



# Security and Copilot for Microsoft 365

Answers to frequently asked questions



# Today's speakers

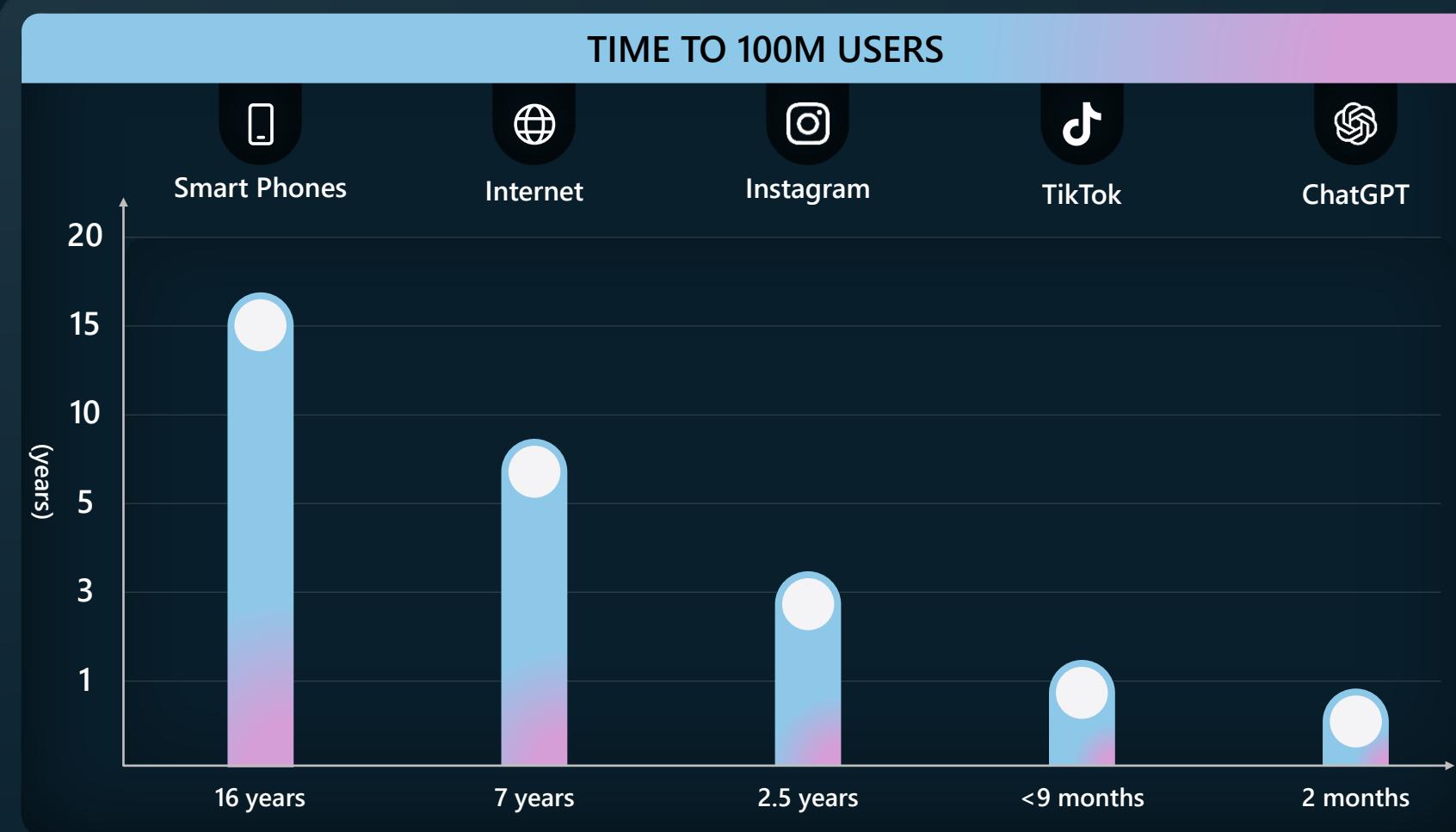


**Rhesa Baar**  
Technical Specialist Data Security & Compliance at Microsoft



**Danny de Vries**  
Solution Architect & Copilot Lead at Avanade

# Generative AI technology is here!



And can help...



Unleash creativity



Unlock productivity



Uplevel skills

# Security questions raised around Copilot for M365

---

Is my data used to train the LLM models?

---

How can we protect information from unauthorized oversharing by Copilot for M365?

---

How can we protect sensitive information from being used by Copilot for M365?

---

How can we get insights in the use of sensitive data with Copilot for M365?

---

What can we do to make sure that our users only use Copilot for M365 and not other Generative AI applications when dealing with company information?

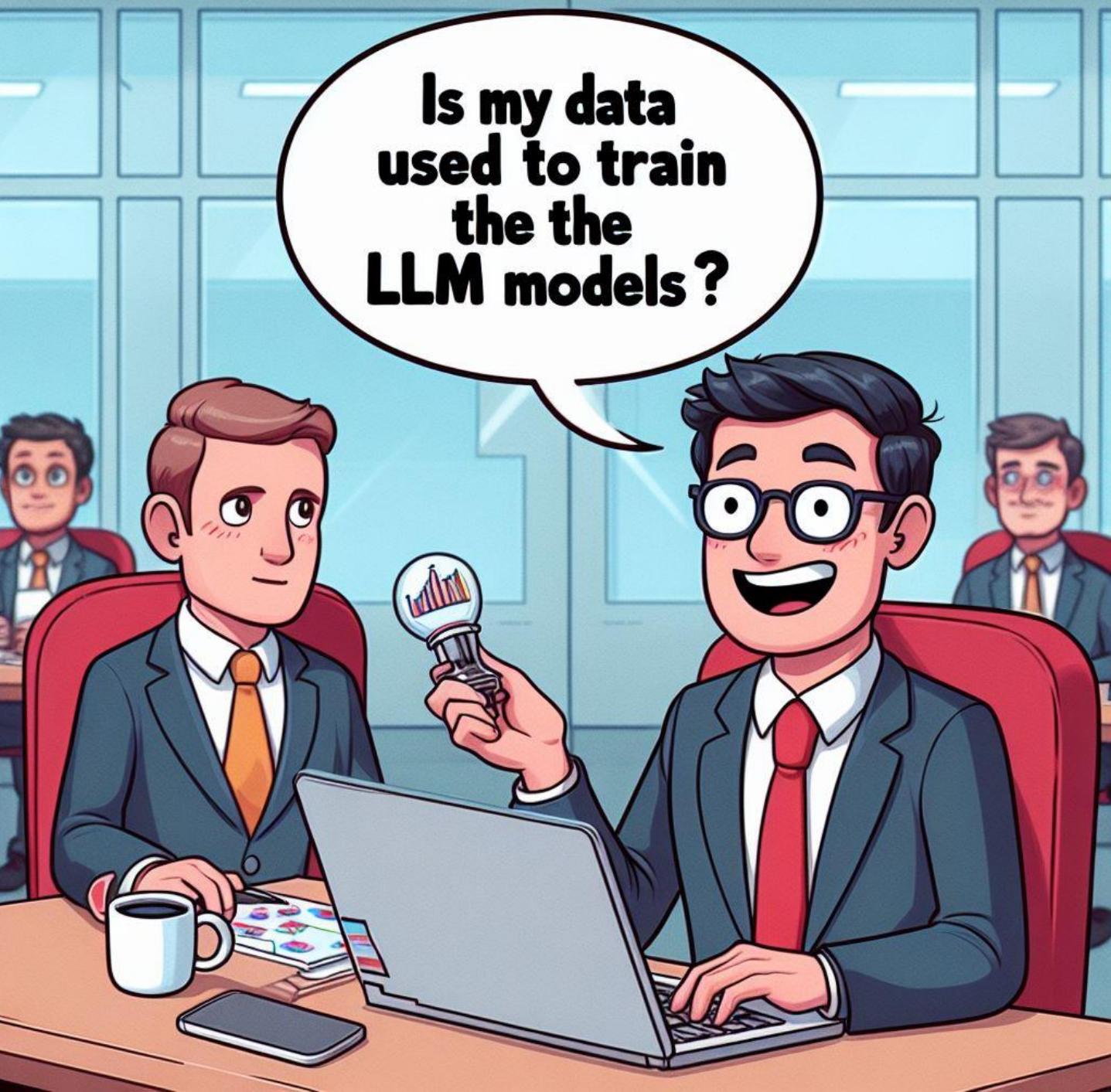
---

What can I do to make sure that only relevant data is being used by Copilot for M365?

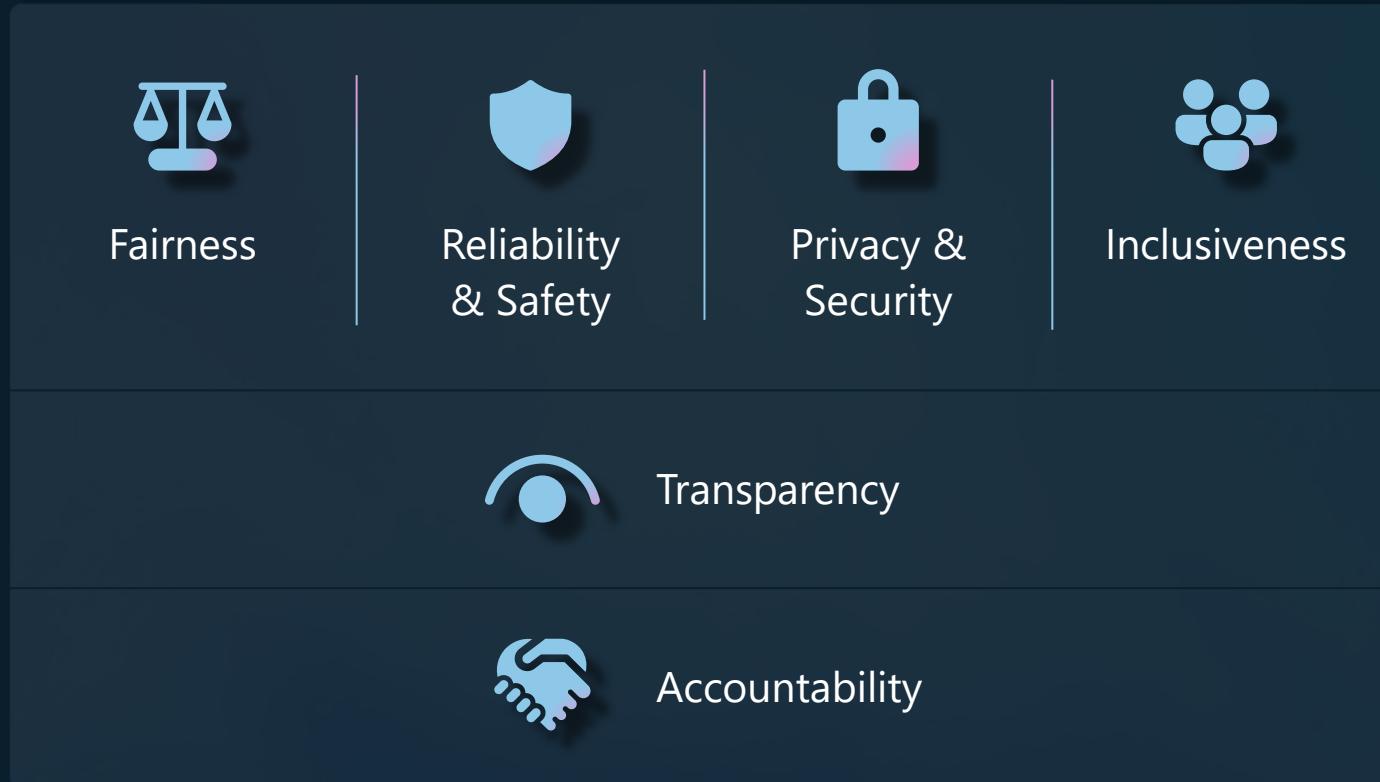
---

What can I do to monitor the use of Copilot for M365 to make sure that it is used according to local regulations and company policies?

Is my data used to  
train the LLM models?



# Microsoft's AI Principles



Microsoft Cloud —  
AI you can trust

Your data is **your** data.

Your data is **not** used to train  
the OpenAI foundation models  
without permission.

Your data is **protected** by the  
most comprehensive enterprise  
compliance and security controls.



How can we protect  
information from  
unauthorized  
oversharing by Copilot  
for M365?



# Copilot for Microsoft 365

Natural language



Large Language  
Models

+



Microsoft Graph  
- your data -



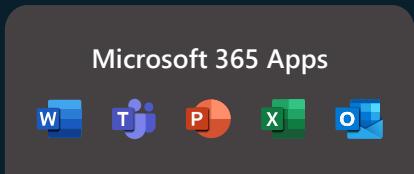
Microsoft  
365 Apps

+



The  
web

# Copilot for Microsoft 365



User prompt



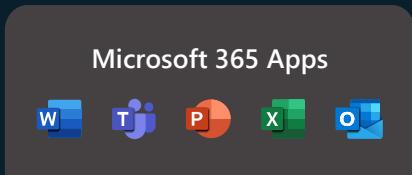
Large Language  
Model



Microsoft Graph



# Copilot for Microsoft 365



User prompt

Pre-processing

Grounding



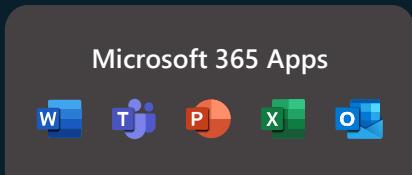
Large Language  
Model



Microsoft Graph



# Copilot for Microsoft 365



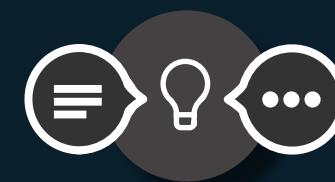
User prompt

Pre-processing

Grounding



Large Language  
Model



Microsoft Graph



Your context and content  
(emails, files, meetings, chats,  
calendars, and contacts)

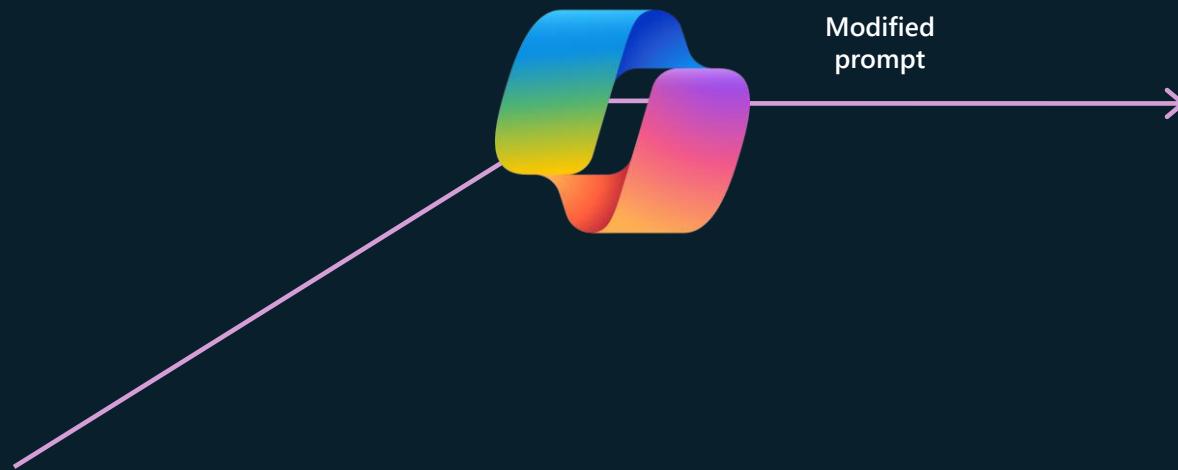
# Copilot for Microsoft 365



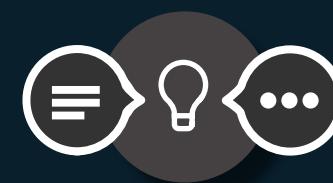
Microsoft Graph



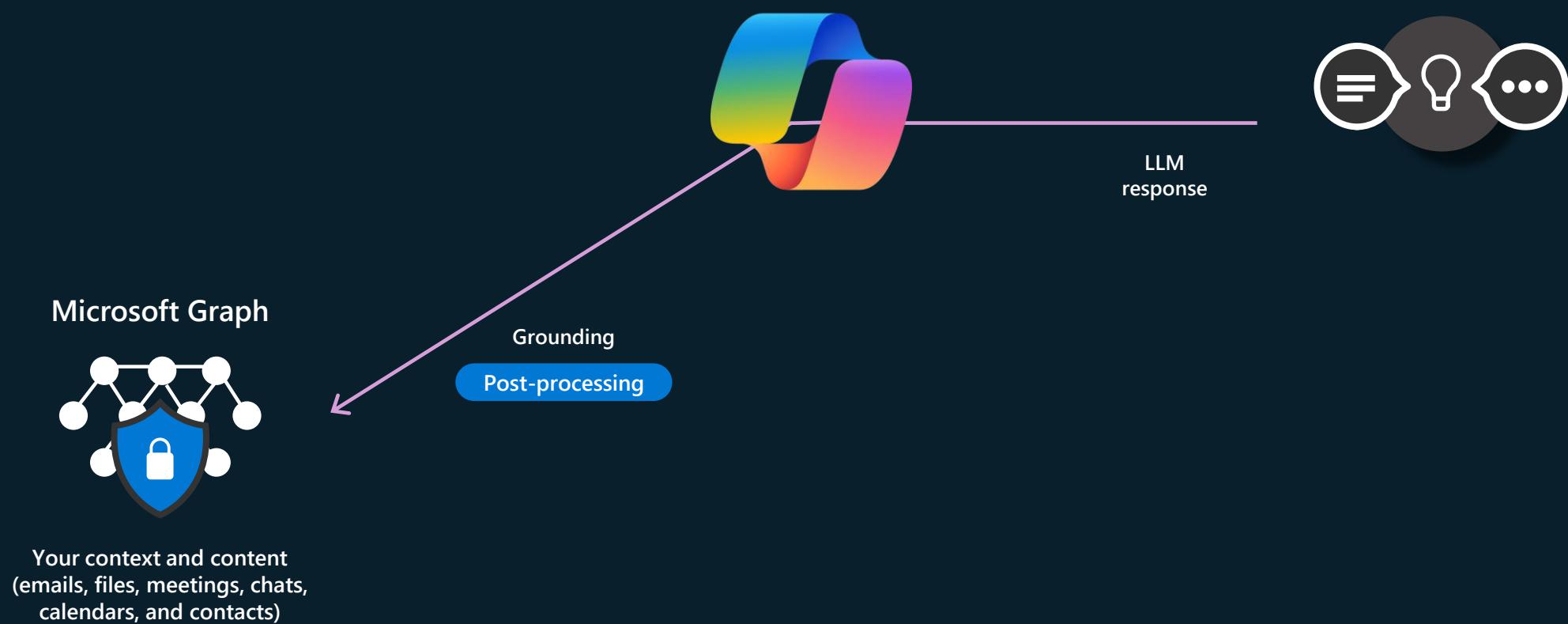
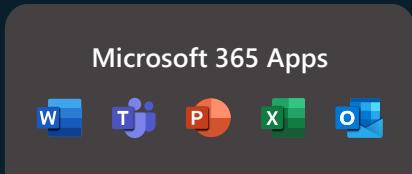
Your context and content  
(emails, files, meetings, chats,  
calendars, and contacts)

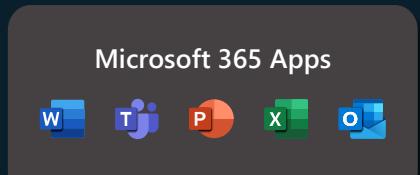


Large Language  
Model



# Copilot for Microsoft 365





Response  
+  
app commands



Large Language  
Model

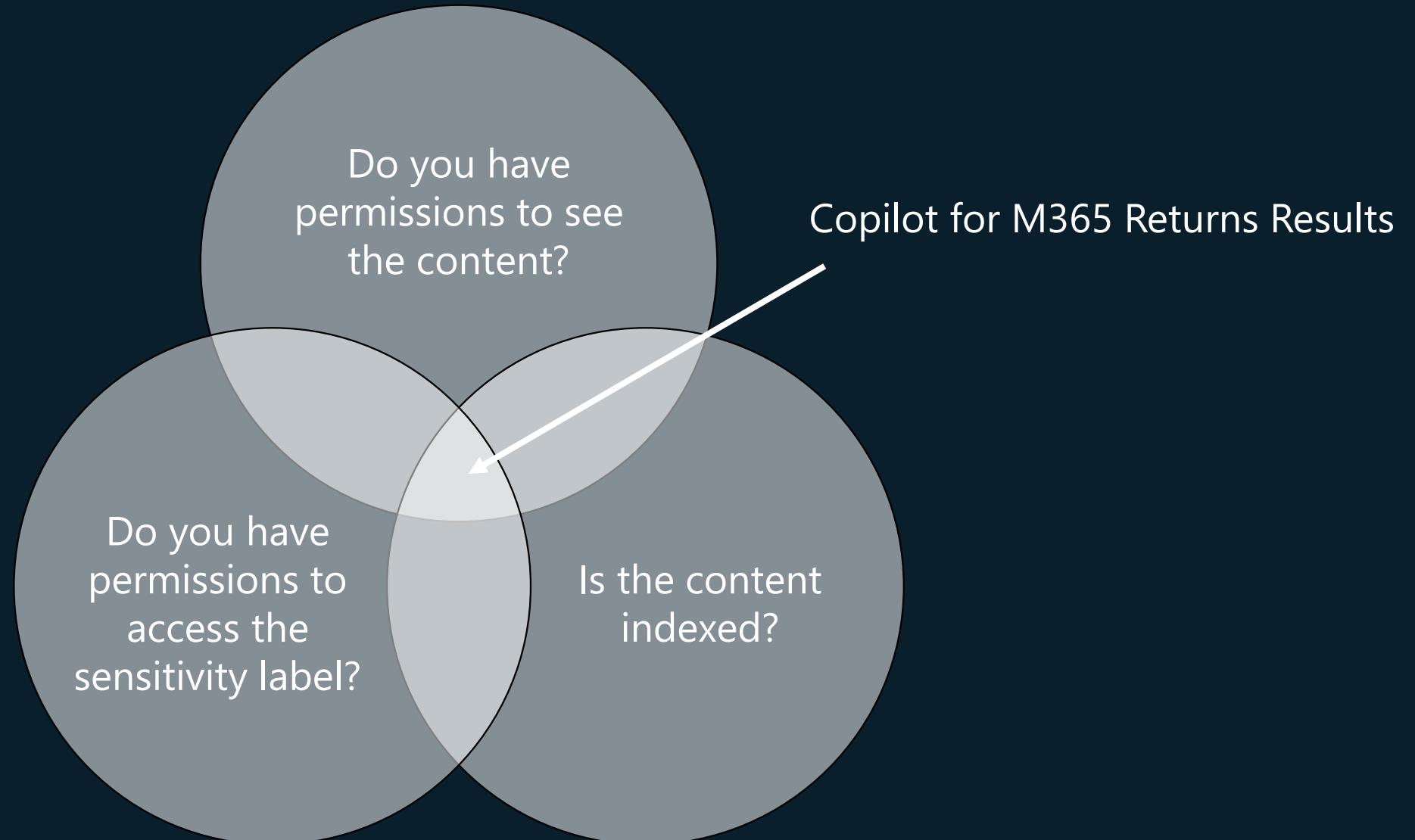


Microsoft Graph

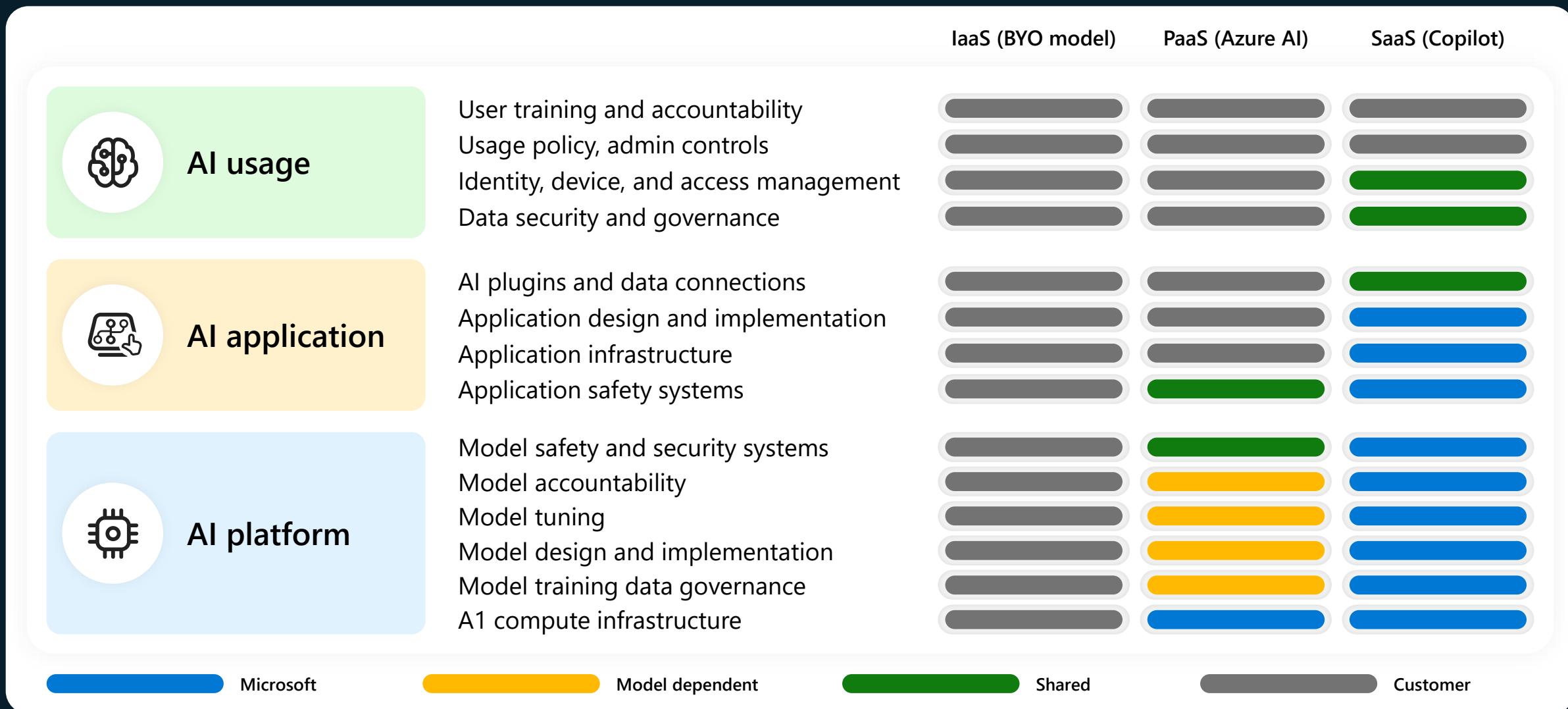


Your context and content  
(emails, files, meetings, chats,  
calendars, and contacts)

# The Simplified Access Model of M365 Data



# Shared responsibility model



# Shared responsibilities of security for AI usage for Microsoft Copilot



**How can we protect  
sensitive information  
from being used by  
Copilot for M365?**



# Automatic discovery of sensitive information

Sensitive info types



Named entities



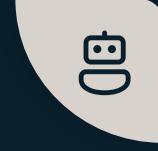
Exact data match



Optical Character  
Recognition (OCR)



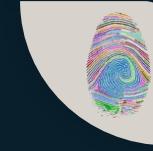
Trainable classifiers



Credentials SITs



Fingerprint SITs



Context-based  
classification



- Home
- Compliance Manager
- Data classification
  - Overview
  - Classifiers
- Content explorer
- Activity explorer
- Data connectors
- Alerts
- Policies
- Roles & scopes
- Trials

---

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

## Overview

Get snapshots of how sensitive info and labels are being used across your organization's locations. [Learn more](#)

### Top trainable classifiers

#### Trainable classifiers used most in your content



### Top sensitive info types

#### Sensitive info types used most in your content



[View all trainable classifiers](#)

[View all sensitive info types](#)

### Top sensitivity labels applied to content

Confidential - Finance	100
General/All Employees (unrestricted)	74
Highly Confidential/Project - Falcon	34
Foo Bar	22
Public	9

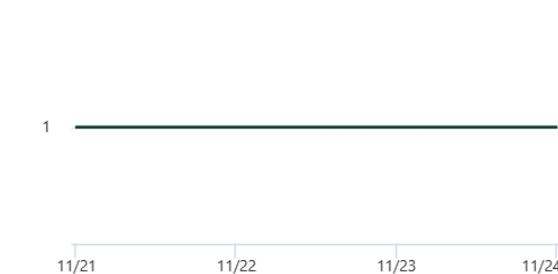
[View all applied sensitivity labels](#)

### Top retention labels applied to content

Demo_Disposition	95
PII Retention Policy	91
Demo_Resume	13
Demo_Resigns	1

[View all applied retention labels](#)

### Daily labeling activity by users



[View all activities](#)

### Top activities detected

**18 activities**

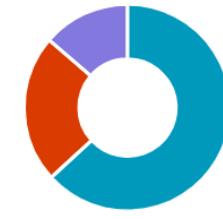
**14 Archive created**

**4 Label applied**

### Locations where sensitivity labels are applied



### Locations where retention labels are applied



[View all activities](#)



## Content explorer

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

 Netherlands

## All locations

Sensitive info types	^	<a href="#">Export</a>	4 items
<strong>Netherlands Physical Addresses</strong>	<strong>202</strong>	<input type="checkbox"/>  Name	<strong>Files</strong>
Netherlands Tax Identification Number	195	<input type="checkbox"/>  Exchange	2 >
Netherlands Citizen's Service (BSN) Number	90	<input type="checkbox"/>  OneDrive	200 >
Netherlands Driver's License Number	3	<input type="checkbox"/>  SharePoint	0 >
		<input type="checkbox"/>  Teams	0 >

# Setting up DLP policies



Template or custom policy Name Admin units**Locations** Policy settings Policy mode Finish

## Choose where to apply the policy

We'll apply the policy to data that's stored in the locations you choose.

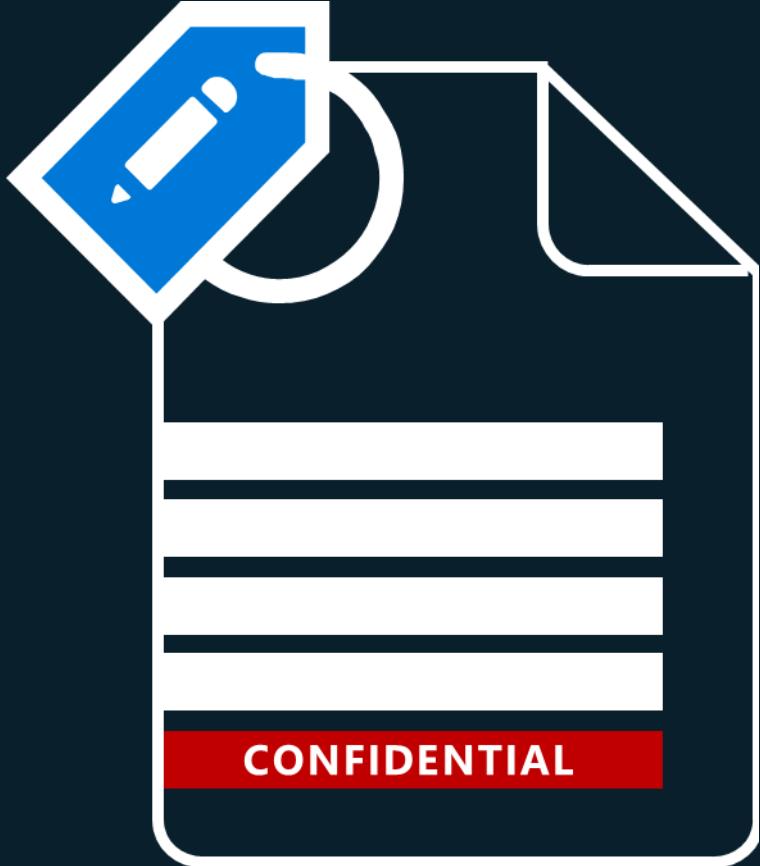
 If your role group permissions are restricted to a specific set of users or groups, you'll only be able to apply this policy to those users or groups. [Learn more about role group permissions.](#) 

[View role groups](#)

 Protecting sensitive info in on-premises repositories (SharePoint sites and file shares) is now in preview. Note that there are prerequisite steps needed to support this new capability. [Learn more about the prerequisites](#)

Location	Scope	
<input type="checkbox"/>  Exchange email	Turn on location to scope	
<input checked="" type="checkbox"/>  SharePoint sites	All sites	<a href="#">Edit</a>
<input type="checkbox"/>  OneDrive accounts	Turn on location to scope	
<input type="checkbox"/>  Teams chat and channel messages	Turn on location to scope	
<input type="checkbox"/>  Devices	Turn on location to scope	
<input type="checkbox"/>  Instances	Turn on location to scope	
<input type="checkbox"/>  On-premises repositories	Turn on location to scope	
<input type="checkbox"/>  Power BI workspaces	Turn on location to scope	

# Setting up sensitivity labels



## Choose permissions

Choose which actions would be allowed for this user/group. [Learn more about permissions](#)

Custom

- View content(VIEW)
- View rights(VIEWRIGHTSDATA)
- Edit content(DOCEDIT)
- Save(EDIT)
- Print(PRINT)
- Copy and extract content(EXTRACT)
- Reply(REPLY)
- Reply all(REPLYALL)
- Forward(FORWARD)
- Edit rights(EDITRIGHTSDATA)
- Export content(EXPORT)
- Allow macros(OBJMODEL)
- Full control(OWNER)

"Edit content (DOCEDIT)" rights are required if you grant "Reply", "Reply all" or "Forward" rights

# User experience with access

AutoSave Off Document1 - Word Search Miriam Graham

File Home Insert Draw Design Layout References Mailings Review View Help

Comments Editing Share

Undo Paste Clipboard Calibri (Body) 11 A A Aa Aa Aa B I U ab x x A A Paragraph Styles Normal No Spacing Heading 1 Editing Dictate Sensitivity Editor Reuse Files

New Blank Document Open Email Print Preview and Print Check Document Read Aloud Draw Table

POLICY TIP Your organization automatically applied the sensitivity: Highly Confidential Label Group\Highly Confidential Label - Internal Only. Highly confidential data that allows all employees view, edit, and reply permissions to this content. Data owners can track and revoke content.

## Project Obsidian Secret Access Key

Samples:

```
string AmazonWebServicesSecretToken = "abcdefghijklmnopqrstuvwxyz0123456789/+ABCDEFGHIJLKLK";
```

Help Link:

<https://docs.aws.amazon.com/toolkit-for-eclipse/v1/user-guide/setup-credentials.html>

<https://docs.aws.amazon.com/general/latest/gr/aws-sec-cred-types.html#access-keys-and-secret-access-keys>



## M365 Chat

What are the important documen...

New chat

...

November 9, 2023 at 07:58 PM

What are the important documents for Project Obsidian?

Here are some important documents for Project Obsidian:

- "**Project Plan for Project Obsidian**" is a document authored by **Alex Wilber** and was last modified Tuesday evening. It provides an overview of the project objectives, scope, deliverables, timeline, and resources. [1](#)

### 1 Project Plan for Project Obsidian

Confidential\Project Obsidian

Word | Alex Wilber modified on 11/07/23

"Project Plan for Project Obsidian A brief overview of the project objectives, scope, Project Objectives The main objective of Project Obsidian is to develop a web-based project ..."

Copy

5 references



● 1/30 AI-generated content may be incorrect



Who is Alex Fromm?

What is the latest update on the engine chip design?

What is the Obsidian FAQ about?



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





Paste



Cut



Copy



Format

Calibri (Body)

11

A<sup>+</sup>A<sup>-</sup>

Aa

A<sup>o</sup>A<sup>z</sup>

Aa

A<sup>o</sup>A<sup>z</sup>

Aa

A<sup>o</sup>A<sup>z</sup>

Aa

A<sup>o</sup>A<sup>z</sup>

Aa

A<sup>o</sup>A<sup>z</sup>

Aa

A<sup>o</sup>A<sup>z</sup>

Aa

A<sup>o</sup>

Clipboard

Font

Paragraph

Styles



Find



Replace



Select



Editing



Dictate



Voice



Sensitivity



Add-ins



Editor



Copilot

## Draft with Copilot

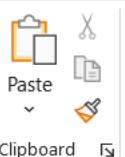


Write a short FAQ on Project Obsidian|

37/2000

Generate

Reference a file



Calibri (Body)

11

A<sup>^</sup>A<sup>v</sup>A<sub>a</sub>A<sub>A</sub>

B

I

U

x<sub>2</sub>x<sup>2</sup>A<sub>v</sub>A<sub>A</sub>A<sub>a</sub>A<sub>A</sub>A<sup>^</sup>A<sub>v</sub>A<sub>A</sub>A<sub>a</sub>A<sup>^</sup>A<sub>v</sub>A<sub>A</sub>A<sub>a</sub>

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



✓ Keep it



For example, "Make it formal"



Focus

Book

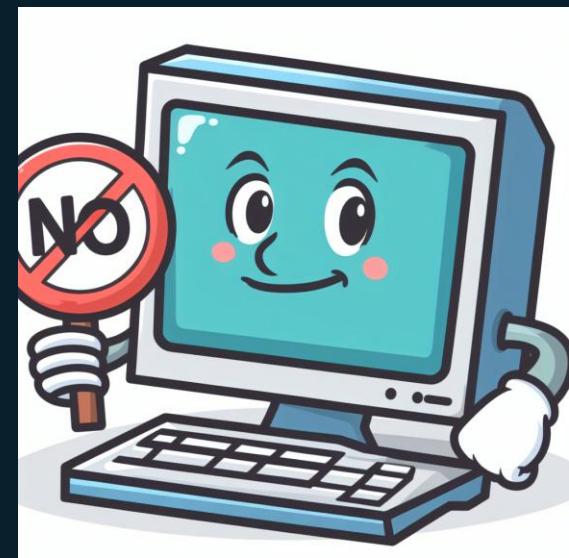
Table

Image

+

110%

# User experience without access





## M365 Chat

what is Project Obsidian about...

New chat

Copilot chats and more

November 8, 2023 at 02:42 PM

what is Project Obsidian about?

I'm sorry, but I couldn't find any specific information about Project Obsidian in my search results. Could you provide more context or details about the project so I can better assist you?

Copy

● 1/30 AI-generated content may be incorrect

Who is the project lead?

What is the goal of the project?

Can you help me with something else?

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





**How can we get  
insights in the use of  
sensitive data with  
Copilot for M365?**

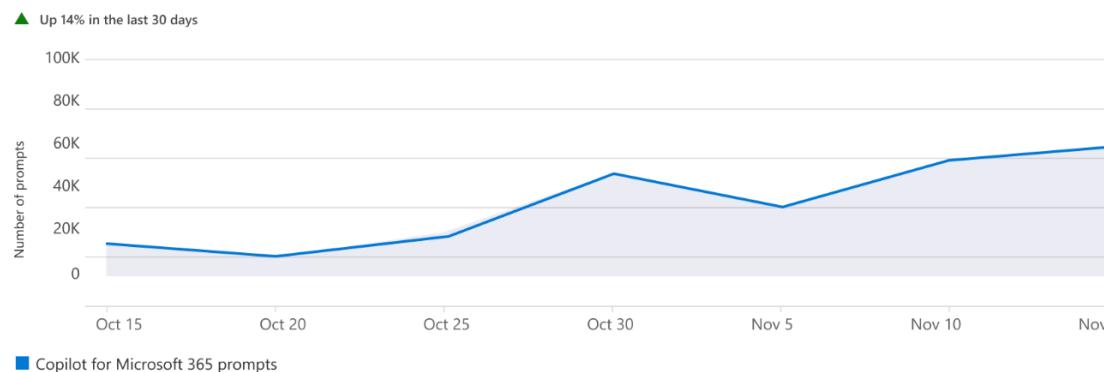
# AI hub (preview)

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

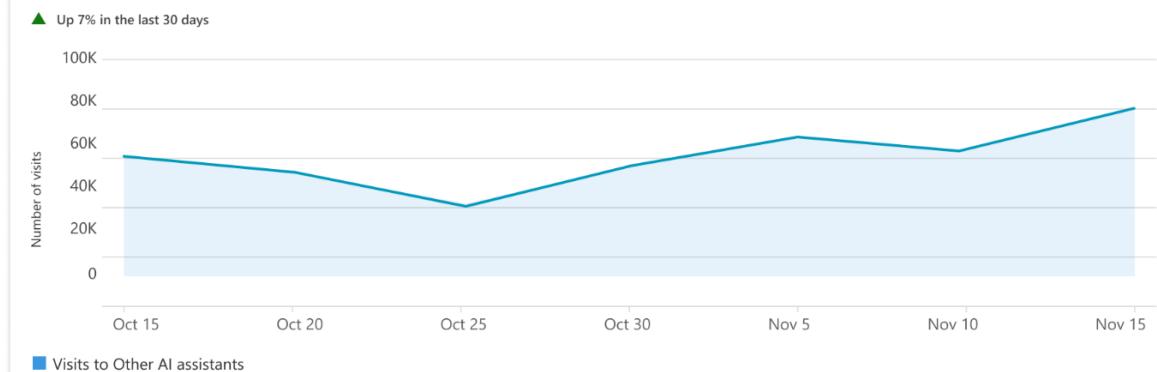
93% of organizations have implemented, developed, or are developing an AI strategy.  
Accelerate productivity with data security and compliance for Microsoft Copilot and other AI-powered assistants.

[Learn more](#)

## Total prompts over time (Microsoft Copilot)

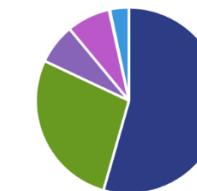
[View details](#)

## Total visits (Other AI assistants)

[View details](#)

## Sensitive data in prompts

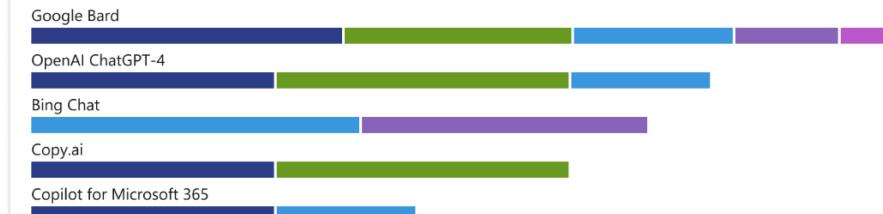
Sensitive data shared with all AI assistants grouped by sensitive information type.



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

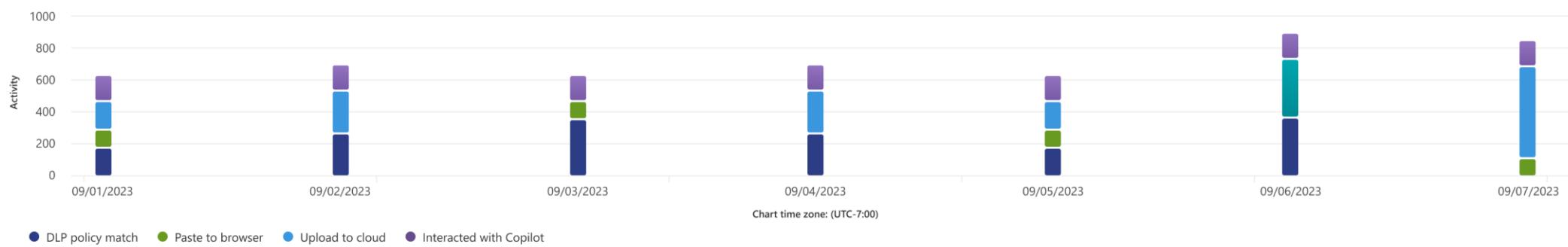
## Total prompts with sensitive data

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

# AI hub (preview)

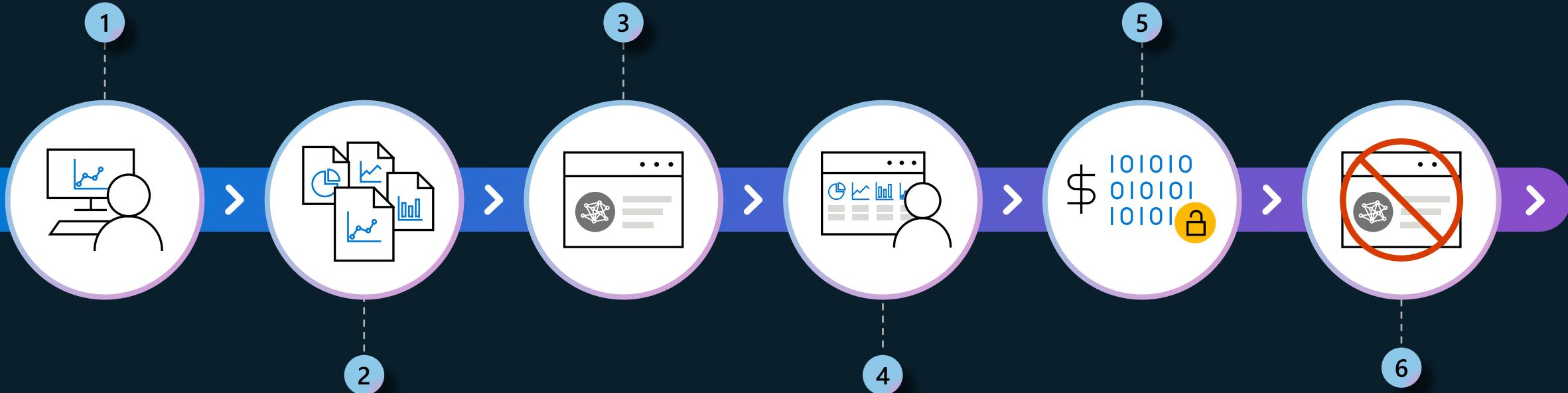
[Analytics](#) [Policies](#) [Activity explorer](#)[Activity: All values](#) [User: All values](#) [DLP policy matched: All values](#) [Sensitive info type: All values](#) [Add filter](#) [Reset all](#)

<input type="checkbox"/>	Activity	User	Time happened	Device full name	Enforcement mode	Sensitive info type	File sensitivity label	DLP policy matched	DLP rules matched	File name
<input type="checkbox"/>	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
<input type="checkbox"/>	Paste to browser	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	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	Sarah Terry	Sep 03, 2023 3:54 PM		Audit	Credit card number				
<input type="checkbox"/>	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
<input type="checkbox"/>	Interacted with Copilot	Dean Renzo	Sep 05, 2023 3:54 PM		Audit	Social security number				
<input type="checkbox"/>	Paste to browser	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	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	Mona Kane	Sep 13, 2023 3:54 PM	Desktop-ASFD213	Audit	Credit card number		AI hub – Data Protection	Audit-UploadToCloud	

What can we do to make sure that our users only use Copilot for M365 and not other Generative AI applications when dealing with company information?



# Let's walk through an example



# Microsoft Defender for Cloud Applications



Cloud appsCloud discoveryCloud app catalogOAuth appsFilesActivity logGovernance logPoliciesMicrosoft 365

## Cloud Discovery

Created on Nov 15, 2023, 1:10 PM

Dashboard Discovered apps Discovered resources IP addresses Users



Ignite2023 GenAI is ready. [View](#) | [Dismiss](#) Ignite2023 GenAI Last 90 days Actions ?

Apps  
287

IP addresses  
1577

Users  
449

Traffic  
47 MB ↑ 35 MB ↓ 13 MB

App categories

< 1-5 of 35 >

Traffic

↓

Sanctioned  Unsanctioned  Other



Risk levels

All categories

by

Traffic

↓



- Traffic from high risk apps
- Traffic from medium risk apps
- Traffic from low risk apps

[Configure score metric](#)

Cloud apps

Cloud discovery

Cloud app catalog

OAuth apps

Files

Activity log

Governance log

Policies

< 1-15 of 287 > [View all apps](#) All categories Traffic ↓

Sanctioned  Unsanctioned  Other



Top entities

[View all users](#)

User

by

Traffic

↓

User

Total

Jazmin@m365security.us

260 KB

Kingsley@m365security.us

246 KB

Contoso Electronics Microsoft 365 Defender Search MA

Health 1.1K

Security 1.1K

Operations management 979

Content management 899

Development tools 780

Collaboration 762

CRM 706

Data analytics 692

News and entertainment 643

Communications 595

Supply chain and logistics 499

Project management 446

Transportation and travel 431

Cloud computing platform 422

Generative AI 413

Business intelligence 389

Cloud storage 386

Advertising 373

Content sharing 330

Property management 303

Product design 260

Sales 252

Google Assistant Generative AI 9

Google DeepMind Generative AI 9

Alphacode Generative AI 9

Adobe Sensei Generative AI 9

OpenAI ChatGPT Generative AI 8

Canva Generative AI 8

OpenAI API Generative AI 8

Dall-e Generative AI 8

H2O.ai Generative AI 8

Forethought Generative AI 8

Tabnine Generative AI 8

CopyAI Generative AI 7

Replit Generative AI 7

Synthesia Generative AI 7

Collaboration	762
CRM	706
Data analytics	692
News and entertainment	643
Communications	595
Supply chain and logistics	499
Project management	446
Transportation and travel	431
Cloud computing platform	422
Generative AI	413
Business intelligence	389
Cloud storage	386
Advertising	373
Content sharing	330
Property management	303
Product design	260
Sales	252
Social network	234
Customer support	232
Online meetings	175
Webmail	163
Internet of Things	151

 Adobe Sensei  
Generative AI

Designing and delivering the perfect customer experience can be complicated. Sensei uses AI and machine learning to make it easier helping you create effortlessly, make informed decisions, and target marketing for better results.

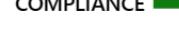
**Suggest an improvement**  **Disclaimer** 

**GENERAL**  8

Category: Generative AI	Headquarters: United States	Data center: Germany
Hosting company: Akamai Technologies	Founded: 1982	Holding: Public
Domain: <a href="http://sensei.adobe.io">*sensei.adobe.io</a>	Terms of service: <a href="http://adobe.com/legal/terms.html">adobe.com/legal/terms.html</a>	Domain registration: Nov 16, 1986
Consumer popularity: 0	Privacy policy: <a href="http://adobe.com/privacy.html">adobe.com/privacy.html</a>	Logon URL: <a href="http://auth.services.adobe.com/en_US/">auth.services.adobe.com/en_US/</a>
Vendor: Adobe	Data types:   Documents, Media files	 Disaster Recovery Plan

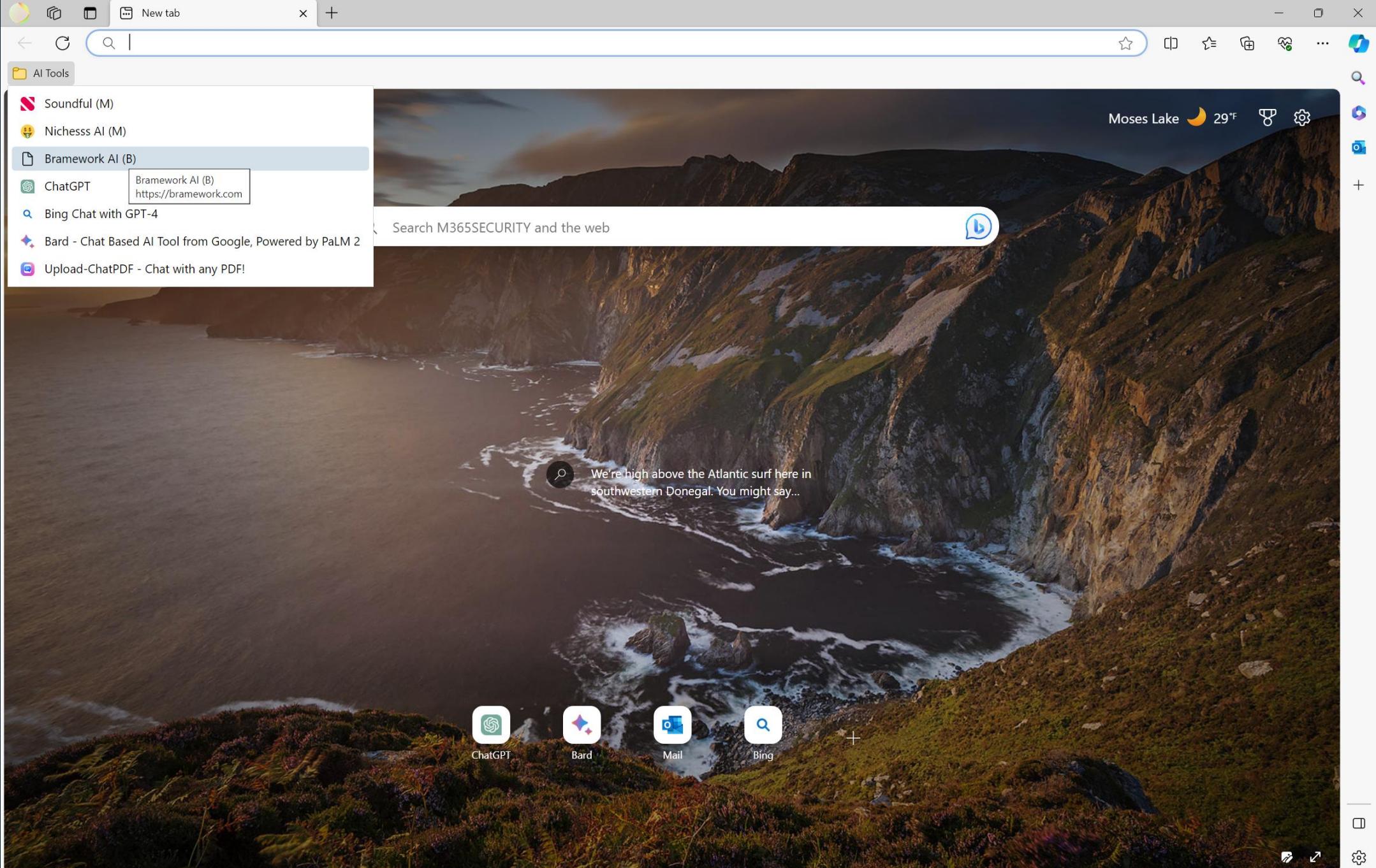
**SECURITY**  9

Latest breach: —	Data-at-rest encryption method: AES	 Multi-factor authentication
 IP address restriction	 User audit trail	 Admin audit trail
 Data audit trail	 User can upload data	 Data classification
 Remember password	 User-roles support	 File sharing
 Valid certificate name	 Trusted certificate	Encryption protocol: TLS 1.3
 Heartbleed patched	 HTTP security headers	 Supports SAML
 Protected against DROWN	 Penetration Testing	 Requires user authentication
Password policy: Partial		

**COMPLIANCE**  10

 ISO 27001	 ISO 27018	 ISO 27017
 ISO 27002	 FINRA	 FISMA
 GAAP	 HIPAA	 ISAE 3402
 ITAR	 SOC 1	 SOC 2





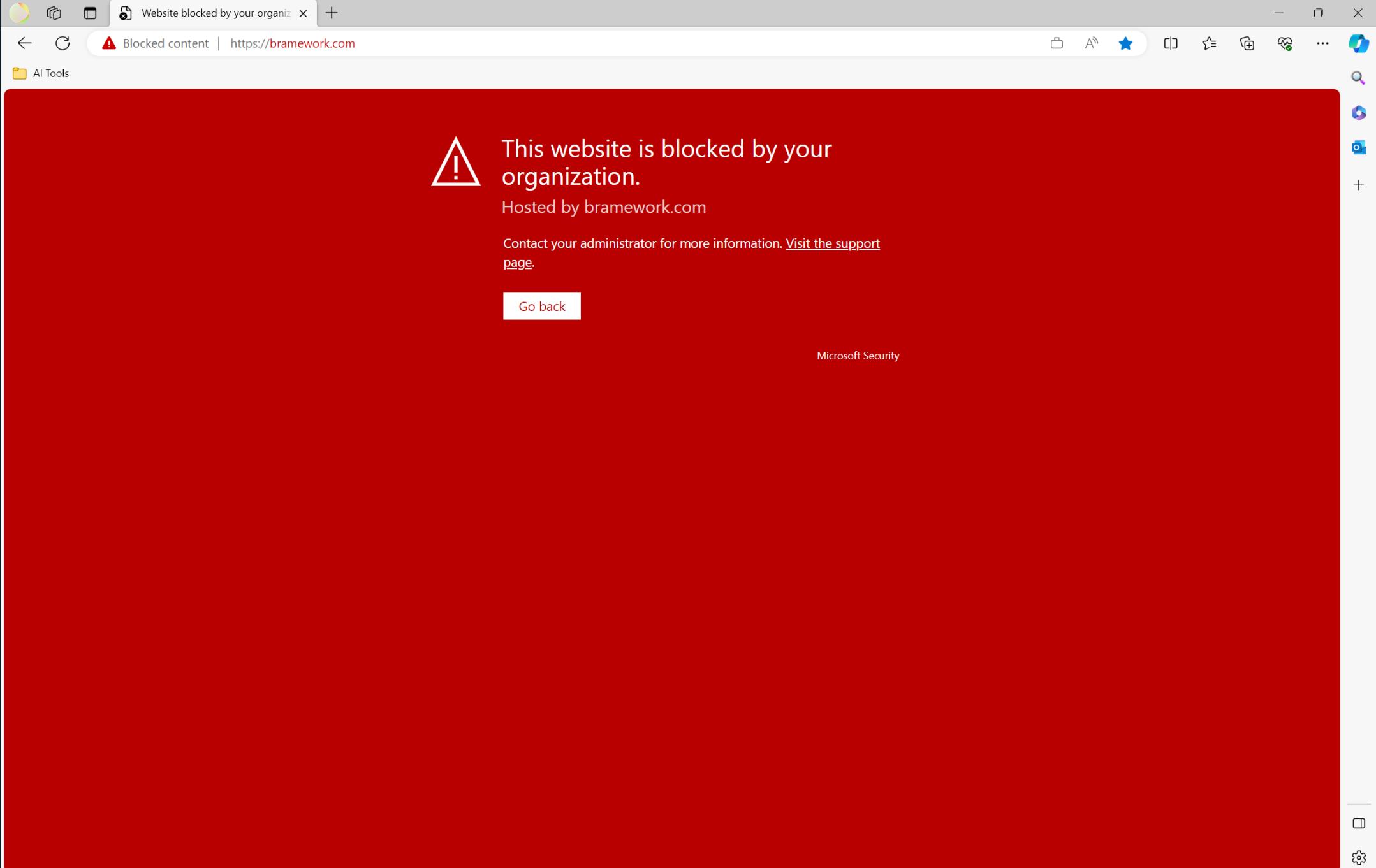
29°F

Clear



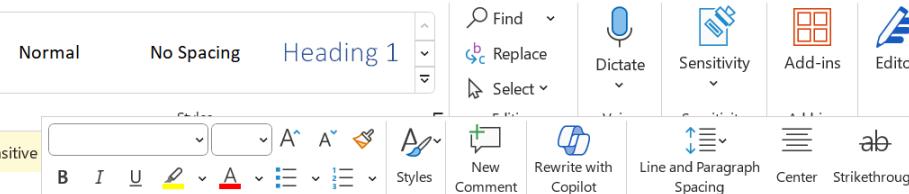
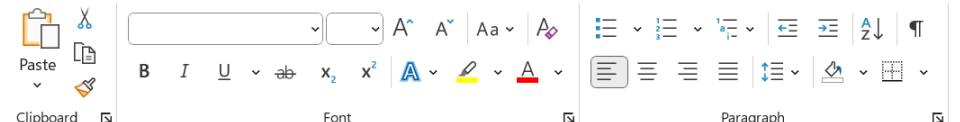
Search

10:29 PM  
ENG  
INTL  
11/15/20234  
2



# Setup an Endpoint DLP policy





**POLICY TIP** Your organization automatically applied the sensitivity: Confidential\Project Obsidian. The organization has detected sensitive

Project Obsidian FAC

## What is project obsidian?

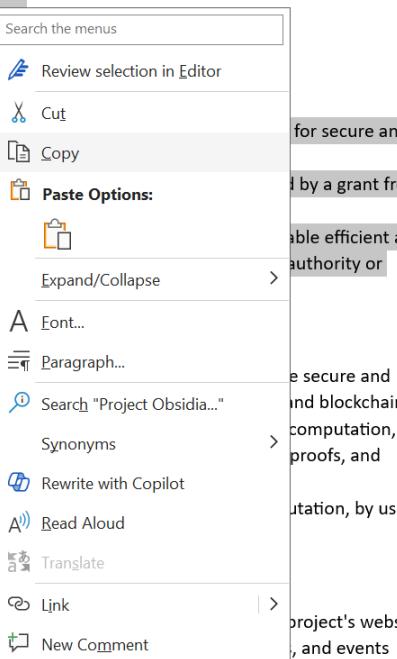
- Project obsidian is a research initiative that explores the potential of scalable distributed computing.
  - The project is led by a team of experts from the National Science Foundation.
  - The project's main goal is to design and implement a trustworthy computation among multiple intermediaries.

What are the benefits of project o

- Project obsidian can potentially enable a scalable computation, such as machine learning, by using advanced techniques such as homomorphic encryption and secure multiparty computation.
  - Project obsidian can also enhance the privacy of users by using novel mechanisms such as sharding, consensus, and blockchains.
  - Project obsidian can also improve the performance of computations by using parallel processing, distributed systems, and efficient algorithms.

How can I get involved in project o

- If you are interested in learning more about the project, you can visit its website at <https://projectobsidian.org>, where you can find information about the project's goals, team, and progress.
  - If you are a researcher or a developer who wants to contribute to the project, you can join the project's GitHub repository at <https://github.com/projectobsidian>, where you can access the project's code, documentation, and issues.
  - If you are a user or a stakeholder who wants to provide feedback or suggestions to the project, you can contact the project's team at [projectobsidian@domain.com](mailto:projectobsidian@domain.com), where you can share your ideas, questions, and comments.



New tab Bard

https://bard.google.com/chat?hl=en

SharePoint Home | Microsoft 3... Project Obsidian AI Tools

Bard Experiment

See the latest updates to the Privacy Help Hub

+ New chat

Recent

AI's Well-Being

# Hello again

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

**Understand**

- how something works
- rules of a sport
- what's behind a trend

Your conversations are private. We don't store anything you wouldn't want us to.

How it works Dismiss

**Create**

- Emoji Win+Period
- Voice typing Win+H
- Undo Ctrl+Z
- Cut Ctrl+X
- Copy Ctrl+C
- Paste Ctrl+V
- Paste as plain text Ctrl+Shift+V
- Select all Ctrl+A
- Add page to sidebar
- Writing direction
- Inspect

**Explore**

- date night planning
- presentation topic ideas
- delicious noodles

Enter a prompt here

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

A screenshot of the Google Bard AI chat interface. The main area displays the message "Hello again" and a placeholder "Tell me what's on your mind, or pick a suggestion.". Below this are three sections: "Understand", "Create", and "Explore". A context menu is open over the input field at the bottom, listing various functions like Paste, Undo, and Select all. The status bar at the bottom shows the location as Washington, USA, the time as 6:33 AM, and the date as 11/16/2023.



40°F  
Cloudy



Search



6:33 AM  
11/16/2023



New tab Bard

https://bard.google.com/chat?hl=en

SharePoint Home | Microsoft 3... Project Obsidian AI Tools

Bard Experiment

+ New chat

Recent

AI's Well-Being

**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

Hello again

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

**Understand**

- how something works
- rules of a sport
- what's behind a trend

**Create**

- game night planning
- sales pitch
- social post

**Explore**

- date night planning
- presentation topic ideas
- delicious noodles

Your conversations are processed by human reviewers to improve the technologies powering Bard. Don't enter anything you wouldn't want reviewed or used.

How it works Dismiss

Enter a prompt here

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

Washington, USA  
From your IP address • Update location



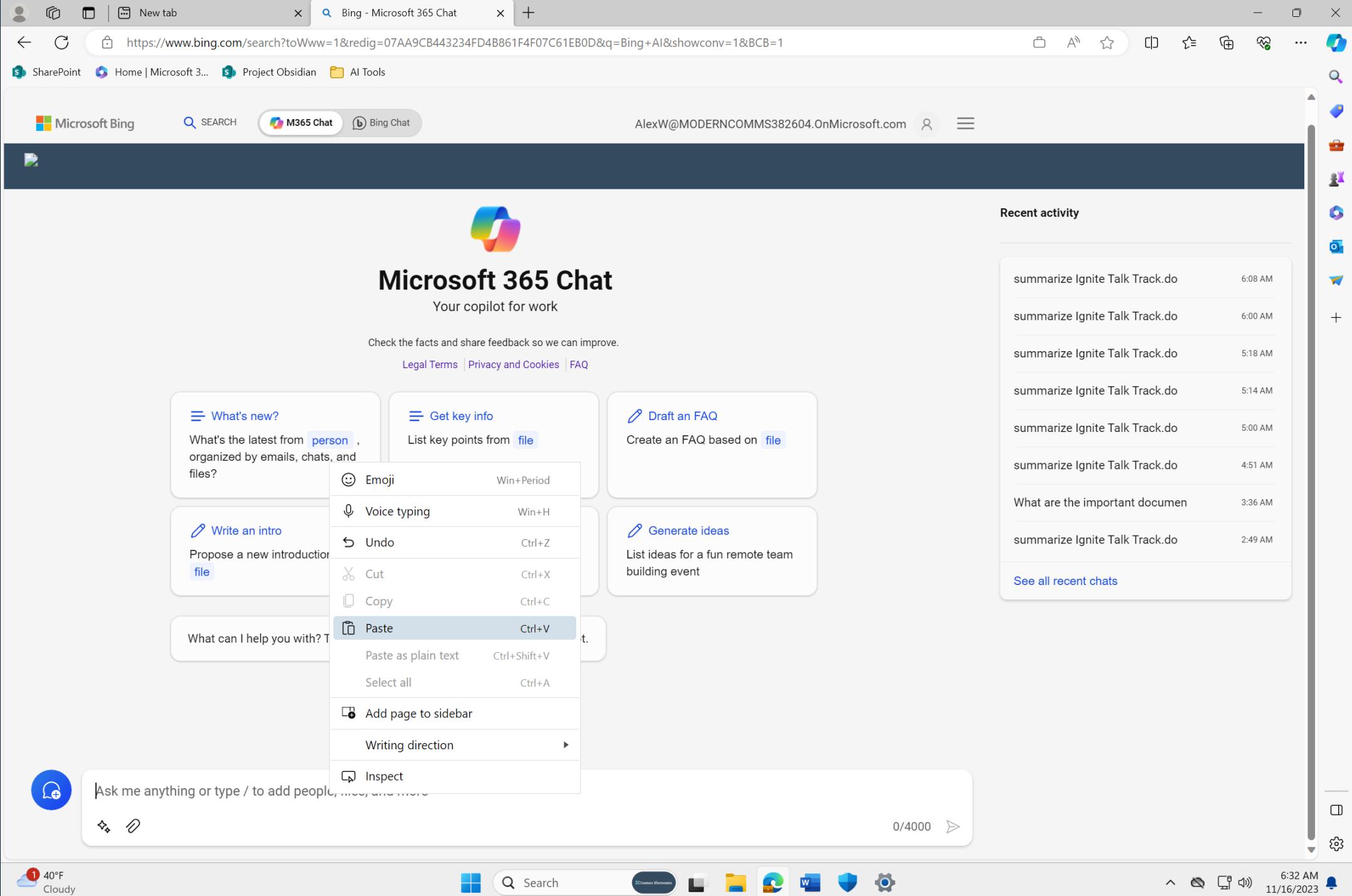
40°F  
Cloudy



Search



6:33 AM  
11/16/2023



New tab

Bing - Microsoft 365 Chat

https://www.bing.com/search?toWww=1&redig=07AA9CB443234FD4B861F4F07C61EB0D&q=Bing+AI&showconv=1&BCB=1

SharePoint Home | Microsoft 3... Project Obsidian AI Tools

Microsoft Bing SEARCH M365 Chat Bing Chat AlexW@MODERNCOMMS382604.OnMicrosoft.com

Check the facts and share feedback so we can improve.

Legal Terms | Privacy and Cookies | FAQ

**What's new?**  
What's the latest from [person](#), organized by emails, chats, and files?

**Get key info**  
List key points from [file](#)

**Draft an FAQ**  
Create an FAQ based on [file](#)

**Write an intro**  
Propose a new introduction to [file](#)

**How to**  
How do I write a request for proposal?

**Generate ideas**  
List ideas for a fun remote team building event

What can I help you with? Try one of the examples or enter your own prompt.

Recent activity

- summarize Ignite Talk Track.do 6:08 AM
- summarize Ignite Talk Track.do 6:00 AM
- summarize Ignite Talk Track.do 5:18 AM
- summarize Ignite Talk Track.do 5:14 AM
- summarize Ignite Talk Track.do 5:00 AM
- summarize Ignite Talk Track.do 4:51 AM
- What are the important documen 3:36 AM
- summarize Ignite Talk Track.do 2:49 AM

See all recent chats



### Project Obsidian FAQ

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 funded by a grant from the National Science Foundation.
- The project's main goal is to design and implement a new protocol that can enable efficient and trustworthy computation among multiple parties, without relying on a central authority or intermediary.

\$



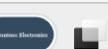
510/4000



40°F  
Cloudy



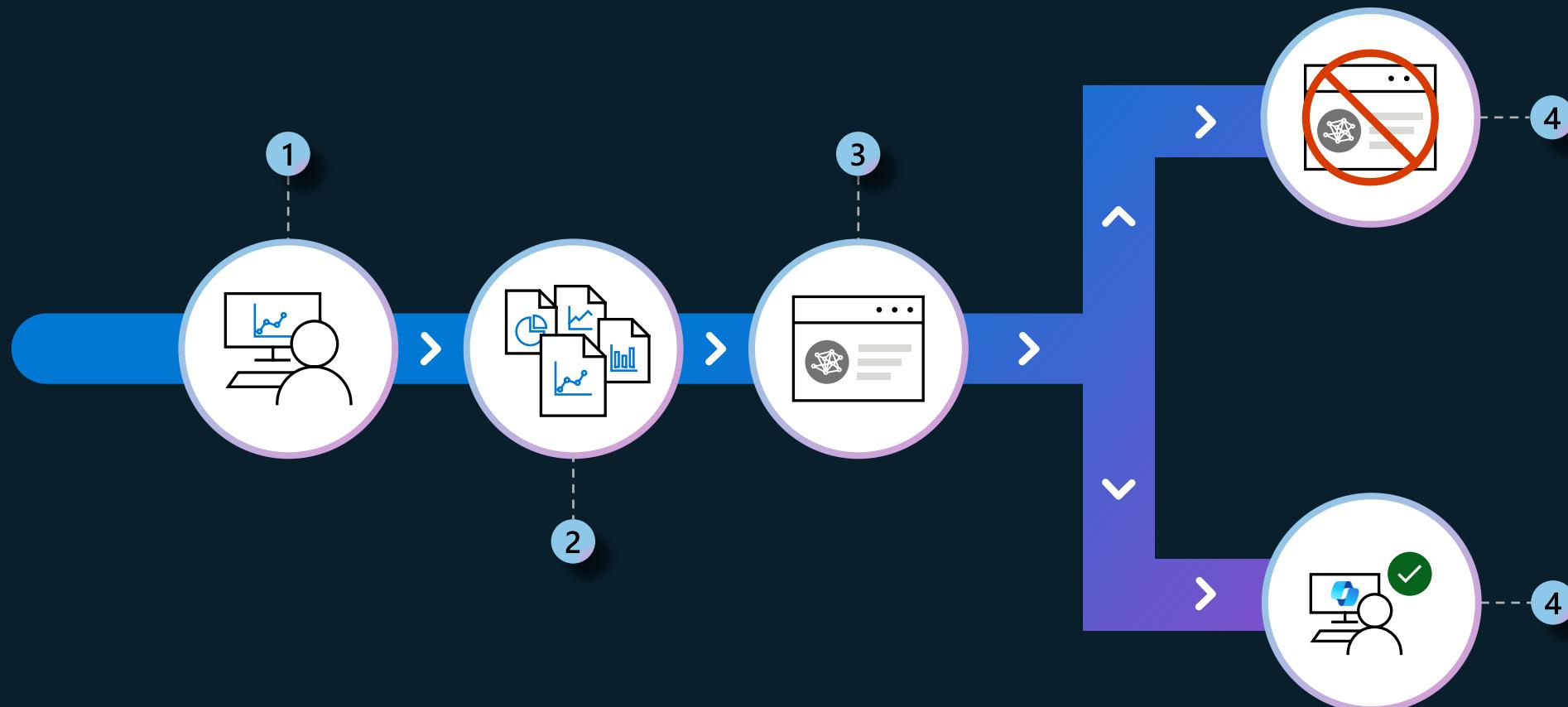
Search



6:32 AM  
11/16/2023

4

# Let's go back to the example





What can I do to make sure that only relevant data is being used by Copilot for M365?

# Data lifecycle and records management

GOVERN  
YOUR DATA

Automatically retain, delete, and store  
information and records in a compliant manner



## Data Lifecycle Management

Manage risk and liability by  
only keeping what you need  
and deleting what you don't  
across your entire digital estate



## Records management

Manage high value content following  
the specialized workflows required to  
meet legal, business, or regulatory  
recordkeeping obligations



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

## Choose where to apply this policy

The policy will apply to content that's stored in the locations you choose.

You can set up data connectors to import content from non-Microsoft apps like Slack, WhatsApp and many more, for use with this solution. [Set up now](#)

Status	Location	Applicable Content	Included	Excluded
<input type="radio"/> Off	Exchange mailboxes	Items in user, shared, and resource mailboxes: emails, calendar items with an end date, notes, and tasks with an end date. Doesn't apply to items in Microsoft 365 Group mailboxes. <a href="#">More details</a>		
<input type="radio"/> Off	SharePoint classic and communication sites	Files in classic sites or communication sites or team sites that aren't connected to a Microsoft 365 group, and files in all document libraries (including default ones like Site Assets). <a href="#">More details</a>		
<input type="radio"/> Off	OneDrive accounts	All files in users' OneDrive accounts. <a href="#">More details</a>		
<input type="radio"/> Off	Microsoft 365 Group mailboxes & sites	Items in the Microsoft 365 Group mailbox, and files in the corresponding group-connected SharePoint team site. Doesn't apply to files in SharePoint classic or communication sites or SharePoint team sites that aren't connected to Microsoft 365 Groups. <a href="#">More details</a>		
<input type="radio"/> Off	Skype for Business	Skype conversations for the users you choose.		
<input type="radio"/> Off	Exchange public folders	Items from all Exchange public folders in your organization.		
<input type="radio"/> Off	Teams channel messages	Messages from channel conversations and channel meetings. Doesn't apply to Teams private channel messages. <a href="#">More details</a>		
<input type="radio"/> Off	Teams chats and Copilot interactions	Messages from individual chats, group chats, meeting chats, bot chats, and interactions with Microsoft Copilot for Microsoft 365. <a href="#">More details</a>		
<input type="radio"/> Off	Teams private channel messages	Messages from Teams private channels. <a href="#">More details</a>		
<input type="radio"/> Off	Yammer community messages	Messages from Yammer community discussions. <a href="#">More details</a>		
<input type="radio"/> Off	Yammer user messages	Private messages and community message		

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

## Decide if you want to retain content, delete it, or both

### Retain items for a specific period

Items will be retained for the period you choose.

#### Retain items for a specific period

7 years

#### Start the retention period based on

When items were created

#### At the end of the retention period

##### Delete items automatically

##### Do nothing

##### Retain items forever

Items will be retained forever, even if users delete them.

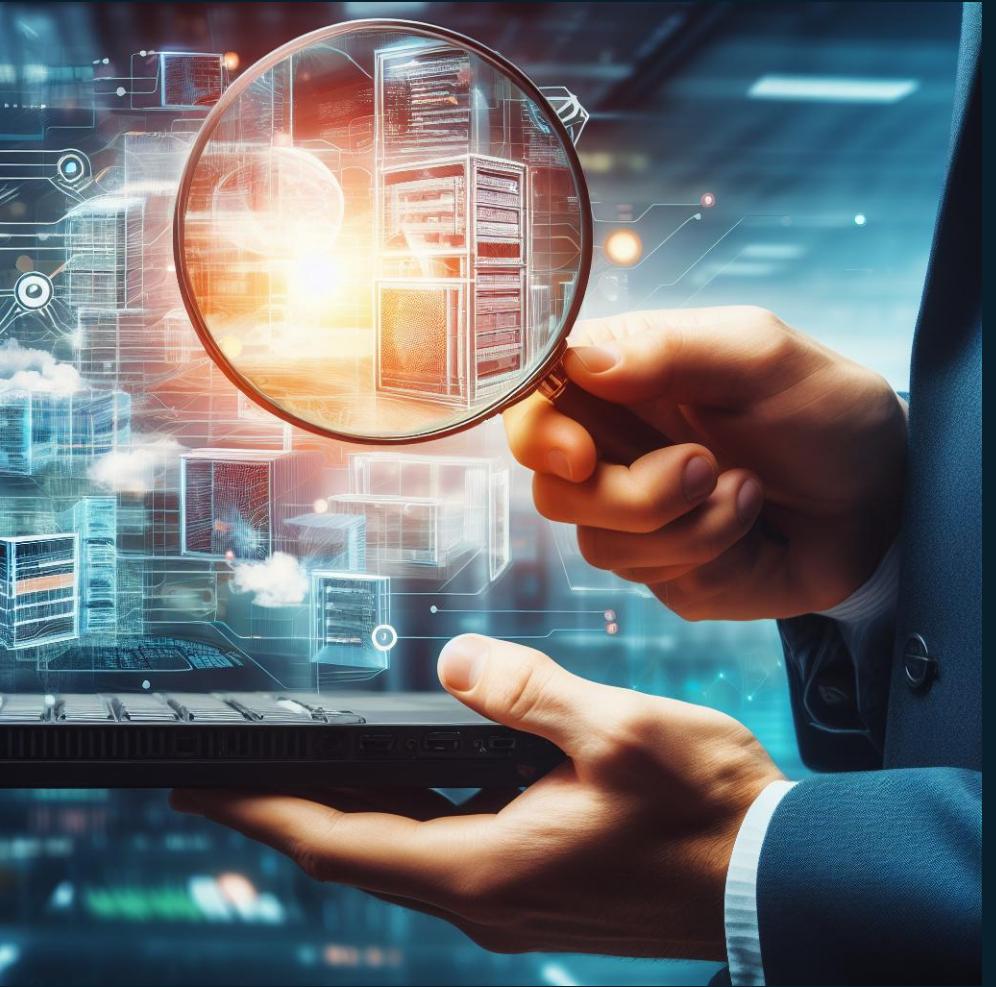
##### Only delete items when they reach a certain age

Items won't be retained, but when they reach the age you choose, we'll delete them from where they're stored.

What can I do to monitor the use of Copilot for M365 to make sure that is used according to local regulations and company policies?



# Audit



Audit &gt; Audit search

X

**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

**Users**

AlexW@MODERNCOMMS382604.OnMicrosoft.com

**Activity**

Interacted with Copilot

**Item****Details****CreationTime**

2023-11-07T18:20:46

**Id**

8a2bfba6-c241-47fd-a6e5-6995b57590b0

**Operation**

CopilotInteraction

**OrganizationId**

b9ba404e-37f1-4363-bb0b-fc387ddfabe6

**RecordType**

261

**UserKey**

23f35b20-f05f-42f6-9ce8-d53c9edd3ce0

**UserType**

0

**Version**

1

**Workload**

Copilot

**Close**

# Communication compliance



Communication compliance > Policies > Sensitive information

 Export files  Export report  Download review activity

Pending (5) Resolved (0) Exports

**Filter**  Save the query  Reset  Filter

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

	Subject	Tags	Sender	Recipients	Sentiment	Date (UTC)
<input type="checkbox"/>	Copilot in Word	...	Alex Wilber <Alex...	Copilot <>, >	Neutral	Nov 7, 2023 8:
<input type="checkbox"/>	Copilot in Word	...	Copilot	Alex Wilber <Alex...	Positive	Nov 7, 2023 8:
<input type="checkbox"/>	Copilot in Word	...	Copilot	Alex Wilber <Alex...	Neutral	Nov 7, 2023 8:
<input type="checkbox"/>	Copilot in Word	...	Alex Wilber <Alex...	Copilot <>, >	Neutral	Nov 7, 2023 8:
<input checked="" type="checkbox"/>	Copilot in BizChat	...	Alex Wilber <Alex...	Copilot <>, >	Neutral	Nov 7, 2023 8:

Copilot in BizChat

**Source** Plain Text User history

#### **Conditions detected:** Sensitive terms (Obsidian)

[View all](#)

**From:** Alex Wilber <AlexW@MODERNCOMMS382604.OnMicrosoft.com>

**Sent on:** Tuesday, November 7, 2023 8:11:35 PM

To: Copilot ◇

**Subject:** Copilot in BizChat

what are the latest files on Project Obsidian?

## Resolve

## Notify

## Tag as

## Escalate

# eDiscovery



eDiscovery (Premium) &gt; Cases &gt; Copilot data spillage &gt; 11.09.2023 Alex

Saved filter queries ▾

Filters Undo filter query Redo filter query

AND

Select a filter

+ Add filter Add subgroup

<input type="checkbox"/>	#	Subject/Title	Status	Tag Status	Date (UTC)	Sender/Author
<input type="checkbox"/>	1	Microsoft 365 Chat...	Ready	No Tag		
<input type="checkbox"/>	2	Create an FAQ bas...	Ready	No Tag	Nov 8, 2023 9:39 PM	Alex Wilber <Alex...
<input checked="" type="checkbox"/>	3	what are the latest ...	Ready	No Tag	Nov 7, 2023 12:11 ...	Alex Wilber <Alex...
<input type="checkbox"/>	4	What are the impo...	Ready	No Tag	Nov 9, 2023 11:59 ...	Alex Wilber <Alex...
<input type="checkbox"/>	5	Summarize Ignite T...	Ready	No Tag	Nov 8, 2023 7:14 PM	Microsoft 365 Chat...
<input type="checkbox"/>	6	Microsoft 365 Chat...	Ready	No Tag		
<input type="checkbox"/>	7	summarize Ignite T...	Ready	No Tag	Nov 8, 2023 3:51 PM	Alex Wilber <Alex...
<input type="checkbox"/>	8	What are the impo...	Ready	No Tag	Nov 8, 2023 5:22 PM	Alex Wilber <Alex...

Viewing: Page 1 of 1 | 50 items/page

what are the latest files on P

Source Plain text Annotate Metadata

 Show pinned metadata

Alex Wilber &lt;AlexW@MODERNCOMMS382604.OnMicrosoft.com&gt; 11/7/2023 8:11 PM

what are the latest files on Project Obsidian?

Microsoft 365 Chat 11/7/2023 8:11 PM

Here are the latest files on Project Obsidian:

Tag

Group by families (2)

Group by conversations (2)

# Security questions raised around Copilot for M365

---

Is my data used to train the LLM models?

---

How can we protect information from unauthorized oversharing by Copilot for M365?

---

How can we protect sensitive information from being used by Copilot for M365?

---

How can we get insights in the use of sensitive data with Copilot for M365?

---

What can we do to make sure that our users only use Copilot for M365 and not other Generative AI applications when dealing with company information?

---

What can I do to make sure that only relevant data is being used by Copilot for M365?

---

What can I do to monitor the use of Copilot for M365 to make sure that it is used according to local regulations and company policies?

# Microsoft Purview

Integrated solutions to secure and govern your entire data estate



## Comprehensive data security

Secure data across its lifecycle,  
wherever it lives



## Modern data governance

Govern data seamlessly to empower  
your organization



## Risk & compliance posture

Manage critical risks  
and regulatory requirements

Unstructured & Structured data

Traditional and AI Generated data

Microsoft 365 and Multi-cloud

- Shared platform capabilities

# Thank you!

## Next steps

Start with your AI data security journey now:

- Get insights
- Set access controls
- Implement sensitivity labels
- Prevent data leakages with DLP policies
- Setup compliance policies

Microsoft, Avanade and other partners are more than happy to help you in this journey!

Together we can ensure that AI is **safe** for everyone.

