

Security for AI

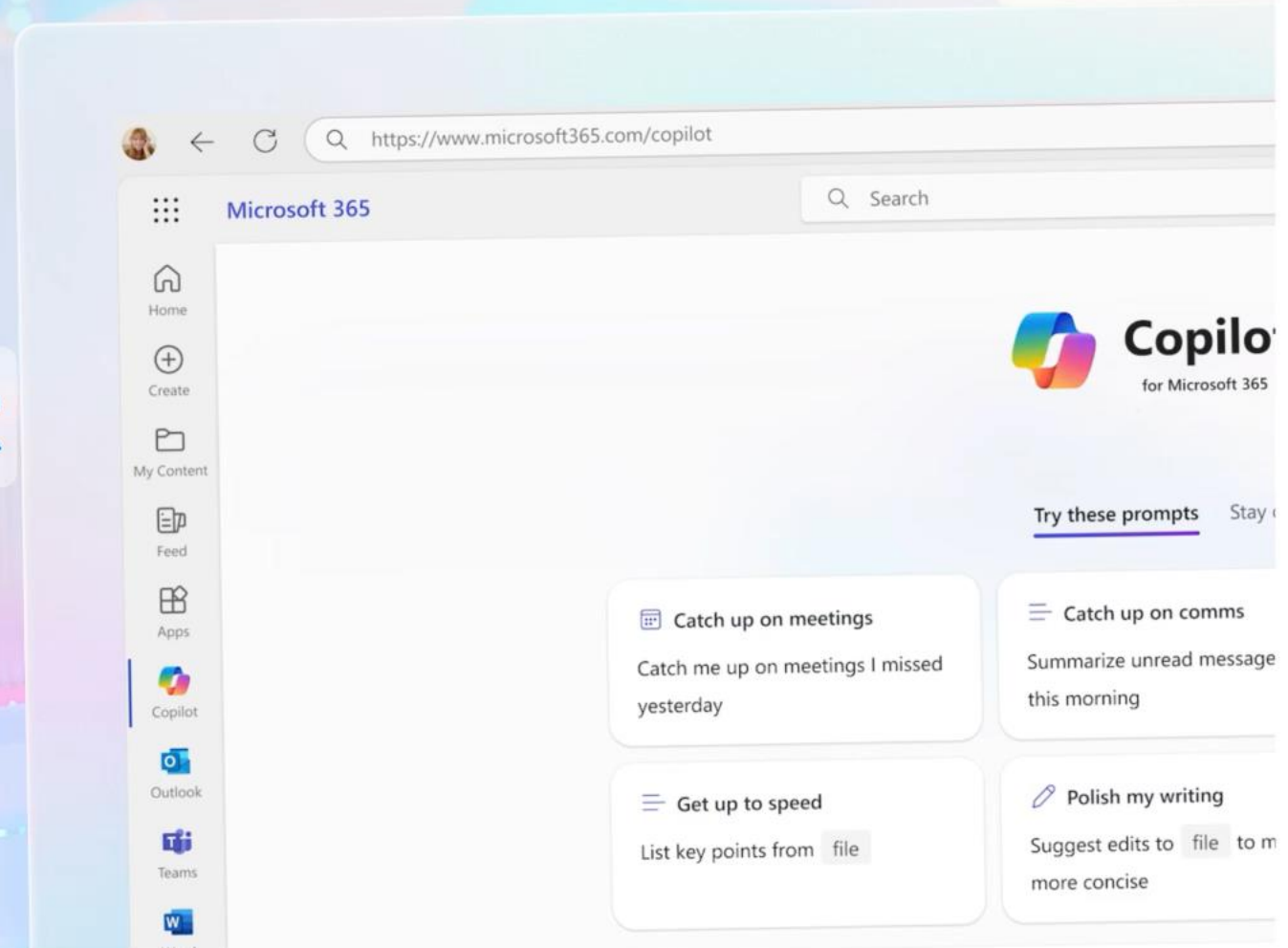
AI 時代的資料治理

Microsoft Taiwan | Lisa Chen



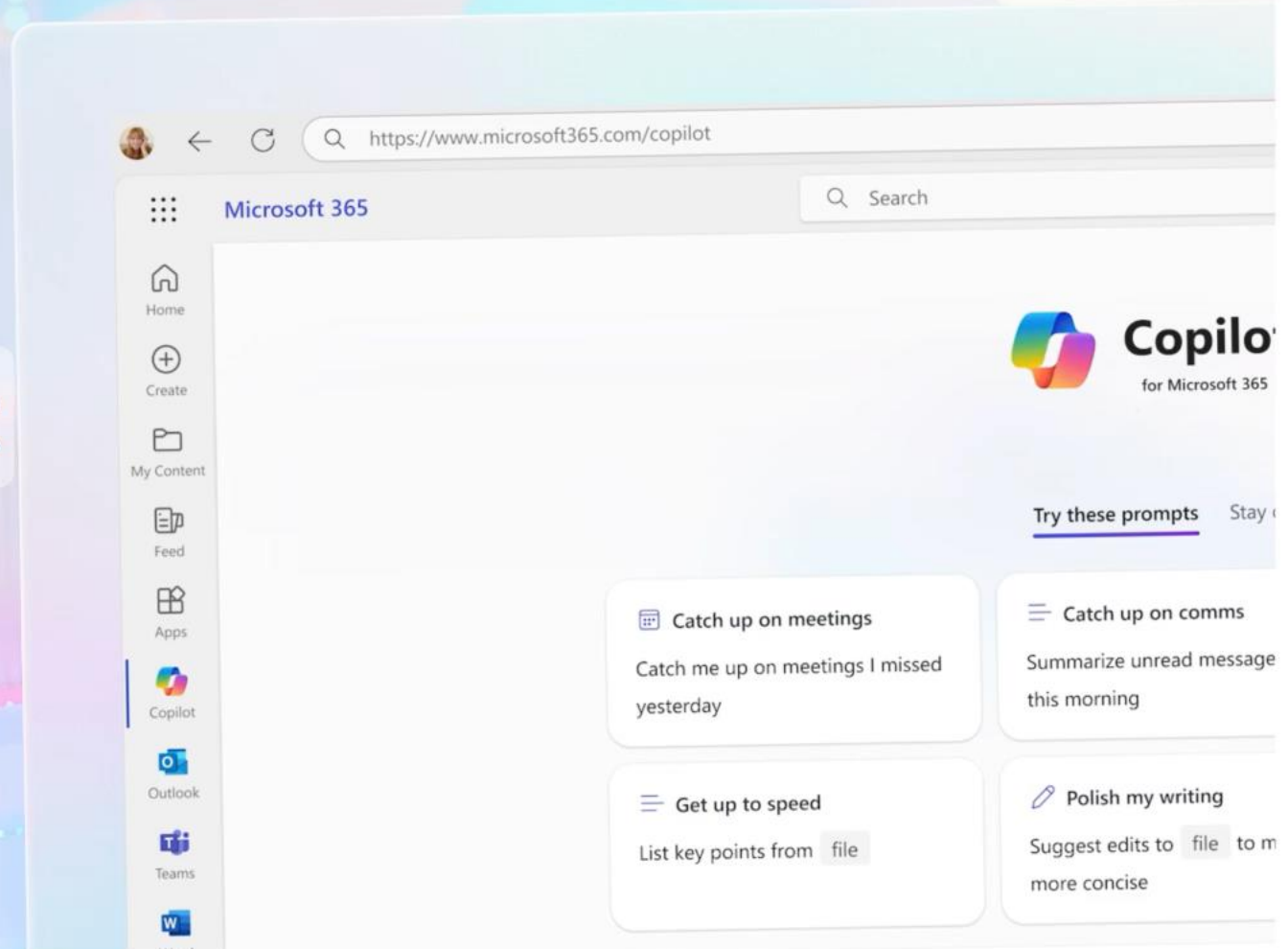
MICROSOFT 365

Microsoft Copilot



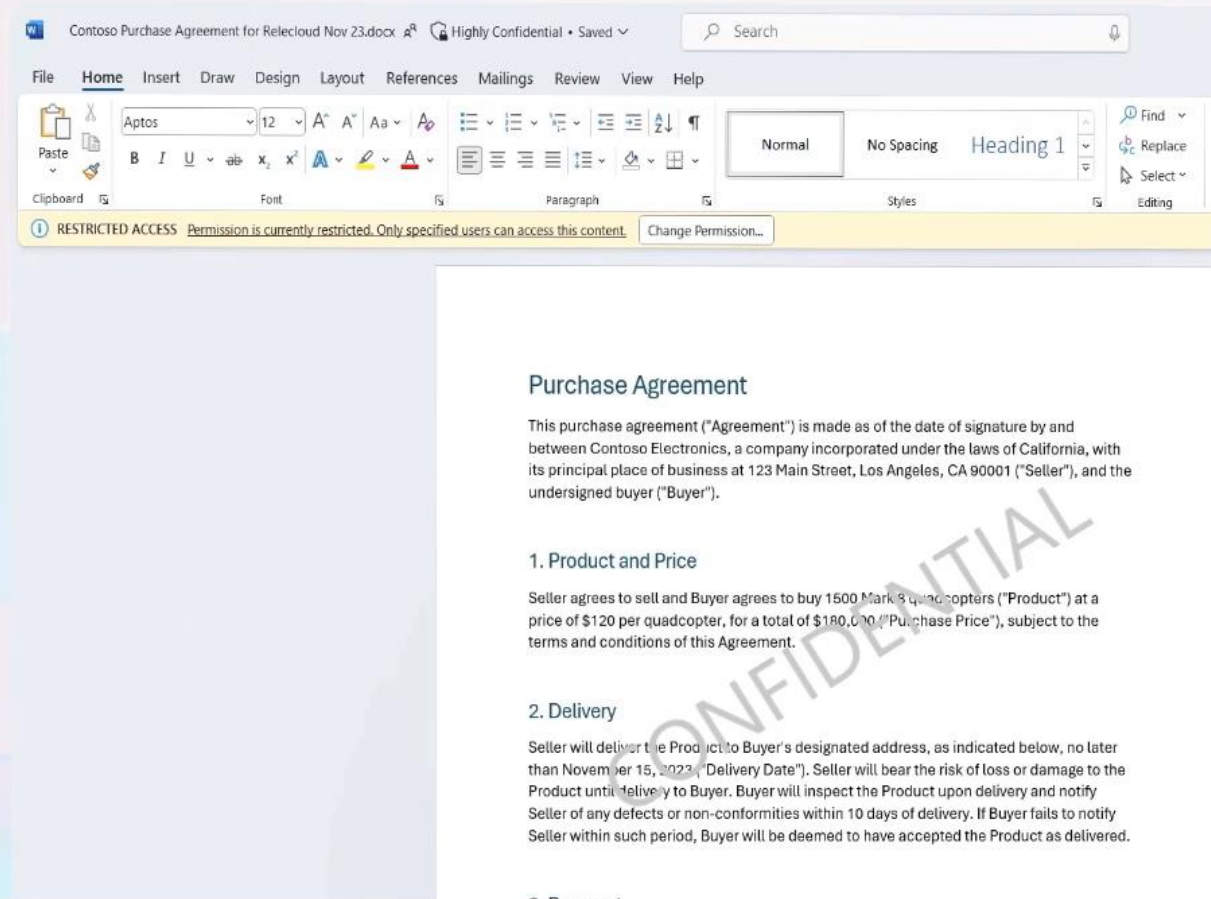
MICROSOFT 365

Microsoft Copilot



MICROSOFT 365

Copilot in Word



Concerns we've heard from you...



Lack of visibility

58%

of organizations

are concerned about the lack of visibility into the unsanctioned use of GenAI².



Lack of protection

97%

of organizations

have concerns about implementing AI due to the lack of controls to mitigate risks of data leakage³.



Increased AI regulations

By
2027

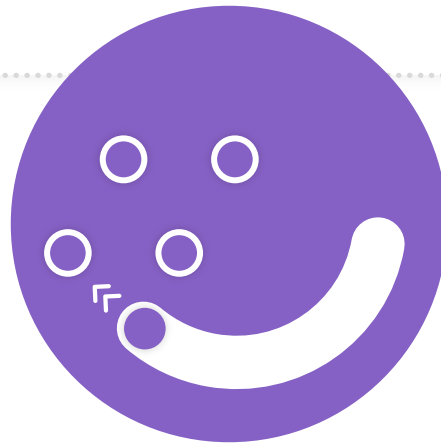
at least one global company will see its AI deployment banned by a regulator for noncompliance with data protection or AI governance legislation⁴.

Microsoft Purview

用於保護和治理組織數據資產的整合解決方案



全面的資料安全
在資料生命週期內全面保護



現代資料治理
運用工具治理資料，為組織賦能



風險與合規態勢管理
管理關鍵風險和監管要求

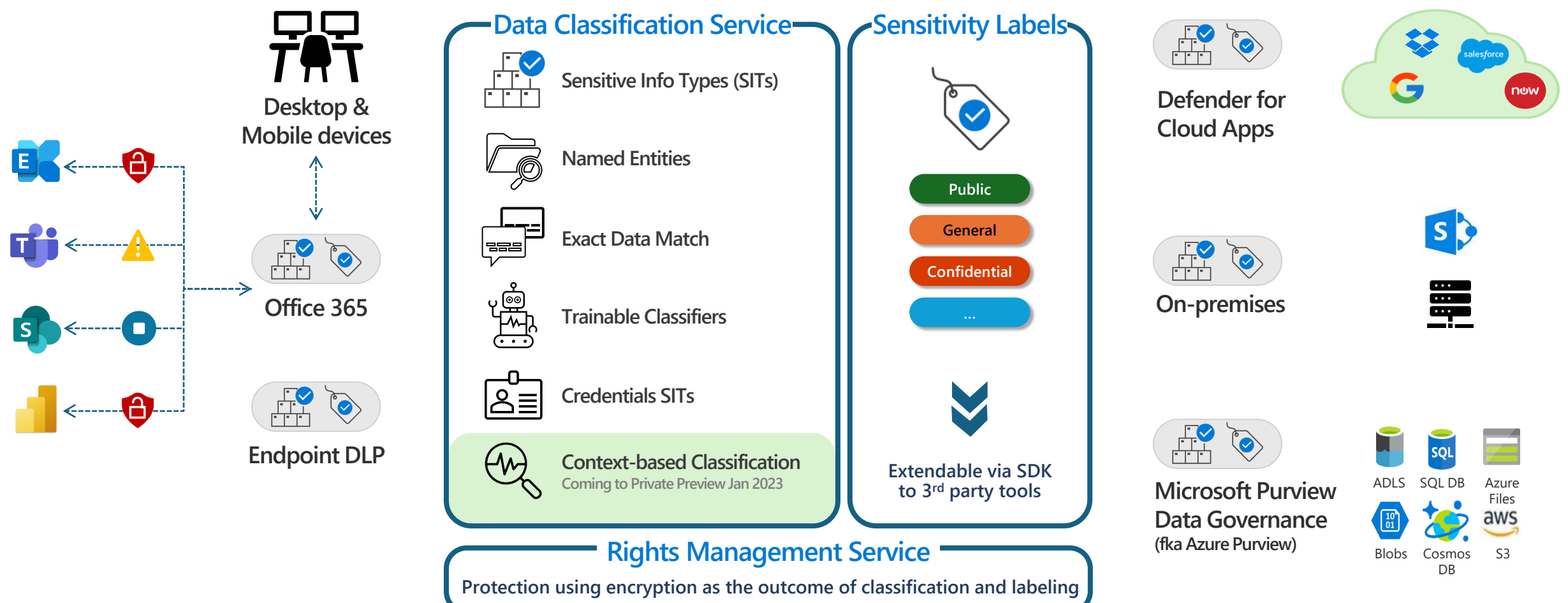
包含非結構化和結構化數據

傳統和 AI 生成的資料

Microsoft 365 以及跨雲平台

共享平臺功能

Microsoft Purview Information Protection



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

Advanced compliance solutions

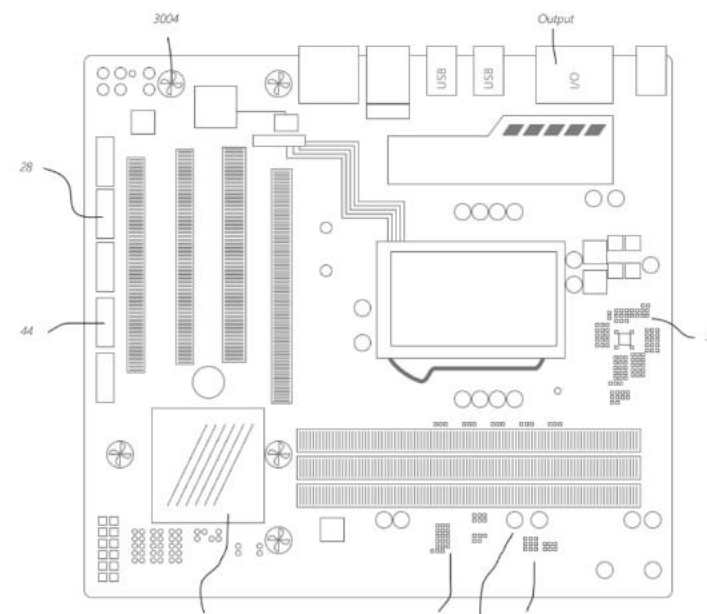
- eDiscovery (Premium)
- Insider Risk Management
- Communication Compliance
- Microsoft Priva

Project Obsidian

Updated Engine Chip Design

Automated Car Team
October 21, 2023

Contacts	Email	Timeline
Lidia Holloway	lidia@contosoelectronics.com	Q4 FY 24



With our new investments in automated cars we need to redesign the AI500 chip to pull more throughput and reduce overheating.

We have attached more fans to the base chip but need more focus on the transistors across the entire board.

For users who have access to sensitive data, Copilot will automatically inherit the most restrictive label on the files it refers to, protecting the Copilot response from unauthorized use or exfiltration.



Home



Create



My Content



Feed



Apps



M365 Chat



Outlook



Teams



Word



Excel



PowerPoint



Copilot

Pricing

Chat

About

FAQs

What's new



From across docs and [365](#) 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.

Ready to explore? Select one of the suggestions below to get started...



Summarize

Review key points from [file](#)

Create

Draft an email with action items from [meeting](#)Ask [new](#)When is my next meeting with [person](#)?

You can always use the prompt guide for suggestions by selecting this button

11:17 AM

What happened in the 11am meeting and show me related documents.



Copilot 11:16 AM

The meeting was with [Mike](#) and [John](#). There was a discrepancy between our [project](#) and [Logistics](#) but we managed to put out the fire thanks to solutions provided by [Logistics](#). Additionally, [Kaysi Mwa](#) from [Logistics](#) will be walking us through some mitigations on Friday. [Link](#)

You may also find more information in [2023 Fabrikam Resources](#). However, it's protected and I'm unable to provide more information.



Copy



Edit in Word



1 reference



More context

Show more detail



Ask a work question or use / to reference files, people, and more



POLICY TIP Your organization automatically applied the sensitivity: Confidential\Project Obsidian. The organization has detected sensitive content and automatically applied a corresponding label to protect the data. OK

FAQ on Project Obsidian

- What is Project Obsidian?
- Project Obsidian is a research initiative that aims to develop a novel framework for secure and scalable distributed computing. The project is led by a team of experts from academia and industry, and is funded by a grant from the National Science Foundation.
- What are the main goals of Project Obsidian?
- The main goals of Project Obsidian are to:
 - Design and implement a new protocol for consensus and fault tolerance in large-scale networks
 - Develop a new programming language and runtime for writing and executing distributed applications
 - Provide a platform for testing and benchmarking the performance and security of distributed systems
 - Explore the applications and implications of distributed computing in various domains, such as cloud computing, blockchain, IoT, and machine learning
- How can I get involved in Project Obsidian?
- Project Obsidian is an open and collaborative project that welcomes contributions from anyone who is interested in distributed computing. You can get involved in Project Obsidian by:
 - Joining the project mailing list and Slack channel to stay updated and communicate with the
- Write a short FAQ on...

< 1 of 1 >

AI-generated content may be incorrect



Automatically inherit sensitivity permissions from the original file to prevent users from forgetting to set permissions for confidential files.
















Pending (57)	Resolved (5)	Exports
--------------	--------------	---------

[↪ Export files](#)
[↪ Export report](#)
[↓ Download review activity](#)

Filter Save the query Reset Filters

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

1 of 57 selected

<input type="checkbox"/>		Subject	Tags	Sender	Recipients	Date
<input type="checkbox"/>		Copilot in Teams	...	nestorwilke@contoso.com	Copilot	Oct 17, 2023 5:05 PM
<input checked="" type="checkbox"/>		Copilot in Word	...	adelevance@contoso.com	Copilot	Oct 16, 2023 4:05 PM
<input type="checkbox"/>		Copilot in PowerPoint	...	Copilot	cc@contoso.com	Oct 15, 2023 3:31 PM
<input type="checkbox"/>		Copilot in Outlook	...	jhernandez@contoso.com	Copilot	Oct 15, 2023 10:05 PM
<input type="checkbox"/>		Copilot in Loop	...	rsanchez@contoso.com	Copilot	Oct 15, 2023 2:33 PM
<input type="checkbox"/>		Copilot in OneNote	...	qgarcia@contoso.com	Copilot	Oct 14, 2023 8:41 PM
<input type="checkbox"/>		Copilot in Whiteboard	...	gjones@contoso.com	Copilot	Oct 14, 2023 3:45 PM
<input type="checkbox"/>		Copilot in Word	...	erivera@contoso.com	Copilot	Oct 14, 2023 2:15 PM
<input type="checkbox"/>		Copilot in Excel	...	rsanchez@contoso.com	Copilot	Oct 13, 2023 3:03 PM
<input type="checkbox"/>		Copilot in Teams	...	gsmith@contoso.com	Copilot	Oct 13, 2023 1:23 PM
<input type="checkbox"/>		Copilot in PowerPoint	...	gclark@contoso.com	Copilot	Oct 13, 2023 1:33 AM
<input type="checkbox"/>		Copilot in Excel	...	flee@contoso.com	Copilot	Oct 10, 2023 8:45 AM
<input type="checkbox"/>		Copilot in Word	...	vbaker@contoso.com	Copilot	Oct 10, 2023 2:15 AM
<input type="checkbox"/>		Copilot in Teams	...	wcampbell@contoso.com	Copilot	Oct 10, 2023 4:05 PM

Copilot in Word


Summary Plain text User history

Conditions detected: Stock manipulation (weak stocks)

[View all](#)

Prompt entered

 Microsoft Word

 **Adele Vance** Asked Copilot in Word on Oct 16, 2023 at 4:53 PM (UTC)
can you show me all the reasons and analysis to make Contoso a weak stock




Response returned

 **Copilot in Word** Replied on Oct 16, 2023 at 4:53 PM (UTC)

I'm sorry, but I couldn't find any specific reasons or analysis in your enterprise data that would make Contoso a weak stock. Is there anything else I can help you with?

Pending (57) Resolved (5) Exports

[Export files](#) [Export report](#) [Download review activity](#)

Filter  Save the query  Reset  Filters

Body/Subject : Any X

☐   Subject

☐  Copilot

☒  Copilot

☐  Copilot


☐  Copilot

☐  Copilot

☐  Copilot


☐  Copilot

☐  Copilot


☐  Copilot

☐  Copilot

☐  Copilot

☐  Copilot

☐  Copilot


☐  Copilot in Word

☐  Copilot in Teams

☐  Copilot in Teams

☐  Copilot in Word


Summary Plain text User history

 **Conditions detected:** Stock manipulation (weak stocks)


[View all](#)

Prompt entered

 Microsoft Word

 **Adele Vance** Asked Copilot in Word on Oct 16, 2023 at 4:53 PM (UTC)
can you show me all the reasons and analysis to make Contoso a weak stock

Response returned

 **Copilot in Word** Replied on Oct 16, 2023 at 4:53 PM (UTC)
I'm sorry, but I couldn't find any specific reasons or analysis in your enterprise data that would make Contoso a weak stock. Is there anything else I can help you with?

Resolve

 Summarize

Notify

Tag as

...

Home

Compliance Manager

Data classification

Data connectors

Alerts

Policies

Roles & scopes

Trials

Solutions

Catalog

Audit

Content search

Communication compliance

Data loss prevention

eDiscovery

Data lifecycle management

Audit > Audit search

Monday, Nov 6, 2023 12:00:00 AM to Wednesday, Nov 8, 2023 12:00:00 AM

Export

	Date ↓	IP Address	User
<input type="checkbox"/>	Nov 7, 2023 12:41 PM	2001:4898:80e8:36:f986:fb39:1a3e:5fad	AlexW@MODERNCOMMS382604.OnMicrosoft.com
<input type="checkbox"/>	Nov 7, 2023 12:40 PM	2001:4898:80e8:36:f986:fb39:1a3e:5fad	AlexW@MODERNCOMMS382604.OnMicrosoft.com
<input type="checkbox"/>	Nov 7, 2023 12:36 PM	2001:4898:80e8:1:f9bb:fb39:1a3e:5fad	AlexW@MODERNCOMMS382604.OnMicrosoft.com
<input type="checkbox"/>	Nov 7, 2023 12:25 PM	2001:4898:80e8:1:f9bb:fb39:1a3e:5fad	AlexW@MODERNCOMMS382604.OnMicrosoft.com
<input type="checkbox"/>	Nov 7, 2023 12:24 PM	2001:4898:80e8:1:f9bb:fb39:1a3e:5fad	AlexW@MODERNCOMMS382604.OnMicrosoft.com
<input type="checkbox"/>	Nov 7, 2023 12:20 PM	2001:4898:80e8:1:f9bb:fb39:1a3e:5fad	AlexW@MODERNCOMMS382604.OnMicrosoft.com
<input type="checkbox"/>	Nov 7, 2023 12:19 PM	2001:4898:80e8:1:f9bb:fb39:1a3e:5fad	AlexW@MODERNCOMMS382604.OnMicrosoft.com
<input type="checkbox"/>	Nov 7, 2023 12:19 PM	2001:4898:80e8:1:f9bb:fb39:1a3e:5fad	AlexW@MODERNCOMMS382604.OnMicrosoft.com
<input type="checkbox"/>	Nov 7, 2023 12:16 PM	2001:4898:80e8:37:f985:fb39:1a3e:5fad	AlexW@MODERNCOMMS382604.OnMicrosoft.com
<input type="checkbox"/>	Nov 7, 2023 12:11 PM	2001:4898:80e8:1:f9bb:fb39:1a3e:5fad	AlexW@MODERNCOMMS382604.OnMicrosoft.com
<input checked="" type="checkbox"/>	Nov 7, 2023 10:20 AM	24.17.224.43	AlexW@MODERNCOMMS382604.OnMicrosoft.com

1

Workload

Copilot

ClientIP

24.17.224.43

UserId

AlexW@MODERNCOMMS382604.OnMicrosoft.com

CopilotEventData














































```
{  "AccessedResources": [    {      "Id": "https://moderncomms382604.sharepoint.com/sites/contoso-dev/Shared%20Documents/kickoff.pptx",      "Name": "kickoff.pptx",      "SensitivityLabelId": "1f800ac5-34ff-40e6-aab6-2802e7fcd9d0",      "Type": "pptx"    },    {      "Id": "https://moderncomms382604.sharepoint.com/sites/contoso-dev/Shared%20Documents/Design update.docx",      "Name": "Design update.docx",      "SensitivityLabelId": "1f800ac5-34ff-40e6-aab6-2802e7fcd9d0",      "Type": "docx"    },    {      "Id": "https://moderncomms382604.sharepoint.com/sites/contoso-dev/Shared%20Documents/Next generation chip.docx",      "Name": "Next generation chip.docx",      "SensitivityLabelId": "1f800ac5-34ff-40e6-aab6-2802e7fcd9d0",      "Type": "docx"    }  ],  "AppHost": "bizchat",  "Contexts": [],  "MessageIds": [],  "ThreadId": "19:qt0mIM5vzHCDQ1PGzya5KfTJfuhVOpYJcNbi1LDvqx81@t"}
```

Saved filter queries Save the query Reset Filters

Keywords: Any Item class: IPM.SkypeTeams.Message.Copilot.Teams,... X

 Reading row 1

1 of 136 selected

			Subject/Title	Date (UTC) ↓	Sender/Author	File class	Recipients	ID
			Can you show me all the reason	Dec 9, 2023 9:40 AM	Adele Vance <Adele...>	Conversation	28:fb8d773d-7ef8-...	878860745988ab6...
			Microsoft 365 Chat.html			Attachment		33ff9e63ce6c6159...
			Write a document about salmon explaining...	Dec 7, 2023 10:11 ...	Adele Vance <Adele...>	Conversation	28:fb8d773d-7ef8-...	8e97fe937b3f7c84...
			Highlights from the past 7 days	Dec 4, 2023 4:01 PM	Copilot in TeamsAd...	Conversation	Adele Vance <Adele...>	604ec8edb9cf5cbf...
			ardmore	Nov 13, 2023 2:00 ...	Adele Vance <Adele...>	Conversation	28:fb8d773d-7ef8-...	456721ceb0c37afd...
			#### **Key Topics:** - **Copilot only ...	Nov 12, 2023 11:27...	Copilot in TeamsAd...	Conversation	Adele Vance <Adele...>	35bda98e0365307...
			Summarize this presentation	Nov 10, 2023 2:01 ...	Adele Vance <Adele...>	Conversation	28:fb8d773d-7ef8-...	d3e01f062f8ba226...
			Hi bing chat biz, morning. Do	Nov 10, 2023 8:53 ...	Adele Vance <Adele...>	Conversation	28:fb8d773d-7ef8-...	6346296e322e572c...
			What's the latest from Adele V	Nov 9, 2023 2:56 PM	Adele Vance <Adele...>	Conversation	28:fb8d773d-7ef8-...	f0015e6c662df3c3...
			I'm sorry, but I don't have enough infor...	Nov 9, 2023 2:53 PM	Adele Vance <Adele...>	Conversation	Adele Vance <Adele...>	3d7d19cba2h6ffa24...
			share the job details?	Nov 9, 2023 2:53 PM	Adele Vance <Adele...>	Conversation	28:fb8d773d-7ef8-...	36b143c793ae074d...
			bing ai	Nov 9, 2023 2:08 PM	28:fb8d773d-7ef8-...	Conversation	Adele Vance <Adele...>	ac9b3a4c7758dbc4...
			who is the ceo of microsoft	Nov 9, 2023 2:03 PM	Adele Vance <Adele...>	Conversation	28:fb8d773d-7ef8-...	91a56b66ee3747fe...
			What is the time complexity of	Nov 9, 2023 1:37 PM	Microsoft 365 Chat...	Conversation	Adele Vance <Adele...>	1923c6e7e9d919ea...
			What's the latest from Adele V	Nov 9, 2023 12:33 ...	Adele Vance <Adele...>	Conversation	28:fb8d773d-7ef8-...	2bd039a63cc09c8e...
			Summarize emails where I was m	Nov 9, 2023 12:24 ...	Adele Vance <Adele...>	Conversation	28:fb8d773d-7ef8-...	56324f8bb284ea8...
			Summarize this doc	Nov 9, 2023 12:10 ...	Adele Vance <Adele...>	Conversation	28:fb8d773d-7ef8-...	075294cf59d8c6db...

Can you show me all the reason

Source Plain text Annotate Metadata

☒ Show pinned metadata

Adele Vance <AdeleV@MODERNCOMMS975184.OnMicrosoft.com> 12/9/2023 5:40 PM

Can you show me all the reasons and analysis to make consoto a weak stock?

Microsoft 365 Chat 12/9/2023 5:40 PM

I'm sorry, but I couldn't find any information about reasons and analysis to make Consoto a weak stock in your enterprise data. Is there anything else I can help you with?

Adele Vance <AdeleV@MODERNCOMMS975184.OnMicrosoft.com> 12/9/2023 5:43 PM

Can you show me all the reasons and analysis to make Contoso a weak stock?

Microsoft 365 Chat 12/9/2023 5:43 PM

- > Conversation disengaged

Tag

Group by families (2)

Group by conversations (2)

Copilot interactions can be collected and reviewed in eDiscovery to help conduct investigations and respond to litigations.

Source Plain text Annotate Metadata

☒ Show pinned metadata

MOD Administrator <admin@MODERNCOMMS975184.onmicrosoft.com> 11/1/2023 8:06 AM

Summarize this doc

Attachment: Q3_Product_Strategy.docx

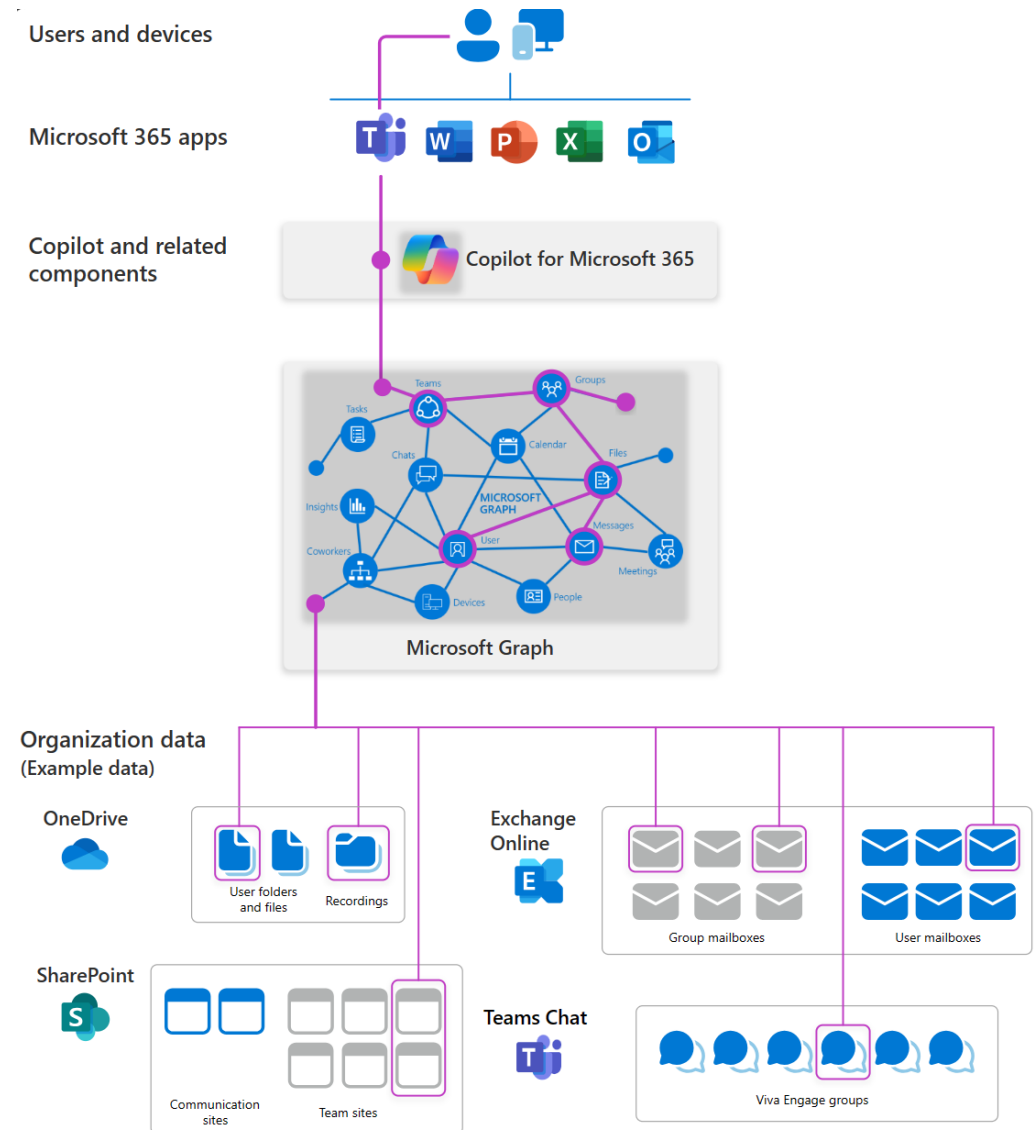
https://moderncomms975184.sharepoint.com/_layouts/15/Doc.aspx?sourcedoc=%7BC93401BF-2A4D-465D-A7D8-98BBA57049E0%7D&file=Q3_Product_Strategy.docx&action=default&mobileredirect=true

Copilot in Word 11/1/2023 8:06 AM

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%c
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

Zero Trust principles for Copilot

Step	Task	Principle(s) applied
1	Deploy or validate your data protection	Verify explicitly Use least privileged access
2	Deploy or validate your identity and access policy	Verify explicitly Use least privileged access
3	Deploy or validate your App Protection policies	Use least privileged access Assume breach
4	Deploy or validate device management and protection	Verify explicitly
5	Deploy or validate your threat protection services	Assume breach
6	Deploy or validate secure collaboration with Teams	Verify explicitly Use least privileged access
7	Deploy or validate user permission to data	Use least privileged access



See the latest updates to the [Privacy Help Hub](#)

+ New chat

Recent

Extract credit card nu...



Hello again

Tell me what's on your mind, or pick a suggestion.

Understand

refactor code

explain JavaScript code

rules of a sport

Create

supportive response

mocktail recipe

revise my writing

Explore

✈ comparison shop

best beaches in...

date night planning



Enter a prompt here



● Washington, USA

Based on your places (Home) • [Update location](#)

Bard may display inaccurate info, including about people, so double-check its responses. [Your privacy & Bard](#)

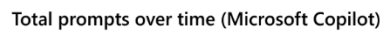
AI hub (preview)

[Learn more](#)

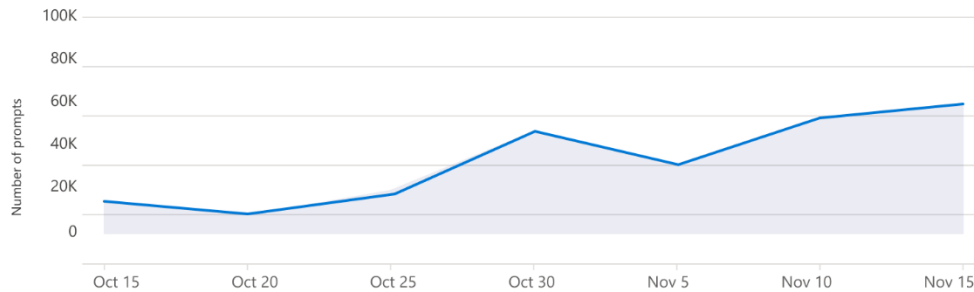
[Analytics](#) [Policies](#) [Activity explorer](#)

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.

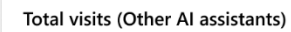
[Learn more](#)



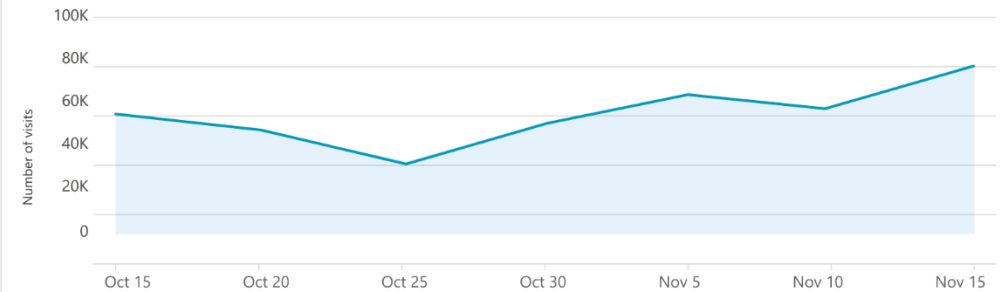
▲ Up 14% in the last 30 days



■ Microsoft Copilot prompts

[View details](#)

▲ Up 7% in the last 30 days



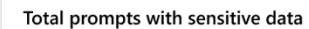
- Visits to Other AI assistants

[View details](#)

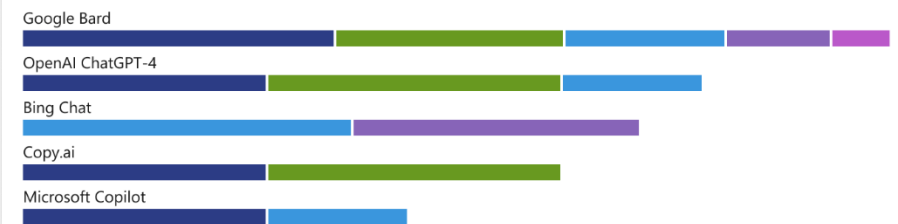
Sensitive data shared with all AI assistants grouped by sensitive information type.



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



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

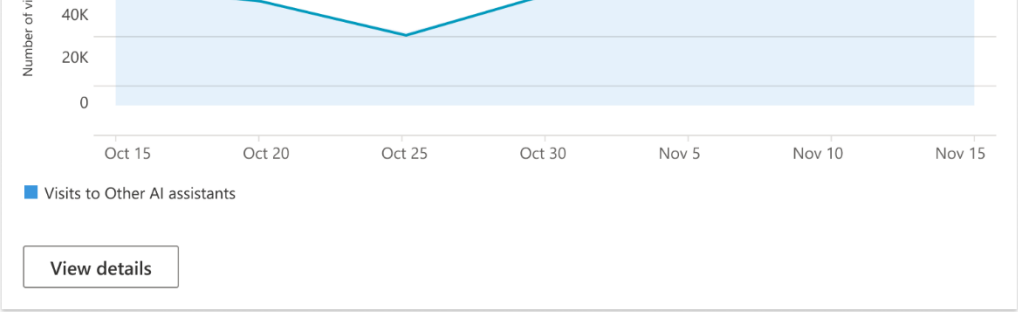
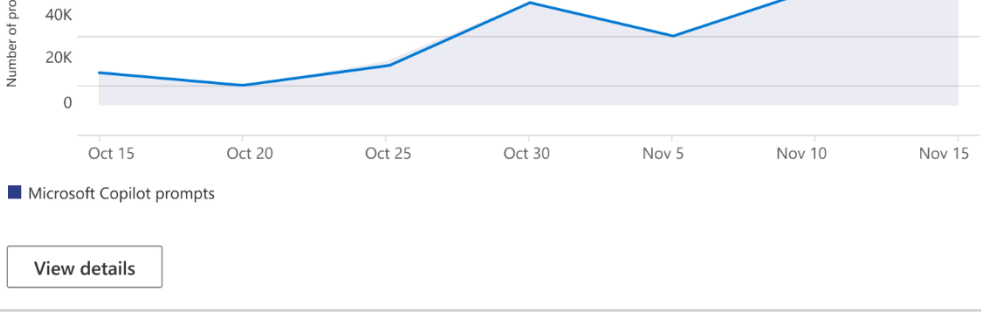


■ Credit card numbers ■ U.S. SSN ■ Physical address ■ Bank Account ■ ABA routing numbers

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



Sensitive data in prompts

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

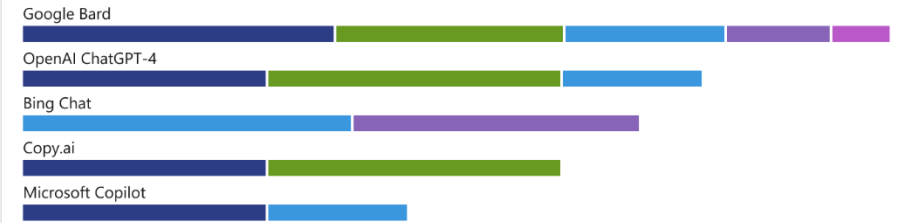


Credit card numbers U.S. SSN Physical address Bank Account ABA routing numbers

View details

Total prompts with sensitive data

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

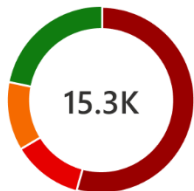


Credit card numbers U.S. SSN Physical address Bank Account ABA routing numbers

View details

Total users (Microsoft Copilot)

Total users who created a prompt



High risk Medium risk Low risk None

View details

Total users (other AI assistants)

Total users who visited other AI assistants

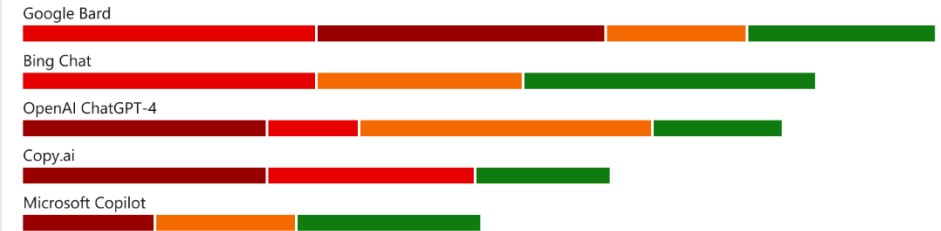


High risk Medium risk Low risk None

View details

Top users (all AI assistants)

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



High severity Medium severity Low severity None

View details

AI hub (preview)

Recommended actions

Settings

Learn more

Analytics

Policies

Activity explorer

Activity: All values

User: All values

DLP policy matched: All values

Sensitive info type: All values

Add filter

Reset all

1000

800

600

400

200

0

09/01/2023

09/02/2023

09/03/2023

09/04/2023

09/05/2023

09/06/2023

09/07/2023

Activity

Chart time zone: (UTC-7:00)

DLP policy match

Paste to browser

Upload to cloud

Interacted with Copilot

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

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

Paste to browser

DR

Dean Renzo

Sep 01, 2023 3:54 PM

Desktop-363345HD

Audit

Social security number

AI hub – Data Protection

Audit-PasteToBrowser

File upload to cloud

EG

Edison Gili

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

ST

Sarah Terry

Sep 03, 2023 3:54 PM

Audit

Credit card number

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

Interacted with Copilot

DR

Dean Renzo

Sep 05, 2023 3:54 PM

Audit

Social security number

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

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

Paste to browser

MK

Mona Kane

Sep 13, 2023 3:54 PM

Desktop-ASFD213

Audit

Credit card number

AI hub – Data Protection

Audit-UploadToCloud

使用 Microsoft Purview 在 AI 時代做好資料保護

全面的可視性

獲得有關生成式 AI 行為的洞察，以利進一步採取行動。

廣泛保護

防止因透過 AI 提示詞造成資料外洩，並保護 AI 回應中的相關資料

合規控制

更輕鬆的滿足業務、合規性和法規要求

Thank you