

**All we hear is Copilot,
But how to make it
(Data) Secure?**

WORKPLACEDUDES
SUMMIT 2024



DANK AAN ONZE SPONSORS

infinity

PATCH MY PC



venéco
Moving you forward





Tim Hermie

Technical Specialist Data Security

Former Microsoft MVP Enterprise Mobility

Former Windows Insider MVP

Microsoft Most Valuable Mentor

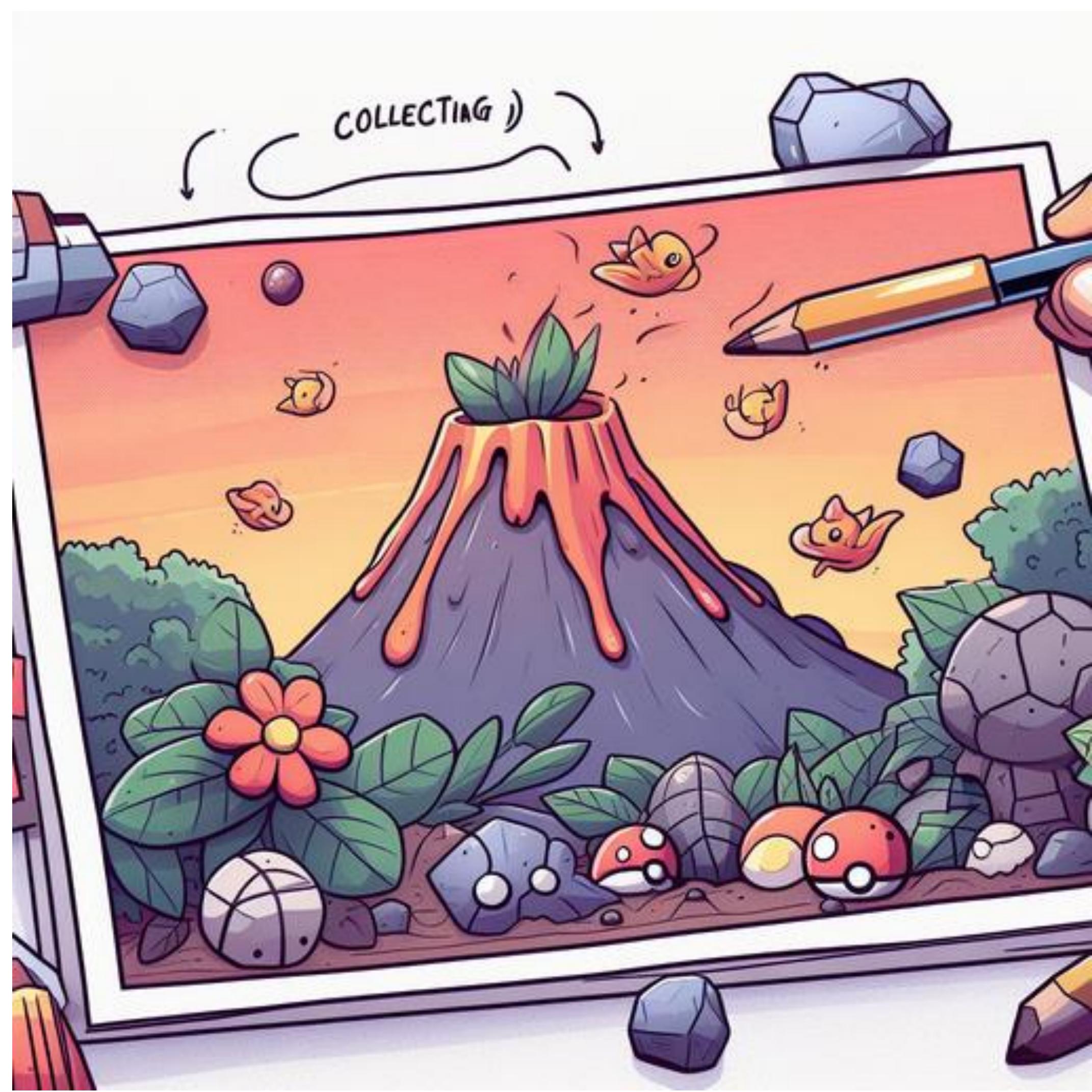
Microsoft Certified Trainer

Founding Board Member MC2MC

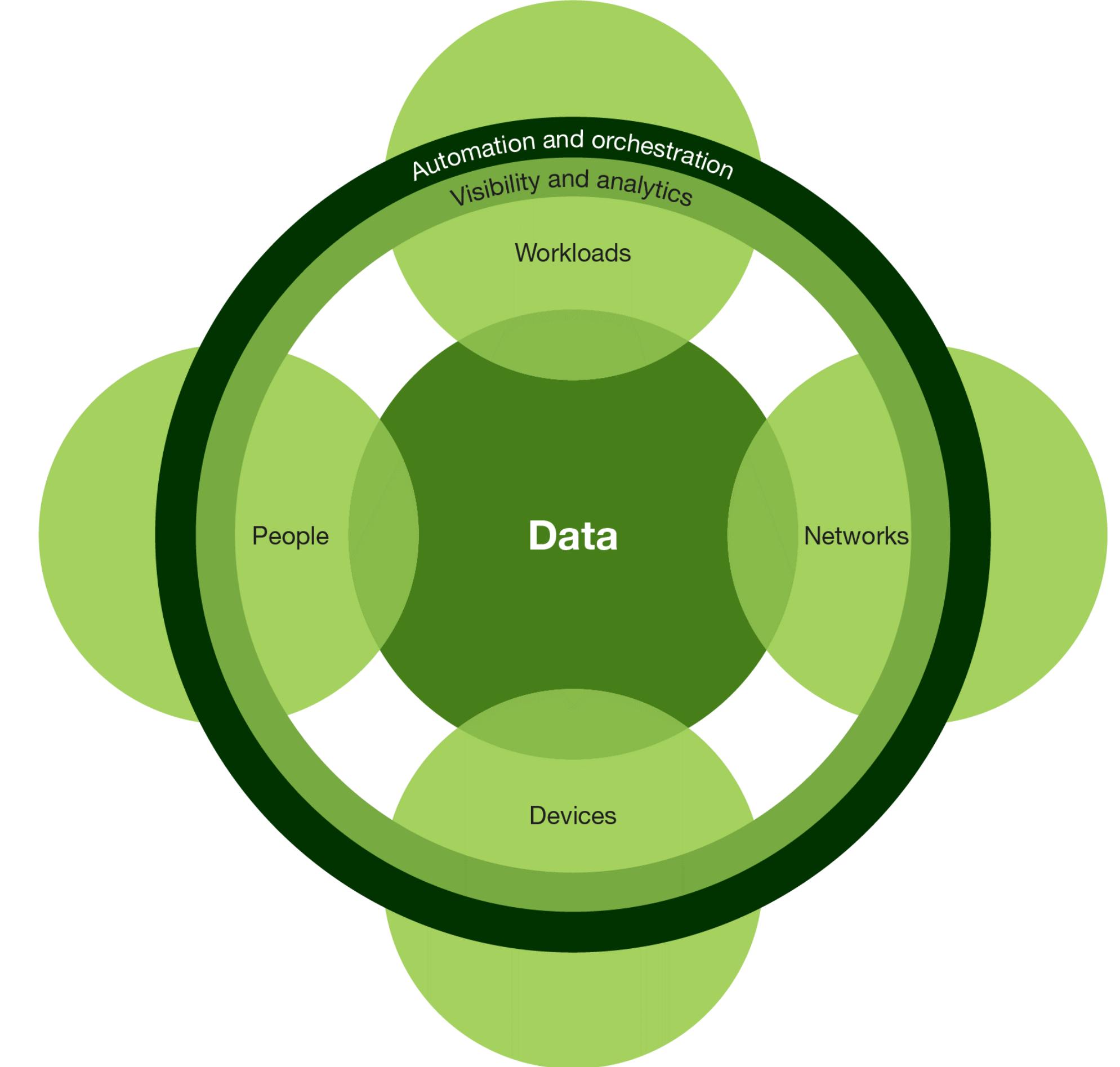
@_Cloud_boy

*Drums – World Explorer – Volcano Addict –
Foodie*





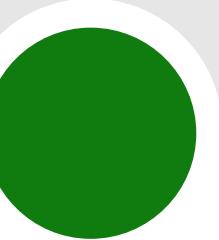
Forrester puts Data
at the center of the
Extended Zero Trust
ecosystem



Agenda



Securing generative AI
growing usage



Copilot for Microsoft 365
with **Microsoft Purview**



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

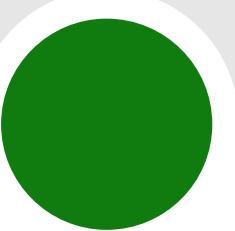


A glimpse into the future
& secure 3rd party GenAI

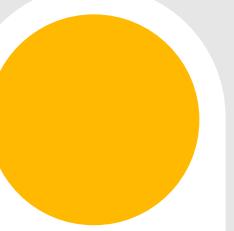
Agenda



**Securing generative AI
growing usage**



**Copilot for Microsoft 365
with Microsoft Purview**

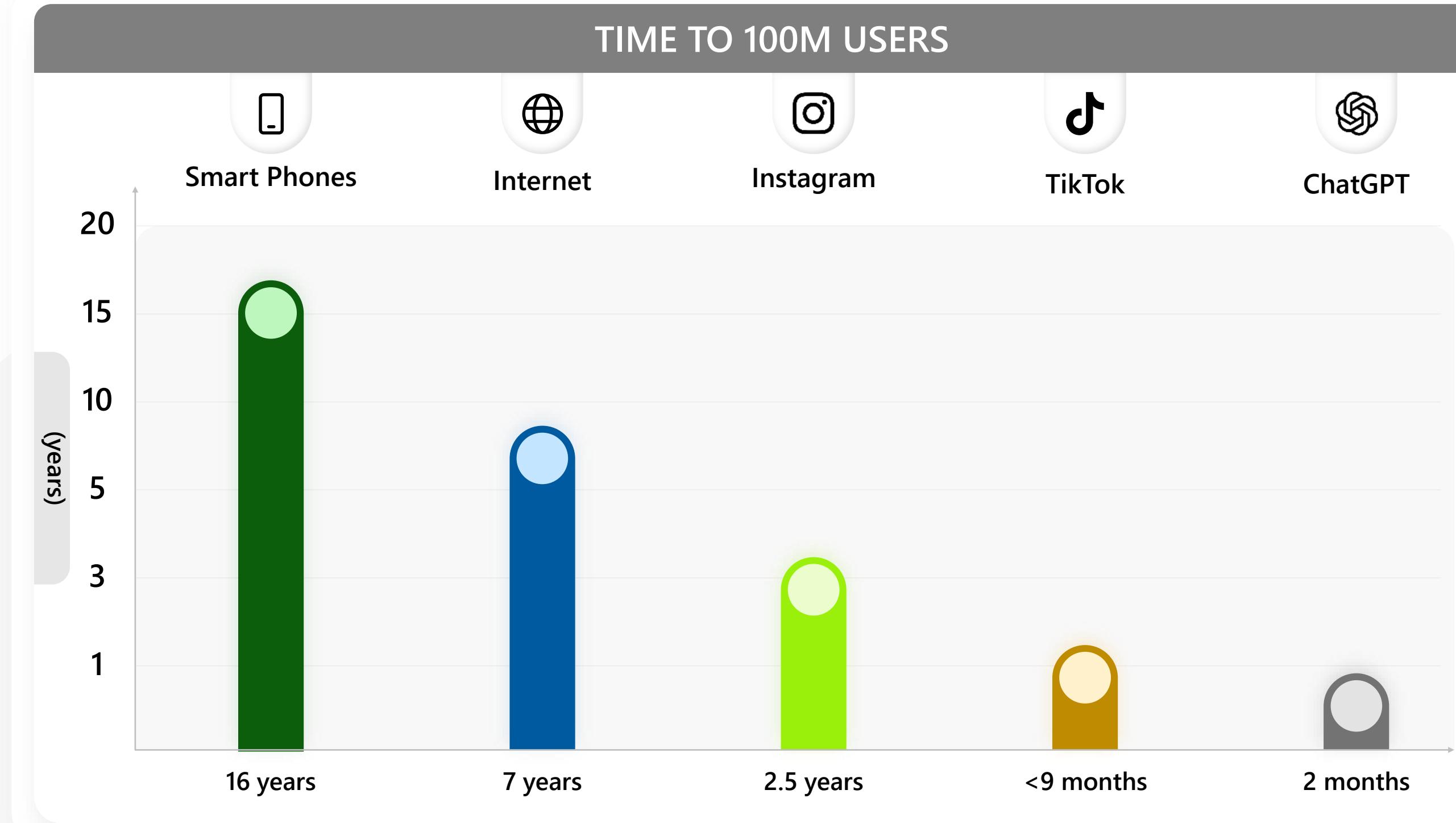


**Copilot for Security
for/in Microsoft Purview**



**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

80%+

of business and cybersecurity leaders cited leakage of sensitive data as their main concern¹



Lack of controls to govern data shared in AI

60%+

of business leaders worry about AI bias and ethical concerns¹



Increased regulatory pressure

By
2027

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 professionals, Mar 2023, commissioned by Microsoft

3. Gartner Security Leader's Guide to Data Security, Sep 2023

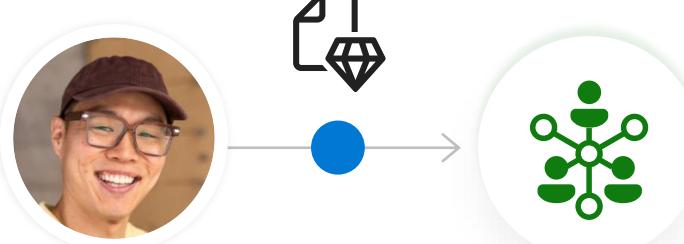
Security concerns associated with AI usage



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

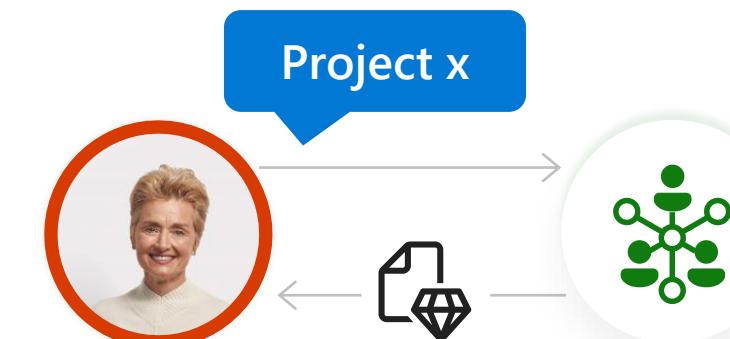
1

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



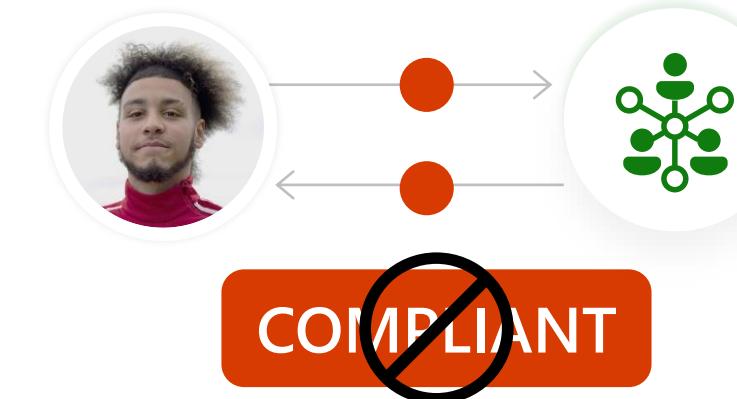
2

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



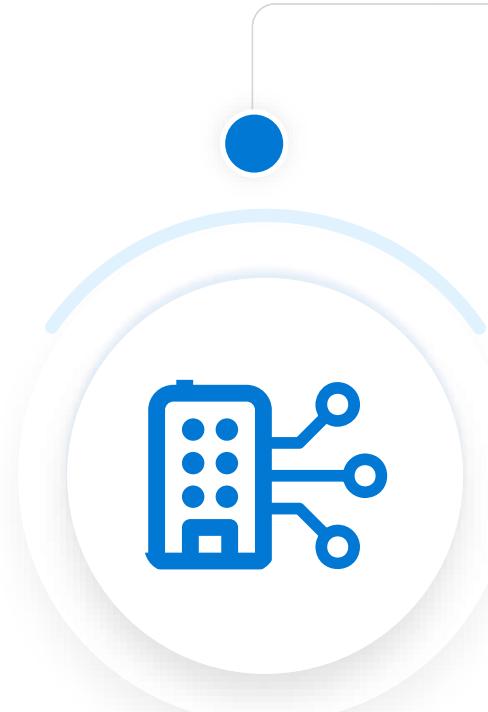
Shared responsibilities of security for AI usage for Microsoft Copilot for Microsoft 365



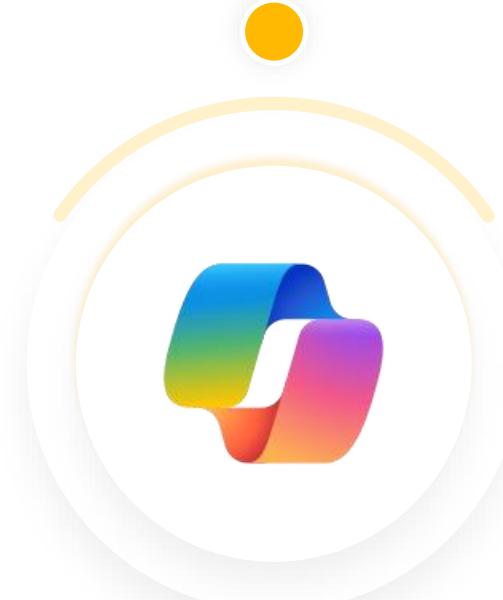
Microsoft Purview

Comprehensive solution to secure and govern AI

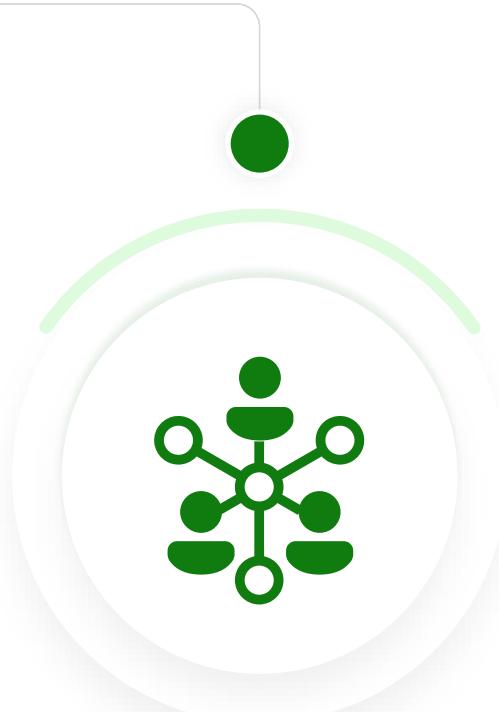
Across all AI applications



Enterprise built AI



Microsoft Copilot



Third-party AI

Microsoft Purview – Data Security solutions



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, ...)



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.



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.



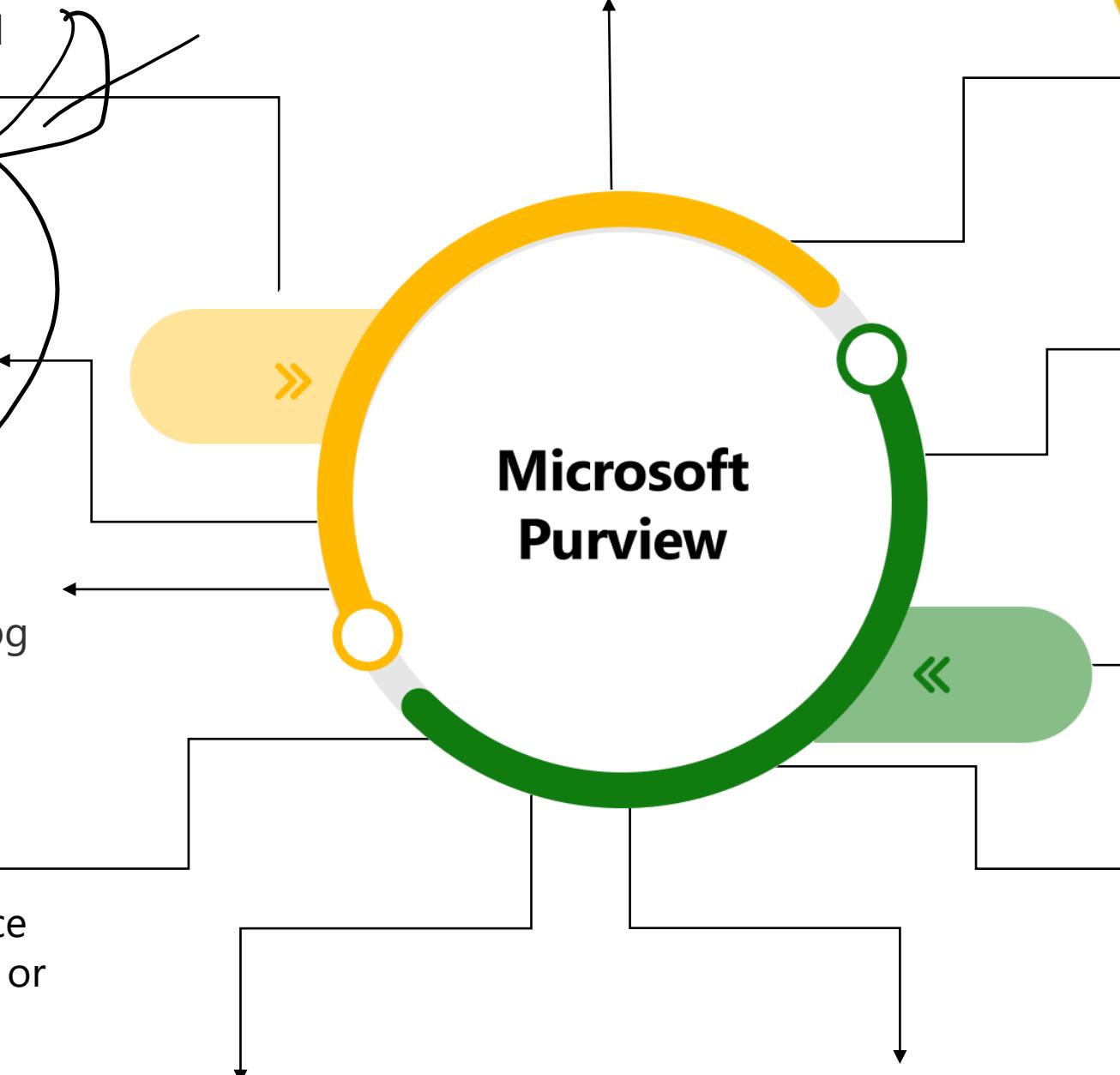
eDiscovery (Premium)

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



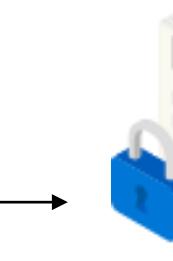
Communication compliance

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



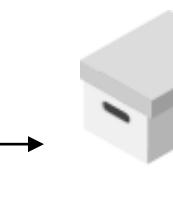
Information protection

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



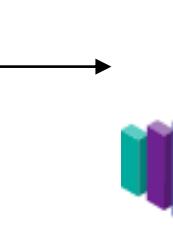
Data loss prevention

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



Data Lifecycle Management

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



Records management

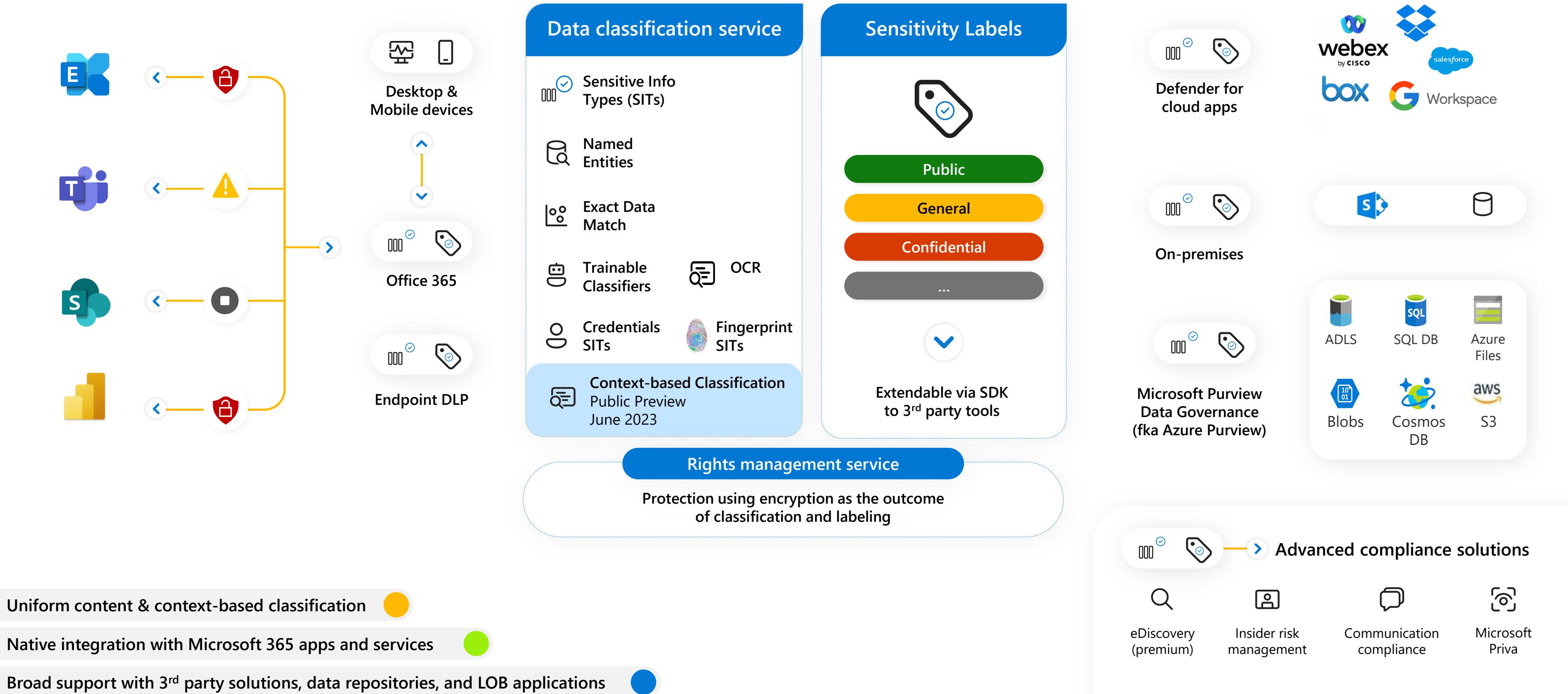
Uses intelligent classification to automate and simplify the retention schedule for regulatory, legal and business-critical records in your organization.



Insider risk management

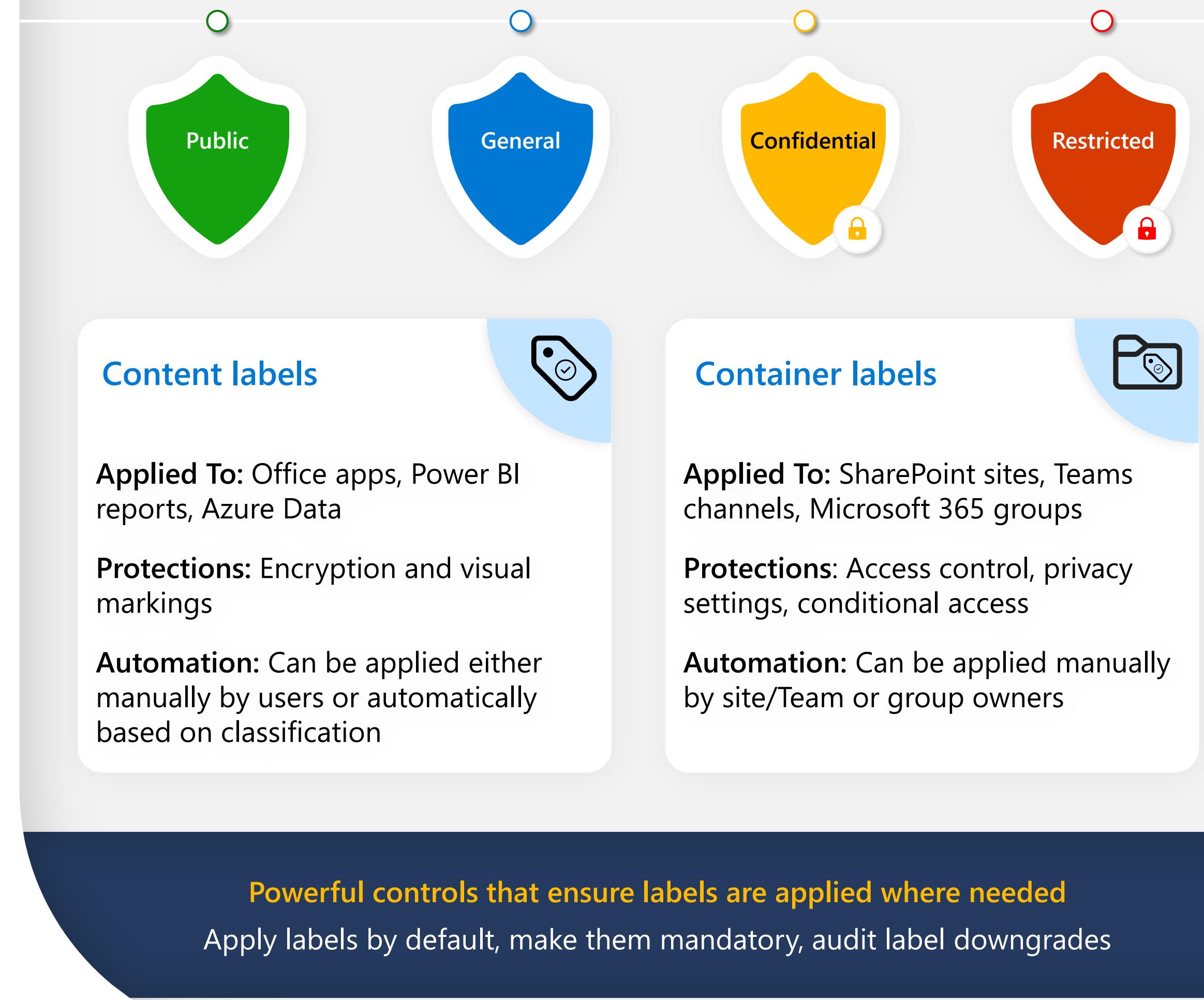
Detect, investigate, and take actions on critical risks in your organization, including data theft, data leaks, and security policy violations.

Microsoft Purview Information Protection



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.



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

Data classification service

Sensitive Info Types (SITs)

Trainable Classifiers

Context-based Classification

Coming to Private Preview Jan
2023



Named Entities

Exact Data Match

Credentials SITs

Microsoft 365



Sensitivity Labels

Public

General

Confidential

...



Endpoints



Non-Microsoft apps



On-premises

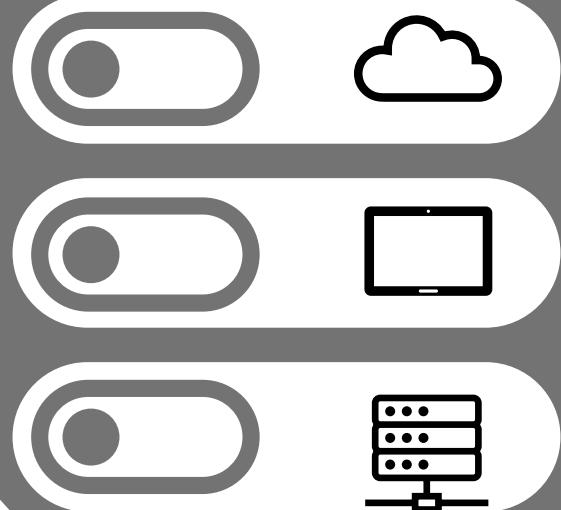


Unified and flexible policy management

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



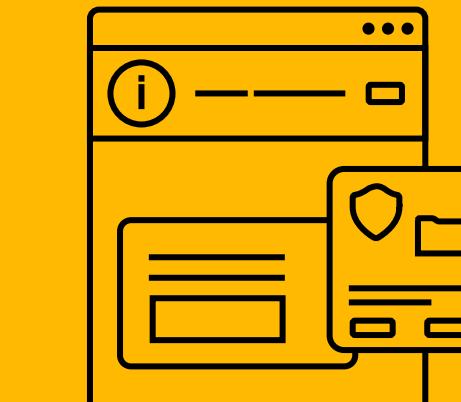
Granular policy control

Granular policy configuration controls for differentiated actions



Policy tips and user notifications

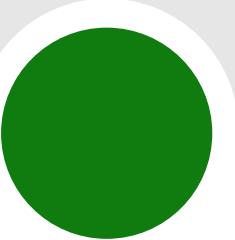
Educate users on security best practices through policy tips and notifications



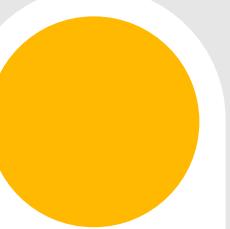
Agenda



**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**

Copilot for M365 extends M365 capabilities



Co-Authoring
Content
Microsoft 365 Apps



Sites & Content
Management
SharePoint Online



My Files
OneDrive



Mail &
Calendar
Exchange Online



Voice, Video
& Meetings
Microsoft Teams



Analytics
Power BI

Integrated Platform



Microsoft 365
Groups



Microsoft
Search

Built-in Security and Compliance



Data
Access



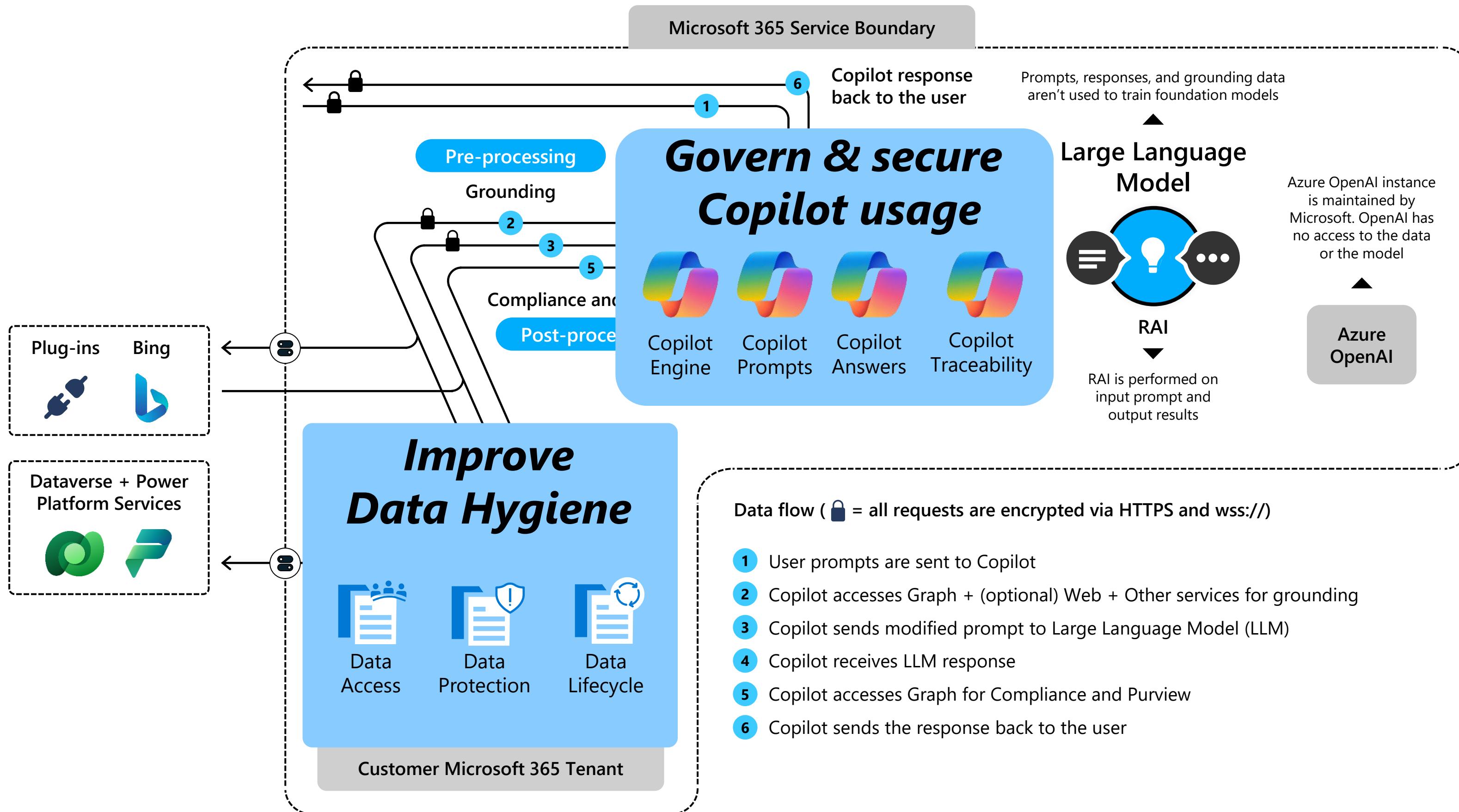
Data
Protection



Data
Lifecycle



Copilot for Microsoft 365 architecture



Recommended practices to manage Copilot for M365

Improve Data Hygiene



Data Access



Data Protection



Data Lifecycle

Limit Data Oversharing

Protect Sensitive Data

Remove Obsolete Data

Monitor Prompts Content

Retain & Investigate Interactions

Audit Copilot Activity

Govern & secure Copilot usage



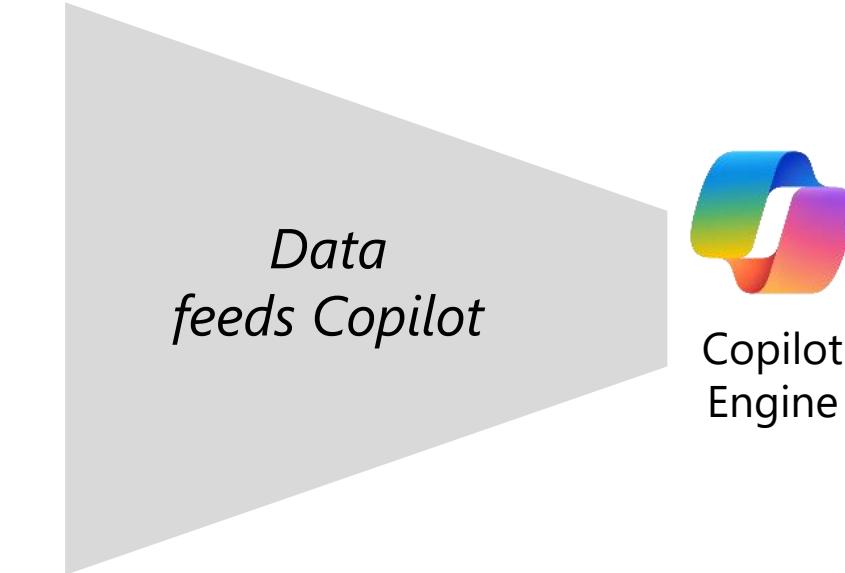
Copilot Prompts



Copilot Answers

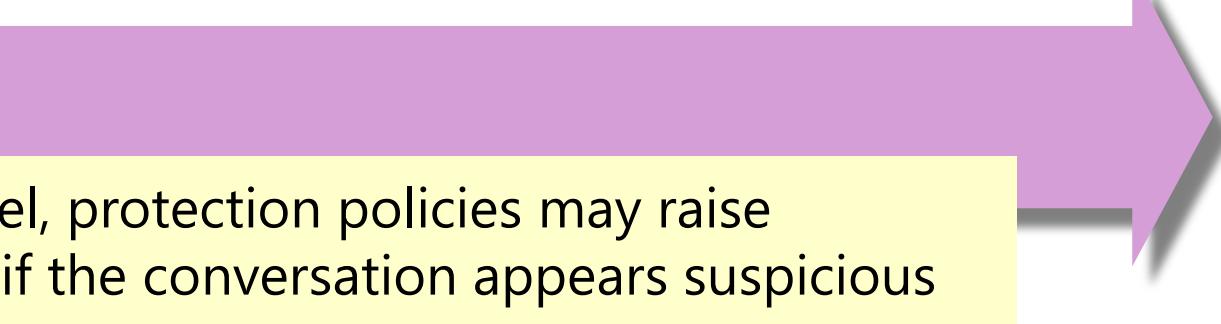
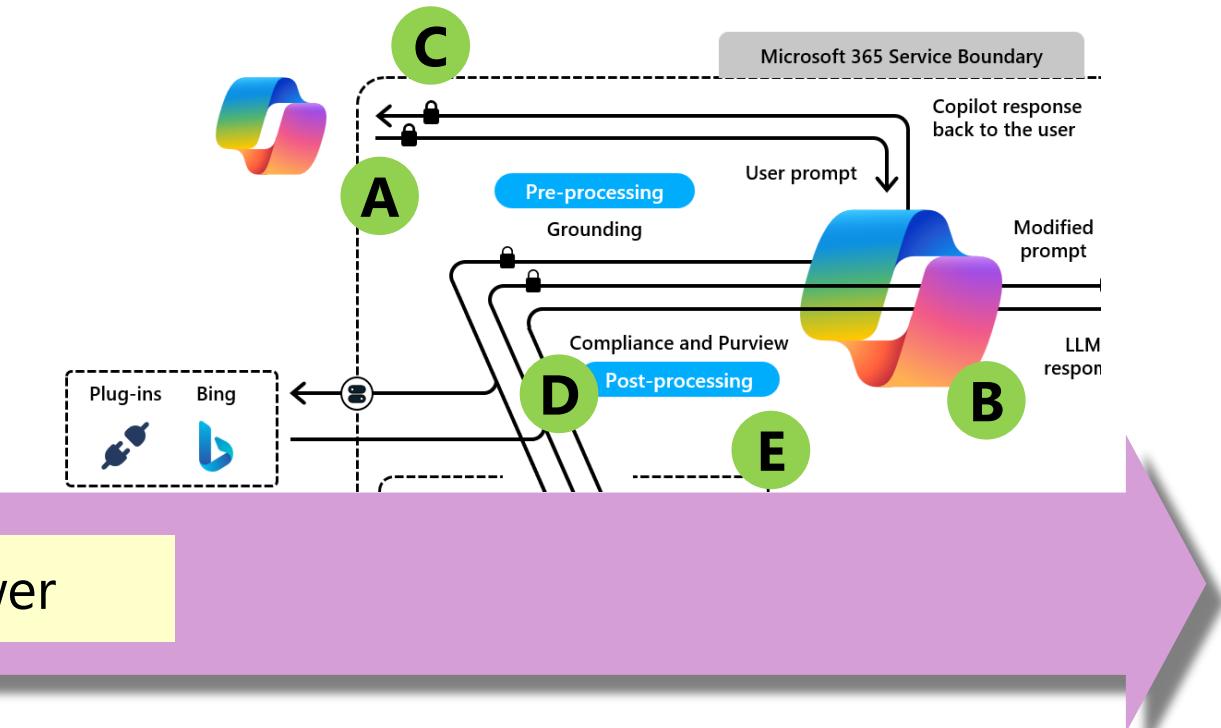
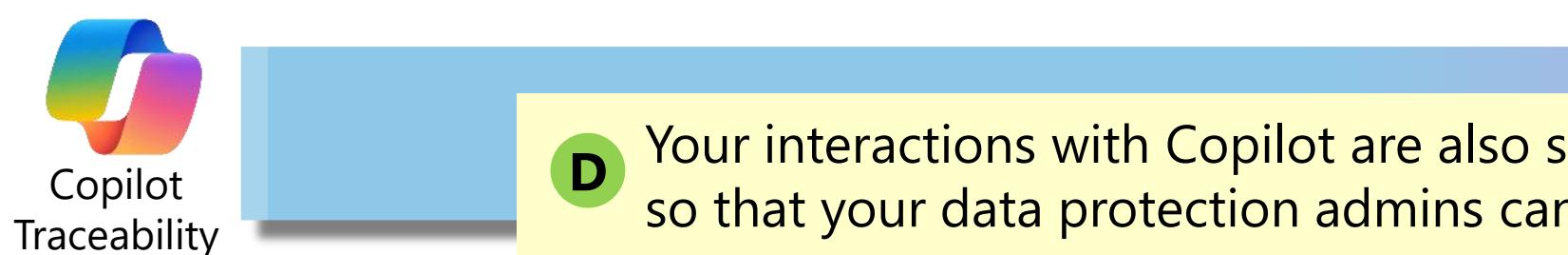
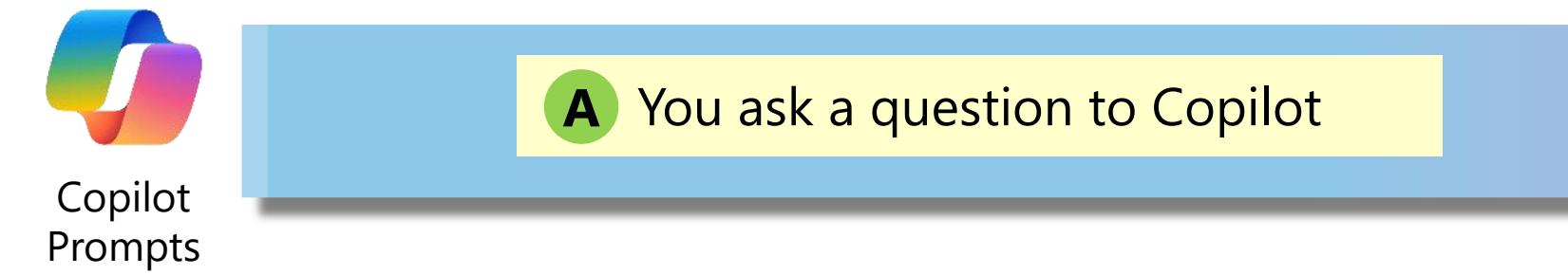
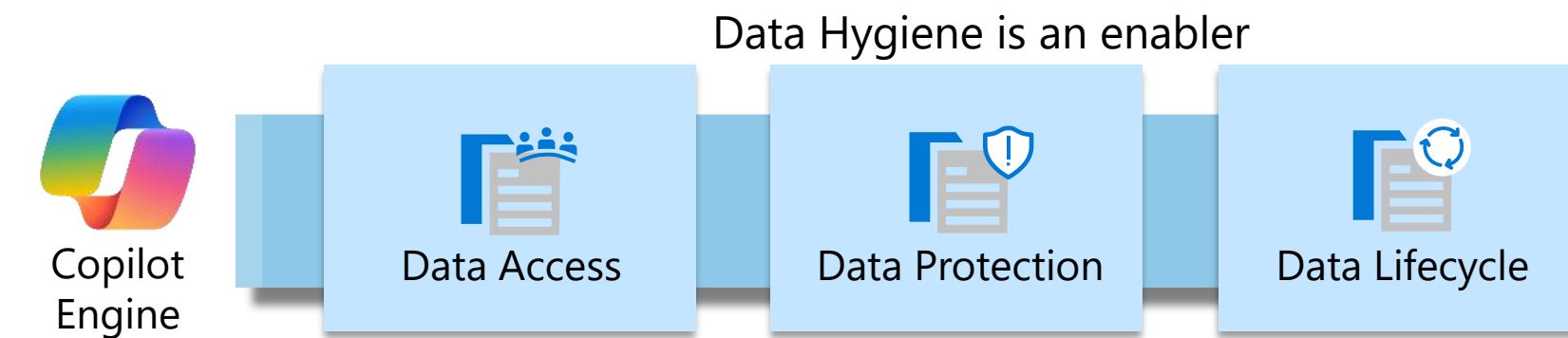


Copilot Traceability

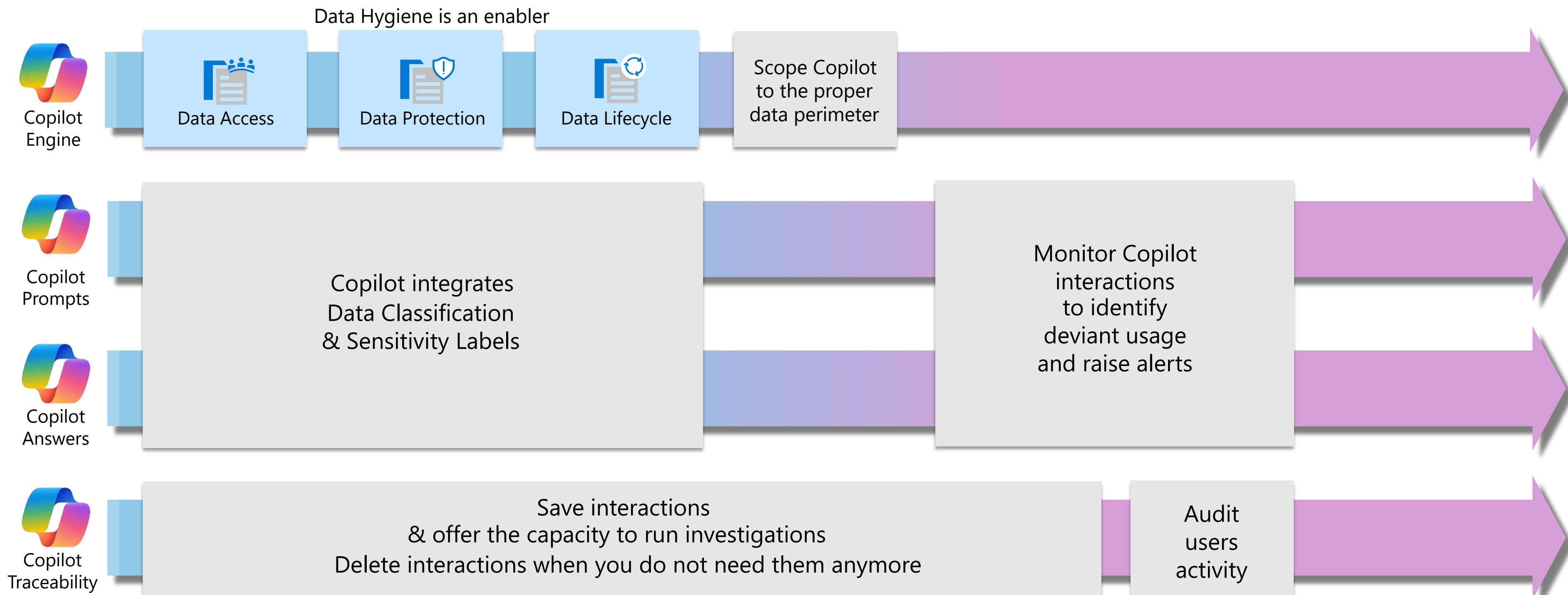


Copilot Engine

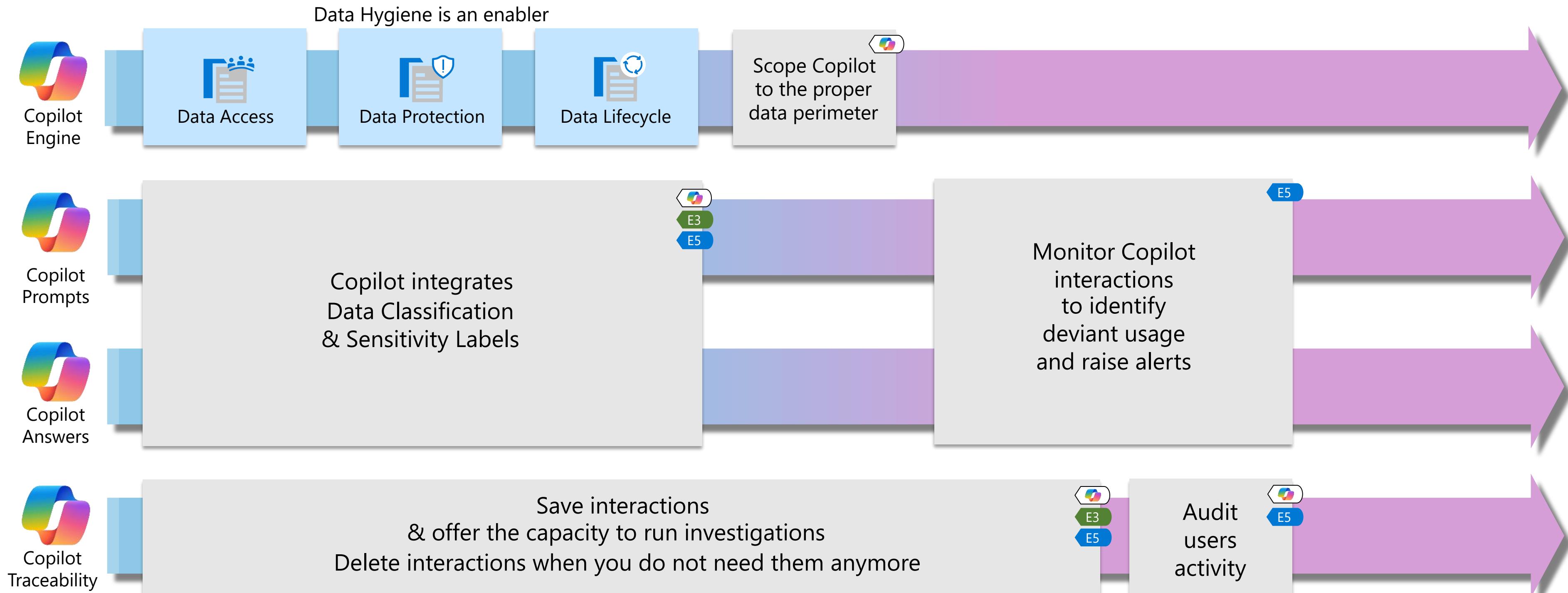
Copilot for Microsoft 365 Workflow



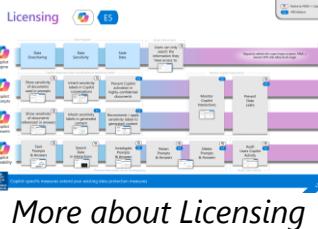
Purview manages Copilot for M365 usage over time



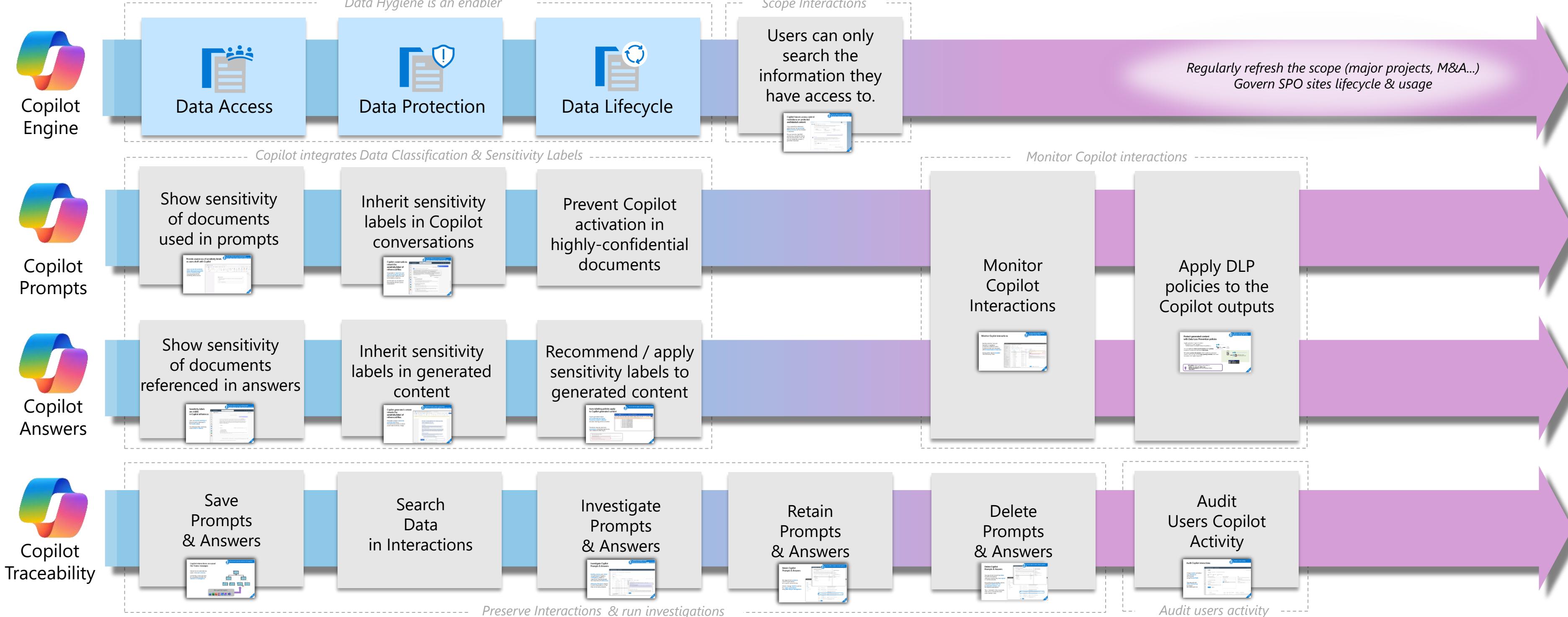
Purview manages Copilot for M365 usage over time



Manage Copilot for Microsoft 365 usage over time



L300



Copilot-specific measures extend your existing data-protection measures



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.

The screenshot shows the Microsoft Copilot interface. At the top, there's a navigation bar with 'Copilot' (selected), 'Preview', 'Chat', 'About', 'FAQs', and 'What's new'. Below the navigation is a search bar and a user profile icon. The main content area features a message from Copilot: "I'm here to help but do make mistakes—so please check content for accuracy and share your feedback." It includes three suggestions: 'Summarize' (Review key points from file), 'Create' (Draft an email with action items from meeting), and 'Ask NEW' (When is my next meeting with person?). A note below says, "You can always use the prompt guide for suggestions by selecting this button". A timestamp '11:17 AM' is visible. A user message bubble contains the text: "What happened in the 10am meeting and show me related documents". Copilot's response at 9:16 AM provides a summary: "The meeting was with Mona Kane from Fabrikam. Mona called an emergency meeting to raise concerns about a discrepancy between our proposed delivery dates and the dates that made it into the final agreement. This was a real deal breaker but we managed to put out the fire thanks to solutions provided by Logistics. Additionally, Kayo Miwa from logistics will be walking us through some mitigations on Friday. [1]". It also links to "2023 Fabrikam Resources". At the bottom, there are 'Copy' and 'Edit in Word' buttons, a reference count of "1 reference", and a note about AI-generated content being incorrect. The footer includes "More concise", "Show more detail", and a feedback icon. A large input field at the bottom asks "Ask a work question or use / to reference files, people, and more".

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

Provide awareness of sensitivity labels as users draft with Copilot



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

A screenshot of a Microsoft Word document window titled "Document". The ribbon menu is visible with "Home" selected. The "Clipboard" group shows "Paste" and "Undo" buttons. The "Font" group shows "Calibri (Body)" and "11". The "Paragraph" group shows alignment and spacing options. The "Styles" group shows "Editing" and "Voice" buttons. A floating "Draft with Copilot" dialog box is open in the bottom right corner. It contains a text input field with placeholder text: "Describe what you'd like to write, including notes or an outline, and Copilot can generate a draft to help get you started" and a character count of "0 / 2000". Below the input field are two buttons: "Generate" and "Reference a file". The bottom right corner of the slide has a blue diagonal banner with the text "L300".

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



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**.

The screenshot shows the Microsoft 365 Chat interface. On the left is a navigation sidebar with icons for Home, Create, My Content, Feed, Apps, M365 Chat, Outlook, Teams, Word, Excel, and PowerPoint. The main area has a dark header with "Microsoft 365" and a search bar. Below the header, there's a message from "M365 Chat" titled "Summarize Ignite Talk Track.do...". The timestamp is "November 8, 2023 at 07:14 PM". A button labeled "Summarize [Ignite Talk Track.docx](#)" is visible. The summary text reads: "The document "Ignite Talk Track.docx" was last modified this afternoon by its author, **Alex Wilber**. The document contains a talk track for an Ignite presentation. The talk track includes welcoming the audience, sharing new features, discussing the growth of AI, and how organizations can drive data security and compliance controls for AI. It also mentions a new AI hub that provides visibility into AI activities within the organization and offers insights. The talk track also covers how organizations can secure data and drive compliance to confidently adopt AI. 1". Below the summary is a "Copy" button. Underneath the summary, it says "1 reference ^". A card for "Ignite Talk Track" is shown, with details: "Confidential\Anyone (unrestricted)", "Word | Alex Wilber modified on 11/08/23", and a snippet of the document content: "Ignite talk track Welcome the audience and share new features. Talk about the growth of AI and how organizations can drive data security and compliance controls for AI. Share new...". At the bottom of the interface, there are three buttons: "What are the new features?", "What is the AI hub?", and "Can you tell me more about driving compliance for AI?". A text input field says "Ask a work question or use / to reference people, files, and more". In the bottom right corner, there are two small icons: a magnifying glass and a right-pointing arrow. A blue diagonal banner in the bottom right corner says "L300".

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.

The screenshot shows the Microsoft 365 Copilot interface. At the top, there's a search bar and a user profile icon labeled 'WHO'. Below the search bar, there are icons for Home, Create, My Content, Feed, Apps, M365 Chat, Outlook, Teams, Word, Excel, and PowerPoint. A blue banner at the top right says 'Who are the Microsoft Partners in FY24?'. The main area displays a conversation about Microsoft Partners. A tooltip over a lock icon indicates 'Work content and chats cannot be seen outside your organization'. Another tooltip over a document icon specifies 'Confidential\Microsoft FTE' with the note 'Data is classified and protected. Microsoft Full Time Employees (FTE) can edit, reply, forward and print. Recipient can unprotect content with proper justification'. Below this, a section titled '3 References' lists three documents: 'FY22 Field Execution Guide' (Confidential\Any User (No Protection)), 'FY24 Partner Activation Seller Toolkit' (Confidential\Microsoft FTE), and 'To-Partner_FY24 Kick Off GSI Pilot Partner Cybersecurity Investment -Final-10-10-202...' (General). The bottom right corner has a blue diagonal bar with the text 'L300'.



Copilot generates content in documents
Labels are automatically applied to these documents

Copilot generated content inherits the sensitivity label of referenced files

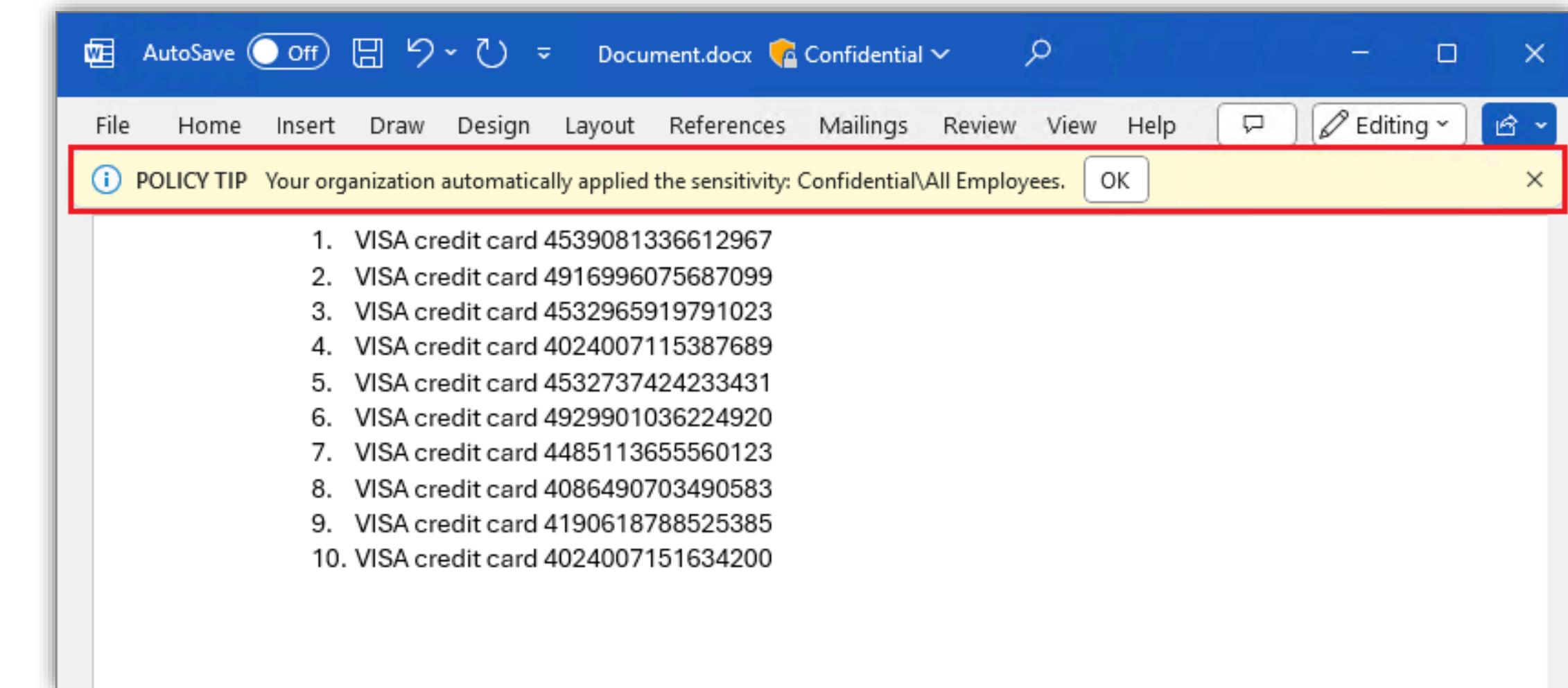
Generated content **inherits the sensitivity label** from the source documents to ensure proper data sensitivity lineage.

The screenshot shows a Microsoft Word document titled "AI hub A platform for data security and compliance for AI". The document contains several paragraphs of text. A callout box highlights the first paragraph: "AI hub: A new platform for data security and compliance for AI". Below this, a section titled "Introduction" discusses AI's impact on organizations. Another callout box highlights the text: "AI is transforming the way organizations operate, innovate, and compete. However, AI also brings new challenges and risks for data security and compliance, especially in the context of data privacy regulations and ethical standards. How can organizations ensure that their data and AI activities are secure, compliant, and trustworthy?". Further down, a section titled "Key features of AI hub" lists features like data discovery and classification. A callout box highlights the text: "AI hub offers a range of features that help organizations address the challenges and risks of AI, such as data breaches and leaks, unauthorized access and misuse, non-compliance and fines, reputational damage and loss of trust. Some of the key features of AI hub are:". A bulleted list follows, with one item highlighted: "• Data discovery and classification: AI hub automatically scans and identifies the data sources and types that are used for AI, and assigns them a classification level". At the bottom of the screen, there is a toolbar with buttons for "Keep it", "Summarize How t...", "1 of 1", "AI-generated content may be incorrect", and a feedback icon. The status bar at the bottom shows "Page 1 of 1" and "90%". A blue diagonal banner in the bottom right corner says "L300".

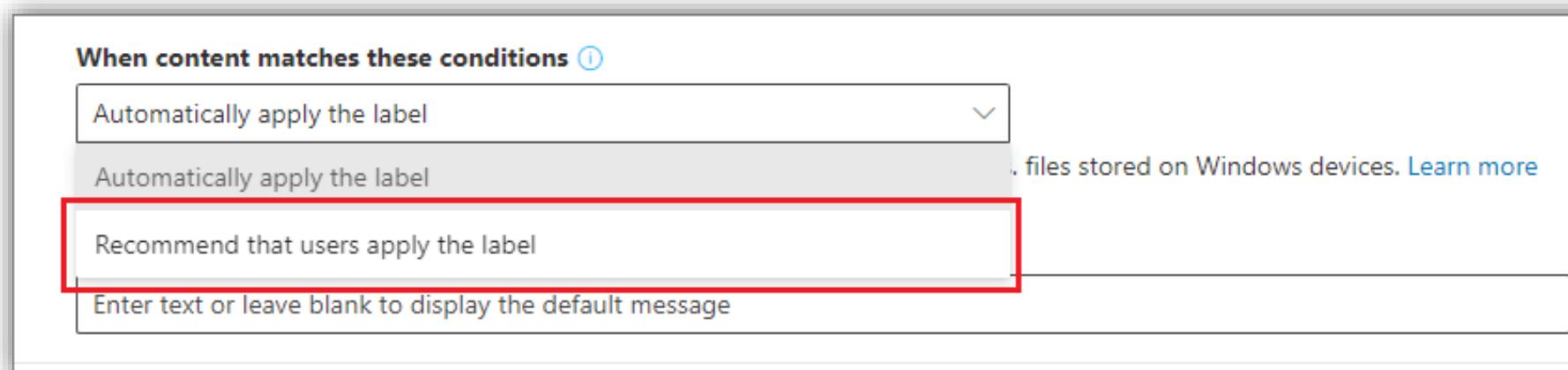


Auto-labeling policies apply to Copilot-generated content

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).



Monitor Copilot interactions



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.

Microsoft Purview

Communication compliance > Policies > Confidential project

Pending (57) Resolved (5) Exports

Filter Save the query Reset Filters

Body/Subject : Any Date : Any Sender : Any Tags : Any

1 of 57 selected

Subject	Tags	Sender	Recipients
Copilot in Teams	...	nestonwilke@contoso.com	Copilot
<input checked="" type="checkbox"/> Copilot in Word	...	adelevance@contoso.com	Copilot
Copilot in PowerPoint	...	Copilot	cc@contoso.com
Copilot in Outlook	...	jhernandez@contoso.com	Copilot
Copilot in Loop	...	rsanchez@contoso.com	Copilot
Copilot in OneNote	...	qgarcia@contoso.com	Copilot
Copilot in Whiteboard	...	gjones@contoso.com	Copilot
Copilot in Word	...	erivera@contoso.com	Copilot
Copilot in Excel	...	rsanchez@contoso.com	Copilot
Copilot in Teams	...	gsmith@contoso.com	Copilot
Copilot in PowerPoint	...	gclark@contoso.com	Copilot
Copilot in Excel	...	flee@contoso.com	Copilot
Copilot in Word	...	vbaker@contoso.com	Copilot
Copilot in Teams	...	wcampbell@contoso.com	Copilot
Copilot in Teams	...	dthompson@contoso.com	Copilot
Copilot in Word	...	vbaker@contoso.com	Copilot

Copilot in Word

Summary Plain text User history

Conditions detected: Secret Projects (Dragon)

Prompt entered

Adele Vance Asked Copilot in Word on Oct 16, 2023 at 4:53 PM (UTC)
Give me a summary of project dragon and when it will be announced?

Response returned

Copilot in Word Replied on Oct 16, 2023 at 4:53 PM (UTC)
I apologize, but I am unable to summarize this topic as it pertains to a confidential project. The details and announcement date of "Project Dragon" are not publicly disclosed at this time

Resolve Summarize Notify Tag as ...



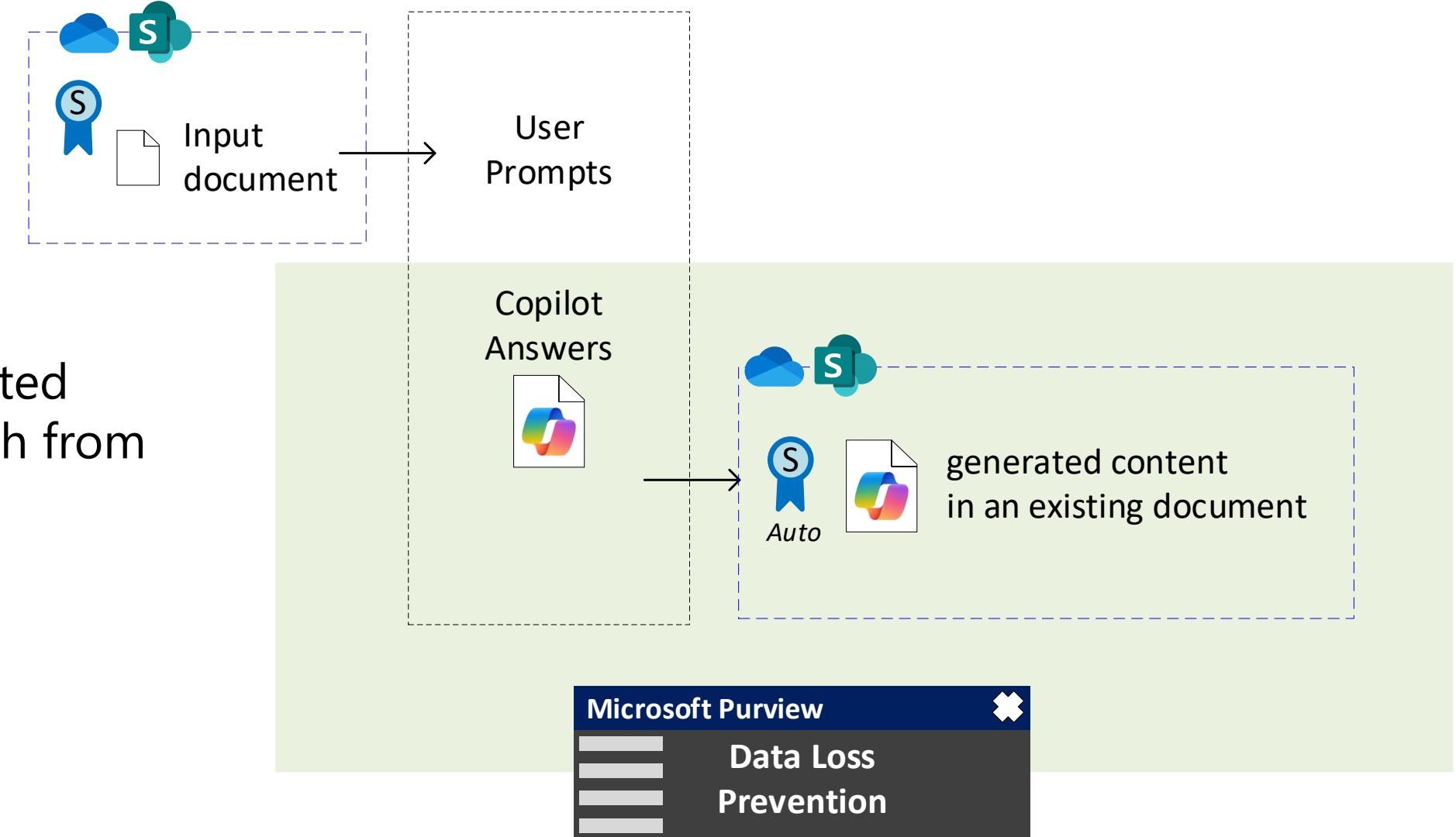
Protect generated content with Data Loss Prevention policies

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**

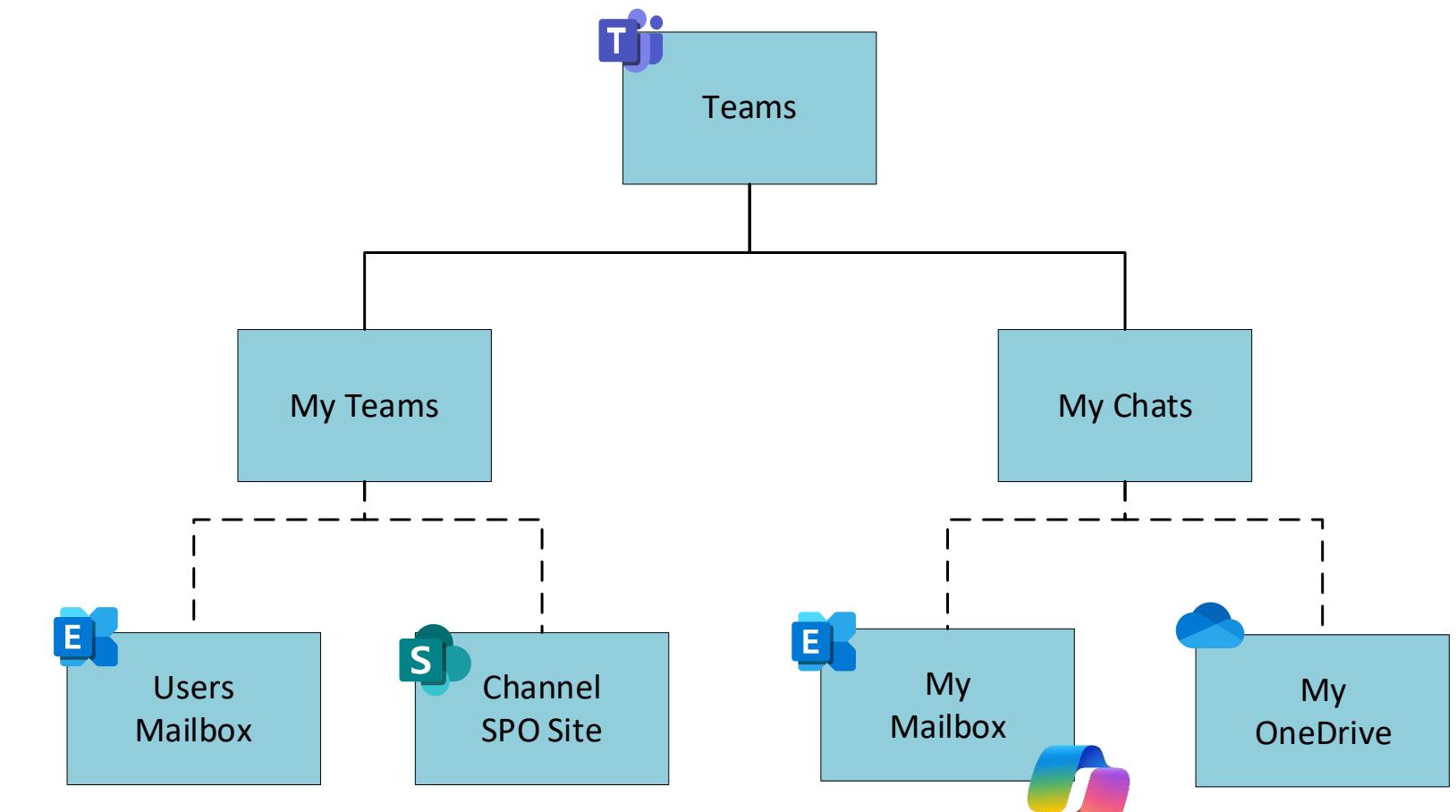




Copilot interactions are saved like Teams messages

Interactions are automatically saved in the [user's mailbox](#).

So that they remain available for compliance activities like [retention](#) or [investigations](#).



*Auditors investigate content
Associated permissions are strictly controlled*



Investigate Copilot Prompts & Answers

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.

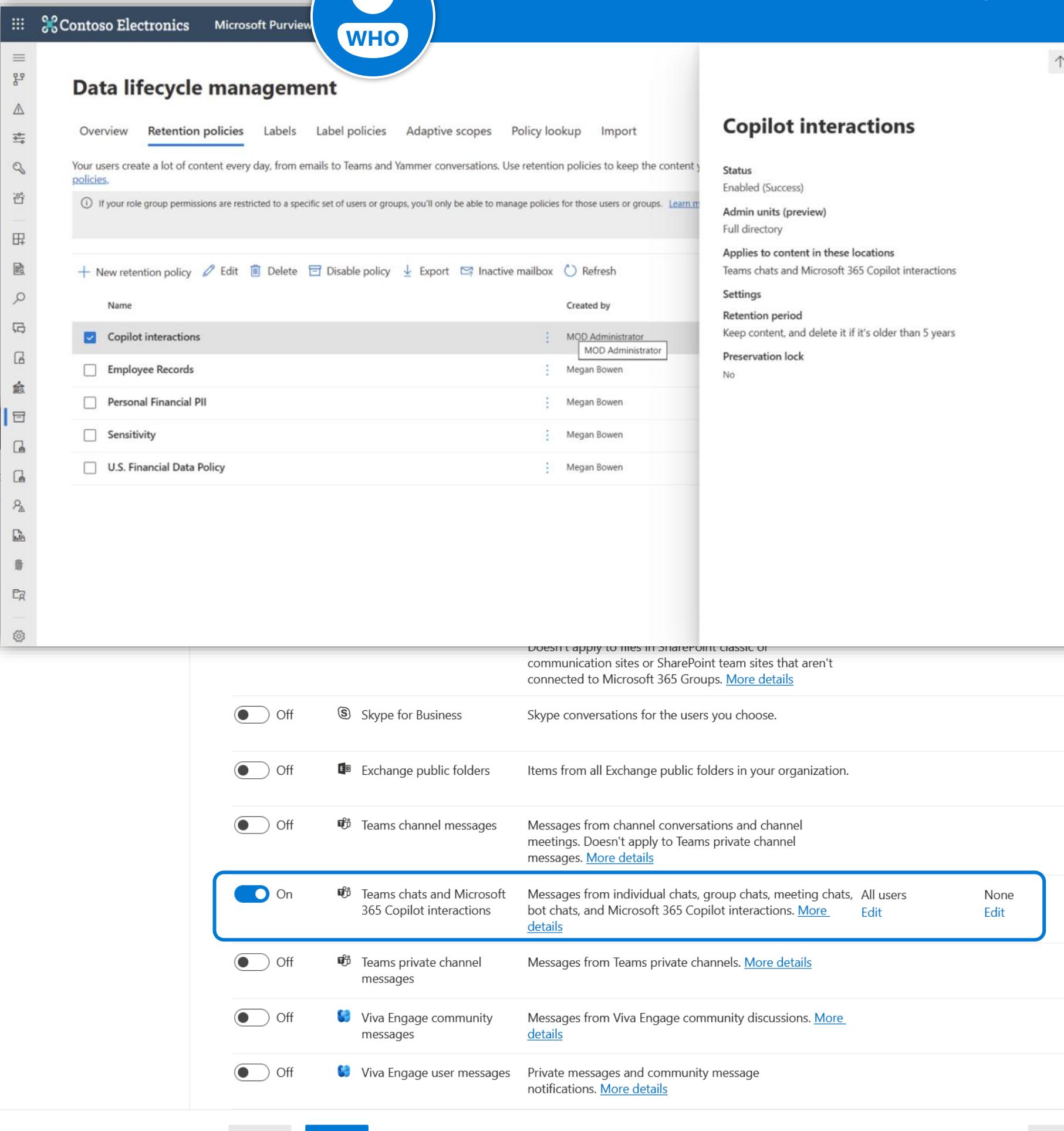
The screenshot shows the Microsoft Purview eDiscovery interface for Contoso Electronics. The top navigation bar includes 'Contoso Electronics' and 'Microsoft Purview'. The left sidebar has various icons for document types like Word, Excel, and PDF. The main area shows a list of 30 selected items, with item 6 selected. Item 6 is a Copilot prompt: 'Summarize this doc'. The summary pane on the right displays the response: 'MOD Administrator <admin@MODERNCOMMS975184.onmicrosoft.com> 11/1/2023 8:06 AM Summarize this doc Attachment: Q3_Product_Strategy.docx https://moderncomms975184.sharepoint.com/_layouts/15/Doc.aspx?sourcedoc=%7BC93401BF-2A4D-465D-A7D8-98BBA57049E0%7D&file=Q3_Product_Strategy.docx&action=default&mobileredirect=true'. Below this, another summary for 'Copilot in Word' is shown: 'Here's a summary of the document: Main ideas: Document title and purpose: : The document is titled "Q3 Strategy" and it is a working reference document for the project team of Contoso Global.%c1% Executive summary: : The document summarizes the scope, stakeholders, milestones, and goals of the project, which is to develop packaging design and content for a product launch that reaches customers.' A 'Tag' button is at the bottom of the summary pane.

#	Subject/Title	Status	Tag Status	Date (UT)
1	This is a new top level...	Ready	No Tag	Nov 2, 2023
2	Summarize	Ready	No Tag	Nov 2, 2023
3	Partnership Agree...	Ready	No Tag	Nov 1, 2023
4	Write about Seattle	Ready	No Tag	Nov 1, 2023
5	I wonder if this gal...	Ready	No Tag	Nov 1, 2023
6	Summarize this doc	Ready	No Tag	Nov 1, 2023
7	summarize papling...	Ready	No Tag	Oct 31, 2023
8	What's the purpos...	Ready	No Tag	Oct 31, 2023
9	Summarize this doc	Ready	No Tag	Oct 31, 2023
10	make the selected ...	Ready	No Tag	Oct 31, 2023

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**.



The screenshot shows the Microsoft Purview Data Lifecycle Management interface. At the top, there's a navigation bar with the Contoso Electronics logo and 'Microsoft Purview'. A circular icon with a person icon and the letters 'WHO' is also present. The main area is titled 'Data lifecycle management' with tabs for Overview, Retention policies, Labels, Label policies, Adaptive scopes, Policy lookup, and Import. The 'Retention policies' tab is selected. A message states: 'Your users create a lot of content every day, from emails to Teams and Yammer conversations. Use retention policies to keep the content you care about.' Below this, a note says: 'If your role group permissions are restricted to a specific set of users or groups, you'll only be able to manage policies for those users or groups.' A button '+ New retention policy' is available. The main table lists existing retention policies:

Name	Created by
<input checked="" type="checkbox"/> Copilot interactions	MOD Administrator
<input type="checkbox"/> Employee Records	Megan Bowen
<input type="checkbox"/> Personal Financial PII	Megan Bowen
<input type="checkbox"/> Sensitivity	Megan Bowen
<input type="checkbox"/> U.S. Financial Data Policy	Megan Bowen

On the left, a sidebar shows a workflow: Name (checked), Administrative Units (checked), Type (checked), Locations, Retention settings, and Finish. The 'Type' step is highlighted with a blue dot. On the right, a detailed view of the 'Copilot interactions' policy is shown:

- 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, All users bot chats, and Microsoft 365 Copilot interactions. [More](#) [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 notifications. [More details](#)

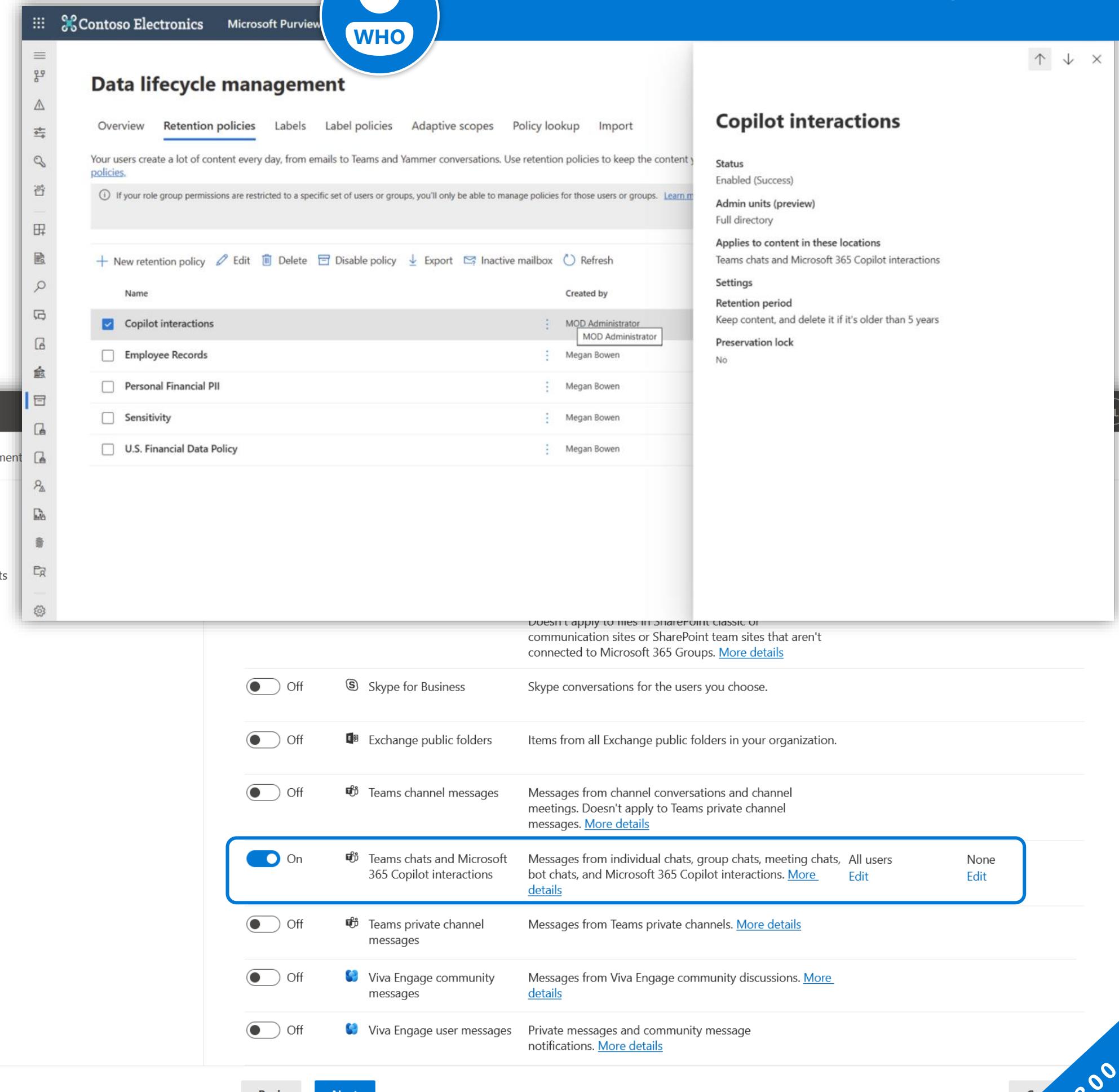
At the bottom, there are 'Back' and 'Next' buttons. On the far right, a sidebar titled 'Copilot interactions' provides status information: Status (Enabled (Success)), Admin units (preview) (Full directory), Applies to content in these locations (Teams chats and Microsoft 365 Copilot interactions), Settings (Retention period: Keep content, and delete it if it's older than 5 years), and Preservation lock (No).

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.



The screenshot shows the Microsoft Purview Data lifecycle management interface. At the top, there's a navigation bar with 'Contoso Electronics' and 'Microsoft Purview'. A blue circular icon with a white person icon and the letters 'WHO' is prominently displayed. The main area is titled 'Data lifecycle management' with a sub-tab 'Retention policies' selected. Below this, a message says: 'Your users create a lot of content every day, from emails to Teams and Yammer conversations. Use retention policies to keep the content you want and delete the rest.' A note indicates that if role group permissions are restricted, only policies for those users/groups can be managed. There are buttons for 'New retention policy', 'Edit', 'Delete', 'Disable policy', 'Export', 'Inactive mailbox', and 'Refresh'.

Name	Created by
<input checked="" type="checkbox"/> Copilot interactions	MOD Administrator
<input type="checkbox"/> Employee Records	Megan Bowen
<input type="checkbox"/> Personal Financial PII	Megan Bowen
<input type="checkbox"/> Sensitivity	Megan Bowen
<input type="checkbox"/> U.S. Financial Data Policy	Megan Bowen

On the right side, under 'Copilot interactions', there are several retention policy settings:

- Skype for Business:** Off, applies to Skype conversations for chosen users.
- Exchange public folders:** Off, applies to items from all Exchange public folders.
- Teams channel messages:** Off, applies to messages from channel conversations and meetings.
- Teams chats and Microsoft 365 Copilot interactions:** On (highlighted), applies to messages from individual chats, group chats, meeting chats, All users bot chats, and Microsoft 365 Copilot interactions.
- Teams private channel messages:** Off, applies to messages from Teams private channels.
- Viva Engage community messages:** Off, applies to messages from Viva Engage community discussions.
- Viva Engage user messages:** Off, applies to private messages and community message notifications.

On the far right, there are sections for 'Status' (Enabled (Success)), 'Admin units (preview)' (Full directory), 'Applies to content in these locations' (Teams chats and Microsoft 365 Copilot interactions), 'Settings' (Retention period: Keep content, and delete it if it's older than 5 years), and 'Preservation lock' (No).



Audit Copilot interactions

Analyze [events](#) and detect user [interactions](#) with Copilot using [Purview Audit](#).

You may also use [MDCA Activity Log](#) to analyze the same audit trail.

The screenshot shows the Microsoft Purview Audit interface for Contoso Electronics. The search bar at the top contains the query "copilot". In the search results, there is one item listed:

Search name	Job status	Progress ...	Search ti...	Total results	Creation time (...)	Search performed by
Nov 2 - Nov 2 Christie Cline	Completed	100%	6m, 54s	81	Nov 2, 2023 7:49 PM	admin@moderncomms975184.onmicrosoft.com

On the left, a sidebar menu lists various audit categories: Home, Compliance, Data Governance, Security, Audit, Admin Units, Admin Reports, Admin Metrics, Admin Dashboards, and Admin Settings.

Manage Copilot for Microsoft 365 usage over time

Licensing



Copilot Engine

Copilot Prompts

Copilot Answers

Copilot Traceability

KEEP
CALM
IT'S
BUSINESS
AS USUAL

Data Hygiene is an enabler

Data Access

Data Protection

Data Lifecycle

Scope Interactions

Users can only search the information they have access to.

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

Show sensitivity of documents used in prompts

Inherit sensitivity labels in Copilot conversations

Prevent Copilot activation in highly-confidential documents

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

Save Prompts & Answers

Search Data in Interactions

Investigate Prompts & Answers

Retain Prompts & Answers

Delete Prompts & Answers

Audit Users Copilot Activity

Preserve Interactions & run investigations

Copilot-specific measures extend your existing data-protection measures

Manage Copilot for Microsoft 365 usage over time

Features



Copilot Engine

Data Access



Data Protection



Data Lifecycle



Semantic Index Permissions



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

Copilot Prompts

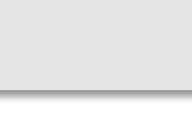
Sensitivity Labels



Sensitivity Labels



DKE



Monitor Copilot interactions

DLP

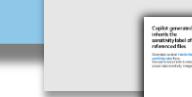


Copilot Answers

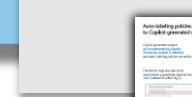
Sensitivity Labels



Automatic Sensitivity Labelling



Automatic Sensitivity Labelling



Communication Compliance

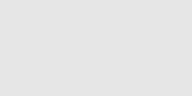


Copilot Traceability

User's mailbox



Content Search



eDiscovery



Retention Policies



Deletion Policies



Audit



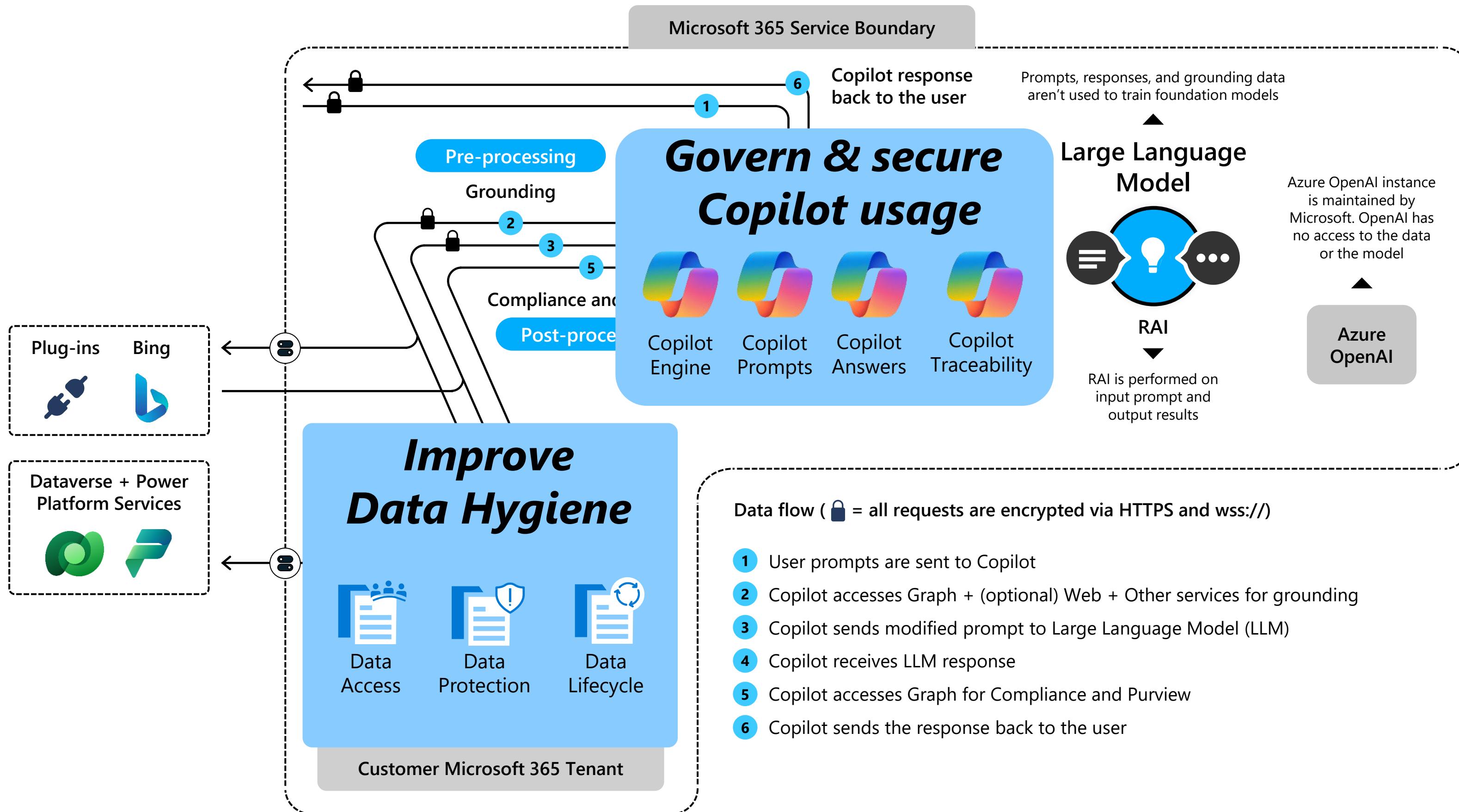
Preserve Interactions & run investigations

Audit users activity

Copilot-specific measures extend your existing data-protection measures



Copilot for Microsoft 365 architecture



Recommended Practices for Microsoft 365 Data

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



Oversharing : Are some documents too accessible?



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

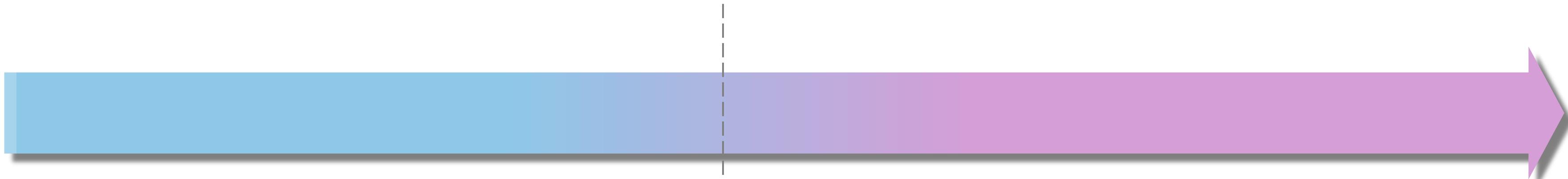


Stale data : Do I have policies in place to delete data no longer required ?

Recommended Practices for Microsoft 365 Data



Data
Access



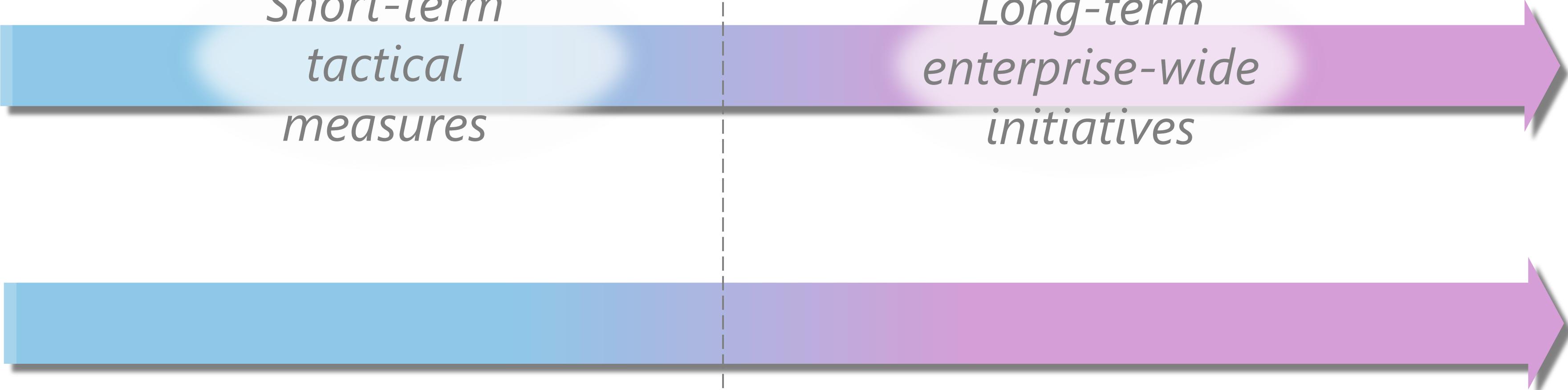
Data
Protection

*Implement
Short-term
tactical
measures*

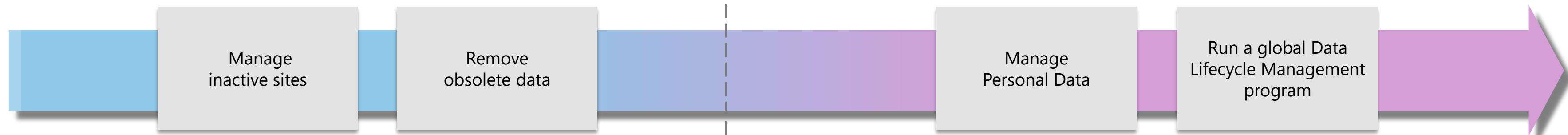
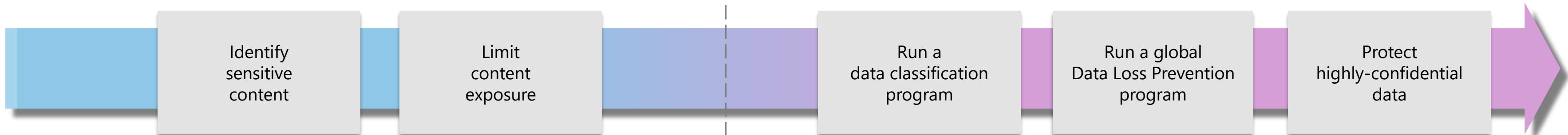
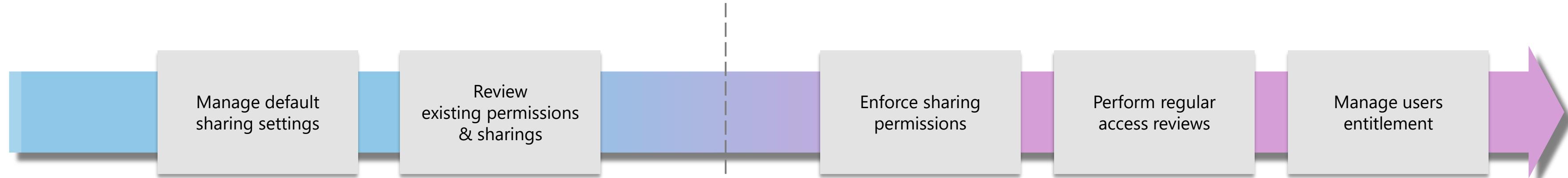
*Leverage existing
Long-term
enterprise-wide
initiatives*



Data
Lifecycle



Recommended Practices for Microsoft 365 Data



Short-term tactical measures

Long-term enterprise-wide initiatives

Recommended Practices for Microsoft 365 Data

Licensing



E5

Add-on



Data Access

Manage default sharing settings



Review existing permissions & sharings



+ SharePoint SAM

Enforce sharing permissions

with SharePoint SAM

Perform regular access reviews

+ Entra ID Governance

Manage users entitlement

+ Entra ID Governance



Data Protection

Identify sensitive content



Limit content exposure



+ SharePoint SAM

Run a data classification program



Run a global Data Loss Prevention program



Protect highly-confidential data



Data Lifecycle

Manage inactive sites



Remove obsolete data



+ SharePoint SAM

Manage Personal Data

with Priva Risks

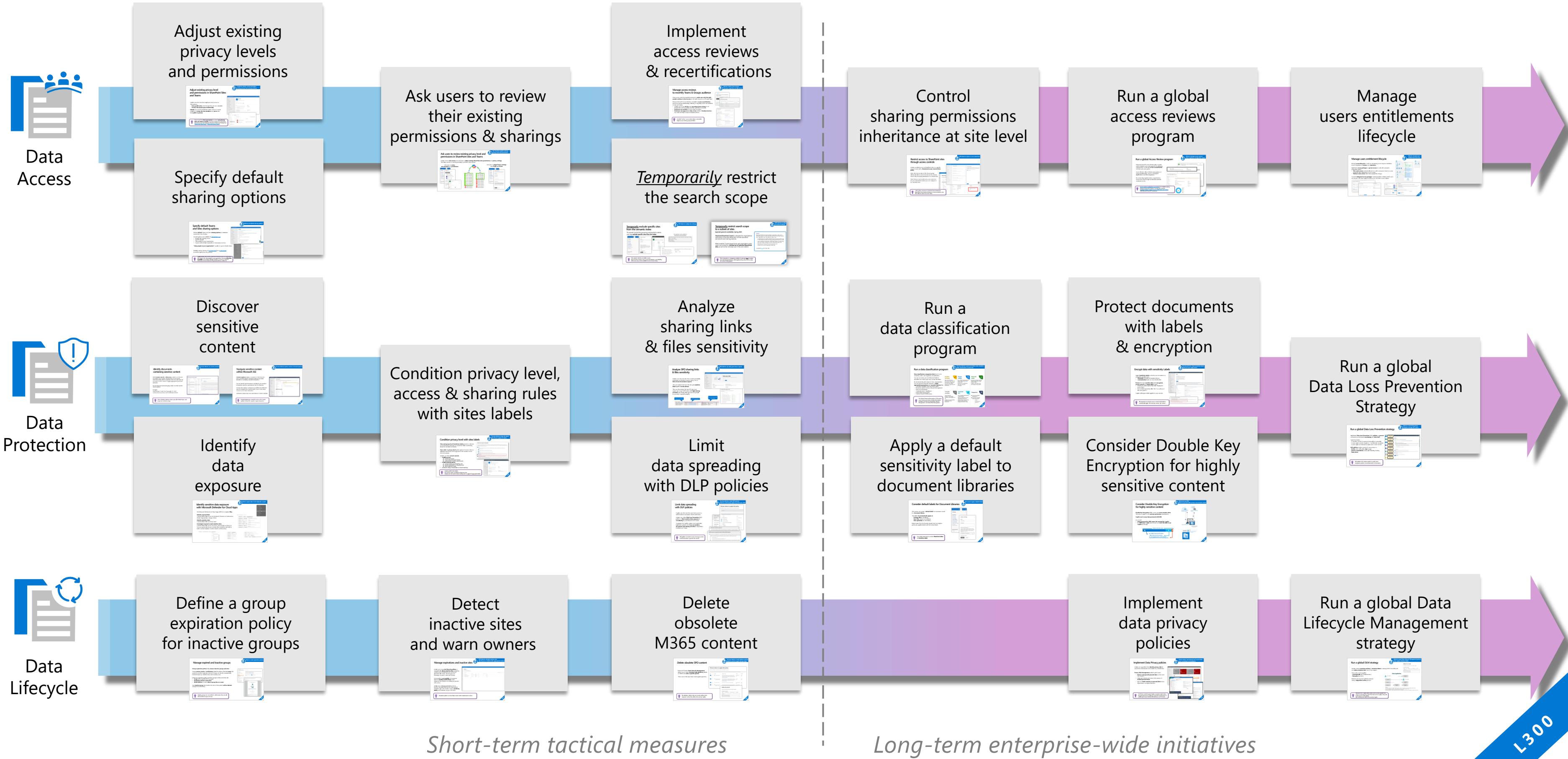
Run a global Data Lifecycle Management program



Short-term tactical measures

Long-term enterprise-wide initiatives

Recommended Practices - More details



Recommended Practices - Microsoft Solutions



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



Discover
sensitive
content



Identify
data
exposure



Condition privacy level,
access & sharing rules
with sites labels



Delete
obsolete
M365 content



Limit
data spreading
with DLP policies



Run a
data classification
program



Apply a default
sensitivity label to
document libraries



Protect documents
with labels
& encryption



Consider Double Key
Encryption for highly
sensitive content



Run a global
Data Loss Prevention
Strategy



Run a global Data
Lifecycle Management
strategy



Define a group
expiration policy
for inactive groups



Implement
access reviews
& recertifications



Run a global
access reviews
program



Manage
users entitlements
lifecycle



Short-term tactical measures

Long-term enterprise-wide initiatives

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



Discover sensitive content



Identify data exposure



Condition privacy level, access & sharing rules with sites labels



Delete obsolete M365 content



Limit data spreading with DLP policies



Run a data classification program



Apply a default sensitivity label to document libraries



Protect documents with labels & encryption



Consider Double Key Encryption for highly sensitive content



Run a global Data Loss Prevention Strategy



Run a global Data Lifecycle Management strategy



Define a group expiration policy for inactive groups



Implement access reviews & recertifications



Run a global access reviews program



Manage users entitlements lifecycle



Short-term tactical measures

Long-term enterprise-wide initiatives

L300

Recommended Practices - Features



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



Microsoft
365

Microsoft 365
SPO - Teams

Microsoft 365
SPO - Teams

Microsoft 365
SPO - Teams

SharePoint
Advanced Management
Sites Lifecycle Policies

SharePoint
Advanced Management
Data Access Governance

Microsoft 365
SPO - Teams

SharePoint
Advanced Management
Restricted Access Control

Priva Risk
Management
Data Privacy policies

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

IPG - E5 Compliance
Sensitivity Labels

IPG - E5 Compliance
Data Loss Prevention

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

IPG - E5 Compliance
DKE

IPG - E5 Compliance
Data Lifecycle
Management

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

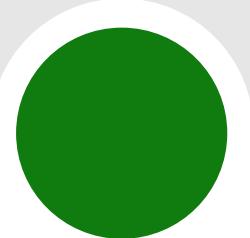
Long-term enterprise-wide initiatives

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)

The screenshot displays two main windows. The top window is titled 'Microsoft Security Copilot (Preview) / My sessions / DLP Alert 376704' and shows a summary of risky activities for a user named John Doe over the last 7 days. It lists four events: browsing to malware websites, sequential activity involving multiple emails, and file uploads to cloud storage. The bottom window is titled 'Microsoft Purview' and shows a detailed alert for a DLP policy match on a document named 'Q2-Customer Data.xlsx'. The alert summary includes details like the alert ID, severity, and the specific SharePoint item involved.

For more information: aka.ms/SecurityCopilot/Purviewblog



Copilot for Security provides two experiences

Standalone experience

Show me the top 5 DLP alerts that I should prioritize today?

> 3 steps completed 38s

Nov 1, 12:34 AM | 38.55s

Displaying top 5 Microsoft Purview Data Loss Prevention (DLP) alerts:

Alert Title	Alert ID	Severity
DLP policy (Avoid Sharing of PAN and Aadhar) matched for email with subject (Details of the users)	dl529eab9c-33b6-42fb-3400-08dbd45e004b	low
DLP policy (Avoid Sharing of PAN and Aadhar) matched for email with subject (Re: Information of the 3 users)	dl43ccf2aa-1cf6-2c46-ee00-08dbd45ddc87	low
DLP policy (Avoid Sharing of PAN and Aadhar) matched for Teams conversation	dle8b407ec-1e0e-0b18-6200-08dbd45d9501	low
DLP policy (Avoid Sharing of PAN and Aadhar) matched for Teams conversation	dl43ccf2aa-1cf6-2c46-0400-08dbd45ce231	low

Export to Excel

Embedded in the Microsoft Purview portal

Contoso | Microsoft Purview

Home

Data Loss Prevention

Overview Reports Recommendations Alerts Policies Explorers Classifiers Scans Apps Related solutions Information Protection Insider Risk Management

Alerts

Export Refresh Filter Reset Filters Time range: 1/23/2023-2/15/2023 User: Any Alert status: Any Alert severity: Any

Alert: DLP policy match for document 'Q2-Customer Data.xlsx'

Alert summary by Security Copilot

The low severity DLP (Data Loss Prevention) alert with ID d583893090588d-2349d-423085-0909328fb2948 was generated on 1 Feb 2023 9:03 AM. The alert is currently in "Active" status and is associated with the user jordan.minke@contoso.com. The file involved in this alert is Q2-Customer Data.xlsx, located at <https://contoso.sharepoint.com/sites/Project1>. The policy responsible for this alert is named "U.S. Financial Data Default Policy" with Policy ID efb767b0-4b45-4948-94b9-b63fb3a773ae. The rule that triggered the alert is "Check Financial Leak" with Rule ID 4bebf668-ab11-4f05-a11a-9cd77323a97. The file was found to contain Credit Card information which is blocked from sharing under the purview of above policy. Additionally, Jordan Minke is marked as Medium risk level in Insider Risk Management.

AI generated. Verify for accuracy.

Alert ID: 583893090588d-2349d-423085-0909328fb2948

Alert status: Active

Alert severity: Low

Time detected: 1 Feb 2023 9:03 AM

View details ...

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

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

Standalone experience

Gain insights on **data risk** and **user risk** profiles, to minimize impending damage.

Start by asking which DLP alerts to prioritize today.

The screenshot shows the Microsoft Security Copilot interface with a dark theme. At the top, it says "Microsoft Security Copilot Preview / My sessions / Show me the top 5 DLP alerts that I should prioritize today?". Below this is a toolbar with icons for copy, share, and export. A modal window is open, titled "Show me the top 5 DLP alerts that I should prioritize today?", indicating "3 steps completed" 38s ago. It displays five DLP alerts:

Alert Title	Alert ID	Severity
DLP policy (Avoid Sharing of PAN and AADHAR) matched for email with subject (Details of the users)	dl529eab9c-33b6-42fb-3400-08dbd45e004b	low
DLP policy (Avoid Sharing of PAN and AADHAR) matched for email with subject (Re: Information of the 3 users)	dl43ccf2aa-1cf6-2c46-ee00-08dbd45ddc87	low
DLP policy (Avoid Sharing of PAN and AADHAR) matched for Teams conversation	dle8b407ec-1e0e-0b18-6200-08dbd45d9501	low
DLP policy (Avoid Sharing of PAN and AADHAR) matched for Teams conversation	dl43ccf2aa-1cf6-2c46-0400-08dbd45ce231	low

At the bottom, there's a prompt bar: "Ask anything about security, or type / for suggestions or * for promptbooks" with a right-pointing arrow. A note at the bottom says "AI-generated content can have mistakes. Make sure it's accurate before using it." A "Private Preview" watermark is in the bottom right corner.

Standalone experience

Gain insights on **data risk** and **user risk** profiles, to minimize impending damage.

Let's **learn more about one specific alert**, by asking Copilot for Security to summarize it.

The screenshot shows the Microsoft Security Copilot interface. At the top, the navigation bar includes 'Microsoft Security Copilot Preview / My sessions / Show me the top 5 DLP alerts that I should prioritize today?'. On the right, there are 'Share' and 'Export' buttons. Below the navigation, two DLP alerts are listed:

- DLP policy (Avoid sharing of PAN and AADHAR) matched for dl43ccf2aa-1cf6-2c46-0400-08dbd45ce231 Teams conversation**: Priority low. Below this alert are three rating buttons: 'Looks right', 'Needs improvement', and 'Inappropriate', followed by a down arrow and a trash icon.
- Can you summarize purview alert 'dl1ee3f0e3-90be-c228-1400-08dbbec1f1ef'**: Status '3 steps completed' 35s ago. Below this is a timestamp 'Nov 1, 12:35 AM | 37.17s'. The summary text details a low-severity DLP alert from September 27, 2023, generated for a user named martinb@woodgrove.ms. It mentions the policy 'Block upload to third party cloud services' with Policy ID 19ba65a6-a0f3-4a1d-924e-9c6b88b14f62, rule 'Block cloud services for Project Olivine' with Rule ID 3c2ef2ec-1d04-4843-be82-e4294fa83449, and a SharePoint workload. The file involved is 'Acquisition timeline.pptx' located at <https://contosodemos2.sharepoint.com/sites/Mark8ProjectTeam/Shared%20Documents/Project%20Documentation/Acquisition%20Timeline.pptx>. It also notes that martinb@woodgrove.ms is marked as High risk level in Insider Risk Management.

At the bottom, a prompt box says 'Ask anything about security, or type / for suggestions or * for promptbooks' with a right-pointing arrow. A note below states 'AI-generated content can have mistakes. Make sure it's accurate before using it.' A question mark icon is in the bottom right corner, and a green diagonal banner in the bottom right corner reads 'Private Preview'.

Standalone experience

Gain insights on **data risk** and **user risk** profiles, to minimize impending damage.

Let's **learn more about the user involved** in this alert and a **summarization of top risk factors**.

The screenshot shows a Microsoft Security Copilot interface. At the top, it says "Microsoft Security Copilot Preview / My sessions / Show me the top 5 DLP alerts that I should prioritize today?". Below the header are standard window controls (close, minimize, maximize). The main content area displays a detailed alert summary for a user:

- User Principal Name: [martinb@woodgrove.ms](#)
- Insider Risk Severity: High
- Alert and case history: 2 active alerts
- User is in scope of 1 policy.
- Top Risk Factors:
 - Sequential activity (Sep 19, 2023 - Sep 25, 2023) - The user is associated with a sequential activity where they downloaded files from OneDrive while syncing, and then copied files to a USB device, for 4 times. The files contained 4 sensitivity labels and priority content, and involved 1 SharePoint site with sensitivity label applied.
 - Cumulative Exfiltration (Sep 11, 2023 - Sep 26, 2023) - The user has done cumulative exfiltration, where he was found to be copying files to a USB device 11 times which is more than 95% compared to teammates, and uploading files to cloud storage 6 times which is more than 97% compared to teammates.
 - User is detected as a potential high impact user (Oct 8, 2023) - User accessed more content with prioritized sensitivity labels than 99% of other users and accessed more content containing sensitive info than other users.
 - Exfiltration (Sep 25, 2023) - User is found to be copying files to a USB device 5 times. The files contained 4 sensitivity labels and priority content.

To get a detailed view of Martin Booth's activities, you can visit: [Microsoft Purview Insider Risk Management](#)

At the bottom, there are three rating buttons: Looks right, Needs improvement, and Inappropriate. To the right of these buttons is a downward arrow and a report abuse icon. A feedback input field at the bottom says "Ask anything about security, or type / for suggestions or * for promptbooks" with a right-pointing arrow. A note at the very bottom states "AI-generated content can have mistakes. Make sure it's accurate before using it."



Copilot for Security provides two experiences

Standalone experience

The screenshot shows a dark-themed web application interface. At the top, a header asks, "Which Purview Data loss prevention alerts/incidents should I prioritize today?". Below this, a section titled "Generated KQL query 1 min" is shown. The main content area displays a table of "Purview Data loss prevention alerts" with columns: Severity, ID, and Time. The table lists four alerts: one High severity and three Medium severity. Below the table, a section titled "Data loss prevention incidents" shows a table with 10 rows and 6 columns. A "Export to Excel" button is available. At the bottom, a note says, "These alerts are ranked from high to low severity. It's important to investigate each alert to determine the potential impact on your organization and take appropriate action." A "How's this response?" link is at the bottom right.

Embedded in the Microsoft Purview portal

The screenshot shows the Microsoft Purview portal interface. On the left, a sidebar menu includes "Home", "Data Loss Prevention" (selected), "Overview", "Reports", "Recommendations", "Alerts" (selected), "Policies", "Explorers", "Classifiers", "Scans", and "Apps". Under "Alerts", there are sections for "Related solutions", "Information Protection", and "Insider Risk Management". The main content area is titled "Alerts" and shows a list of alerts with checkboxes. One alert is selected: "DLP policy match for document 'Q2-Customer Data.xlsx'". To the right, a detailed view of this alert is shown. It includes fields for "Alert ID" (583893090588d-2349d-423085-0909328fbk2948), "Alert status" (Active), "Alert severity" (Low), and "Time detected" (1 Feb 2023 9:03 AM). The alert details state: "The low severity DLP (Data Loss Prevention) alert with ID d583893090588d-2349d-423085-0909328fbk2948 was generated on 1 Feb 2023 9:03 AM. The alert is currently in "Active" status and is associated with the user jordan.minke@contoso.com. The file involved in this alert is Q2-Customer Data.xlsx, located at https://contoso.sharepoint.com/sites/Project1. The policy responsible for this alert is named "U.S. Financial Data Default Policy" with Policy ID efb767b0-4b45-4948-94b9-b63fb3a773ae. The rule that triggered the alert is "Check Financial Leak" with Rule ID 4bebff68-ab11-4f05-a11a-9cd7732a397. The file was found to contain Credit Card information which is blocked from sharing under the purview of above policy. Additionally, Jordan Minke is marked as Medium risk level in Insider Risk Management." An "AI generated. Verify for accuracy." note is present. A "View details" button is at the bottom right.

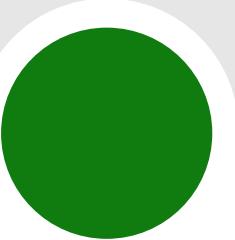
Bring together signals across
Defender XDR, Sentinel,
Intune, Entra and Purview
into a single pane of glass

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

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.

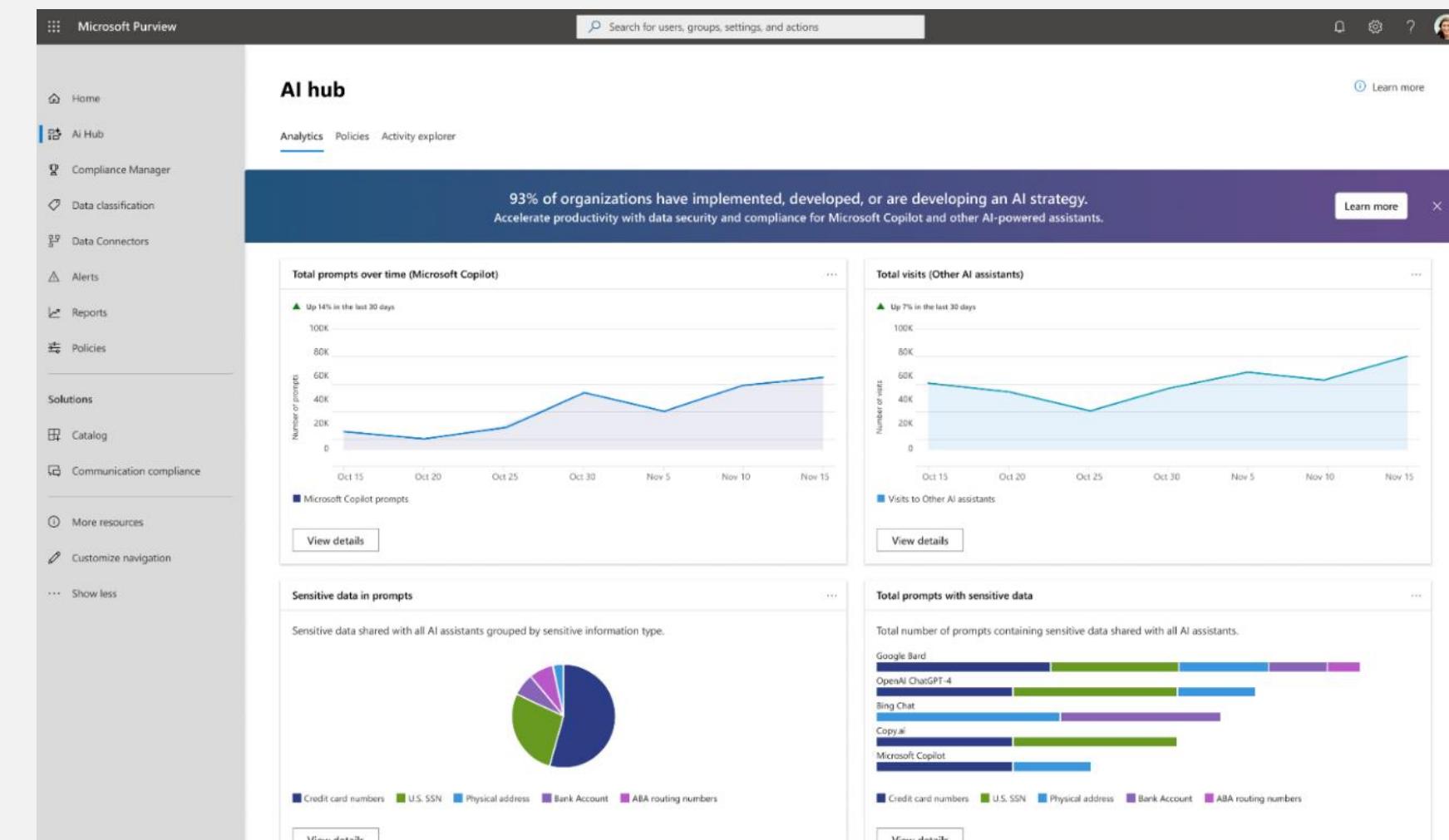
Copilot for M365 understand and honors sensitivity labels and the permissions that come with it.

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.

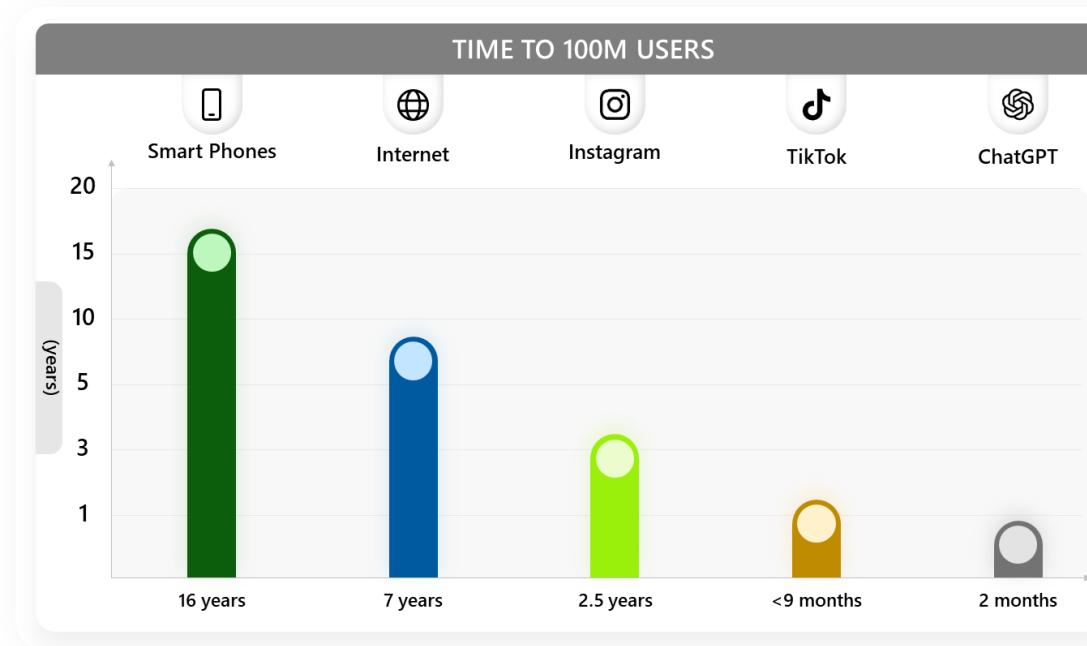
Compliance controls for Copilot for M365 including:

- 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



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



Microsoft Purview AI hub (preview) - Learn more

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.

Total prompts over time (Microsoft Copilot): Up 14% in the last 30 days. Microsoft Copilot prompts (blue line).

Total visits (Other AI assistants): Up 7% in the last 30 days. Visits to Other AI assistants (blue line).

Sensitive data in prompts: Sensitive data shared with all AI assistants grouped by sensitive information type. A pie chart shows the distribution of data types.

Total prompts with sensitive data: Total number of prompts containing sensitive data shared with all AI assistants. A horizontal bar chart lists platforms and their prompt volumes.

Total users (Microsoft Copilot): Total users who created a prompt. A donut chart shows user risk levels.

Total users (other AI assistants): Total users who visited other AI assistants. A donut chart shows user risk levels.

Top users (all AI assistants): Users with Microsoft Copilot activity and browsing activity in other AI assistants. A horizontal bar chart lists platforms and their user counts.

Private Preview

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](#)

X

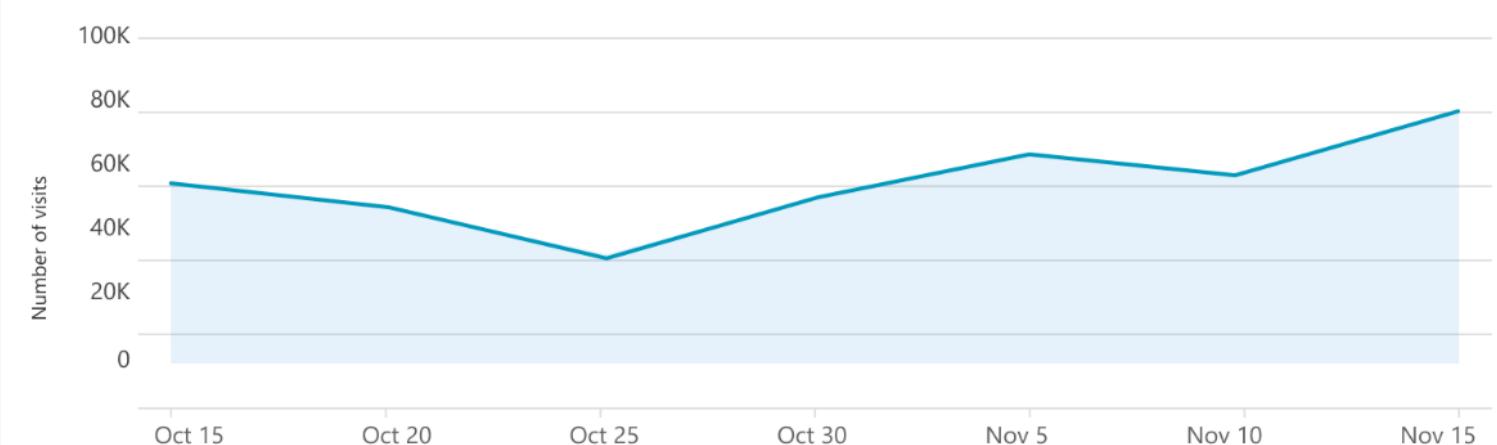
Total prompts over time (Microsoft Copilot)

▲ Up 14% in the last 30 days

[View details](#)

Total visits (Other AI assistants)

▲ Up 7% in the last 30 days

[View details](#)

Sensitive data in prompts

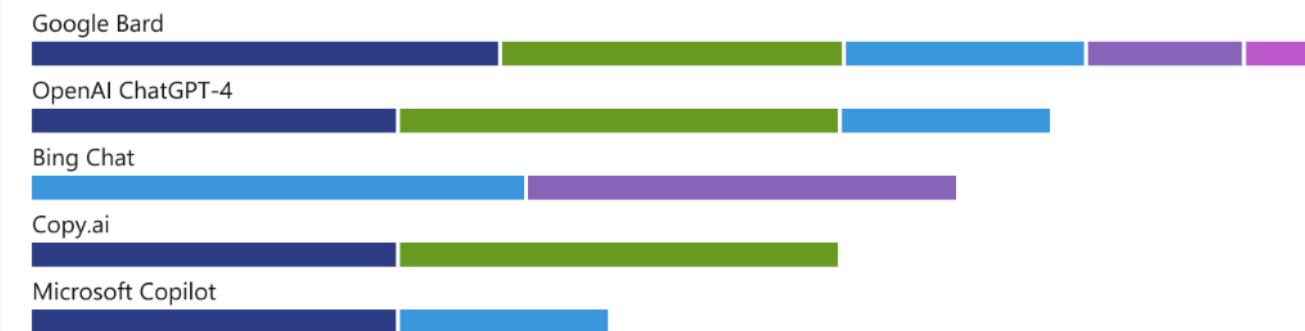
Sensitive data shared with all AI assistants grouped by sensitive information type.



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

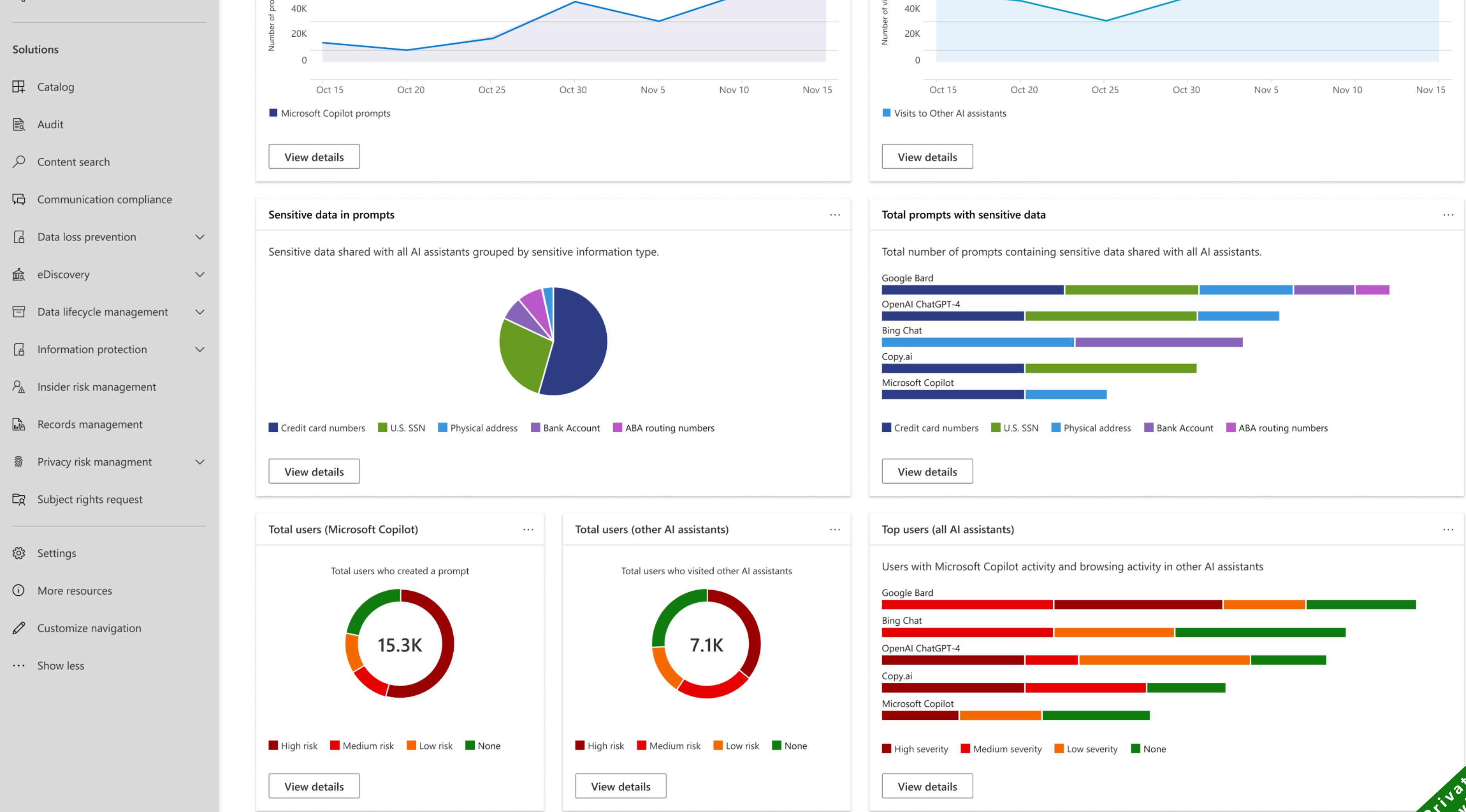
Total prompts with sensitive data

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

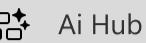


Private
Preview

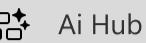
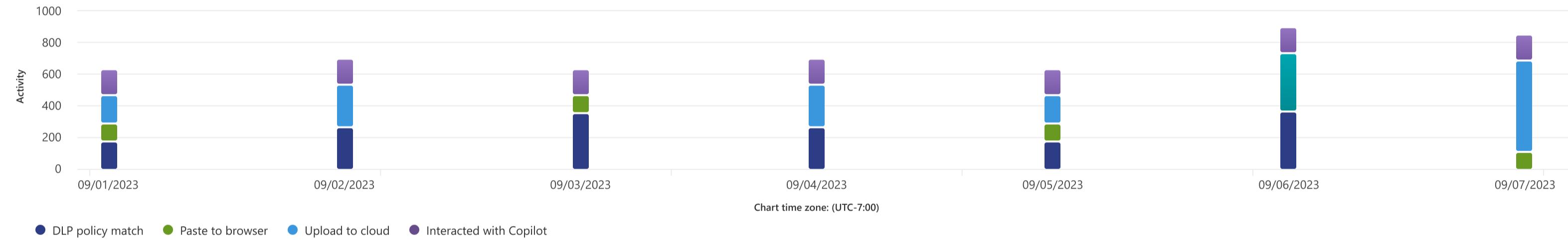
AI hub (preview)

[Recommended actions](#) [Settings](#) [Learn more](#)

Home



Ai Hub


[Analytics](#) [Policies](#) [Activity explorer](#)
[Activity: All values](#)[User: All values](#)[DLP policy matched: All values](#)[Sensitive info type: All values](#)[Add filter](#)[Reset all](#)

Solutions

Catalog



	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

Records management





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

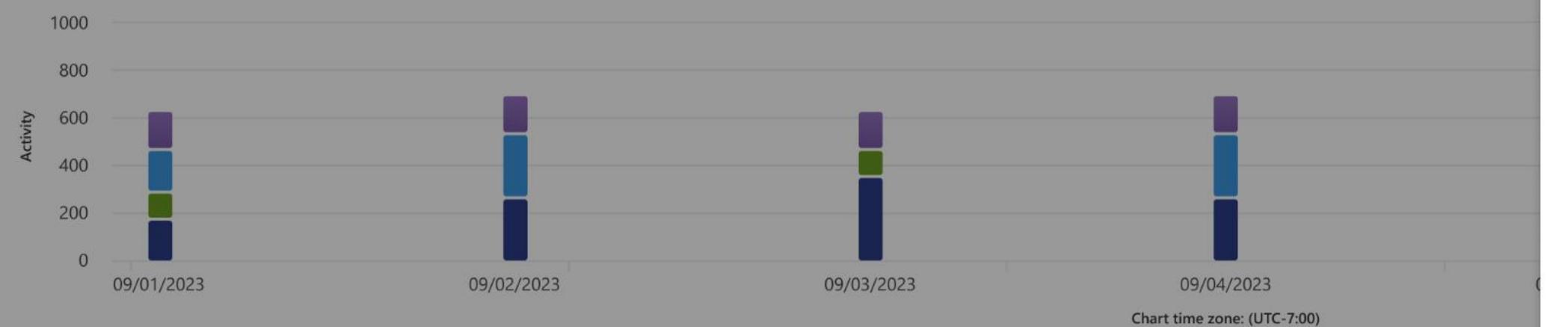
User: All values

DLP policy matched: All values

Sensitive info type: All values

Add filter

Reset all



File upload to cloud

Activity details

Activity
File upload to cloudHappened
Sep 13, 2023 3:54 PM

Client IP

131.109.147.63

Enforcement mode

Audit

Target domain
bard.google.comJIT triggered
False

About this item

User

Mona.Kane@contoso.com

Sensitive info type
Credit card numberPolicy
AI hub – Data Protection

Rule

Audit-UploadToCloud

Location details

Source location type

Destination location type

Unknown

Unknown

Platform

Application

Windows

msedge.exe

Application

Desktop-3453HD

[View device details](#)

MDAIP device ID

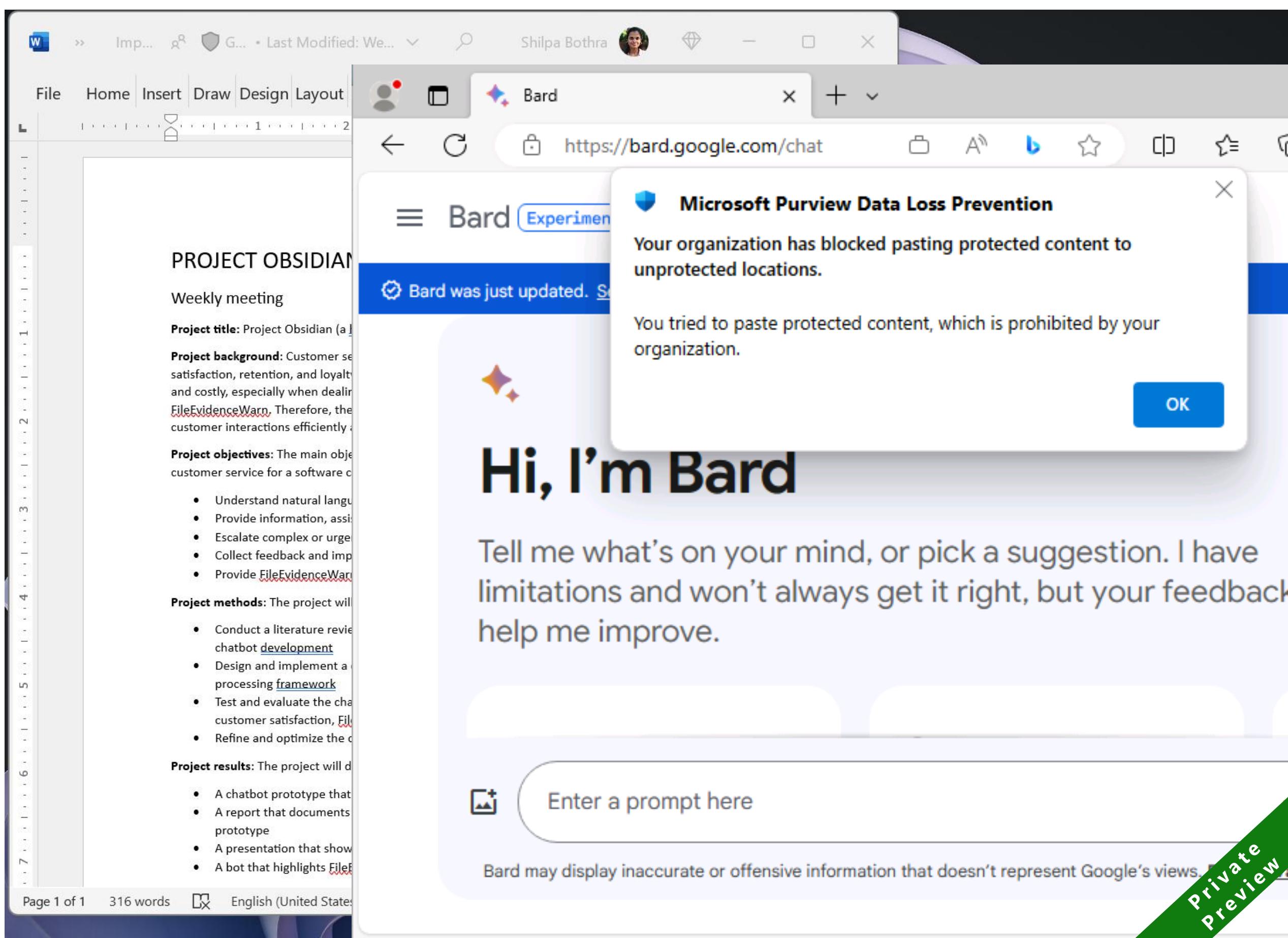
33oe9ca0778b9ec2ab7933ac9f7ehsd1987bacd8

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.

The screenshot shows a Microsoft Word document titled "Important Details on Project O.docx". The document contains several sections with headings and bullet points:

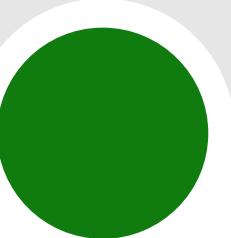
- PROJECT OBSIDIAN**
- Weekly meeting**
- Project title:** Project Obsidian (a high tech chat bot) for Customer Service Improvement
- Project background:** Customer service is an essential aspect of any business, as it affects customer satisfaction, retention, and loyalty. However, providing high-quality customer service can be challenging and costly, especially when dealing with large volumes of inquiries, requests, complaints or FileEvidenceWarn. Therefore, there is a need for an automated and intelligent system that can handle customer interactions efficiently and effectively and perform FileEvidenceWarn.
- Project objectives:** The main objective of this Project Obsidian is to develop a chatbot that can provide customer service for a software company. The chatbot should be able to:
 - Understand natural language inputs from customers and respond appropriately
 - Provide information, assistance, or solutions for common issues or queries
 - Escalate complex or urgent cases to human agents if needed
 - Collect feedback and improve its performance over time
 - Provide FileEvidenceWarn
- Project methods:** The project will use the following methods to develop the chatbot:
 - Conduct a literature review and a market analysis to identify the best practices and tools for chatbot development
 - Design and implement a chatbot prototype using a cloud-based platform and a natural language processing framework
 - Test and evaluate the chatbot prototype using various metrics, such as accuracy, usability, and customer satisfaction, FileEvidenceWarn
 - Refine and optimize the chatbot prototype based on the test results and feedback
- Project results:** The project will deliver the following results:
 - A chatbot prototype that can provide customer service for a software company
 - A report that documents the design, implementation, testing, and evaluation of the chatbot prototype
 - A presentation that showcases the features, benefits, and challenges of the chatbot prototype
 - A bot that highlights FileEvidenceWarn
- Project conclusion:** The project will conclude by demonstrating that a chatbot can be an effective and efficient solution for customer service improvement. The project will also provide insights and

At the bottom of the screen, there is a green diagonal banner with the text "Private Preview".

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?