



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





# Tim Hermie

**Technical Specialist Data Security**

Former Microsoft MVP Enterprise Mobility

Former Windows Insider MVP

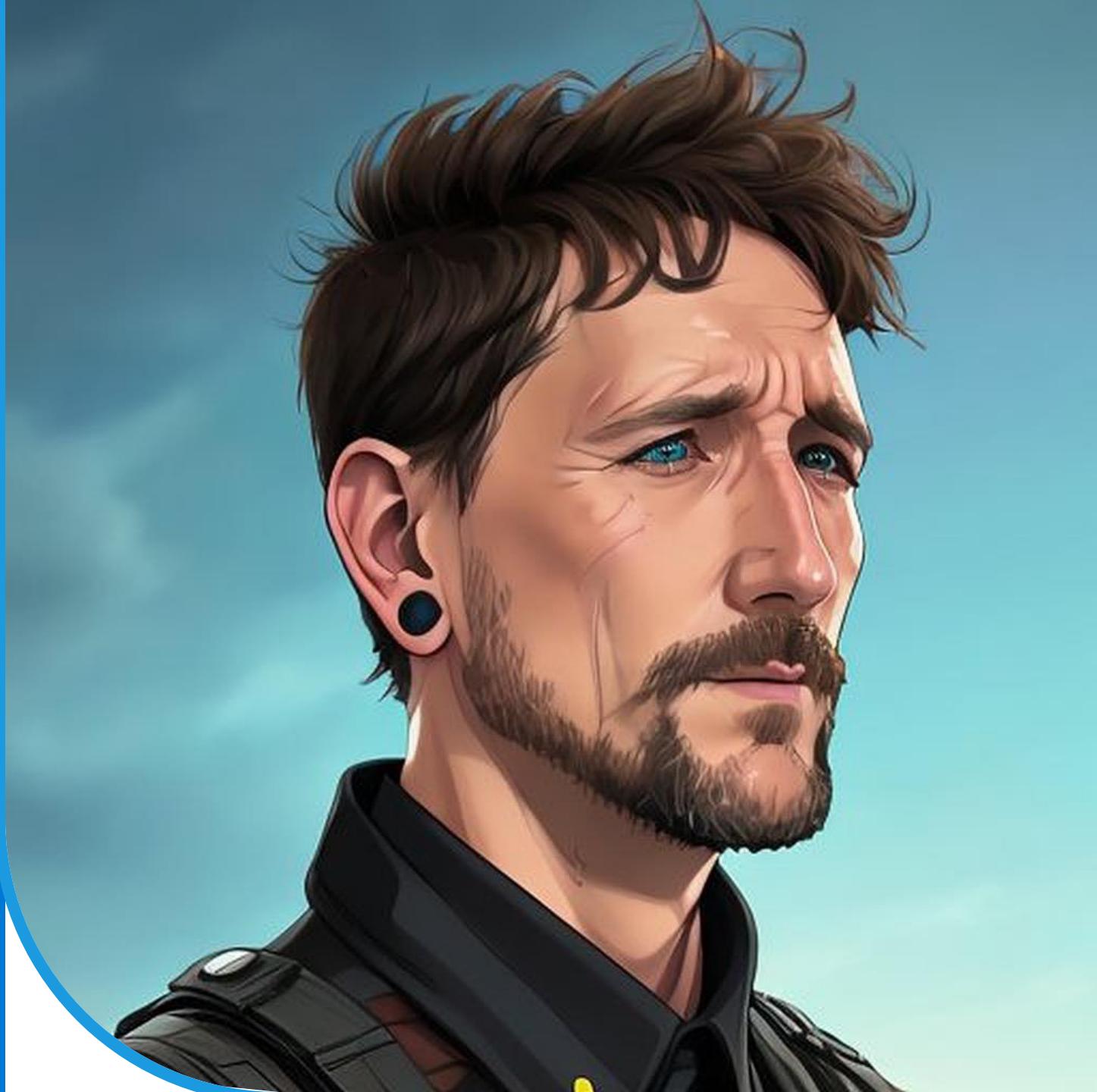
Microsoft Most Valuable Mentor

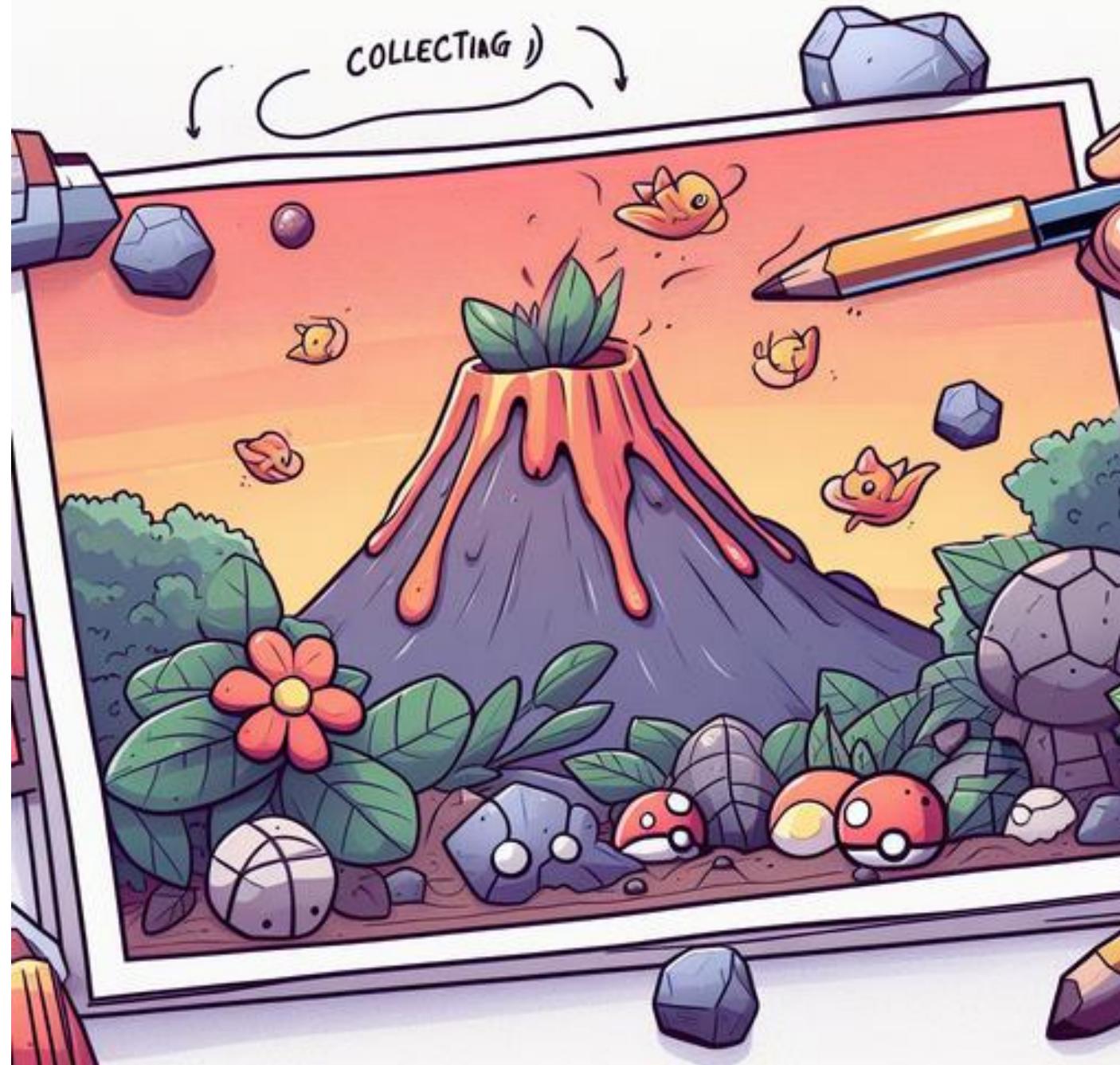
Microsoft Certified Trainer

Founding Board Member MC2MC

@\_Cloud\_boy

*Drums – World Explorer – Volcano Addict – Foodie*





# Agenda



**Securing generative AI**  
growing usage



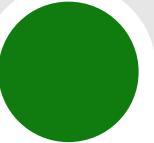
**Copilot for Microsoft 365**  
with **Microsoft Purview**



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



**A glimpse into the future**  
& **secure 3<sup>rd</sup> party GenAI**



# Agenda



## **Securing generative AI growing usage**



## **Copilot for Microsoft 365 with Microsoft Purview**



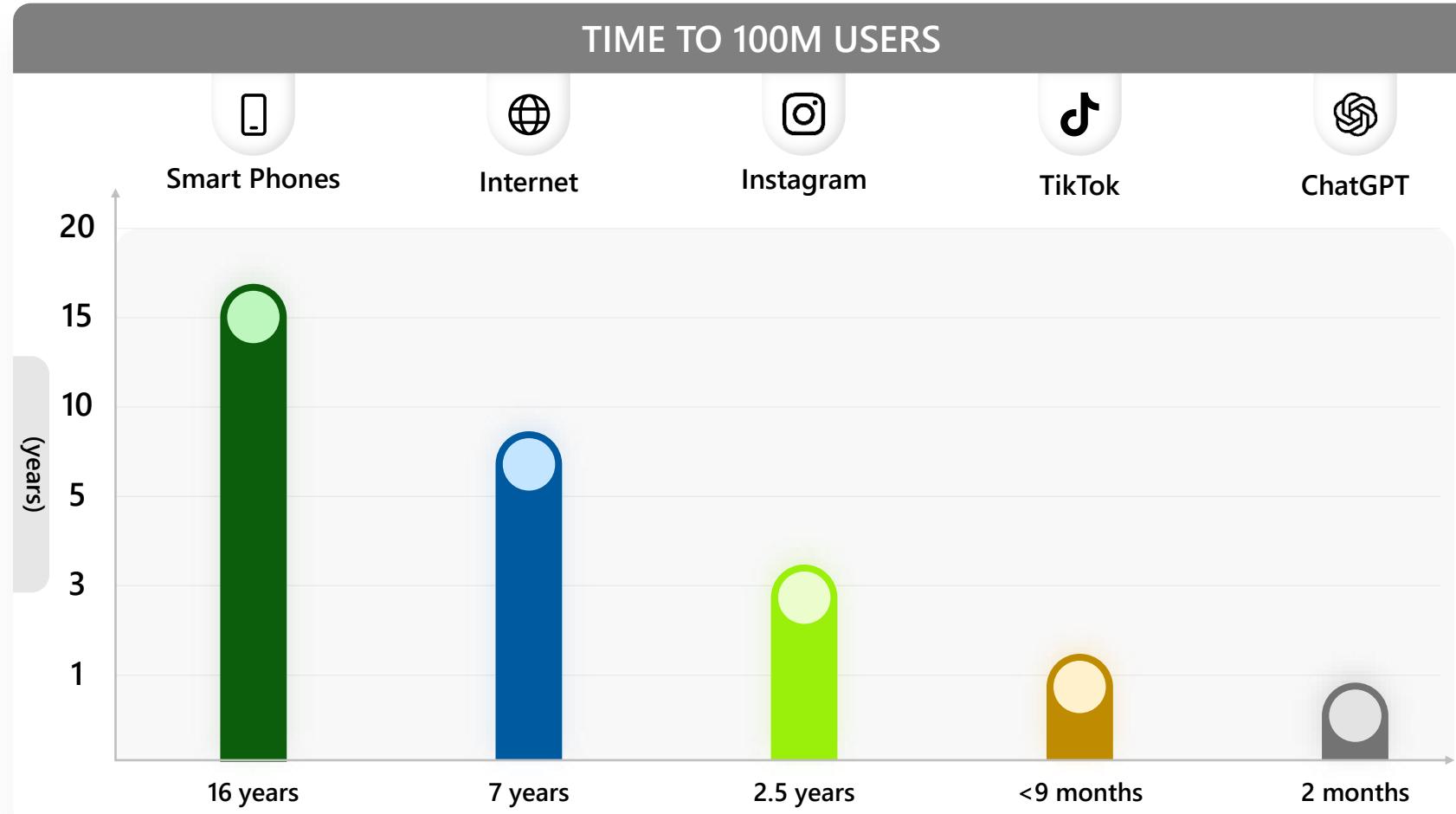
## **Copilot for Security for/in Microsoft Purview**



## **A glimpse into the future & secure 3<sup>rd</sup> 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 concern<sup>1</sup>



Lack of controls to govern data shared in AI

60%+

of business leaders worry about AI bias and ethical concerns<sup>1</sup>



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.<sup>3</sup>

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

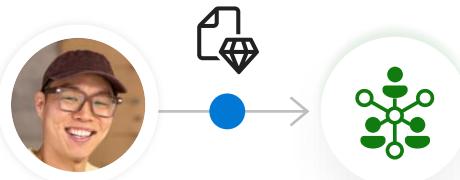


Insufficient visibility into the usage of AI applications can result in security and compliance challenges.

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



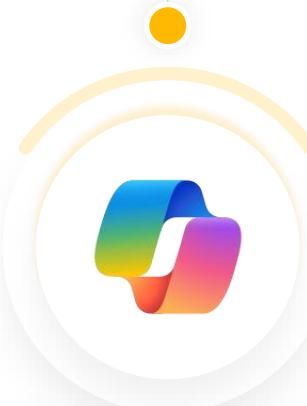
# Microsoft Purview

Comprehensive solution to secure and govern AI

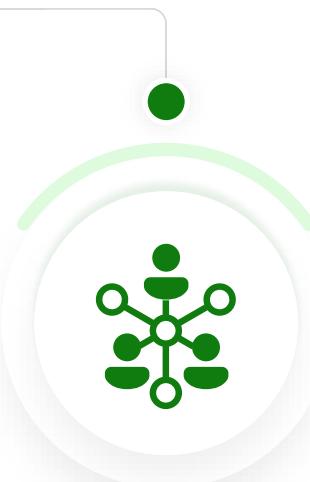
Across all AI applications



Enterprise built AI



Microsoft Copilot



Third-party AI

# Microsoft Purview – High Level Overview



## 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.

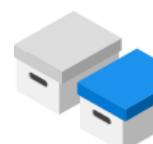


## Audit (Premium)

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.

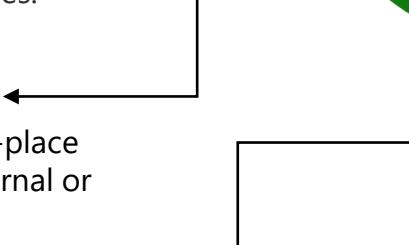
## Data Lifecycle Management

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.



## 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.

## Records management

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



# 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.



## 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

## 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



## Endpoints



## Sensitivity Labels

Public  
Confidential  
General  
...



## Non-Microsoft apps



## On-premises

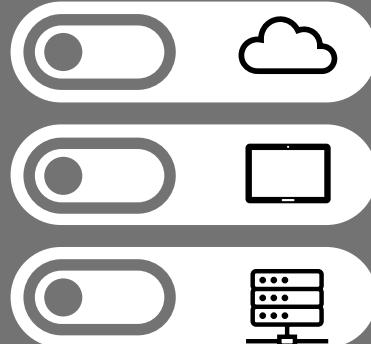


# Unified and **flexible** policy management

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



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

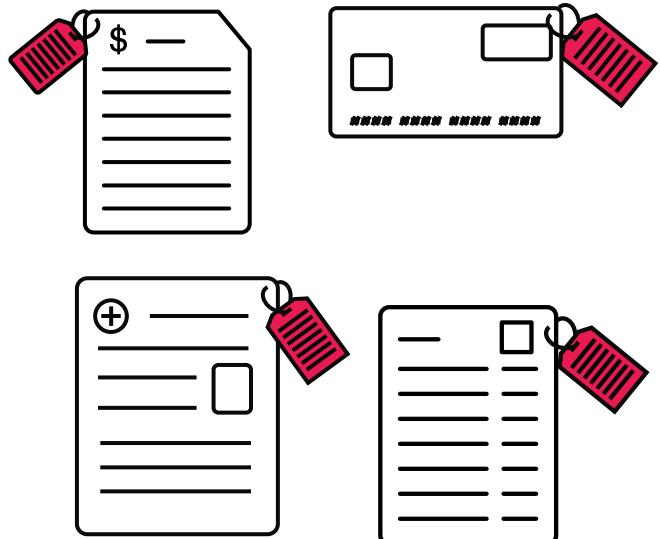


# Integrated insights and alerting

Enrich policy and investigation with rich signals

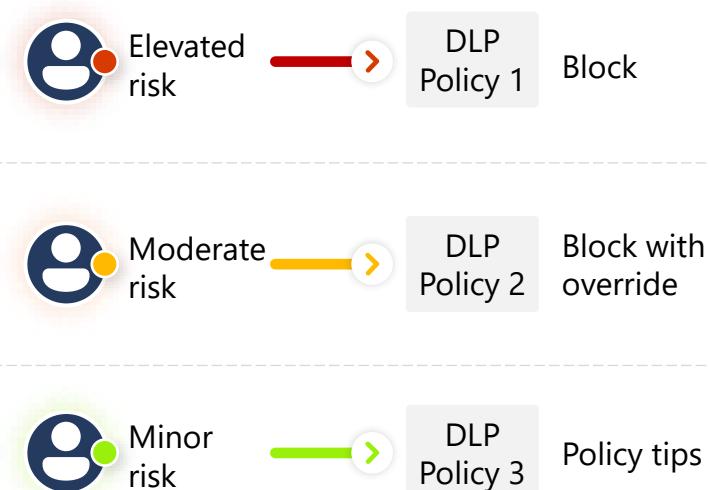
## Know the context

Leverage classification and labeling on sensitive data from Information Protection



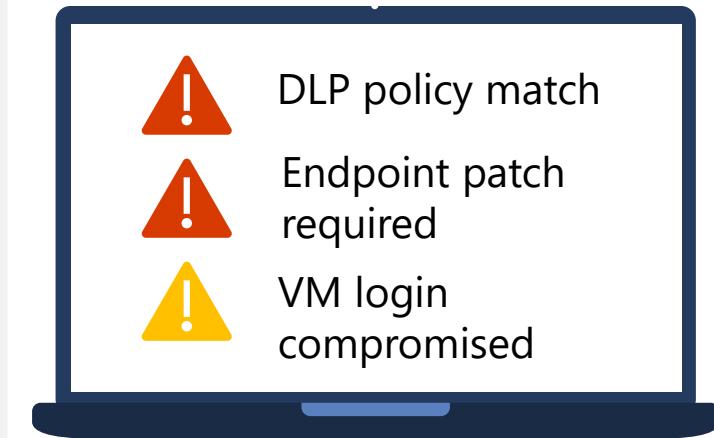
## Understand the intent

Automatically apply risk insights from Insider Risk Management to DLP policies



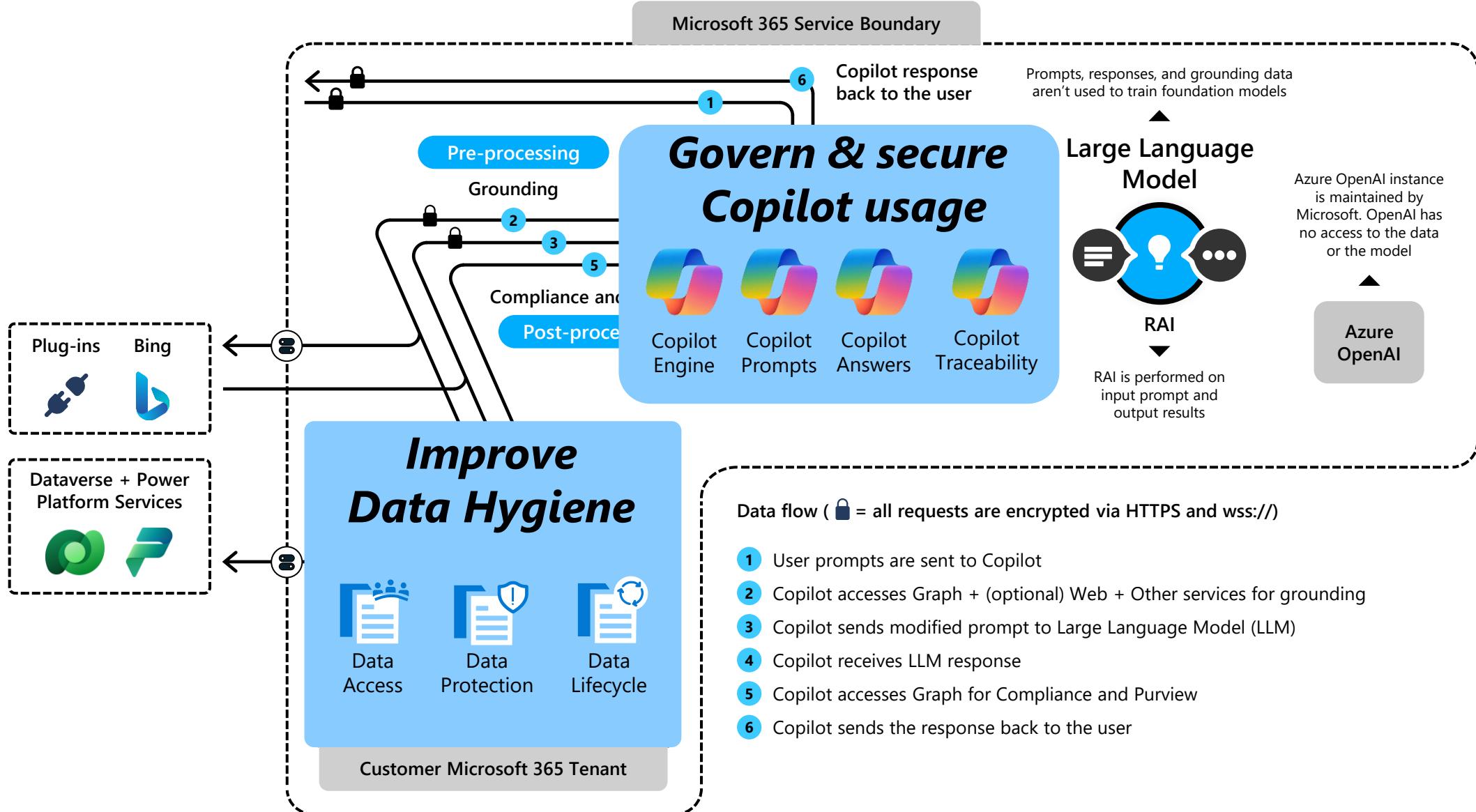
## Integrate alert investigation

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





# 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

## **Govern & secure Copilot usage**



Copilot  
Prompts



Copilot  
Answers

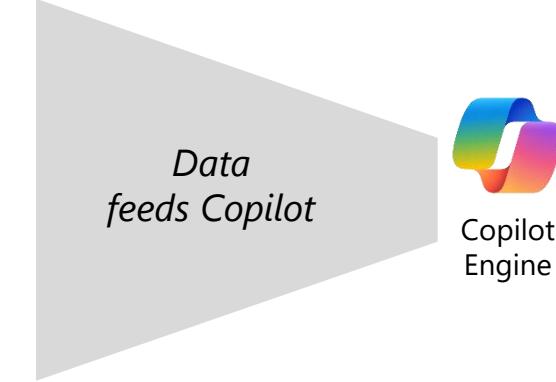


Copilot  
Traceability

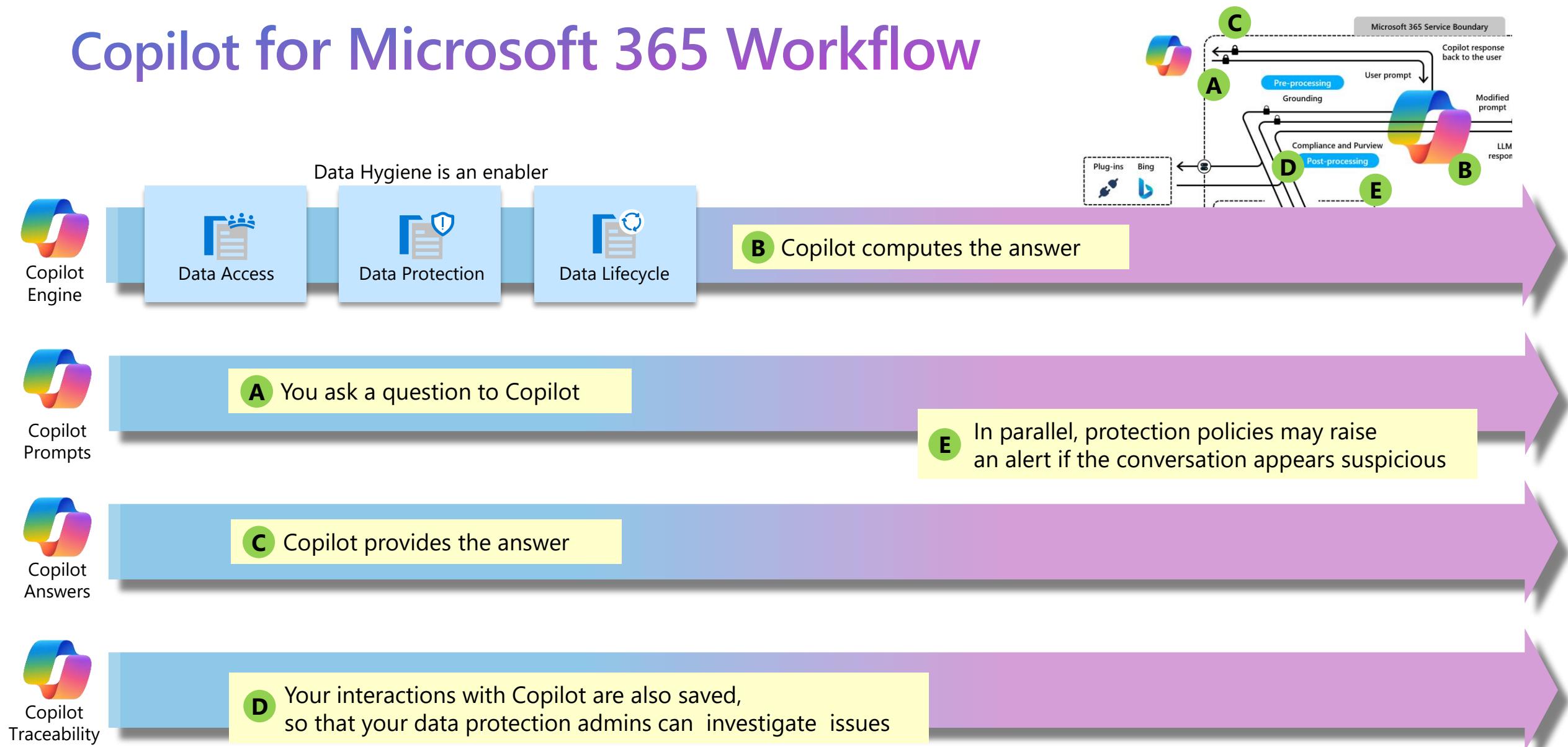
Monitor Prompts Content

Retain & Investigate Interactions

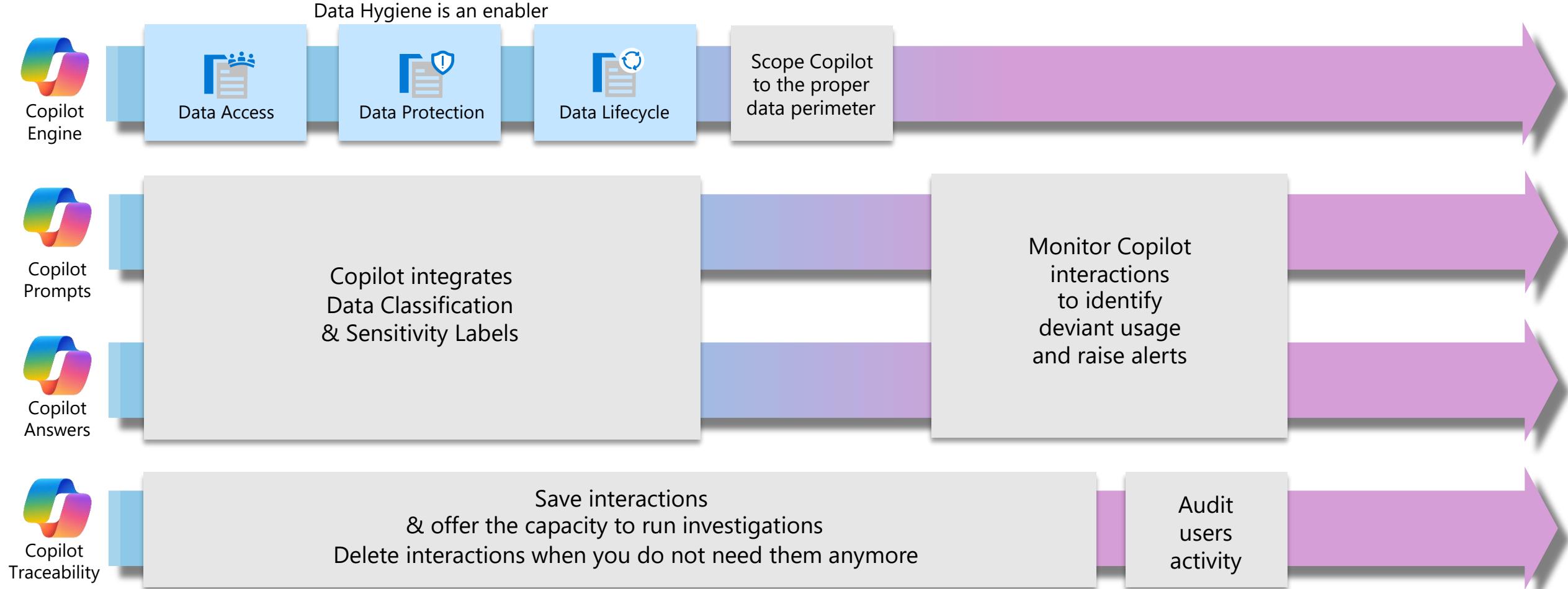
Audit Copilot Activity



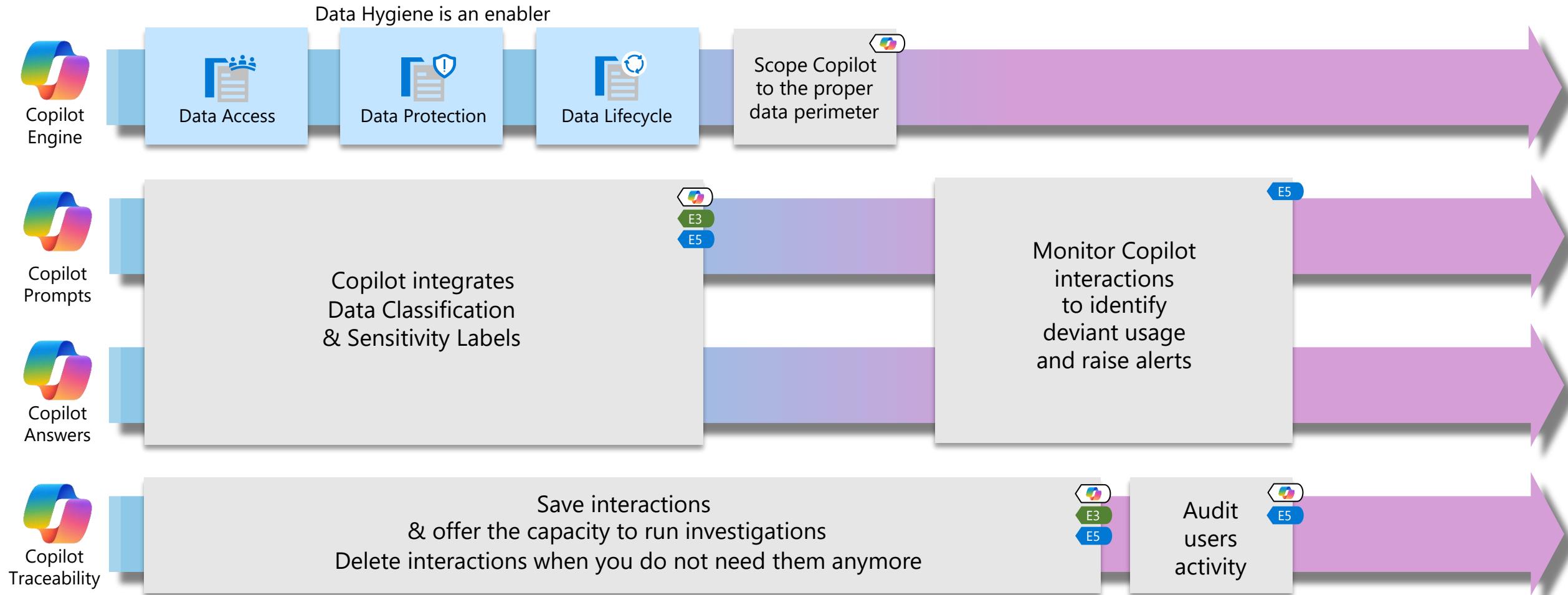
# Copilot for Microsoft 365 Workflow



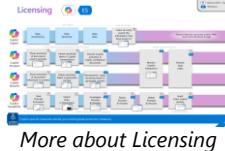
# Purview manages Copilot for M365 usage over time



# Purview manages Copilot for M365 usage over time



# Manage Copilot for Microsoft 365 usage over time



Data Access

Data Hygiene is an enabler



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



Monitor Copilot interactions



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

Audit users activity

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 search bar and a navigation menu with 'Copilot' (highlighted), 'Preview', 'Chat', 'About', 'FAQs', and 'What's new'. Below the menu, a message from Copilot says: 'I can search across docs and messages to give you summaries, help you answer business questions, and quickly draft content. I'm here to help but do make mistakes—so please check content for accuracy and share your feedback.' It asks the user to 'Ready to explore? Select one of the suggestions below to get started...' with three options: '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 says: 'You can always use the prompt guide for suggestions by selecting this button' with a small icon. In the main conversation area, a user message at 11:17 AM reads: 'What happened in the 10am meeting and show me related documents'. Copilot responds at 9:16 AM: '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.' A link to '2023\_Fabrikam\_Resources' is provided. Below the response, Copilot offers 'Copy' and 'Edit in Word' buttons. At the bottom, it says '1 reference' and '1/20 AI-generated content may be incorrect'. The footer includes 'More concise', 'Show more detail', and a 'Copilot' button. A large input field at the bottom says 'Ask a work question or use / to reference files, people, and more' with a placeholder 'Ask a work question or use / to reference files, people, and more' and icons for 'More concise', 'Show more detail', and a 'Copilot' button.



# 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. The ribbon menu is visible at the top, showing tabs like File, Home, Insert, Layout, References, Review, View, and Help. The Home tab is selected. Below the ribbon are the standard font and paragraph toolbars. A floating "Draft with Copilot" dialog box is open in the center of the screen. The dialog has a text input area that says "Describe what you'd like to write, including notes or an outline, and Copilot can generate a draft to help get you started" with a character count of "0 / 2000". At the bottom of the dialog are two buttons: "Generate" and "Reference a file". In the bottom right corner of the slide, there is a blue diagonal banner with the text "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**.

A screenshot of the Microsoft 365 Chat interface. On the left is a vertical navigation bar with icons for Home, Create, My Content, Feed, Apps, M365 Chat, Outlook, Teams, Word, Excel, and PowerPoint. The main area shows a conversation with "M365 Chat" and the subject "Summarize Ignite Talk Track.do...". Below the subject is the date "November 8, 2023 at 07:14 PM". A blue button labeled "Summarize Ignite Talk Track.docx" is visible. A callout box contains text about the document "Ignite Talk Track.docx", mentioning it was last modified by Alex Wilber and describes its content. A "Copy" button is present. Below the text is a note: "1 reference ^" followed by a citation card for "Ignite Talk Track". The citation card includes the file type (Word), author (Alex Wilber), modification date (11/08/23), and a snippet of the document's 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 screen 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 large blue diagonal banner in the bottom right corner contains the text "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. A user has asked the AI: "Who are the Microsoft Partners in FY24?". The AI has provided a response and included three references:

- 1 FY22 Field Execution Guide**: Confidential\Any User (No Protection)
- 2 FY24 Partner Activation Seller Toolkit**: Confidential\Microsoft FTE
- 3 To-Partner\_FY24 Kick Off GSI Pilot Partner Cybersecurity Investment -Final-10-10-202...**: General

A callout box highlights the sensitivity label for the first reference: "Confidential\Microsoft FTE Data is classified and protected. Microsoft Full Time Employees (FTE) can edit, reply, forward and print. Recipient can unprotect content with proper justification." A note at the bottom right says "AI-generated content may be incorrect".



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.

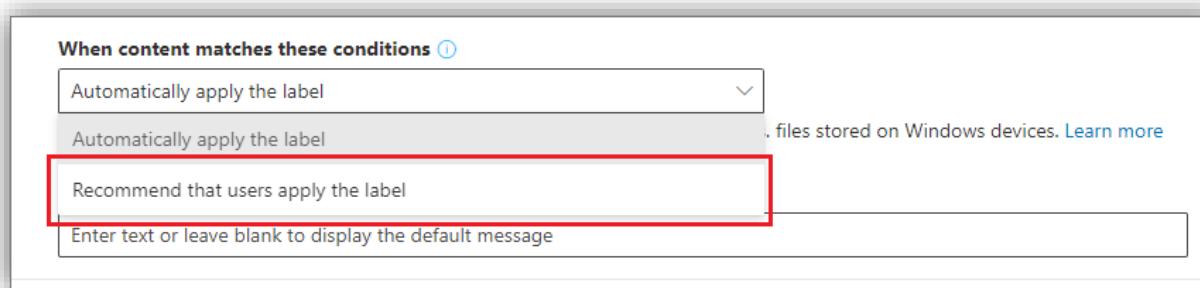
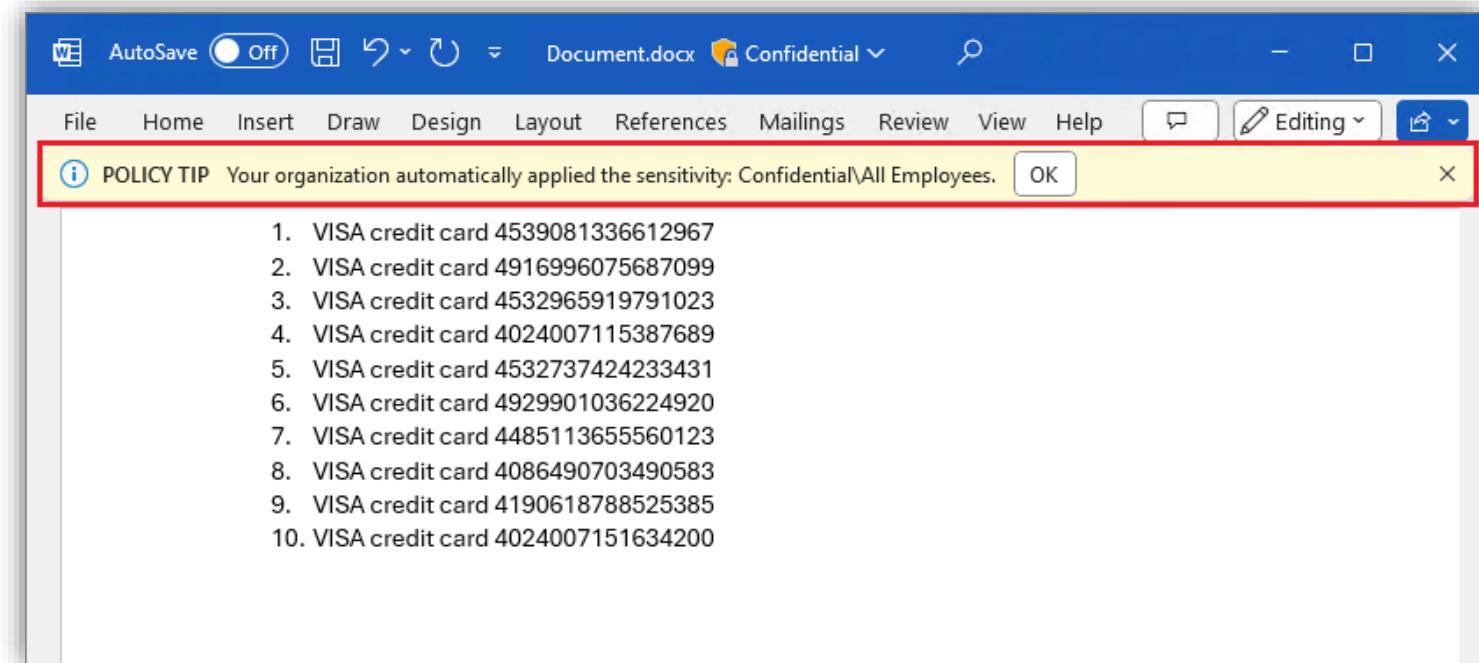
The screenshot shows a Microsoft Word document titled "AI hub A platform for data security and compliance for AI". The document contains several paragraphs of text. A callout bubble highlights the first paragraph: "AI hub: A new platform for data security and compliance for AI". Below this, a sub-section titled "Introduction" discusses the challenges and risks of AI in the context of data privacy regulations and ethical standards. Another callout bubble highlights the section "Key features of AI hub", which lists features such as data discovery and classification. At the bottom of the screen, a Copilot interface is visible with options to "Summarize How t...", "Keep it", and "For example, 'Make it more engaging'". The status bar at the bottom indicates the document has 214 words and is in English (U.S.).



# 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.

The screenshot shows the Microsoft Purview interface for Communication Compliance. On the left, a navigation pane lists various compliance categories like Home, Compliance Manager, Data classification, Data connectors, Alerts, Policies, Roles & scopes, Trials, Solutions, Catalog, Audit, Content search, and several sub-sections under Communication compliance (Data loss prevention, eDiscovery, Data lifecycle management, Information protection, Information barriers, Insider risk management, Records management, Privacy risk management, Subject rights requests). The main area displays a list of alerts under the heading "Communication compliance > Policies > Confidential project". The alert list shows 57 pending and 5 resolved alerts, with filters for Body/Subject, Date, Sender, and Tags. A specific alert for "Copilot in Word" is selected, showing details about the sender (adelevance@contoso.com) and recipient (Copilot). To the right, a detailed view of the Copilot interaction in Microsoft Word is shown. It includes a summary of the prompt ("Conditions detected: Secret Projects (Dragon)"), the prompt itself ("Give me a summary of project dragon and when it will be announced?"), and the response from Copilot ("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"). Action buttons at the bottom include Resolve, Summarize, Notify, and Tag as.



Admins create DLP policies  
Analysts manage DLP alerts

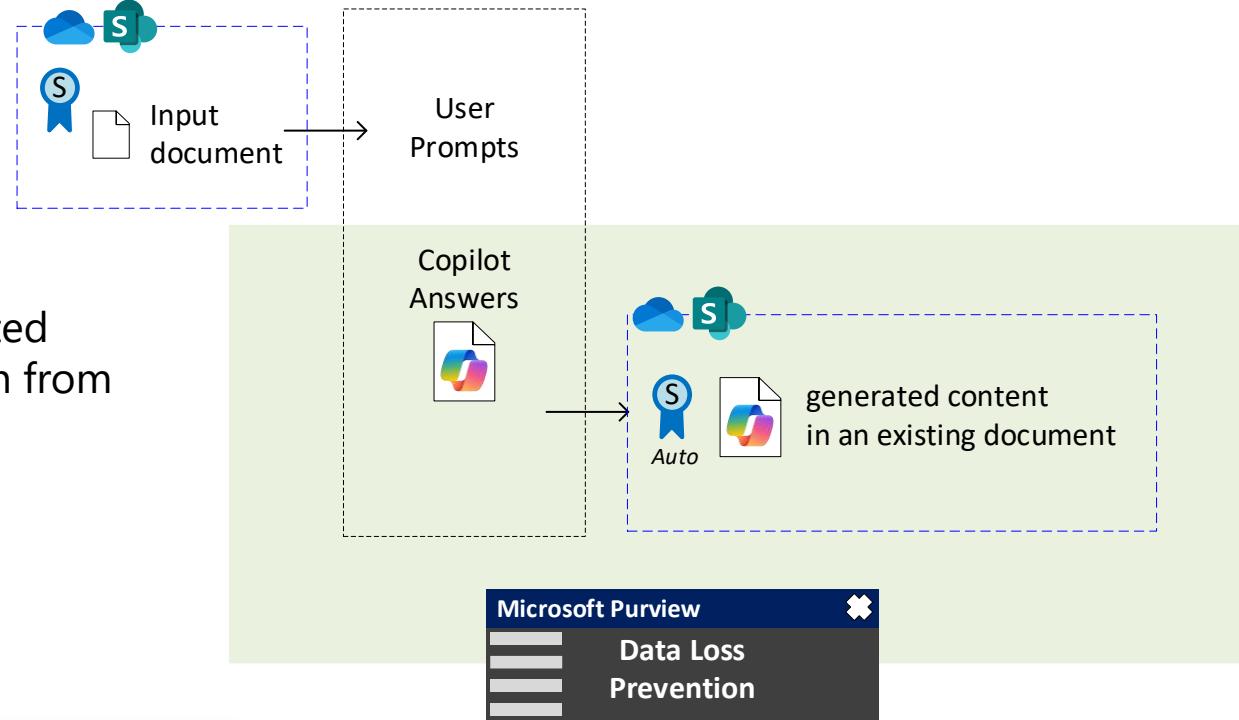
# Protect generated content with Data Loss Prevention policies

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**



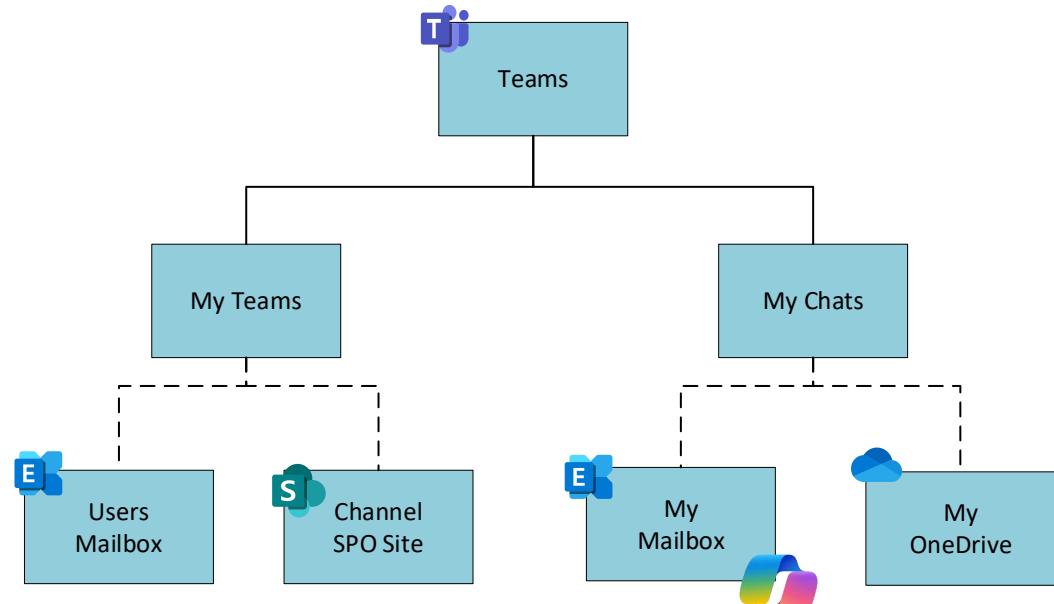


*This process is purely automatic & transparent*

# 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](#).



Microsoft 365 Copilot



# 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 the company logo, 'Contoso Electronics', 'Microsoft Purview', and various global navigation icons. The main workspace displays a list of 30 selected items under the heading 'eDiscovery (Premium) > Cases > Check Copilot data is available > Only Word CP without date'. A sidebar on the left contains a vertical list of icons for document types like Word, Excel, and PDF. The central area features a table with columns for Subject/Title, Status, Tag Status, and Date (UT). Item 6 is highlighted with a blue checkmark. To the right, there's a 'Summarize this doc' section with tabs for Source, Plain text, Annotate, and Metadata. Below this, pinned metadata from MOD Administrator is shown, including the email address, timestamp (11/1/2023 8:06 AM), and a summary of the document content. At the bottom, a 'Copilot in Word' summary is provided, detailing the document's purpose and executive summary. The footer indicates 'Viewing: Page 1 of 1' and '50 items/page'.

Subject/Title	Status	Tag Status	Date (UT)
This is a new top le...	Ready	No Tag	Nov 2, 2023
Summarize	Ready	No Tag	Nov 2, 2023
Partnership Agree...	Ready	No Tag	Nov 1, 2023
Write about Seattle	Ready	No Tag	Nov 1, 2023
I wonder if this gal...	Ready	No Tag	Nov 1, 2023
Summarize this doc	Ready	No Tag	Nov 1, 2023
summarize papling...	Ready	No Tag	Oct 31, 2023
What's the purpos...	Ready	No Tag	Oct 31, 2023
Summarize this doc	Ready	No Tag	Oct 31, 2023
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 'Contoso Electronics' and 'Microsoft Purview'. A circular profile icon with 'WHO' is in the top right. Below the navigation, the title 'Data lifecycle management' is displayed, along with tabs for 'Overview', 'Retention policies' (which is selected), 'Labels', 'Label policies', 'Adaptive scopes', 'Policy lookup', and 'Import'. A note 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 care about.' A tooltip indicates that if role group permissions are restricted, only policies for those users/groups can be managed. Below this, there are buttons for 'New retention policy', 'Edit', 'Delete', 'Disable policy', 'Export', 'Inactive mailbox', and 'Refresh'. A table lists 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

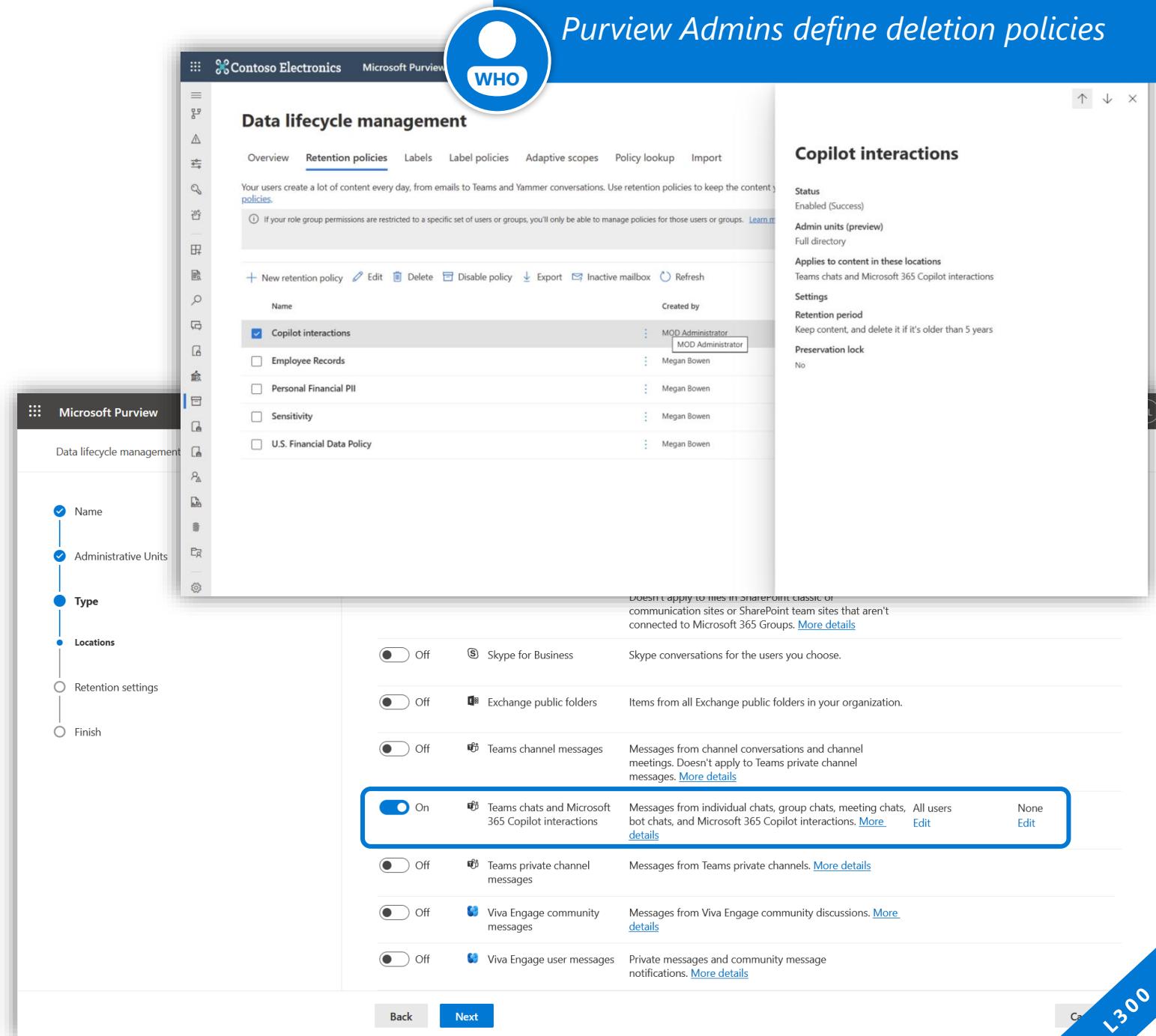
On the right side, there are sections for 'Copilot interactions' status (Enabled (Success)), 'Admin units (preview)', 'Full directory', 'Applies to content in these locations' (Teams chats and Microsoft 365 Copilot interactions), 'Settings', 'Retention period' (Keep content, and delete it if it's older than 5 years), and 'Preservation lock' (No). Below these, there's a note about SharePoint classic sites. The main table has rows for 'Skype for Business', 'Exchange public folders', 'Teams channel messages', and 'Teams chats and Microsoft 365 Copilot interactions' (which is highlighted with a blue border). Other rows include 'Teams private channel messages', 'Viva Engage community messages', and 'Viva Engage user messages'. At the bottom, there are 'Back' and 'Next' buttons.

# 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 circular profile icon with 'WHO' is in the top right. Below the navigation, the title 'Data lifecycle management' is displayed, along with tabs for 'Overview', 'Retention policies' (which is selected), 'Labels', 'Label policies', 'Adaptive scopes', 'Policy lookup', and 'Import'. A note 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 care about.' A tooltip indicates that if role group permissions are restricted, only policies for those users/groups can be managed.

The main area shows a table of 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 wizard-like flow: 'Name' (checked), 'Administrative Units' (checked), 'Type' (checked), 'Locations', 'Retention settings', and 'Finish'. The 'Type' step is highlighted with a blue dot.

The 'Retention policies' section has a table of rules:

Type	Status	Description
Skype for Business	Off	Skype conversations for the users you choose.
Exchange public folders	Off	Items from all Exchange public folders in your organization.
Teams channel messages	Off	Messages from channel conversations and channel meetings. Doesn't apply to Teams private channel messages. <a href="#">More details</a>
Teams chats and Microsoft 365 Copilot interactions	On	Messages from individual chats, group chats, meeting chats, All users bot chats, and Microsoft 365 Copilot interactions. <a href="#">More details</a> <a href="#">Edit</a>
Teams private channel messages	Off	Messages from Teams private channels. <a href="#">More details</a>
Viva Engage community messages	Off	Messages from Viva Engage community discussions. <a href="#">More details</a>
Viva Engage user messages	Off	Private messages and community message notifications. <a href="#">More details</a>

At the bottom, there are 'Back' and 'Next' buttons. On the right side of the slide, there's a blue diagonal banner with 'L300'.

**Copilot interactions**

- 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
- 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 contains the query "copilot". Under the "Copilot activities" section, the option "Interacted with Copilot" is selected. The search results table shows one item: "Nov 2 - Nov 2 Christie Cline" with a status of "Completed" and 81 results. The interface includes sections for "Date and time range (UTC)", "Keyword Search", "Admin Units", and "Users", "File, folder, or site", and "Workloads". A sidebar on the left provides navigation links for various audit types.

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

# Manage Copilot for Microsoft 365 usage over time

## Licensing



E5



Copilot Engine

Data Access

Data Hygiene is an enabler



Data Protection

Data Lifecycle



Scope Interactions

Users can only search the information they have access to.

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



Copilot Prompts

Show sensitivity of documents used in prompts



Inherit sensitivity labels in Copilot conversations



Prevent Copilot activation in highly-confidential documents

E5

Monitor Copilot interactions

E5

Apply DLP policies to the Copilot outputs

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



Copilot Traceability

Save Prompts &amp; Answers



Search Data in Interactions



Investigate Prompts &amp; Answers

E5

Retain Prompts &amp; Answers

E5

Delete Prompts &amp; Answers

E5

Audit Users Copilot Activity

E5

Preserve Interactions &amp; run investigations

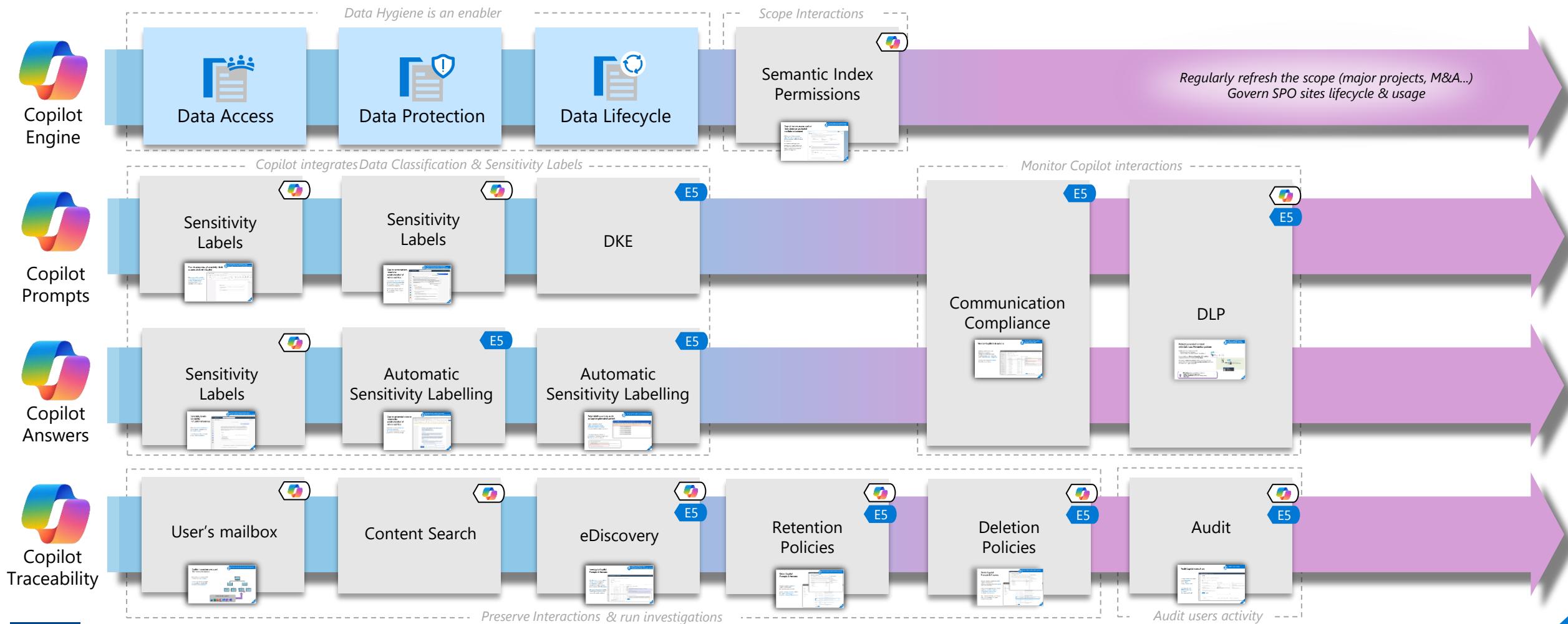
Audit users activity

# Manage Copilot for Microsoft 365 usage over time

## Features



E5



Copilot-specific measures extend your existing data-protection measures

# 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

*Implement  
Short-term  
tactical  
measures*

*Leverage existing  
Long-term  
enterprise-wide  
initiatives*

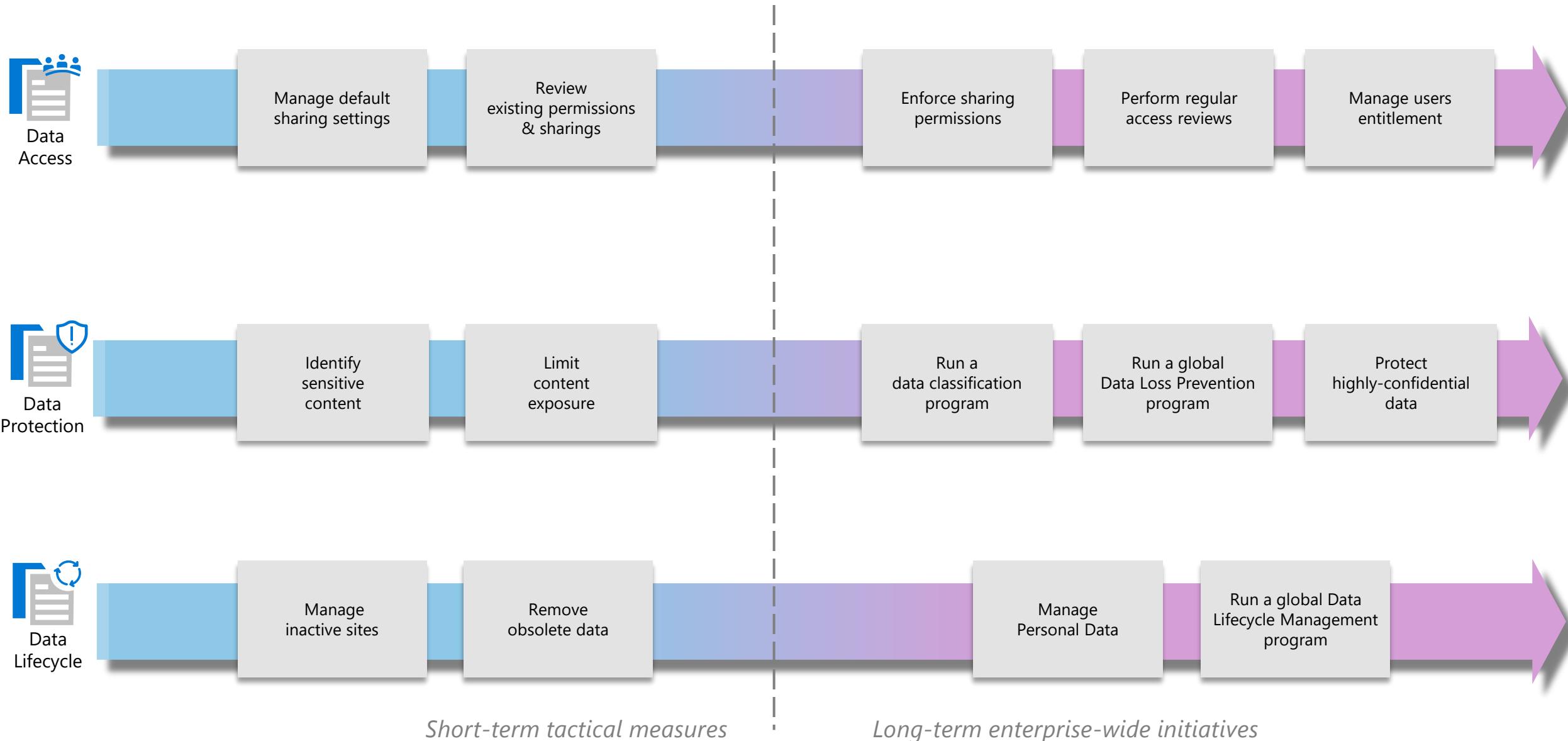


Data  
Protection



Data  
Lifecycle

# Recommended Practices for Microsoft 365 Data



# Recommended Practices for Microsoft 365 Data Licensing



E5

Add-on



Data Access

Manage default sharing settings



Review existing permissions & sharings



E5

+ SharePoint SAM

Enforce sharing permissions

with SharePoint SAM

Perform regular access reviews

+ Entra ID Governance

Manage users entitlement

+ Entra ID Governance



E5



Data Protection

Identify sensitive content



E5

Limit content exposure



E5

+ SharePoint SAM

Run a data classification program



E5

Run a global Data Loss Prevention program



E5

Protect highly-confidential data



E5



Data Lifecycle

Manage inactive sites



E5

Remove obsolete data



E5

+ SharePoint SAM

Manage Personal Data

with Priva Risks

Run a global Data Lifecycle Management program



E5

Short-term tactical measures

Long-term enterprise-wide initiatives

# Recommended Practices - Licensing

-  Native to O365 + 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



Protect documents with labels & encryption



Run a global Data Loss Prevention Strategy



Define a group expiration policy for inactive groups



Implement access reviews & recertifications



Run a global access reviews program



Manage users entitlements lifecycle



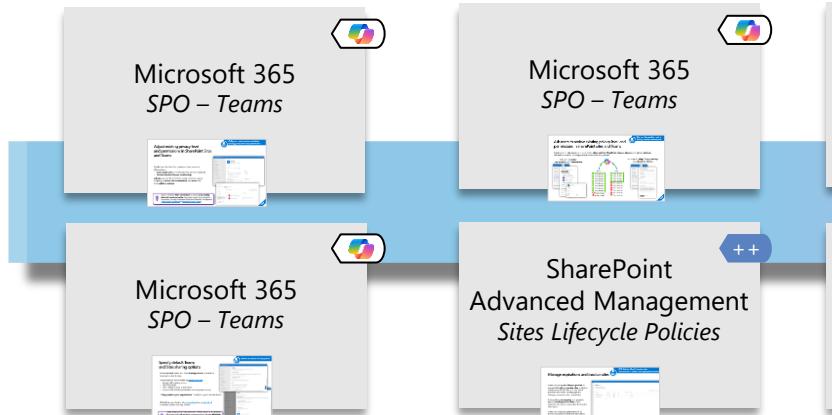
Short-term tactical measures

Long-term enterprise-wide initiatives

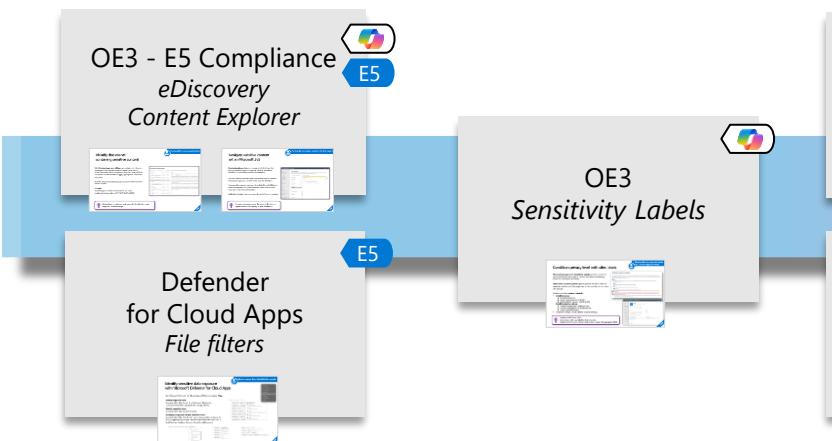
# Recommended Practices - Features



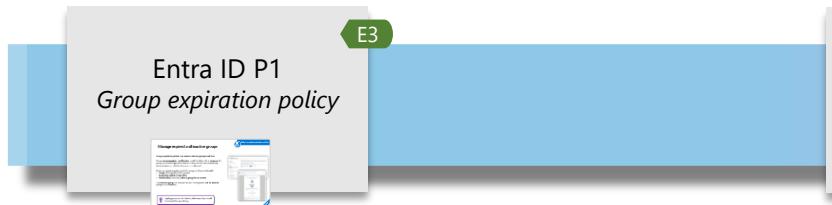
Microsoft  
365



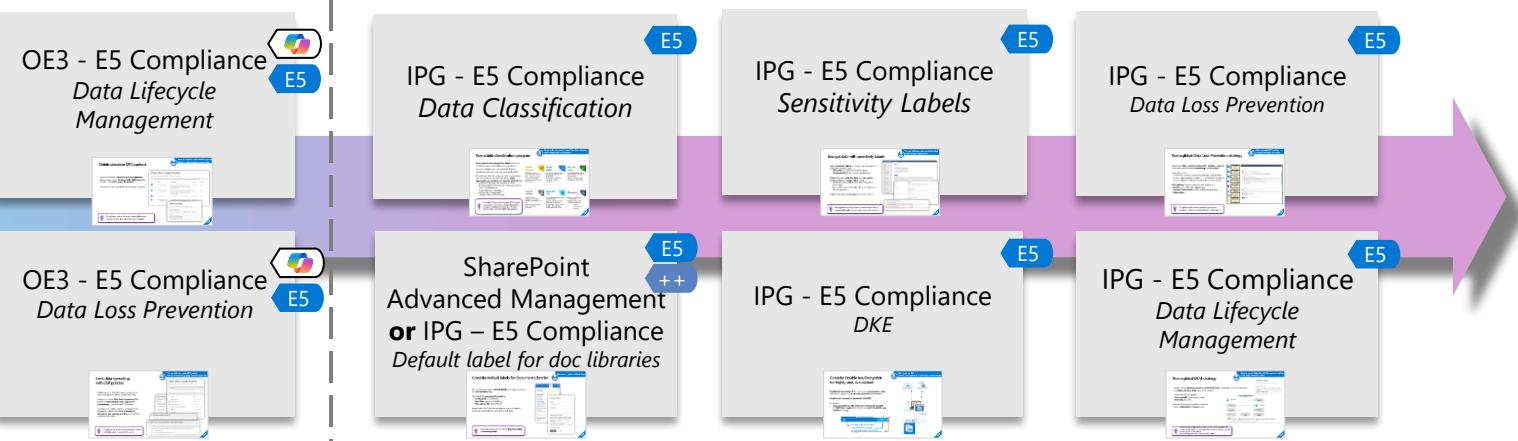
Microsoft  
Purview



Microsoft  
Entra



Short-term tactical measures



Long-term enterprise-wide initiatives

# 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 3<sup>rd</sup> 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 the Microsoft Security Copilot interface. At the top, it shows a navigation bar with 'Microsoft Security Copilot' and 'My sessions'. Below the navigation bar, there are two main sections:

- Alerts:** A card titled 'Show me any risky activities from this user in the past 30 days' with a status of '3 steps completed' and 1 min. It lists several risky activities:
  - Browsed to Malicious websites (Oct 18th, 2023)
  - Downloaded attachments from SharePoint, OneDrive, or Microsoft 365
  - Sequential activity (Oct 18th, 2023 - Oct 18th, 2023) The user is associated with a sequential activity where they downloaded files from SharePoint and then sent emails with attachments outside the organization 3 times.
  - Exfiltration attempt (Oct 18th, 2023) The file contained 1 sensitive file.The files contained 3 sensitive files and priority content.
- File Activity:** A card titled 'Can you share all the files this user worked on or accessed in last 7 days?' with a status of '2 steps completed' and 1 min. It shows a list of files:
  - RevenueDetailsForProject.xlsx
  - RevenueProjects.xlsx
  - CuttingApprovals.pdf
  - ProjectDeadlineScope.docx5 items > 2 columns.

Below these cards, there is a search bar and a 'How's this response?' button. The bottom of the page features a 'Related solutions' sidebar with links to 'Information Protection' and 'Insider Risk Management'.

On the right side of the screen, there is a separate window titled 'Alert: DLP policy match for document 'Q2-Customer Data.xlsx''. This window contains detailed information about the alert, including:

- Alert summary:** Summary of the alert.
- Details:** A table with columns for 'Alert ID', 'Alert status', 'User', 'Event ID', 'Time detected', and 'Alert severity'.
- Event Log:** A table showing event details for the alert.
- User Activity Summary:** A table showing user activity related to the alert.
- Data:** A table showing data details for the alert.

For more information: [aka.ms/SecurityCopilot/Purviewblog](https://aka.ms/SecurityCopilot/Purviewblog)



# 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" displays a table of alerts. The table has columns for Severity (High/Medium), ID, and Time. There are four entries:

Severity	ID	Time
High	9a87660d-dd45-d3fa-f600-08dbd0c22cfb	19 Jun 2023 9:43 AM
Medium	583893090588d-2349d-423085-0909328fbk2948	1 Feb 2023 at 9:03 AM
Medium	a7b0f87f-1f2e-1e2e-f200-08dbd0bf1a33	10 Oct 2023 5:20 PM
High	48ff601b-9003-07f3-0a00-08dbd09be5fb	5 May 2023 at 2:08 PM

Below the table, a section titled "Data loss prevention incidents" shows "10 rows x 6 columns". A "Export to Excel" button is available. A note at the bottom states: "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 also present.

## Embedded in the Microsoft Purview portal

The screenshot shows the Microsoft Purview portal interface with a sidebar for "Data Loss Prevention" and a main "Alerts" page. The alerts list shows multiple entries, with one specific alert expanded. The expanded alert details are as follows:

**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-423085-0909328fbk2948 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/Project>.

The policy responsible for this alert is named "U.S. Financial Data Default Policy" with Policy ID efb7b70-4b45-4948-94b9-b63fb3a773ae. The rule that triggered the alert is "Check Financial Leak" with Rule ID 4b4eff68-a011-4f05-a11a-9cde77323a97.

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-423085-0909328fbk2948  
**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

# Agenda



**Securing generative AI**  
growing usage



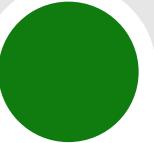
**Copilot for Microsoft 365**  
with **Microsoft Purview**



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



**A glimpse into the future**  
& secure 3<sup>rd</sup> 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.

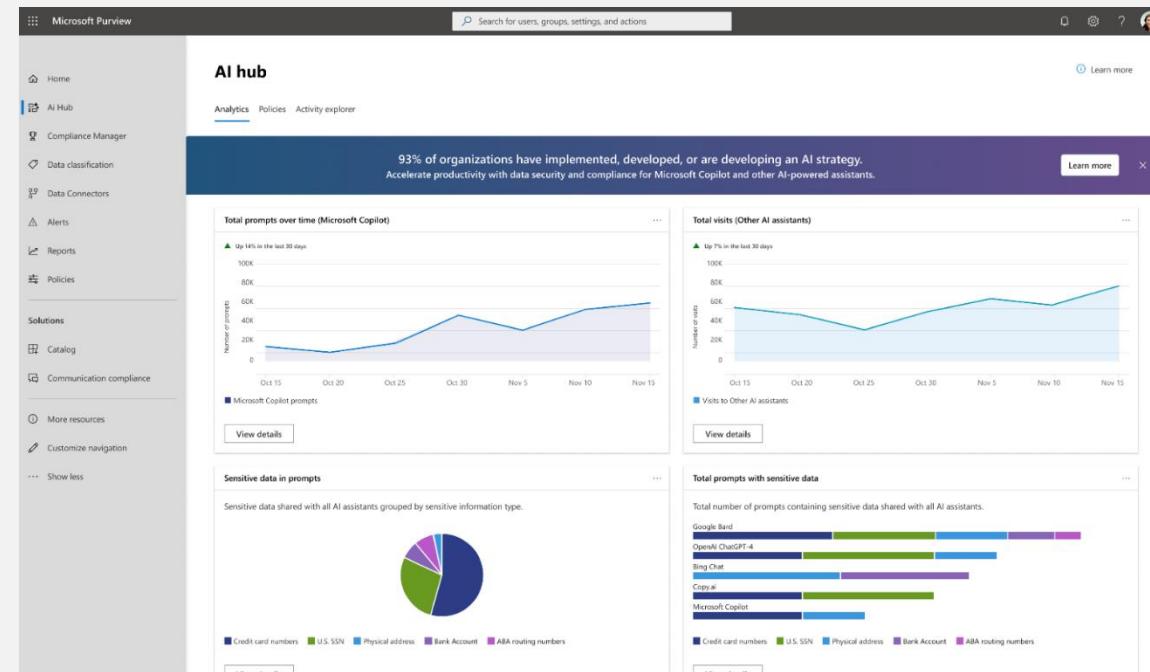
### Policies to secure data in AI prompts and responses.

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:

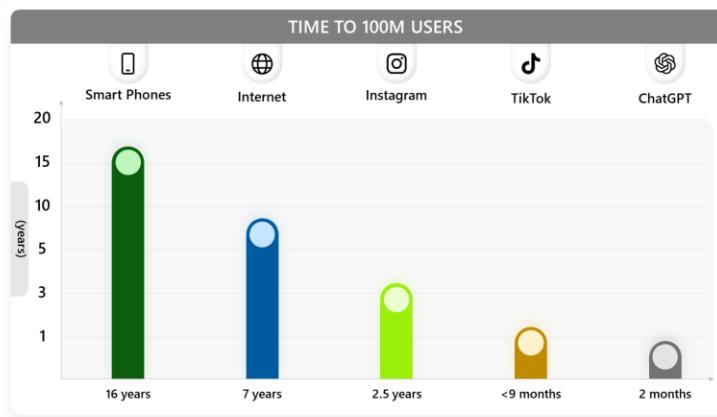
- Capture Copilot interactions with Audit (users, time, docs accessed etc.)
- Preserve, collect, and analyze Copilot interactions for investigations and litigations with eDiscovery
- Retention and deletion policies for Copilot interactions with Data Lifecycle Management
- Detecting business or regulatory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



For more information: [aka.ms/PurviewAI/Blog](https://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



The screenshot shows the Microsoft Purview AI hub (preview) interface. The left sidebar includes links for 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, Privacy risk management, Subject rights request, Settings, More resources, Customize navigation, and Show less. The main content area features several cards:

- AI hub (preview)**: A banner stating "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." with a "Learn more" button.
- Total prompts over time (Microsoft Copilot)**: A line chart showing the number of prompts from Oct 15 to Nov 15. It indicates a 14% increase in the last 30 days. The chart includes a "View details" button.
- Total visits (Other AI assistants)**: A line chart showing visits from Oct 15 to Nov 15. It indicates a 7% increase in the last 30 days. The chart includes a "View details" button.
- Sensitive data in prompts**: A pie chart showing the distribution of sensitive data types. The categories are Credit card numbers (blue), U.S. SSN (green), Physical address (red), Bank Account (purple), and ABA routing numbers (pink). The chart includes a "View details" button.
- Total prompts with sensitive data**: A horizontal bar chart showing the total number of prompts containing sensitive data for various AI assistants. The assistants listed are Google Bard, OpenAI ChatGPT-4, Bing Chat, Copy.ai, and Microsoft Copilot. The chart includes a "View details" button.
- Total users (Microsoft Copilot)**: A donut chart showing the total users who created a prompt for Microsoft Copilot, with a value of 15.3K. The chart includes a "View details" button.
- Total users (other AI assistants)**: A donut chart showing the total users who visited other AI assistants, with a value of 7.1K. The chart includes a "View details" button.
- Top users (all AI assistants)**: A horizontal bar chart showing users with Microsoft Copilot activity and browsing activity in other AI assistants. The assistants listed are Google Bard, Bing Chat, OpenAI ChatGPT-4, Copy.ai, and Microsoft Copilot. The chart includes a "View details" button.

A green diagonal banner in the bottom right corner reads "Private Preview".

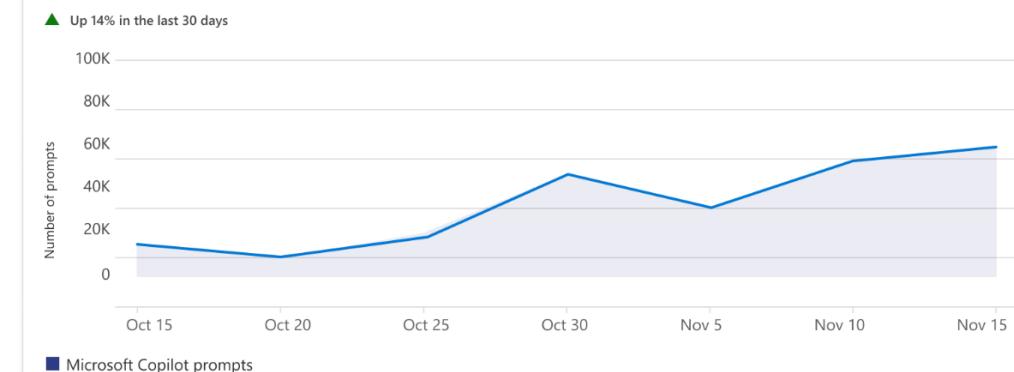
# AI hub (preview)

[Learn more](#)[Analytics](#) [Policies](#) [Activity explorer](#)

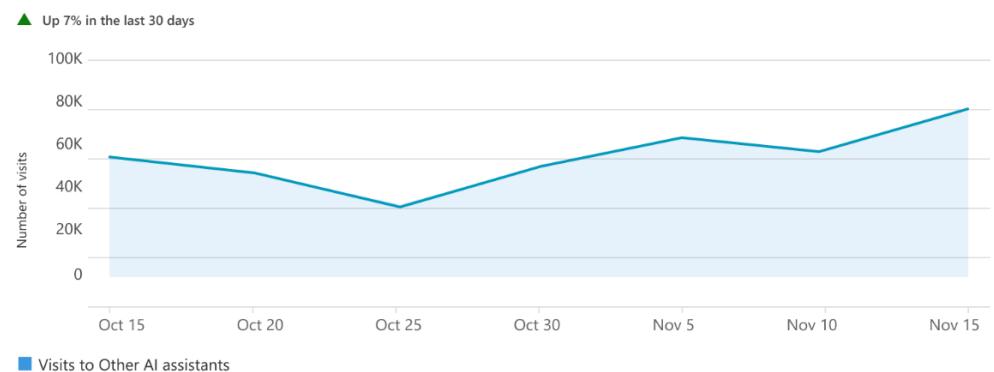
93% of organizations have implemented, developed, or are developing an AI strategy.  
Accelerate productivity with data security and compliance for Microsoft Copilot and other AI-powered assistants.

[Learn more](#)

## Total prompts over time (Microsoft Copilot)

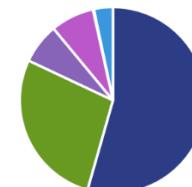


## Total visits (Other AI assistants)



## Sensitive data in prompts

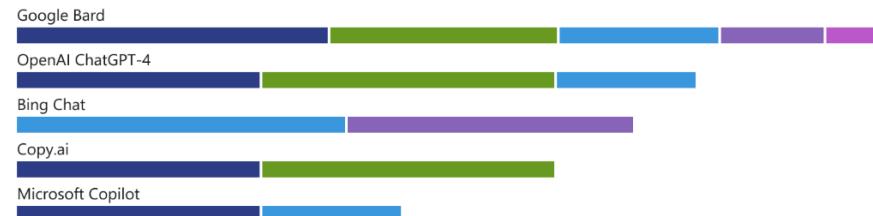
Sensitive data shared with all AI assistants grouped by sensitive information type.



■ 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 management

Subject rights request

Settings

More resources

Customize navigation

Show less



[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

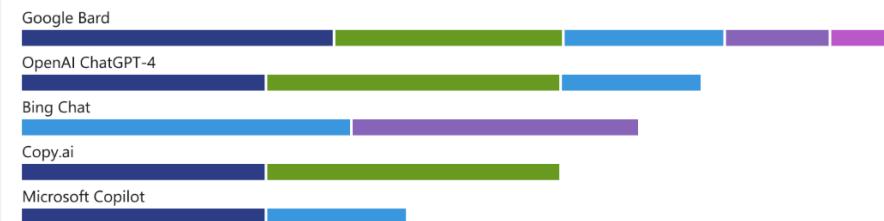
[View details](#)



[View details](#)

### Total prompts with sensitive data

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

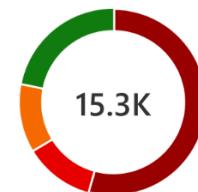


Credit card numbers   U.S. SSN   Physical address   Bank Account   ABA routing numbers

[View details](#)

### Total users (Microsoft Copilot)

Total users who created a prompt



15.3K

High risk   Medium risk   Low risk   None

[View details](#)

### Total users (other AI assistants)

Total users who visited other AI assistants



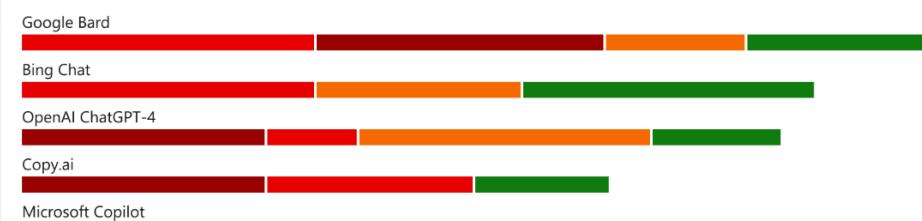
7.1K

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



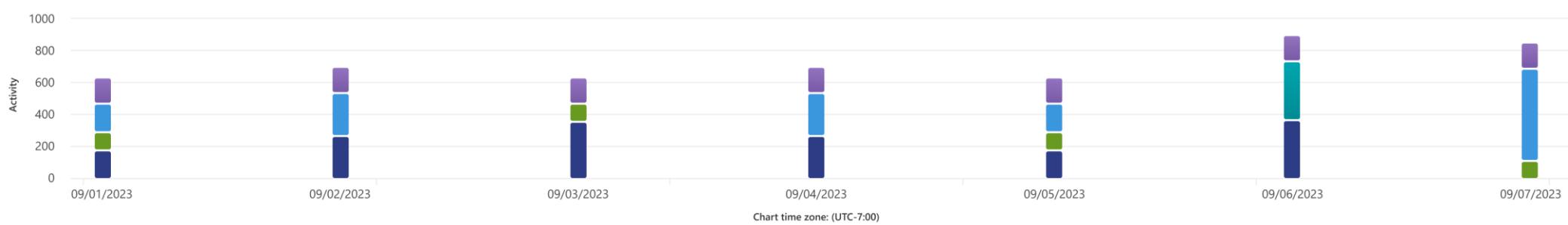
High severity   Medium severity   Low severity   None

[View details](#)

Private  
Preview



# AI hub (preview)

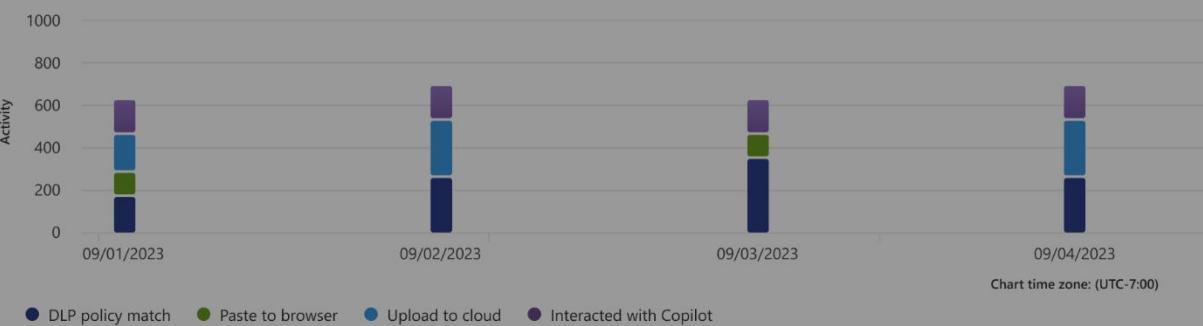
[Recommended actions](#) [Settings](#) [Learn more](#)[Home](#)[Ai Hub](#)[Compliance Manager](#)[Data classification](#)[Data Connectors](#)[Alerts](#)[Reports](#)[Policies](#)[Permissions](#)[Solutions](#)[Catalog](#)[Audit](#)[Content search](#)[Communication compliance](#)[Data loss prevention](#)[eDiscovery](#)[Data lifecycle management](#)[Information protection](#)[Insider risk management](#)[Records management](#)[Analytics](#) [Policies](#) [Activity explorer](#)[Activity: All values](#)[User: All values](#)[DLP policy matched: All values](#)[Sensitive info type: All values](#)[Add filter](#)[Reset all](#)

<input type="checkbox"/> Activity	User	Time happened	Device full name	Enforcement mode	Sensitive info type	File sensitivity label	DLP policy matched	DLP rules matched	File name
<input type="checkbox"/> File upload to cloud	MK 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
<input type="checkbox"/> Paste to browser	DR Dean Renzo	Sep 01, 2023 3:54 PM	Desktop-363345HD	Audit	Social security number		AI hub – Data Protection	Audit-PasteToBrowser	
<input type="checkbox"/> File upload to cloud	EG Edison Gill	Sep 02, 2023 3:54 PM	Desktop-53544EF	Audit	Physical address	Confidential	AI hub – Data Protection	Audit-UploadToCloud	AddressList_08-2022.xls
<input type="checkbox"/> Interacted with Copilot	ST Sarah Terry	Sep 03, 2023 3:54 PM		Audit	Credit card number				
<input type="checkbox"/> File upload to cloud	EG 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
<input type="checkbox"/> Interacted with Copilot	DR Dean Renzo	Sep 05, 2023 3:54 PM		Audit	Social security number				
<input type="checkbox"/> Paste to browser	ST Sarah Terry	Sep 06, 2023 3:54 PM	Desktop-3534345-LD	Audit	Bank account		Purview for AI – Data Protection	Audit-PasteToBrowser	
<input type="checkbox"/> Interacted with Copilot	ST Sarah Terry	Sep 06, 2023 3:54 PM	Desktop-3534345-LD	Audit	Bank account		Purview for AI – Data Protection	Audit-PasteToBrowser	
<input type="checkbox"/> Paste to browser	MK Mona Kane	Sep 13, 2023 3:54 PM	Desktop-ASFD213	Audit	Credit card number		AI hub – Data Protection	Audit-UploadToCloud	

Private  
Preview



# 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](#)


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

## File upload to cloud

### Activity details

**Activity**  
File upload to cloud

**Happened**  
Sep 13, 2023 3:54 PM

**Client IP**
**Enforcement mode**

131.109.147.63

Audit

**Target domain**
**JIT triggered**

bard.google.com

False

### About this item

**User**  
Mona.Kane@contoso.com

**Sensitive info type**
**Policy**  
Credit card number  
AI hub – Data Protection

**Rule**

Audit-UploadToCloud

### Location details

**Source location type**  
Unknown

**Destination location type**  
Unknown

**Platform**
**Application**  
Windows  
msedge.exe

**Application**

Desktop-3453HD

[View device details](#)
**MDAIP device ID**

33oe9ca0778b9ec2ab7933ac9f7ehsd1987bacd8

[Done](#)

Private Preview

# Prevent sensitive data to 3<sup>rd</sup> party Gen AI applications

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

The screenshot shows a Microsoft Purview Data Loss Prevention (DLP) dialog box overlaid on a Google Bard interface. The dialog is titled "Microsoft Purview Data Loss Prevention" and states: "Your organization has blocked pasting protected content to unprotected locations. You tried to paste protected content, which is prohibited by your organization." It includes an "OK" button. In the background, a Microsoft Word document is open, showing a project plan for "PROJECT OBSIDIAN". The document contains several redacted sections, indicated by the DLP policy. The Google Bard interface features a large "Hi, I'm Bard" greeting and a prompt input field.

Microsoft Purview Data Loss Prevention

Your organization has blocked pasting protected content to unprotected locations.

You tried to paste protected content, which is prohibited by your organization.

OK

Hi, I'm Bard

Enter a prompt here

Bard may display inaccurate or offensive information that doesn't represent Google's views.

Project OBSIDIAN

Weekly meeting

**Project title:** Project Obsidian (a)

**Project background:** Customer satisfaction, retention, and loyalty are costly, especially when dealing with customer interactions efficiently.

**Project objectives:** The main objective is to provide a customer service for a software company.

- Understand natural language processing
- Provide information, assistance, and feedback
- Escalate complex or urgent issues
- Collect feedback and improve the system
- Provide evidence-based recommendations

**Project methods:** The project will involve the following steps:

- Conduct a literature review on chatbot development
- Design and implement a natural language processing framework
- Test and evaluate the chatbot's performance based on customer satisfaction, feedback, and refinement
- Refine and optimize the chatbot's responses

**Project results:** The project will deliver the following outcomes:

- A chatbot prototype that can handle basic user queries
- A report that documents the chatbot's prototype
- A presentation that showcases the chatbot's capabilities
- A bot that highlights specific features and benefits

Page 1 of 1 316 words English (United States)

# Prevent sensitive data to 3<sup>rd</sup> 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 of text, some of which are redacted with a large black redaction mark. The Word ribbon is visible at the top, showing tabs like File, Home, Insert, etc. The status bar at the bottom indicates "Page 1 of 2" and "317 words". A green ribbon banner in the bottom right corner says "Private Preview".

**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

# 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](https://aka.ms/PurviewTrial)



Thank You!  
Questions?