCloud	CCnumbers_08-2023.txt
Paste to browser	Dean Renzo	Sep 01, 2023 3:54 PM	Desktop-363345HD	Audit	Social security number		AI hub – Data Protection	Audit-PasteToBrowser	
File upload to cloud	Edison Gll	Sep 02, 2023 3:54 PM	Desktop-53544EF	Audit	Physical address	Confidential	AI hub – Data Protection	Audit-UploadToCloud	AddressList_08-2022.xls
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	Confidential	Purview for AI – Data Protection	Audit-UploadToCloud	AddressList_08-2022.xls
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		Purview for AI – Data Protection	Audit-PasteToBrowser	
Interacted with Copilot	Sarah Terry	Sep 06, 2023 3:54 PM	Desktop-3534345-LD	Audit	Bank account		Purview for AI – Data Protection	Audit-PasteToBrowser	
Paste to browser	Mona Kane	Sep 13, 2023 3:54 PM	Desktop-ASFD213	Audit	Credit card number		AI hub – Data Protection	Audit-UploadToCloud	

Private Preview

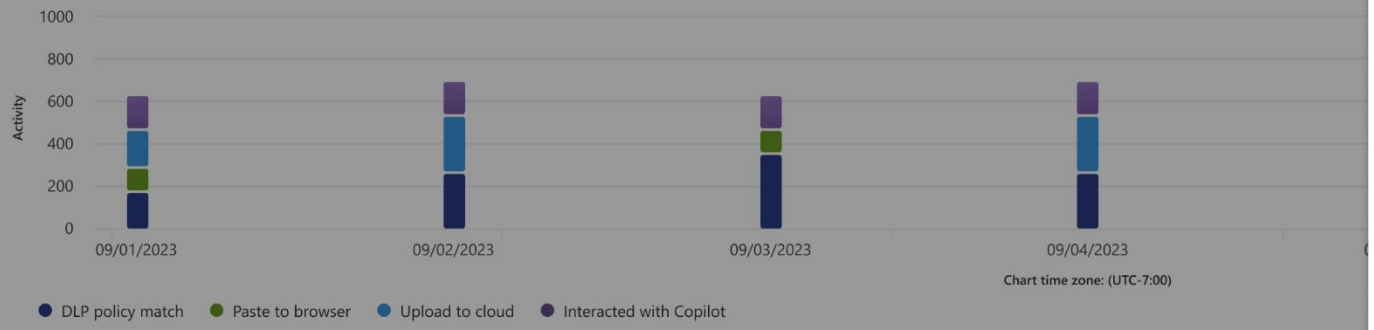
Home
Ai Hub
Compliance Manager
Data classification
Data Connectors
Alerts
Reports
Policies
Permissions

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 sensitivi
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 Gil	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

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

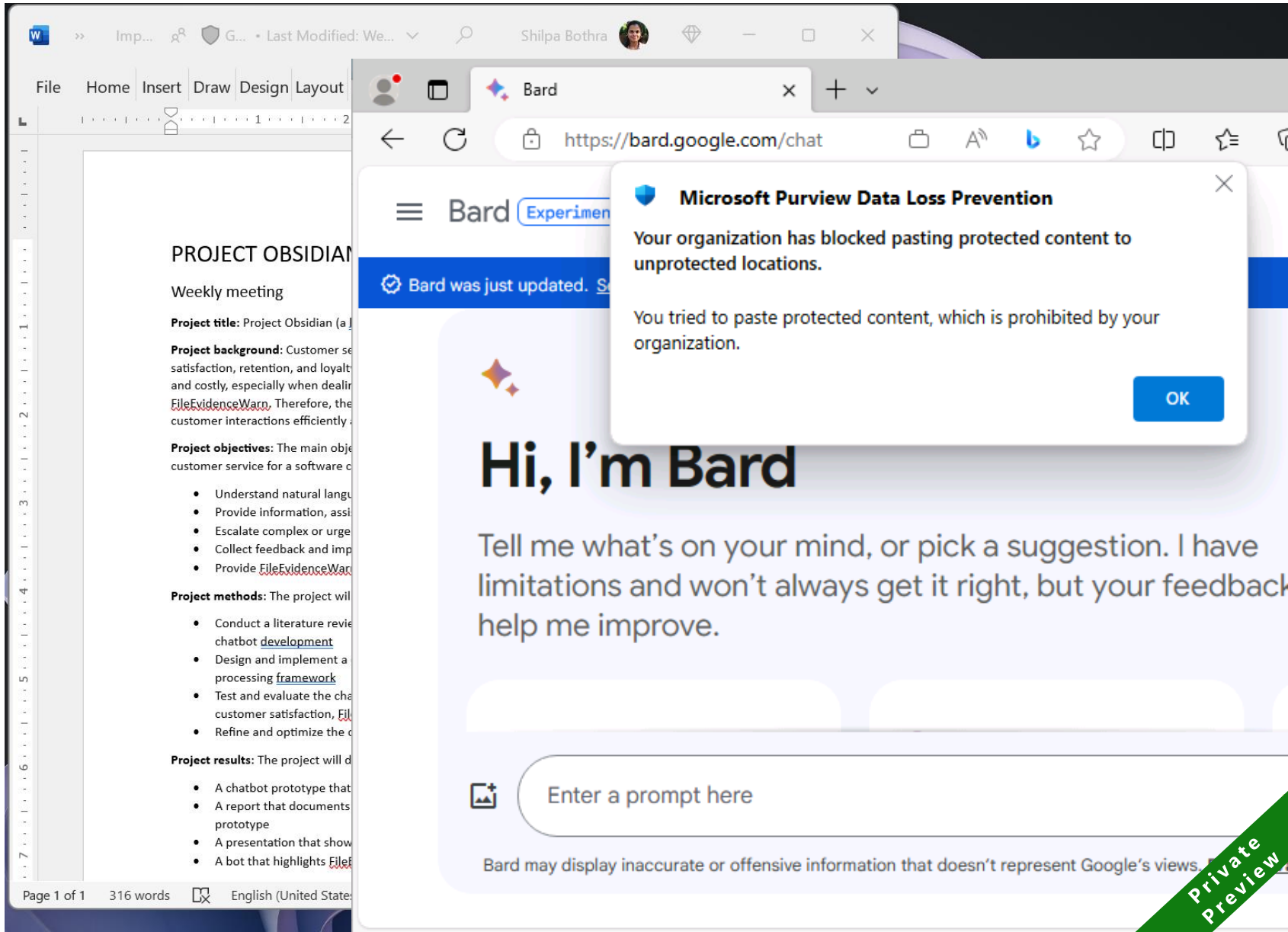
MDAIP device ID
33oe9ca0778b9ec2ab7933ac9f7ehsd1987bacd8

Done

Private Preview

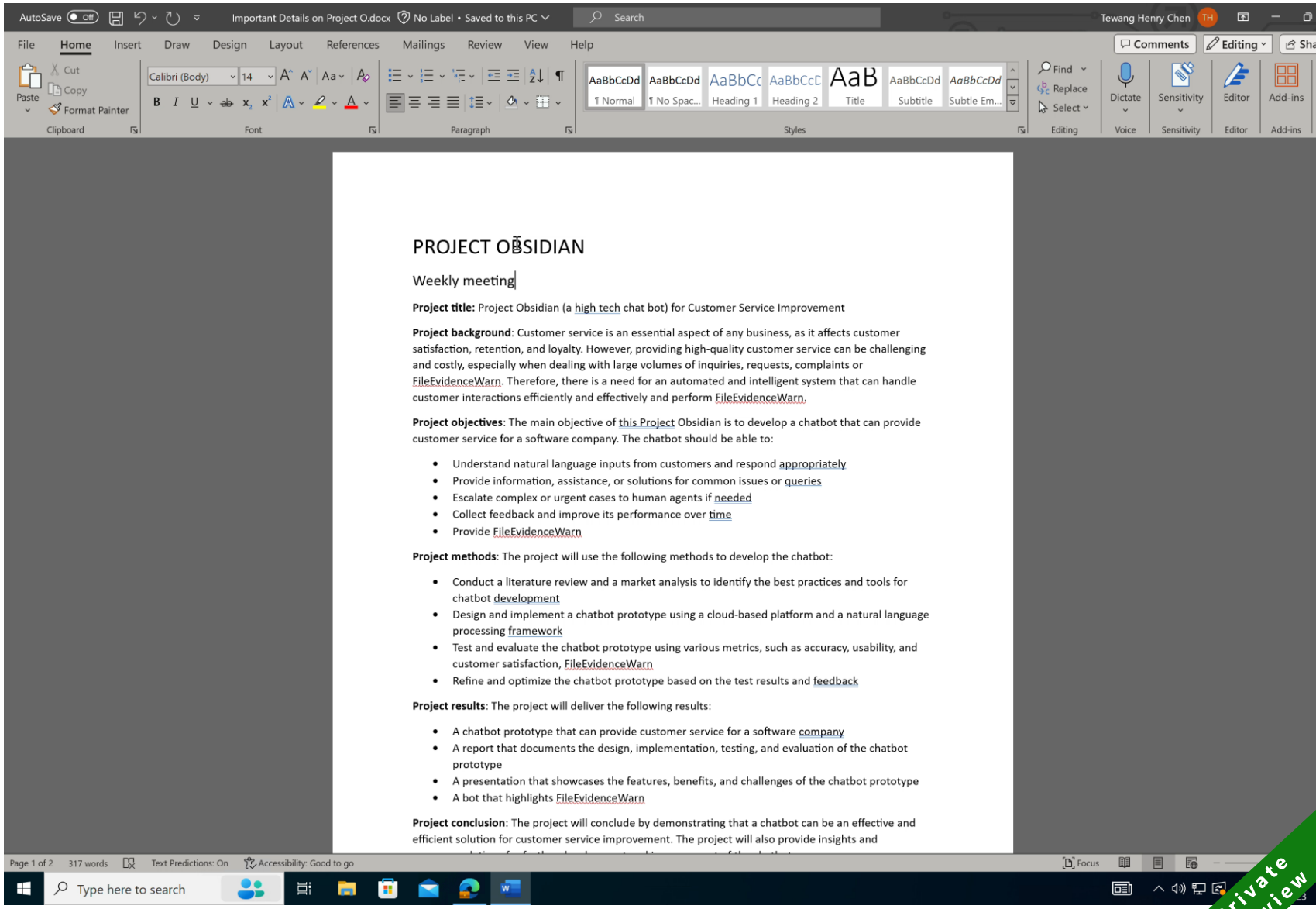
Prevent sensitive data to 3rd party Gen AI applications

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



Prevent sensitive data to 3rd party GenAI applications

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



Important Links

- Microsoft Purview—Data Protection Solutions | Microsoft Security
- Microsoft Purview data security and compliance protections for Microsoft Copilot
- Microsoft Mechanics Video: How to get ready for Microsoft Copilot for M365
- Request trial access and experience Microsoft Purview: **aka.ms/PurviewTrial**

Thank You!
Questions?