



# Data, security, and compliance practices for Microsoft 365 Copilot

**Henry Yang, Microsoft Hong Kong**  
**Felix Chan, SoftwareOne Hong Kong**





# Securing and governing Microsoft 365 Copilot



Microsoft 365 Copilot



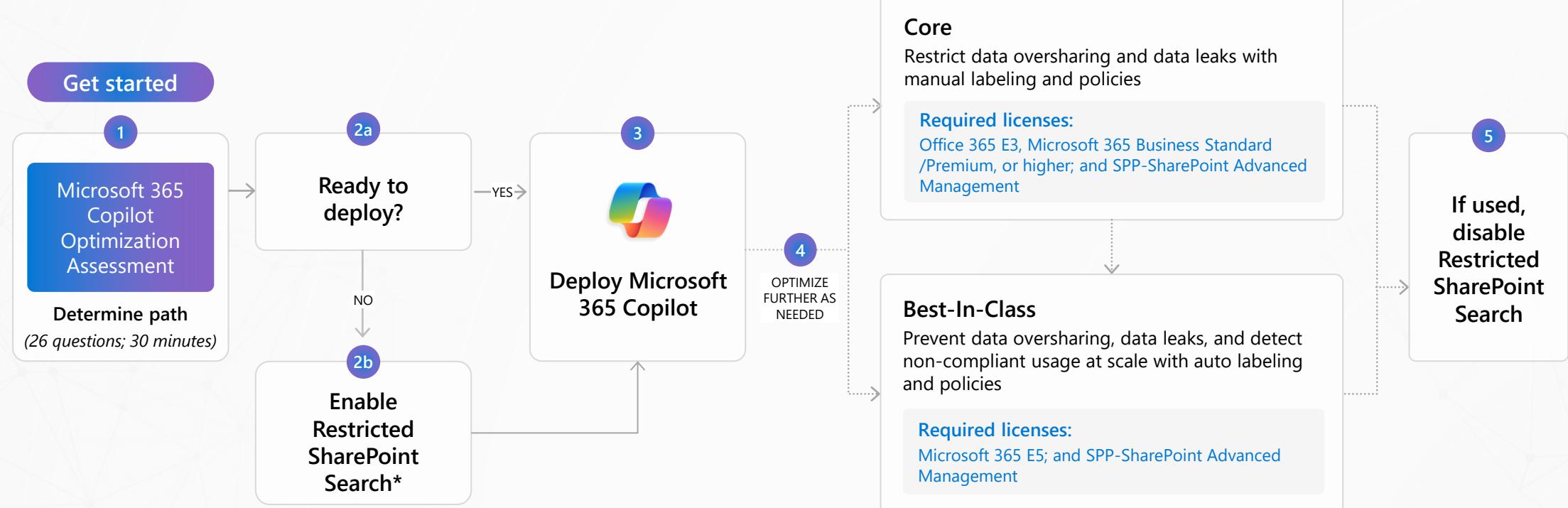
SharePoint



Microsoft  
Purview

# Apply appropriate Data Security controls

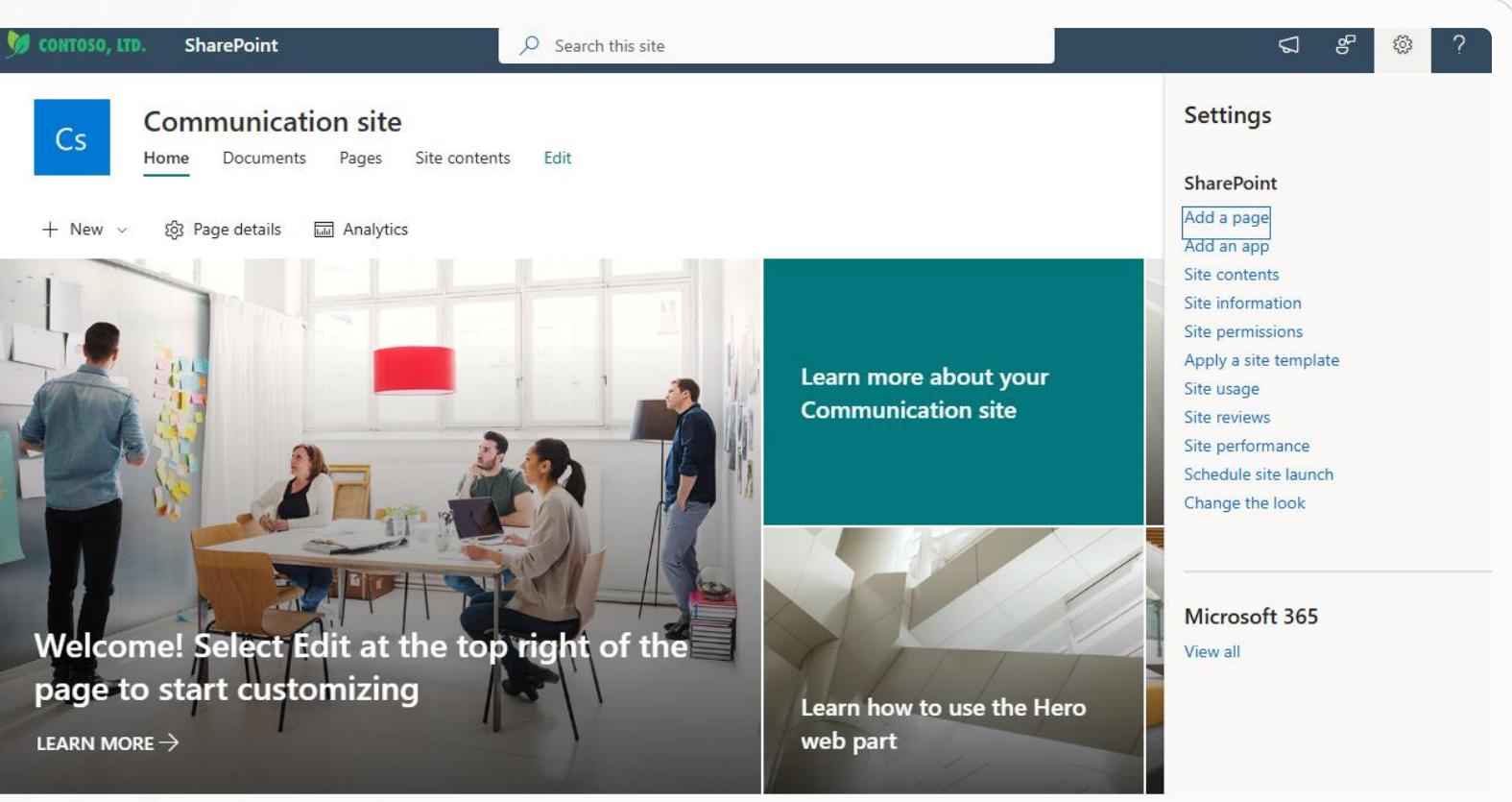
Get started quickly and continue to optimize along the way



\*Restricted SharePoint Search will limit Microsoft 365 Copilot experiences and organization-wide search. It is a temporary option which gives you time to address oversharing concerns while getting started on your Copilot journey.

# Review SharePoint site permissions

Ask site owners to manually review SharePoint site permissions and correct as needed



The screenshot shows a SharePoint Communication site homepage. At the top, there's a navigation bar with the Contoso logo, the word "SharePoint", a search bar, and several icons. Below the navigation, the page title is "Communication site". The main content area features a large image of people working in an office, a "Welcome!" message, and a "LEARN MORE →" button. To the right, there's a sidebar titled "Settings" with sections for "SharePoint" (including "Add a page" which is highlighted) and "Microsoft 365". A large, semi-transparent callout box on the right side of the page contains the text "Shared with external users" and a "Run report" button.

Welcome! Select Edit at the top right of the page to start customizing

LEARN MORE →

Communication site

Home Documents Pages Site contents Edit

+ New Page details Analytics

Search this site

CONTOSO, LTD. SharePoint

Settings

SharePoint

- Add a page (highlighted)
- Add an app
- Site contents
- Site information
- Site permissions
- Apply a site template
- Site usage
- Site reviews
- Site performance
- Schedule site launch
- Change the look

Microsoft 365

View all

Shared with external users

Run report

# Restricted SharePoint Search

This is intended as a temporary solution to give you time to review and audit site permissions, while implementing robust data security solutions from Microsoft Purview and content management with SharePoint Advanced Management

- **Restricted SharePoint Search** is designed for organizations particularly concerned about unintentional oversharing of content
- When enabled, Copilot experiences and organization-wide search are limited to a select set of SharePoint sites, as well as the individual user's files and content



## Prerequisites

- Available to tenants with Microsoft 365 Copilot subscriptions
- Activation requires Global/Tenant/SharePoint admin rights



## Impact

Restricted SharePoint Search disables organization-wide search, while allowing you to select sites that you trust. This means users in your organization can use Copilot to reason over:

- An allowed list of curated SharePoint sites set up by admins (up to 100 SharePoint sites), honoring existing permissions on a site
- Users' OneDrive for Business, chats they are part of, emails they send and receive, calendars to which they have access, etc.
- Files that are shared with, and accessed by users
- Content from users' frequently visited sites

Turning on Restricted SharePoint Search does not affect the site's index or associated DLP and labeling policies

Access this [blog](#) for more info

# Update Default Sharing Link Type

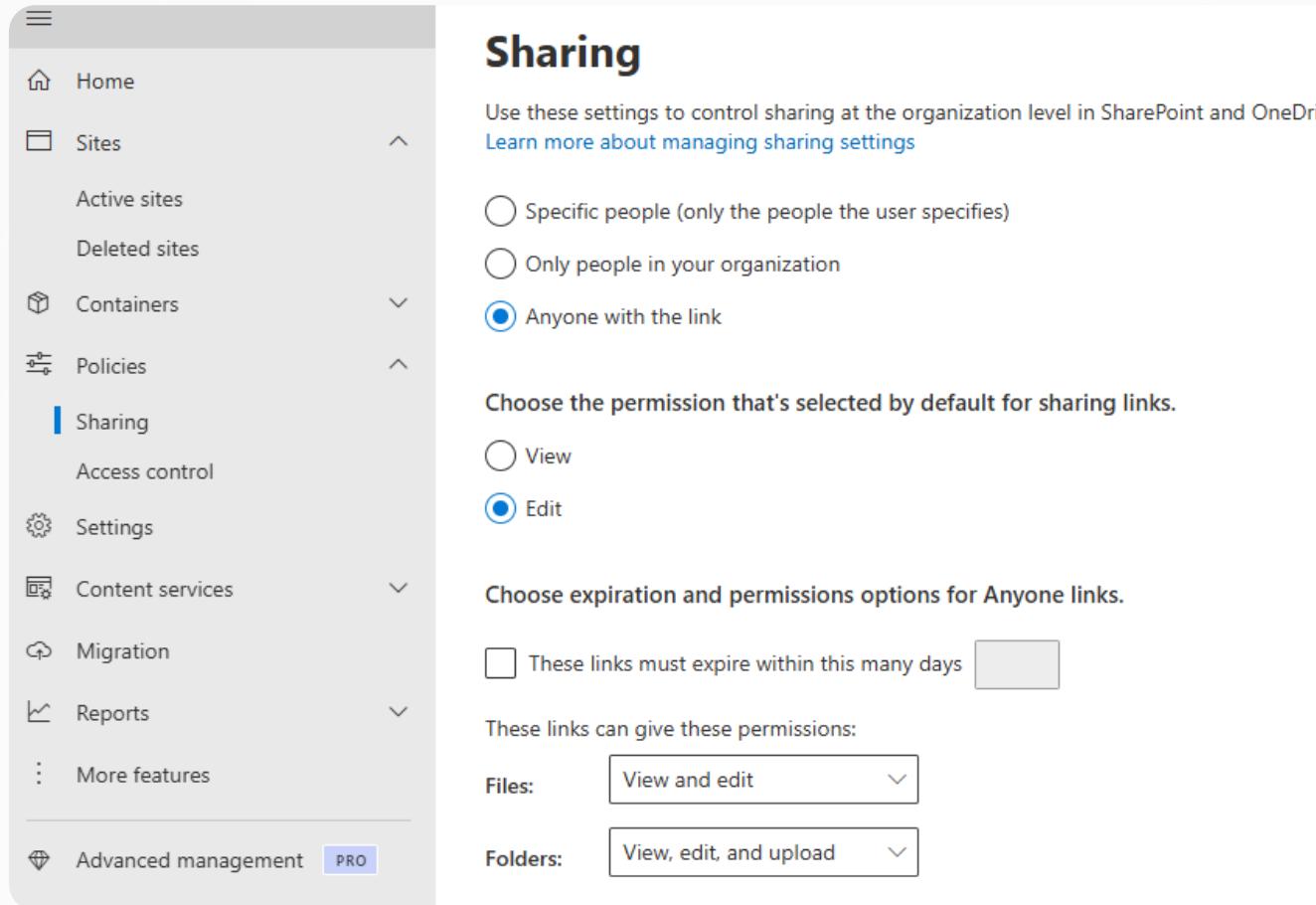
- Set default sharing link type on tenant
- Optionally set the sharing link type on specific sites

The screenshot shows the SharePoint Admin Center interface. On the left, there's a navigation pane with options like Home, Sites, Active sites, Deleted sites, Containers, Policies, Sharing, Access control, and more. The 'Sharing' option is highlighted. In the main area, it says 'Active sites' and provides instructions to sort and filter sites. It lists two sites: 'All Company' and 'Communication site'. A context menu is open over the 'Communication site', with 'Edit sharing settings' being the selected option. This leads to a detailed sharing settings dialog.

The screenshot shows the 'Sharing' settings page in the SharePoint Admin Center. The left sidebar has 'Sharing' selected under 'Content services'. The main content area is titled 'Sharing' and includes a note about controlling sharing at the organization level. It shows a scale from 'Most permissive' (Any user can share) to 'Least permissive' (Only people in your organization can share). Below this, there are sections for 'File and folder links' and 'Choose the permission that's selected by default for sharing links', where 'Edit' is selected.

# Set sharing link expiration on anyone links

Set sharing link expiration on anyone links



The screenshot shows the SharePoint admin center's Sharing page. On the left is a navigation menu with Home, Sites, Containers, Policies, Sharing (which is selected), Access control, Settings, Content services, Migration, Reports, More features, and Advanced management (PRO). The main area is titled "Sharing" and contains instructions: "Use these settings to control sharing at the organization level in SharePoint and OneDrive." It includes a link to "Learn more about managing sharing settings". There are three radio button options for sharing scope: "Specific people (only the people the user specifies)", "Only people in your organization", and "Anyone with the link", with "Anyone with the link" selected. Below this, it says "Choose the permission that's selected by default for sharing links" with "Edit" selected. It also says "Choose expiration and permissions options for Anyone links" and has a checkbox for "These links must expire within this many days" which is unchecked. Under "These links can give these permissions:", "Files:" is set to "View and edit" and "Folders:" is set to "View, edit, and upload".

# SharePoint Advanced Management

Manage Data Oversharing



# Data access governance insights

As sprawl and oversharing of SharePoint sites increase with exponential data growth, organizations need to help govern their data.



Discover sites that contain potentially **overshared or sensitive content**.



Use reports to assess and **apply appropriate security and compliance policies**.



Identify potential **oversharing** by seeing the sites where users created the newest sharing links.

The screenshot shows the SharePoint Data Access Governance interface. On the left is a navigation sidebar with options like Home, Sites, Policies, Sharing, Access control, Settings, Content services, Migration, Reports (which is selected), and More features. The main content area has a header "Welcome to data access governance" with a sub-header "These new reports help you maintain the security and compliance of your data in SharePoint." It features a "Sharing links" section with a blue padlock icon and a "Sensitivity labels applied to files" section with a blue file icon. Both sections have "View reports" buttons. At the bottom right is a search bar.

[Data access governance reports for SharePoint sites](#)

## Data access governance

This page provides reports to help you maintain the security and compliance of your data in SharePoint.

[Learn more about data access governance](#)

### Sharing links

Identify potential oversharing by monitoring sites where users created new sharing links in SharePoint.

[View reports](#)

### Sensitivity labels applied to files

Monitor sensitive content by reviewing the sites where sensitive files are stored and the policies applied to these sites.

[View reports](#)

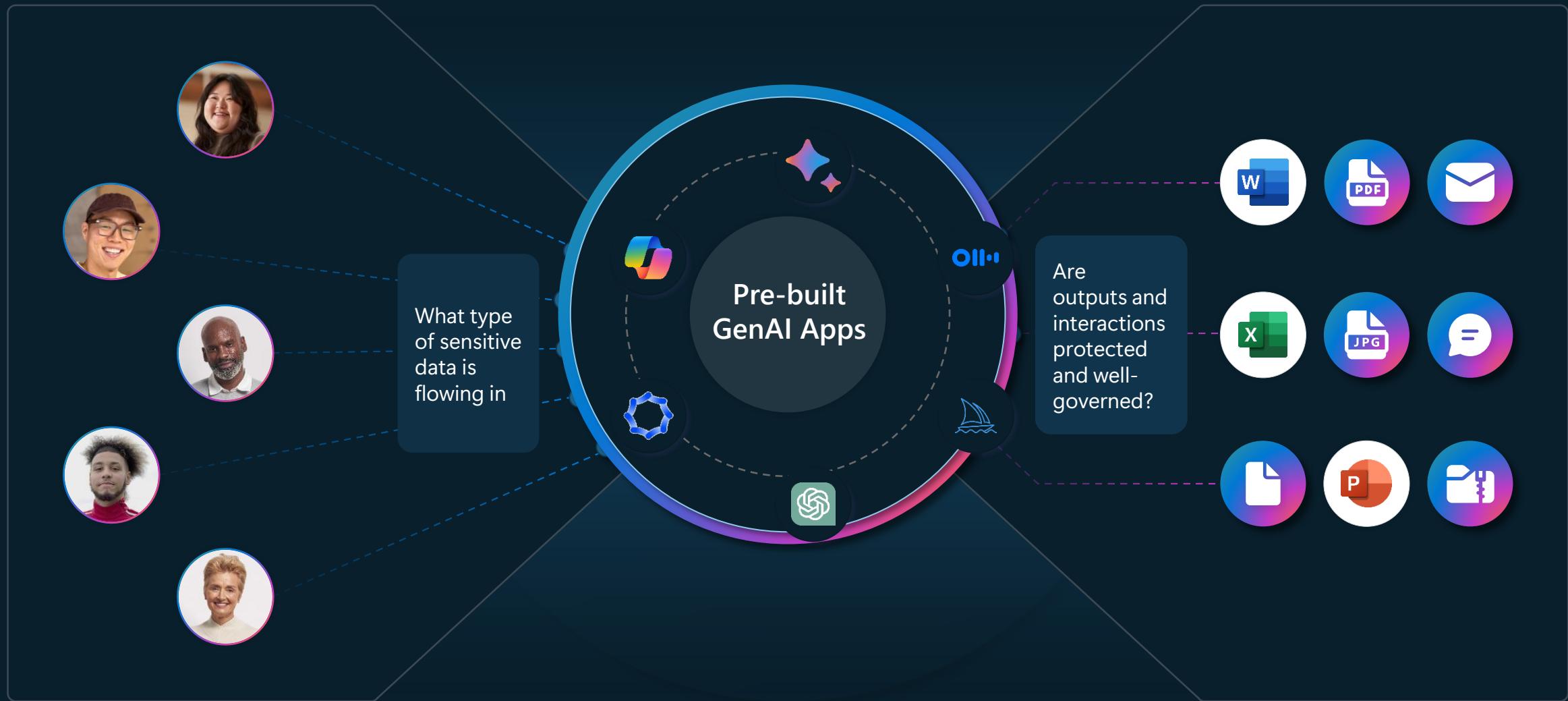
### Content shared with 'Everyone except external users'

IN PREVIEW

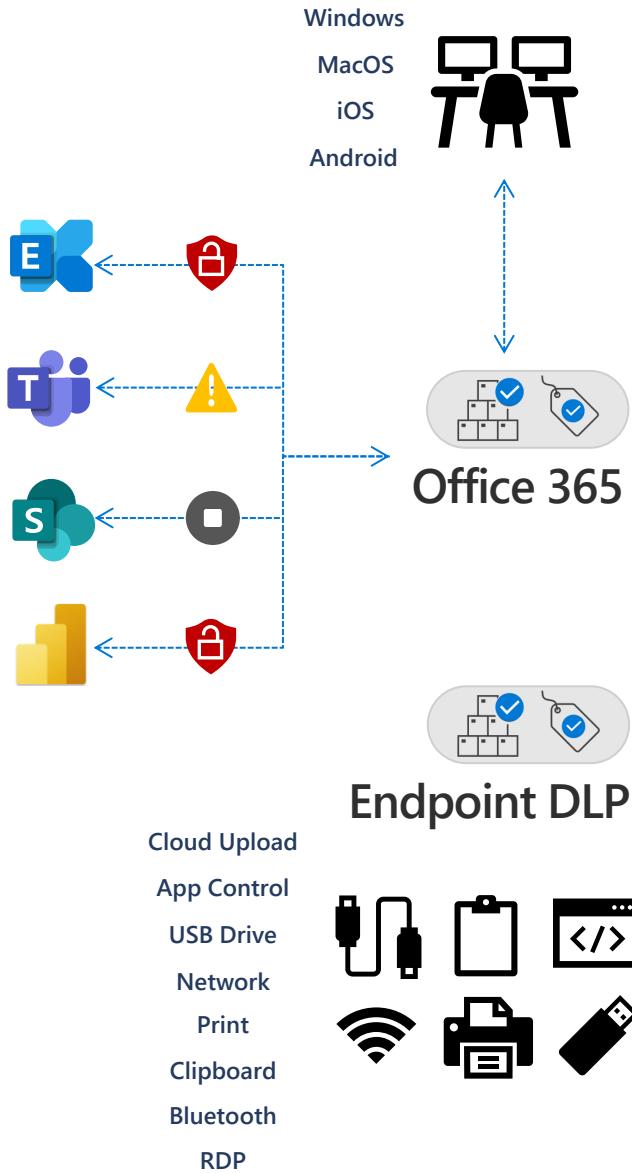
Discover potential oversharing by reviewing content shared with 'Everyone except external users'.

[View reports](#)

# Risks evolving across data, users, and AI apps



# Microsoft Purview Information Protection



## Data Classification Service



### Sensitive Information Types

Out of the Box  
CCN/SSN/License  
[Double Key Encryption](#)  
[Named entity](#)  
[10 templates \(Finance, IP, Legal, Healthcare...\)](#)

Custom  
RegEx  
Dictionary  
Fingerprint  
[Exact Data Match \(EDM\)](#)

Trainable Classifiers  
Sample Content  
Test  
Validate  
Publish



### Sensitivity Labels

- Public
- General
- Confidential
- ...

>>> Extendable via SDK to 3<sup>rd</sup> party tools

## Advanced compliance solutions



eDiscovery  
(Premium)



Insider Risk Management



Communication Compliance



Microsoft Priva

# 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.

Public	General	Confidential	Restricted
 <b>Content labels</b> 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	 <b>Container labels</b> 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, prevent label downgrades

# Default sensitivity labels



Secure SharePoint and OneDrive document libraries with default sensitivity labels (Office files and PDFs)



Classify and protect Document Libraries, within a site, with labels-based policies

The screenshot shows a SharePoint document library interface for a site named "Financial Planning 2023". The top navigation bar includes "SharePoint", a search icon, and user account information. Below the navigation is a toolbar with "New", "Upload", and other actions. A filter bar shows "All Documents\*" and various filters. The main area displays two documents: "New Litware-Contoso Partnership.d..." and "Strategic Objectives.pptx", both listed as "Confidential". A sidebar on the right shows a "Sensitivity" dropdown menu with "Confidential" selected. Several UI elements are highlighted with blue boxes: the "General" share permission button, the "Confidential" label in the toolbar, the "Confidential" label in the document list, and the "Sensitivity" dropdown menu.

Name	Modified	Sensitivity
New Litware-Contoso Partnership.d...	About a minute ago	Confidential
Strategic Objectives.pptx	About a minute ago	Confidential

# Copilot conversation inherits the sensitivity label of referenced files

Conversations **inherit the most restrictive sensitivity labels** from the references used to formulate a response.

The screenshot shows the Microsoft 365 Copilot interface. At the top, there's a purple banner with the text "Data protection stakeholders define a set of labels. Users see and apply these labels." and a circular icon with a person icon labeled "Who". Below the banner is the Microsoft 365 navigation bar with icons for Home, Create, My Content, Feed, Apps, M365 Chat, Outlook, Teams, Word, Excel, and PowerPoint. The main area displays a conversation about Microsoft Partners in FY24. The user asks, "Who are the Microsoft Partners in FY24?". The AI response includes a note about work content and chats being protected within the organization. It then lists three references:

- FY22 Field Execution Guide**: Confidential\Any User (No Protection). Last modified on 10/09/23.
- FY24 Partner Activation Seller Toolkit**: Confidential\Microsoft FTE. Last modified on 11/16/23.
- To-Partner\_FY24 Kick Off GSI Pilot Partner Cybersecurity Investment -Final-10-10-202...**: General. Last edited on 10/10/23 by Uriel Rootshtain; Paul Simpson.

A callout bubble from the AI response states: "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 generated content inherits the sensitivity label of referenced files

Generated contents **inherit the sensitivity label** from the source documents.

The screenshot shows a Microsoft Word document titled "AI hub A platform for data security and compliance for AI". The document contains the following text:

AI hub: A new platform for data security and compliance for AI

A brief overview of the new features and benefits of AI hub

**Introduction**

AI is transforming the way organizations operate, innovate, and compete. However, AI also brings new challenges and risks for data security and compliance, especially in the context of data privacy regulations and ethical standards. How can organizations ensure that their data and AI activities are secure, compliant, and trustworthy?

AI hub is a new platform that helps organizations manage, monitor, and secure their AI activities. AI hub provides a comprehensive solution for data discovery and classification, AI activity tracking and auditing, data protection and encryption, and compliance and governance policies. AI hub enables organizations to drive data security and compliance controls for AI, and to gain visibility and insights into their AI activities.

**Key features of AI hub**

AI hub offers a range of features that help organizations address the challenges and risks of AI, such as data breaches and leaks, unauthorized access and misuse, non-compliance and fines, reputational damage and loss of trust. Some of the key features of AI hub are:

- Data discovery and classification: AI hub automatically scans and identifies the data sources and types that are used for AI, and assigns them a classification level

At the bottom of the screen, there is a blue bar with the text "Keep it" and a "For example, 'Make it more engaging'" button.

Top right corner: Who (purple icon) and a purple box containing text about data protection stakeholders and labels.

Bottom right corner: Give Feedback to Microsoft

# Label your emails and documents with OOTB sensitivity labels

Utilizing AI hub we can quickly confirm default sensitivity labels

The screenshot shows the Microsoft Purview AI Hub (preview) interface. The left sidebar includes Home, AI Hub (preview), Analytics, Policies (selected), Learn, Activity explorer, and Settings. The main content area has a search bar and a toggle for the New Microsoft Purview portal. A central section titled "AI Hub policies use Microsoft Purview solutions to discover policies" contains a "Recommendations" card for "Data security". The card features a "Fortify your data security for AI" heading, a list of two bullet points about adaptive protection and data leakage prevention, and a "Get started" button. To the right, there are sections for "Data security for AI" (with a note about managing risks), "Policy to be created" (adaptive protection for AI apps), "Labels exist" (information protection policy for sensitivity labels), and "What to expect" (a list of six bullet points about policy behavior). A "Create policies" button is at the bottom.

Microsoft Purview

Search

New Microsoft Purview portal

AI Hub (preview)

Policies

Analytics

Learn

Policies

Activity explorer

AI Hub (preview)

Information protection

Audit

AI Hub policies use Microsoft Purview solutions to discover policies

Recommendations

Data security

Fortify your data security for AI

- Keep your sensitive data protected with Adaptive Protection.
- Prevent data leakages in other generative AI apps.

Get started

Data security for AI

Adaptive protection to block sensitive information pasted or uploaded to 3P AI apps

Data loss prevention policy: Microsoft AI hub - Adaptive Protection in AI assistants

Uses Adaptive Protection to give a warn-with-override to elevated risk users attempting to paste or upload sensitive information to other AI assistants in Edge, Chrome, and Firefox. This policy covers all users and groups in your org in test mode.

Policy to be created

Labels exist

Information protection policy for sensitivity labels

Information Protection

Sets up default sensitivity labels to preserve document access rights and protect Copilot output. Users can choose to label items in Outlook, Word, Excel, PowerPoint, and other locations.

What to expect

- Adaptive Protection must be enabled for the policies to work correctly.
- If an Adaptive Protection policy is not already created to adjust policy behavior based on user risk, then a default Adaptive Protection policy will be created.
- If an Adaptive Protection policy has already been created, then it will remain the same.
- If sensitivity label policy has already been created, then it will remain the same.
- DLP rule matches will be shown within Activity Explorer.

Create policies

# Create DLP Policies

## Importance of Purview DLP Policies

**Data Loss Prevention (DLP) Policies** are essential for protecting sensitive information and ensuring compliance with regulatory requirements. They help organizations:

- **Prevent Data Leakage:** By monitoring and controlling the flow of sensitive data, DLP policies prevent unauthorized sharing and accidental data leaks.
- **Ensure Compliance:** DLP policies help organizations comply with industry regulations and standards by enforcing data protection rules.
- **Protect Intellectual Property:** By safeguarding sensitive information, DLP policies protect an organization's intellectual property and competitive advantage.
- **Enhance Security Posture:** Implementing DLP policies strengthens an organization's overall security posture by mitigating risks associated with data breaches.

## Policies

Use data loss prevention (DLP) policies to help identify and protect your organization's sensitive info. For example you can set up policies to help make sure information in email and docs isn't shared with the wrong people. [Learn more about DLP](#)

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

[View role groups](#)

[+ Create policy](#) [Export](#) [Refresh](#)

5 items

[Search](#)

[Customize columns](#)

Search

Work Web

New chat

...

AV

Copilot Summarize https://fabrikampur...

November 11, 2024 at 10:10 PM

Summarize [Project Obsidian M&A.docx](#)

The document titled [Project Obsidian M&A](#) is authored by you and was last modified this afternoon [1](#). Unfortunately, I can't provide more detailed information as the content is protected [1](#).

Is there anything specific you would like to know or any other document you need help with?

[Project Obsidian M&A](#)  
SharePoint: ObsidianMerger > Shared Documents  
Adele Vance modified 9 hours ago

Ask

1 [Project Obsidian M&A](#)

[Edit in Pages](#) [Copy](#)

1 of 30 responses AI-generated content may be incorrect

Can you list the sections or headings in the document? Can you provide a summary of the document's purpose?

Is there a way to access the content of the document? [View prompts](#)

Message Copilot

Add people, files, and more for better results

0 / 16000

@ [Edit](#) [File](#) [Send](#)

Copilot Visual Creator

Get Copilot agents

Chats Show more

Summarize https://fabri... 10:10 PM

Summarize Project Obsidi... 10:09 PM

give me examples of work ... 7:17 PM

Project obsidian 11/7

Can you summarize https://fa... 11/7

SearchWorkWebNew chat...BB

**Copilot**  
Tell me the key points from ht...

November 11, 2024 at 10:04 PM

Tell me the key points from [Project Obsidian M&A.docx](#)

Sure, here are the key points from the document Project Obsidian M&A:

**Executive Summary:** Project Obsidian is a strategic merger between Company A and Company B aimed at creating a more competitive and innovative entity in the market. The merger will combine the strengths of both companies to enhance market share, improve operational efficiencies, and drive long-term growth [①](#).

**Objectives:**

- **Market Expansion:** Leverage the combined market presence to enter new markets and increase market share.
- **Operational Efficiency:** Streamline operations by integrating processes, reducing redundancies, and optimizing resources.
- **Innovation:** Foster a culture of innovation by combining the R&D capabilities of both companies to develop new products and services.
- **Financial Performance:** Improve financial performance through cost synergies, increased revenue, and enhanced profitability [①](#).

**Key Terms:**

- **Transaction Structure:** The merger will be executed as a stock-for-stock transaction, with shareholders of Company A receiving shares of Company B.
- **Valuation:** The combined entity will be valued at \$22 billion, with Company A valued at \$15 billion and

Can you provide more details on the financial projections? What are the specific cost synergies expected?

How will the cultural integration be managed? [View prompts](#)

Message Copilot  
Add people, files, and more for better results  
0 / 16000

@   

**Copilot**  
Visual Creator  
Get Copilot agents

Chats

Tell me the key points fr... 10:04 PM

Tell me about project obsidian 11/8

What is this https://fabrikamp... 11/6

The screenshot shows the Microsoft Copilot interface within a workspace environment. The left sidebar contains icons for Home, Copilot, Create, OneDrive, Feed, Pages, and Apps. The main area features a Copilot card with a message about project Obsidian M&A, a preview of a SharePoint document titled 'Obsidian Merger' with a 'Label to protect top secret project Obsidian Merger' note, and options to 'Edit in Pages' or 'Copy'. Below this is a message input field with placeholder text 'Message Copilot' and a button to 'Add people, files, and more for better results'. The top navigation bar includes a search bar, tabs for 'Work' and 'Web', and buttons for 'New chat', '... (ellipsis)', and 'Copilot' (circled in blue). The right sidebar displays a list of chats, including a recent message from Copilot and Visual Creator, and links to 'Get Copilot agents' and 'Chats'.

**Copilot**  
Tell me the key points from ht...

company culture.

- **Operational Disruptions:** Minimize disruptions by developing a detailed integration plan and closely monitoring progress.
- **Regulatory Approval:** Ensure compliance with regulatory requirements and obtain necessary approvals in a timely manner.
- **Customer Retention:** Retain key customers by maintaining high service levels and communicating the benefits of the merger ①.

**Conclusion:** Project Obsidian represents a significant opportunity for both Company A and Company B to create a stronger, more competitive entity. By leveraging the strengths of both companies, the merger will drive growth, innovation, and value creation for shareholders, employees, and customers ①.

If you need more details or have any specific questions, feel free to ask!

**Project Obsidian M&A**  
SharePoint: ObsidianMerger > Shared Documents  
Adele Vance modified 9 hours ago

**Obsidian Merger**  
Label to protect top secret project Obsidian Merger

1 Project Obsidian M&A

Edit in Pages Copy 1 of 30 responses AI-generated content may be incorrect

Can you provide more details on the financial projections? What are the specific cost synergies expected?

How will the cultural integration be managed? View prompts

Message Copilot

Add people, files, and more for better results

0 / 16000

@ |

**Copilot**  
Visual Creator

Get Copilot agents

Chats

Tell me the key points fr... 10:04 PM

Tell me about project obsidian 11:8

What is this https://fabrikamp... 11:6

# Microsoft Purview across spectrum of AI apps



## M365 Copilot

Built on Microsoft's security, compliance, privacy, and responsible AI framework



## 3<sup>rd</sup> party Enterprise apps

Development can range in security and compliance standards

### Microsoft Security



Prepare



Discover



Protect



Govern

Microsoft Purview

https://purview.microsoft.com/fabrikam/en-us/

Microsoft Purview Preview

Search

Try the new Microsoft Purview

Home

Solutions

Learn

Settings

DSPM for AI

Overview

Recommendations

Reports

Policies

Activity explorer

Data assessments Preview

## Data Security Posture Management for AI

Discover and secure all AI activity in Microsoft Copilot and other AI apps. Keep your data safe and stay on track with industry regulations. Learn more about DSPM for AI

### Get started

<b>Activate Microsoft Purview Audit</b> Get insights into user interactions with Microsoft Copilot experiences.	Required	⌚ 7 Minutes
<b>Install Microsoft Purview browser extension</b> Detect risky user activity and get insights into user interactions with other AI apps.	Required	⌚ 1 Hour
<b>Onboard devices to Microsoft Purview</b> Protect sensitive data from leaking to other AI apps.	Required	⌚ 1 Hour
<b>Extend your insights for data discovery</b> Discover sensitive data in user interactions with other AI apps.	Required	⌚ 10 Minutes

### Recommendations

[View all recommendations →](#)

New AI regulations

#### Get guided assistance to AI regulations

Stay on track with newly established industry regulations for AI, such as ISO 42001 and NIST AI RMF. To ensure safe AI interactions, we've identified the key actions associated with these regulations.

[View details](#)

Interactions with sensitive data Last 30 days

**509**

[View details](#)

Data Security Investigations

#### Protect sensitive data referenced in Copilot responses

In the last 30 days, 0 unprotected files were referenced in Copilot responses. Start a data investigation or take steps to avoid potential oversharing of sensitive data.

Unlabeled files in Copilot responses Last 30 days

0

Unlabeled files

SharePoint Sites with unlabeled files

0

[View details](#)

### Reports

[View all reports →](#)

Microsoft Purview Preview

https://purview.microsoft.com/fabrikam/en-us/

Microsoft Purview Try the new Microsoft Purview

Search

Home Solutions Learn Settings DSPM for AI Overview Recommendations Reports Policies Activity explorer Data assessments

← Overview

## Reports

Microsoft Copilot experiences Enterprise AI apps Other AI apps

### Activity

Total interactions over time (Microsoft Copilot)

▲ Up 20% in the last 30 days

Date	Microsoft 365	Copilot Studio
09/01/2023	500	200
09/02/2023	1000	500
09/03/2023	1000	2000
09/04/2023	3000	2500
09/05/2023	3000	2500
09/06/2023	3500	2800

View details

Total interactions over time (enterprise AI apps)

▲ Up 14% in the last 30 days

Date	OpenAI ChatGPT Enterprise
10/01/2024	2800
10/02/2024	4200
10/03/2024	3800
10/04/2024	3800
10/05/2024	3800
10/06/2024	1800
10/07/2024	3800

View details

Total interactions over time (other AI apps)

▲ Up 14% in the last 30 days

Date	Yellow Line	Orange Line	Purple Line	Red Line
09/01/2023	1800	2800	1000	2000
09/02/2023	3000	3800	1000	3500
09/03/2023	2200	3500	1500	3500
09/04/2023	4200	3200	1000	3500
09/05/2023	4200	3200	1500	3200
09/06/2023	4500	2800	2000	1800

Total visits (other AI apps) ⓘ

▲ Up 14% in the last 30 days

Date	Visits
09/01/2023	1000
09/02/2023	1500
09/03/2023	1800
09/04/2023	1500
09/05/2023	1800
09/06/2023	2000
09/07/2023	2200
09/08/2023	2500

Microsoft Purview

https://purview.microsoft.com/fabrikam/en-us/

Microsoft Purview Preview

Search

Try the new Microsoft Purview

Activity explorer

Review AI activity including AI interactions (prompts and response), activity with sensitive info types, and more.

Filters: Timestamp: 10/16/2024-11/14/2024, Activity type: AI Interaction, AI app category: Microsoft Copilot Experiences, App: Any, App accessed in: Any, User: Any, User risk level: Any, Sensitive info type: Any

Resources accessed: Any, Sensitive files referenced: Any, Scope: Any, Reset all

The chart displays the number of AI interactions per day. The x-axis shows dates from 11/4/2024 to 11/14/2024. The y-axis ranges from 0 to 100. The data shows a peak on November 6th with approximately 75 interactions, followed by a high on November 7th with about 70 interactions, and smaller peaks on November 5th (~25), November 11th (~25), and November 12th (~20). Other days show very low activity.

AI Interaction

Export

248 items

Activity type	User	User risk level	Timestamp (UTC)	AI app category	App	App accessed in	Sensitive info type	Resources access...	Sensitive files ref...
AI Interaction	ericat@fabrikampurviewignite2024.o...		Nov 14, 2024 8:48 PM	Microsoft Copilot Experie...	Word		No	No	
AI Interaction	ericat@fabrikampurviewignite2024.o...		Nov 14, 2024 8:48 PM	Microsoft Copilot Experie...	Word		No	No	
AI Interaction	ericat@fabrikampurviewignite2024.o...		Nov 14, 2024 8:47 PM	Microsoft Copilot Experie...	Office		Yes	Yes	
AI Interaction	ericat@fabrikampurviewignite2024.o...		Nov 14, 2024 8:46 PM	Microsoft Copilot Experie...	Office		Yes	Yes	
AI Interaction	ericat@fabrikampurviewignite2024.o...		Nov 14, 2024 8:42 PM	Microsoft Copilot Experie...	Office		Yes	Yes	
AI Interaction	lisab@fabrikampurviewignite2024.o...		Nov 13, 2024 8:56 PM	Microsoft Copilot Experie...	Office		Yes	No	
AI Interaction	lisab@fabrikampurviewignite2024.o...		Nov 13, 2024 7:43 PM	Microsoft Copilot Experie...	Office		Yes	No	
AI Interaction	andrewm@fabrikampurviewignite20...	Medium	Nov 13, 2024 7:42 PM	Microsoft Copilot Experie...	Word		No	No	

Microsoft Purview

https://purview.microsoft.com/fabrikam/en-us/

Microsoft Purview Preview

Search

Try the new Microsoft Purview

AI Interaction

Record ID: a04bb747-25ae-47a1-8ad0-6e3d0cbe37f5

Client IP: 2600:8800:7089:f900:69bb:c58:2694:2f12

About this user

User: Erica T

View more user details in insider risk management

App details

AI app category: Microsoft Copilot Experiences

App accessed in: Word

Interaction details

You can view prompts and responses with your Microsoft Purview Content Explorer Content Viewer role. Learn more about permissions for DSPM for AI

Prompt: Project Obsidian M&A.docx [AutoGenerated]Summarize

Sensitive info types detected: View related classification activity

Response: Project Obsidian M&A.docx [AutoGenerated]Project Obsidian is a merger between Company A and Company B to create a more competitive and innovative market entity. The merger aims to combine strengths, enhance market share, improve

## Activity explorer

Review AI activity including AI interactions (prompts and response), activity with sensitive info types, and more.

Filters: Timestamp: 10/16/2024-11/14/2024, Activity type: AI Interaction, AI app category: Microsoft Copilot Experiences, App: Any, App accessed in: Any, User: Any

Resources accessed: Any, Sensitive files referenced: Any, Scope: Any, Reset all

AI Interaction

Export Selected Items

Activity type	User	User risk level	Timestamp (UTC)	AI app category	App
AI Interaction	ericat@fabrikampurviewignite2024.o...		Nov 14, 2024 8:48 PM	Microsoft Copilot Experie...	
AI Interaction	ericat@fabrikampurviewignite2024.o...		Nov 14, 2024 8:48 PM	Microsoft Copilot Experie...	
AI Interaction	ericat@fabrikampurviewignite2024.o...		Nov 14, 2024 8:47 PM	Microsoft Copilot Experie...	
AI Interaction	ericat@fabrikampurviewignite2024.o...		Nov 14, 2024 8:46 PM	Microsoft Copilot Experie...	
AI Interaction	ericat@fabrikampurviewignite2024.o...		Nov 14, 2024 8:42 PM	Microsoft Copilot Experie...	
AI Interaction	lisab@fabrikampurviewignite2024.o...		Nov 13, 2024 8:56 PM	Microsoft Copilot Experie...	
AI Interaction	lisab@fabrikampurviewignite2024.o...		Nov 13, 2024 7:43 PM	Microsoft Copilot Experie...	
AI Interaction	andrewm@fabrikampurviewignite2024.o...	Medium	Nov 13, 2024 7:42 PM	Microsoft Copilot Experie...	

11/7/2024      11/8/2024      11/11/2024  
Chart time zone: UTC

AI app category  
Microsoft Copilot Experiences  
App accessed in  
Word

## Interaction details

You can view prompts and responses with your Microsoft Purview Content Explorer Content Viewer role. [Learn more about permissions for DSPM for AI](#)

### Prompt

[Project Obsidian M&A.docx](#)  
[AutoGenerated]Summarize

Sensitive info types detected [View related classification activity](#)

### Response

[Project Obsidian M&A.docx](#)  
[AutoGenerated]Project Obsidian is a merger between Company A and Company B to create a more competitive and innovative market entity. The merger aims to combine strengths, enhance market share, improve efficiencies, and drive growth. \* \*\*\*Objectives of the Merger\*\*: The merger

Sensitive info types detected [View related classification activity](#)

Microsoft Purview

https://purview.microsoft.com/fabrikam/en-us/

Microsoft Purview Preview

Search

Try the new Microsoft Purview

Solutions

Home

DSPM for AI

Overview

Recommendations

Reports

Policies

Activity explorer

Data assessments

Activity explorer

Review AI activity including AI interactions (prompts and response), activity with sensitive info types, and more.

Filters: Timestamp: 10/16/2024-11/14/2024, Activity type: AI Interaction, AI app category: Microsoft Copilot Experiences, App: Any, App accessed in: Any, User: Any

Resources accessed: Any, Sensitive files referenced: Any, Scope: Any, Reset all

Activity details

Activity type: AI Interaction, Timestamp: Nov 14, 2024 8:48 PM, Sensitive info types: Microsoft Copilot Experiences

Record ID: 70ec5a71-89f3-4b83-8a2a-9781b89635bd

About this user

User: Erica T

View more user details in insider risk management

App details

AI app category: Microsoft Copilot Experiences, App accessed in: Word

Interaction details

Sensitive info types detected: ObsidianMerger\_Financial\_Data, Finance

## Activity explorer

AI Interaction

Date	AI Interaction Count
11/4/2024	~5
11/5/2024	~28
11/6/2024	~98
11/7/2024	~72
11/8/2024	~15
11/11/2024	~25

Chart time zone: UTC

Export Selected Items

Activity type	User	User risk level	Timestamp (UTC)	AI app category	App
AI Interaction	ericat@fabrikampurviewignite2024.o...	Medium	Nov 14, 2024 8:48 PM	Microsoft Copilot Experie...	Word
AI Interaction	ericat@fabrikampurviewignite2024.o...	Medium	Nov 14, 2024 8:48 PM	Microsoft Copilot Experie...	Word
AI Interaction	ericat@fabrikampurviewignite2024.o...	Medium	Nov 14, 2024 8:47 PM	Microsoft Copilot Experie...	Word
AI Interaction	ericat@fabrikampurviewignite2024.o...	Medium	Nov 14, 2024 8:46 PM	Microsoft Copilot Experie...	Word
AI Interaction	ericat@fabrikampurviewignite2024.o...	Medium	Nov 14, 2024 8:42 PM	Microsoft Copilot Experie...	Word
AI Interaction	lisab@fabrikampurviewignite2024.o...	Medium	Nov 13, 2024 8:56 PM	Microsoft Copilot Experie...	Word
AI Interaction	lisab@fabrikampurviewignite2024.o...	Medium	Nov 13, 2024 7:43 PM	Microsoft Copilot Experie...	Word
AI Interaction	andrewm@fabrikampurviewignite2024.o...	Medium	Nov 13, 2024 7:42 PM	Microsoft Copilot Experie...	Word



Home



DSPM for AI



Overview



Recommendations



Reports



Policies



Activity explorer



Data assessments

Preview

with these regulations.

[View details](#)

Data discovery

## Discover and govern interactions with ChatGPT Enterprise AI (preview)

Register ChatGPT Enterprise workspace to discover and govern interactions with ChatGPT Enterprise AI

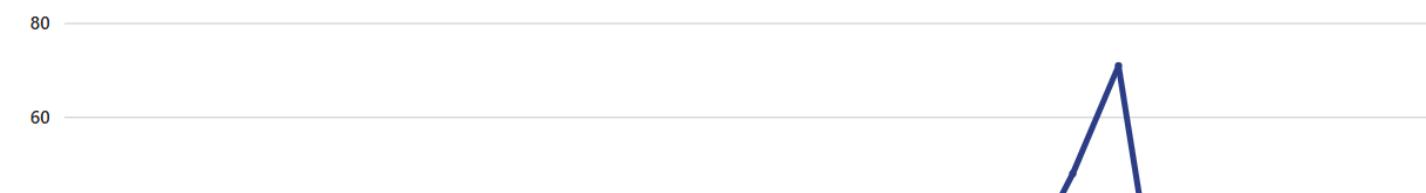
[View details](#)

## Reports

[View all reports →](#)

### Total interactions over time (Microsoft Copilot)

▲ 243 activities in the last 31 days



- Home
- Solutions
  - DSPM for AI
    - Overview
    - Recommendations
    - Reports
    - Policies
    - Activity explorer
    - Data assessments
- Learn
- Settings
- DSPM for AI

with these regulations.

[View details](#)[Data discovery](#)

## Discover and govern interactions with ChatGPT Enterprise AI (preview)

Register ChatGPT Enterprise workspace to discover and govern interactions with ChatGPT Enterprise AI

### Prerequisites:

- A Microsoft Azure account with an active subscription. Create an account for free.
- An active Microsoft Purview account.
- Make sure appropriate permissions are granted to access and use these features:
  - Permissions for users
  - Permissions for the non-Microsoft app

### Steps at a glance

- In Microsoft Azure, use Key Vault to manage credentials for third-party connectors:** Use Key Vault to create and manage the secret for the ChatGPT Enterprise Connector.
- In Microsoft Purview, configure the new connector using Data Map**
- Create and start a new scan:** Create a new scan, select credential, review, and run the scan.

### Useful resources

[Learn more about connectors](#)[Learn more about DSPM for AI](#)[Microsoft Purview compliance and data security for GenAI apps](#)

## Discover and govern interactions with ChatGPT Enterprise AI (preview)

Register ChatGPT Enterprise workspace to discover and govern interactions with ChatGPT Enterprise AI

[View details](#)

## Reports

### Total interactions over time (Microsoft Copilot)

▲ 243 activities in the last 31 days

80

60

[Mark as complete](#)

...

Export Selected Items

1 of 287 selected

<input type="checkbox"/>	Activity type	User	User risk level	Timestamp (UTC)	AI app category	App	App accessed in	Sensitive info types
<input type="checkbox"/>	AI Interaction	adelev@fabrikampurviewi...		Nov 12, 2024 11:57 PM	Enterprise AI App	ChatGPT Enterprise	ChatGPT Enterprise	
<input checked="" type="checkbox"/>	AI Interaction	adelev@fabrikampurviewi...		Nov 12, 2024 11:57 PM	Enterprise AI App	ChatGPT Enterprise	ChatGPT Enterprise	
<input type="checkbox"/>	AI Interaction	adelev@fabrikampurviewi...		Nov 12, 2024 11:57 PM	Enterprise AI App	ChatGPT Enterprise	ChatGPT Enterprise	
<input type="checkbox"/>	Sensitive info types	andrewm@fabrikampurvie...		Nov 12, 2024 11:43 PM	Microsoft Copilot...		Word	ObsidianMerge!
<input type="checkbox"/>	Sensitive info types	andrewm@fabrikampurvie...		Nov 12, 2024 11:43 PM	Microsoft Copilot...		Word	Obsidian... +1 m
<input type="checkbox"/>	Sensitive info types	andrewm@fabrikampurvie...		Nov 12, 2024 11:43 PM	Microsoft Copilot...		Word	ObsidianMerge!
<input type="checkbox"/>	Sensitive info types	andrewm@fabrikampurvie...		Nov 12, 2024 11:43 PM	Microsoft Copilot...		Word	Obsidian... +1 m
<input type="checkbox"/>	AI Interaction	andrewm@fabrikampurvie...	■■■ Medium	Nov 12, 2024 11:43 PM	Microsoft Copilot...		Word	
<input type="checkbox"/>	AI Interaction	andrewm@fabrikampurvie...	■■■ Medium	Nov 12, 2024 11:43 PM	Microsoft Copilot...		Word	
<input type="checkbox"/>	Sensitive info types	andrewm@fabrikampurvie...		Nov 12, 2024 10:14 PM	Microsoft Copilot...		BizChat	ObsidianMerge!
<input type="checkbox"/>	Sensitive info types	andrewm@fabrikampurvie...		Nov 12, 2024 10:14 PM	Microsoft Copilot...		BizChat	ObsidianMerge!
<input type="checkbox"/>	AI Interaction	andrewm@fabrikampurvie...	■■■ Medium	Nov 12, 2024 10:14 PM	Microsoft Copilot...		Office	
<input type="checkbox"/>	Sensitive info types	adelev@fabrikampurviewi...		Nov 12, 2024 10:14 PM	Microsoft Copilot...		BizChat	ObsidianMerge!
<input type="checkbox"/>	Sensitive info types	adelev@fabrikampurviewi...		Nov 12, 2024 10:14 PM	Microsoft Copilot...		BizChat	ObsidianMerge!
<input type="checkbox"/>	AI Interaction	adelev@fabrikampurviewi...	■■■ High	Nov 12, 2024 10:14 PM	Microsoft Copilot...		Office	
<input type="checkbox"/>	Sensitive info types	adelev@fabrikampurviewi...		Nov 12, 2024 10:13 PM	Microsoft Copilot...		BizChat	ObsidianMerge!

- Home
- Solutions
- Learn
- Settings
- DSPM for AI**
  - Overview
  - Recommendations
  - Reports
  - Policies
  - Activity explorer**
  - Data assessments

**Export Selected Items**

<input type="checkbox"/>	Activity type	User	User risk level	Timestamp
	AI Interaction	adelev@fabrikampurviewi...		Nov 12, 2024 11:57 PM
<input checked="" type="checkbox"/>	AI Interaction	adelev@fabrikampurviewi...		Nov 12, 2024 11:57 PM
	AI Interaction	adelev@fabrikampurviewi...		Nov 12, 2024 11:57 PM
	AI Interaction	adelev@fabrikampurviewi...		Nov 12, 2024 11:57 PM
	Sensitive info types	andrewm@fabrikampurvie...		Nov 12, 2024 11:57 PM
	Sensitive info types	andrewm@fabrikampurvie...		Nov 12, 2024 11:57 PM
	Sensitive info types	andrewm@fabrikampurvie...		Nov 12, 2024 11:57 PM
	Sensitive info types	andrewm@fabrikampurvie...		Nov 12, 2024 11:57 PM
	AI Interaction	andrewm@fabrikampurvie...	■■■ Medium	Nov 12, 2024 11:57 PM
	AI Interaction	andrewm@fabrikampurvie...	■■■ Medium	Nov 12, 2024 11:57 PM
	Sensitive info types	andrewm@fabrikampurvie...		Nov 12, 2024 11:57 PM
	Sensitive info types	andrewm@fabrikampurvie...		Nov 12, 2024 11:57 PM
	AI Interaction	andrewm@fabrikampurvie...	■■■ Medium	Nov 12, 2024 11:57 PM
	Sensitive info types	adelev@fabrikampurviewi...		Nov 12, 2024 11:57 PM
	Sensitive info types	adelev@fabrikampurviewi...		Nov 12, 2024 11:57 PM
	AI Interaction	adelev@fabrikampurviewi...	■■■ High	Nov 12, 2024 11:57 PM
	Sensitive info types	adelev@fabrikampurviewi...		Nov 12, 2024 11:57 PM

**AI Interaction**

**Some data may not be available.** Responses and any files referenced are not available for other AI apps.

**Activity details**

Activity type      Timestamp  
AI Interaction      Nov 12, 2024 11:57 PM

Record ID  
9a049117-5f4a-416f-bf46-70a1c1b44b97

**About this user**

User  
**A** Adele V

[View more user details in insider risk management](#)

**App details**

AI app category      App  
Enterprise AI App      ChatGPT Enterprise  
App accessed in  
ChatGPT Enterprise

- Home
- Solutions
- Learn
- Settings
- DSPM for AI
  - Overview
  - Recommendations
  - Reports
  - Policies
- Activity explorer
- Data assessments

Preview

## Export Selected Items

<input type="checkbox"/>	Activity type	User	User risk level	Timestamp
<input type="checkbox"/>	AI Interaction	andrewm@fabrikampurviewi...	Medium	Nov 12, 2023
<input type="checkbox"/>	AI Interaction	adelev@fabrikampurviewi...	Medium	Nov 12, 2023
<input checked="" type="checkbox"/>	AI Interaction	adelev@fabrikampurviewi...	Medium	Nov 12, 2023
<input type="checkbox"/>	Sensitive info types	andrewm@fabrikampurvie...	Medium	Nov 12, 2023
<input type="checkbox"/>	Sensitive info types	andrewm@fabrikampurvie...	Medium	Nov 12, 2023
<input type="checkbox"/>	Sensitive info types	andrewm@fabrikampurvie...	Medium	Nov 12, 2023
<input type="checkbox"/>	Sensitive info types	andrewm@fabrikampurvie...	Medium	Nov 12, 2023
<input type="checkbox"/>	AI Interaction	andrewm@fabrikampurvie...	Medium	Nov 12, 2023
<input type="checkbox"/>	AI Interaction	andrewm@fabrikampurvie...	Medium	Nov 12, 2023
<input type="checkbox"/>	Sensitive info types	andrewm@fabrikampurvie...	Medium	Nov 12, 2023
<input type="checkbox"/>	Sensitive info types	andrewm@fabrikampurvie...	Medium	Nov 12, 2023
<input type="checkbox"/>	AI Interaction	andrewm@fabrikampurvie...	Medium	Nov 12, 2023
<input type="checkbox"/>	Sensitive info types	adelev@fabrikampurviewi...	Medium	Nov 12, 2023
<input type="checkbox"/>	Sensitive info types	adelev@fabrikampurviewi...	Medium	Nov 12, 2023
<input type="checkbox"/>	AI Interaction	adelev@fabrikampurviewi...	High	Nov 12, 2023
<input type="checkbox"/>	Sensitive info types	adelev@fabrikampurviewi...	Medium	Nov 12, 2023

## AI Interaction

## About this user

## User

 Adele V[View more user details in insider risk management](#)

## App details

## AI app category

Enterprise AI App

## App

ChatGPT Enterprise

## App accessed in

ChatGPT Enterprise

## Interaction details

 You can view prompts and responses with your Microsoft Purview Content Explorer Content Viewer role. [Learn more about permissions for DSPM for AI](#)

## Prompt

Valuation: The combined entity will be valued at \$23 billion, with Company A valued at \$Y billion and Company B valued at \$92 billion.

# Data assessments





Home



Solutions



Learn



Settings



(preview)



## DSPM for AI (preview)

[Overview](#)[Recommendations](#)[Reports](#)[Policies](#)[Activity explorer](#)[Data assessments \(preview\)](#)

# Data assessments (preview)

## Identify oversharing risks

Use data assessments to identify potential oversharing risks in your organization. They also provide fixes to limit access to sensitive data.

## Assess and prevent oversharing

### ① Create an assessment

Choose the sources and users you want to assess.

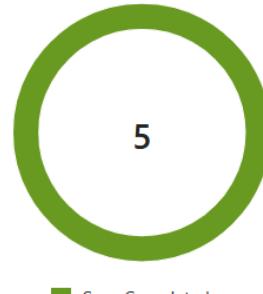
### ② Evaluate data

Review the assessment for potential oversharing risks within the sources and users.

### ③ Apply remediations

Limit Microsoft Copilot access to sensitive data, apply label and retention policies to sites and data. Conduct site and access review to evaluate site permissions and user access.

## Assessment status



Scan Completed

+ Create assessment

## Oversharing Assessment for the week of November 4, 2024

Default data assessments scans the top 100 sites in your organization

### Sensitivity labels on data of top 100 sites

Labeled



Not labeled



No Sensitive Information Types Detected 2 more

5 items Group

### Assessment name

Status

Scan started

### Default assessments (1)

Oversharing Assessment for the week of November 4, 2024

Scan completed

Nov 8, 2024 1

### Custom assessments (4)

Oversharing Assessment for Nov 4, 2024

Scan completed

Nov 6, 2024 1

Oversharing Assessment for Obsidian Merger

Scan completed

Nov 6, 2024 8

- Home
- Solutions
- Learn
- Settings
- AI Hub (preview)
- DSPM for AI (preview)
- Overview
- Recommendations
- Reports
- Policies
- Activity explorer
- Data assessments (preview)

Data assessments (preview) > Oversharing Assessment for the week of November 4, 2024

## Oversharing Assessment for the week of November 4, 2024

### Assessment info

Description  
Default assessment created by Purview

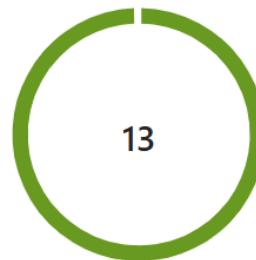
Total items

13

Sources included

7

### Total items



Scanned For Sensitive Info Types

Not Scanned

### Sensitivity labels on data

Labeled



Not labeled



● No Sensitive Information Types Detected

● Sensitive Information Types Detected

● Data Not Scanned

### Data with sharing links

Shared with anyone

0

Shared organization wide



Shared with specific people



Shared externally



● SharePoint

Data source ID	Source type	Total items ↓	Total items accessed	Times users accessed	Unique users accessed	Total sensitive items	Total scanned items
/sites/obsidianmerger/	SharePoint	8	Coming soon	Coming soon	Coming soon	7	8
/sites/marketanalysis/	SharePoint	2	Coming soon	Coming soon	Coming soon	0	2
/sites/projectblue/	SharePoint	1	Coming soon	Coming soon	Coming soon	0	1

- Home
- Solutions
- Learn
- Settings
- AI Hub (preview)
- DSPM for AI (preview)
- Overview
- Recommendations
- Reports
- Policies
- Activity explorer
- Data assessments (preview)

Data assessments (preview) > Oversharing Assessment for the week of November 4, 2023

## Oversharing Assessment for the week of November 4, 2023

### Assessment info

Description  
Default assessment created by Purview

Total items  
13

Sources included  
7

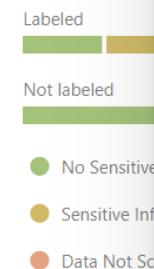
### Total items



Scanned For Sensitive Info Types

Not Scanned

### Sensitivity labels



/sites/obsidianmerger/

Overview Protect Monitor

### Limit Microsoft 365 Copilot access to this site

Choose how you would like Copilot to access data in this SharePoint site.

#### Restrict access by label

Microsoft Purview Data Loss Prevention

#### Restrict all items

SharePoint Restricted Content Discovery

Use a Microsoft Purview Data Loss Prevention policy to limit access to any files in your organization with sensitivity labels.

### Steps at a glance

1. Go to the [Data Loss Prevention in Microsoft Purview portal](#)
2. [Create new policy](#). Select "Policies" to create a new policy
3. [Choose a custom policy](#). Select Custom policy in the Custom category
4. [Customize your policy](#). Name your policy, and then select "Microsoft 365 Copilot" in the location
5. [Create a new advanced DLP rule](#).
6. [Add labels you want to exclude](#). In the fields for the new rule, select "Content contains sensitivity labels" and add the labels
7. [Select an action](#). Choose "Exclude Copilot from processing"
8. [Save the rule and the policy](#).

### Other labeling policies

#### Default sensitivity label for SharePoint document library

When a default sensitivity label is added to a SharePoint document library, the label will only apply to new items added to the site. Navigate to library settings on the SharePoint site and select a sensitivity label.



Create default sensitivity label for SharePoint document library

- Home
- Solutions
- Learn
- Settings
- AI Hub (preview)
- DSPM for AI (preview)
  - Overview
  - Recommendations
  - Reports
  - Policies
  - Activity explorer
- Data assessments (preview)

Data assessments (preview) > Oversharing Assessment for the week of November 4, 2023

## Oversharing Assessment for the week of November 4, 2023

### Assessment info

Description  
Default assessment created by Purview

Total items  
13

Sources included  
7

### Total items



Scanned For Sensitive Info Types:

Not Scanned

### Sensitivity label



## /sites/obsidianmerger/

### Other labeling policies

#### Default sensitivity label for SharePoint document library

When a default sensitivity label is added to a SharePoint document library, the label will only apply to new items added to the site. Navigate to library settings on the SharePoint site and select a sensitivity label.



Create default sensitivity label for SharePoint document library  
Microsoft SharePoint location

#### Default labels

Label all new items by default using sensitivity labels. Labels can have no protection or protection defined by the admin.



Create default sensitivity label  
Microsoft Purview Information Protection

#### Sensitive information auto-labeling policy

Use auto-labeling policies based on sensitive content or keywords.

Files with sensitive info types

7

[View items](#)



Create auto-labeling policy for sensitive information  
Microsoft Purview Information Protection

#### SharePoint site sensitivity label

Apply a sensitivity container label at the site level. Warning: this label will only apply to the site and not the contents of the site, including all files on the site. To protect the files on the site, add sensitivity labels to the files.



Edit SharePoint site sensitivity container label

Data source ID	Source type	Total items	Last updated
/sites/obsidianmerger/	SharePoint	8	Nov 4, 2023
/sites/marketanalysis/	SharePoint	2	Nov 4, 2023
/sites/orojectblue/	SharePoint	1	Nov 4, 2023

- Home
- Solutions
- Learn
- Settings
- AI Hub (preview)
- DSPM for AI (preview)
- Overview
- Recommendations
- Reports
- Policies
- Activity explorer
- Data assessments (preview)

Data assessments (preview) > Oversharing Assessment for the week of November 4, 2023

## Oversharing Assessment for the week of November 4, 2023

### Assessment info

Description  
Default assessment created by Purview

Total items  
13

Sources included  
7

### Total items



### Sensitivity label

Labeled

Not labeled

- No Sensitive
- Sensitive Info
- Data Not Scan

Data source ID	Source type	Total items	Items older than 3 years
/sites/obsidianmerger/	SharePoint	8	0
/sites/marketanalysis/	SharePoint	2	0
/sites/projectblue/	SharePoint	1	0

/sites/obsidianmerger/



Create default sensitivity label  
Microsoft Purview Information Protection

### Sensitive information auto-labeling policy

Use auto-labeling policies based on sensitive content or keywords.

Files with sensitive info types

7

View items



Create auto-labeling policy for sensitive information  
Microsoft Purview Information Protection

### SharePoint site sensitivity label

Apply a sensitivity container label at the site level. Warning: this label will only apply to the site and not the contents of the site, including all files on the site. To protect the files on the site, add sensitivity labels to the files.



Edit SharePoint site sensitivity container label  
Microsoft SharePoint location

### Review unused files

Protect sensitive data from oversharing with retention policies.

Items older than 3 years

0

View items



Create retention policies  
Microsoft Purview Data Lifecycle Management

- Home
- Solutions
- Learn
- Settings
- AI Hub (preview)
- DSPM for AI (preview)
- Overview
- Recommendations
- Reports
- Policies
- Activity explorer
- Data assessments (preview)

Data assessments (preview) > Oversharing Assessment for the week of November 4, 2023

## Oversharing Assessment for the week of November 4, 2023

### Assessment info

Description  
Default assessment created by Purview

Total items  
13

Sources included  
7

### Total items



### Sensitivity label



Data source ID	Source type	Total items ↓
/sites/obsidianmerger/	SharePoint	8
/sites/marketanalysis/	SharePoint	2
/sites/projectblue/	SharePoint	1

/sites/obsidianmerger/

Overview Protect Monitor

### Limit Microsoft 365 Copilot access to this site

Choose how you would like Copilot to access data in this SharePoint site.

#### Restrict access by label

Microsoft Purview Data Loss Prevention

#### Restrict all items

SharePoint Restricted Content Discovery

SharePoint Administrators or Global Administrators can enable Restricted Content Discoverability in SharePoint Online in your organization.

### Steps at a glance

- Download and install SharePoint Online Management Shell. Download the latest version of [SharePoint Online Management Shell](#)
- Connect to SharePoint Online as a Global Administrator or SharePoint Administrator in Microsoft 365. To learn how, see [Getting started with SharePoint Online Management Shell](#)
- Apply Restricted Content Discoverability on a SharePoint site. Run the following command in SharePoint Online Management Shell:

```
Set-SPOSite -identity <site-url>
-RestrictContentOrgWideSearch $true
```

- View the Restricted Content Discoverability configuration for a given site. Run the following command in SharePoint Online Management Shell:

```
Get-SPOSite -identity <site-url> | Select
RestrictContentOrgWideSearch
```

### Other labeling policies

#### Default sensitivity label for SharePoint document library

When a default sensitivity label is added to a SharePoint document library, the label

- Home
- Solutions
- Learn
- Settings
- AI Hub (preview)
- DSPM for AI (preview)
- Overview
- Recommendations
- Reports
- Policies
- Activity explorer
- Data assessments (preview)

Data assessments (preview) > Oversharing Assessment for the week of November 4, 2023

## Oversharing Assessment for the week of November 4, 2023

### Assessment info

Description  
Default assessment created by Purview

Total items  
13

Sources included  
7

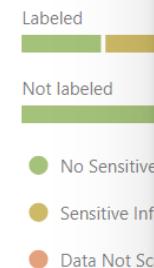
### Total items



Scanned For Sensitive Info Types:

Not Scanned

### Sensitivity label



/sites/obsidianmerger/

Overview Protect Monitor

### Run a site access review

SharePoint site access review lets IT administrators delegate the process of reviewing data access to site owners of overshared sites.

Shared with anyone

0

[View items](#)

Shared organization wide

0

[View items](#)

Shared with specific people

2

[View items](#)

Shared externally

1

[View items](#)

 [Start a SharePoint site access review](#)

SharePoint Admin Portal

### Run an identity access review

Manage group memberships, access to enterprise applications, and role assignments. User access can be reviewed regularly to make sure only the right people have continued access.

 [Run a Microsoft Entra ID user access review](#)

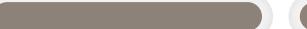
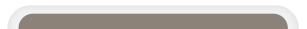
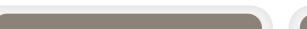
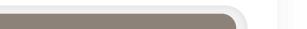
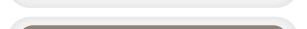
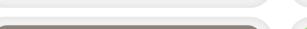
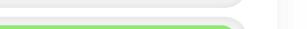
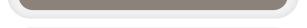
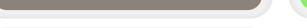
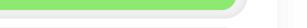
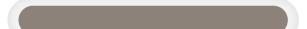
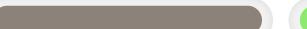
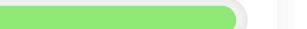
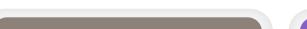
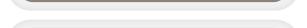
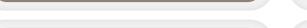
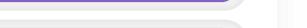
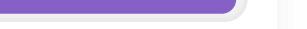
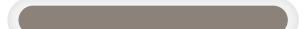
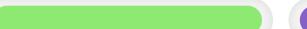
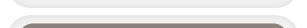
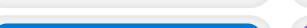
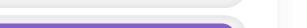
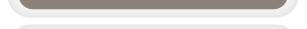
Microsoft Entra

Data source ID	Source type	Total items	...
/sites/obsidianmerger/	SharePoint	8	...
/sites/marketanalysis/	SharePoint	2	...
/sites/projectblue/	SharePoint	1	...

# What we heard after 50+ customer engagements....

- Users worried the privacy
- Admins worried the access control
- Management wants to push AI

# Shared responsibility model for AI

	IaaS (BYO model)	PaaS (Azure AI)	SaaS (Copilot)
<b>AI usage</b> 	User training and accountability Usage policy, admin controls Identity, device, and access management Data security and governance	           	
<b>AI application</b> 	AI plugins and data connections Application design and implementation Application infrastructure Application safety systems	           	
<b>AI platform</b> 	Model safety and security systems Model accountability Model tuning Model design and implementation Model training data governance AI compute infrastructure	              	

Microsoft

Model dependent

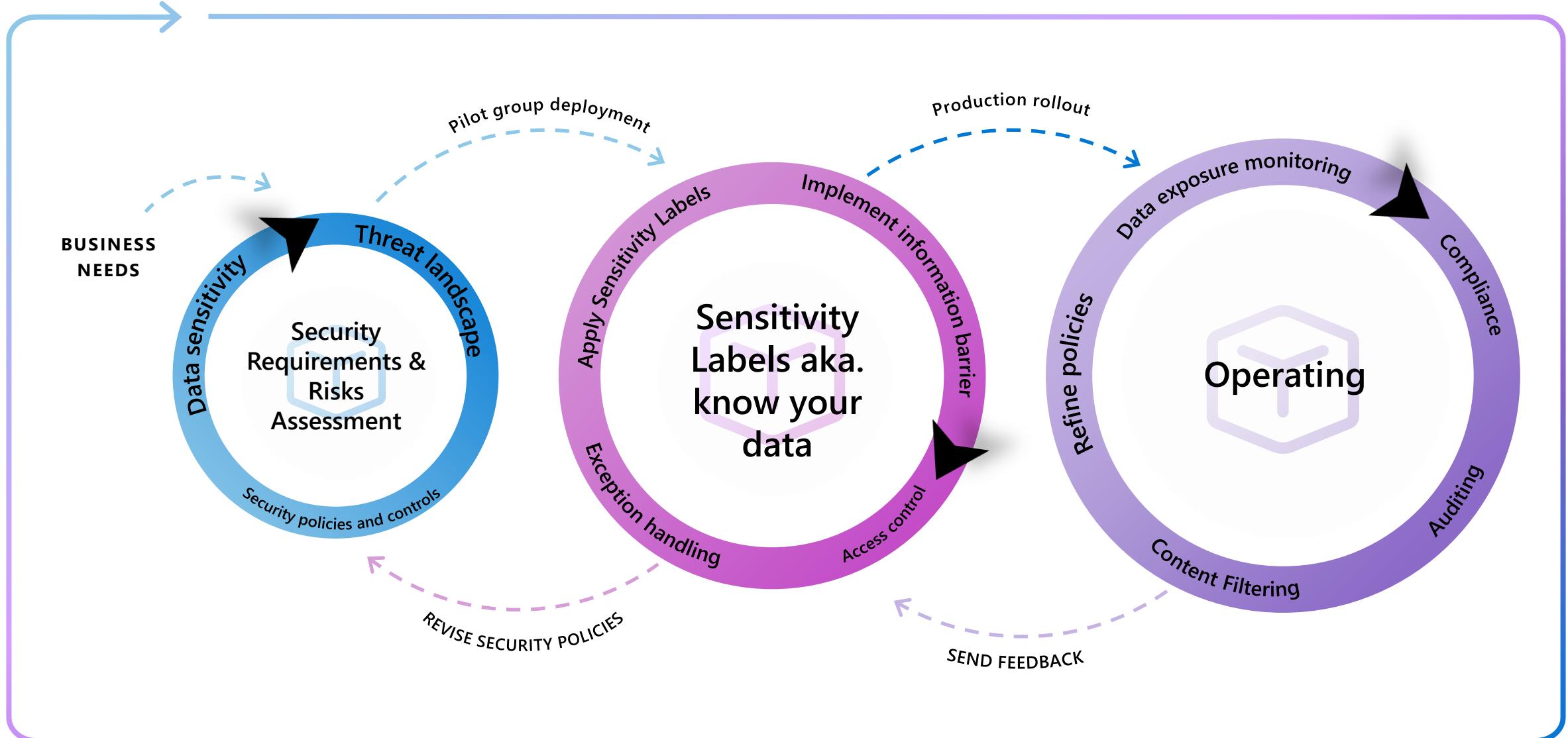
Shared

Customer

# Shared responsibilities of security for AI usage for Microsoft Copilot



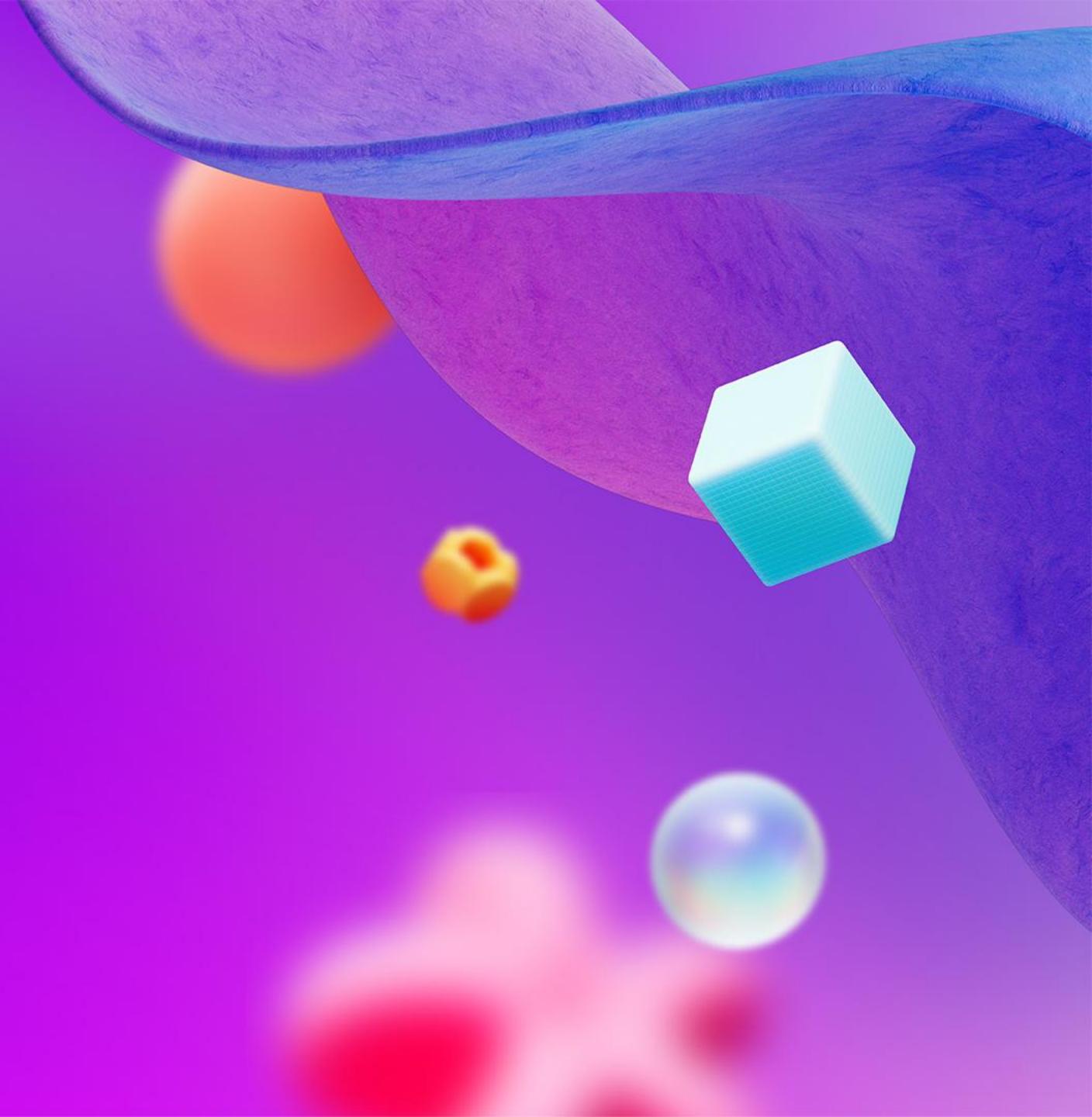
# Securing Copilot, or AI, is a continuous journey



# Demo: Labeling and Classification



# Demo: Auditing and Compliance



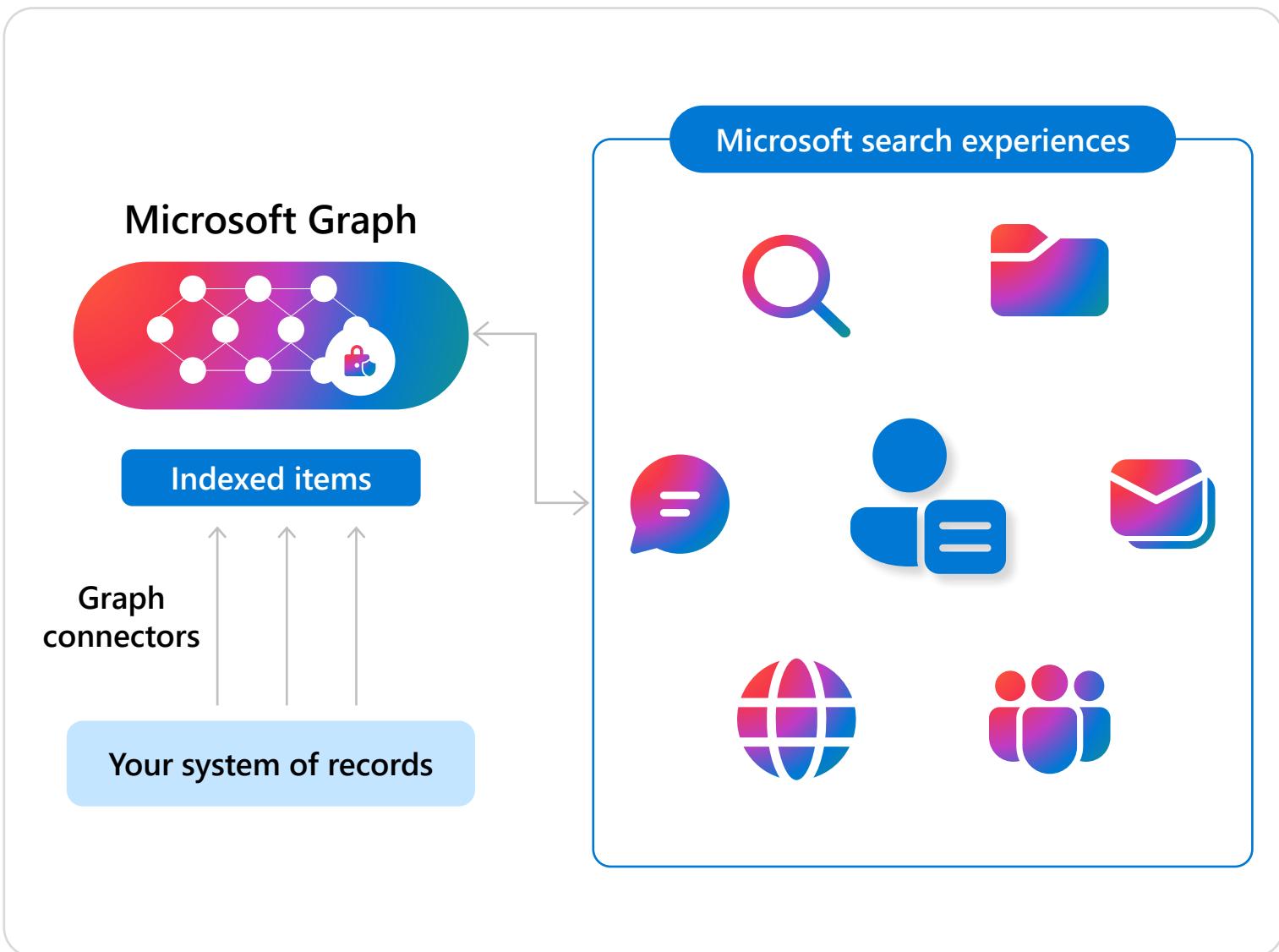
# Unite siloed data through Graph connectors

## Integrate unstructured data

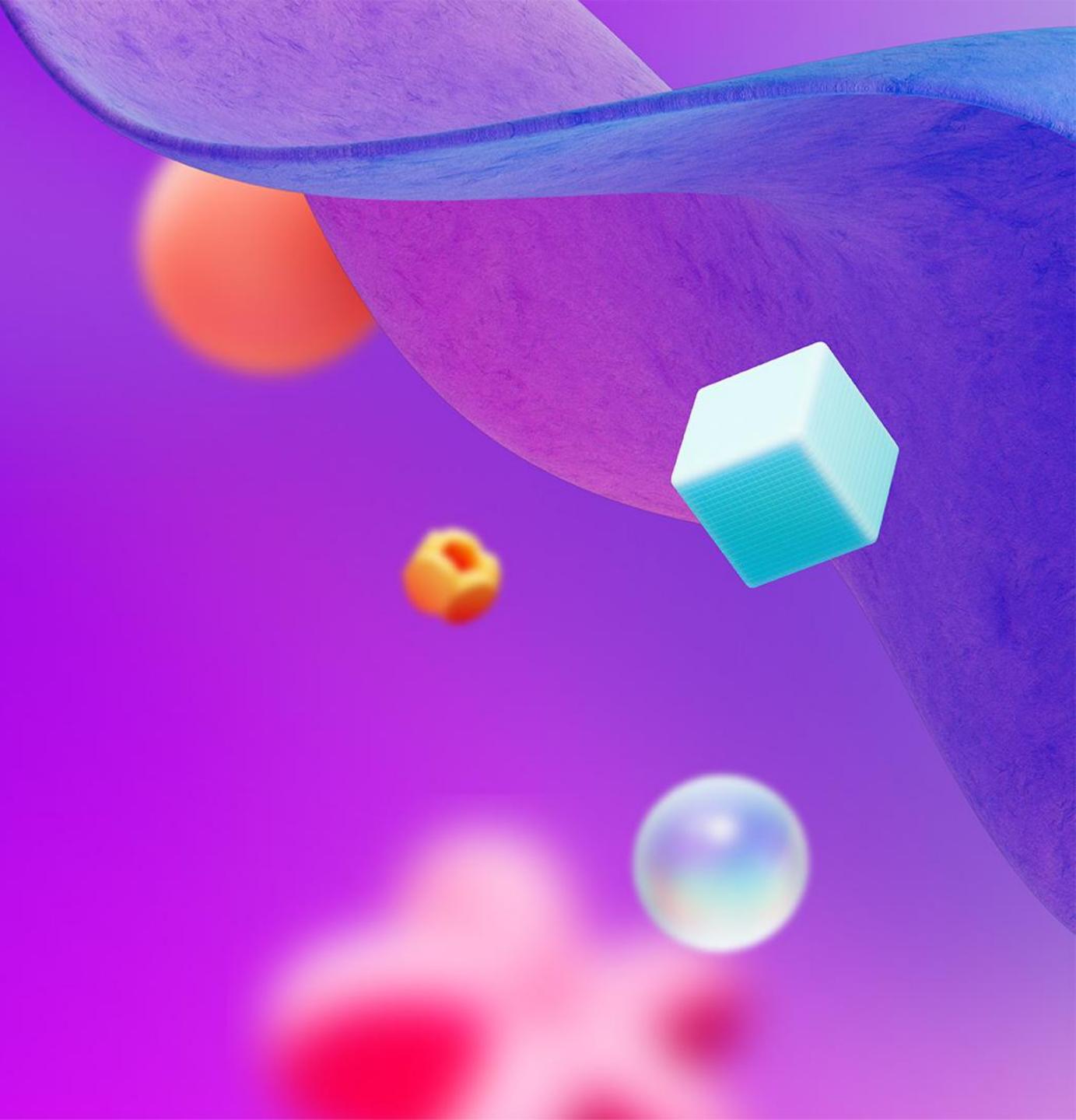
Ingest a variety of types of data from third-party services, on-premises data, any cloud, Microsoft apps, customer data, and more.

## Unify data across your organization

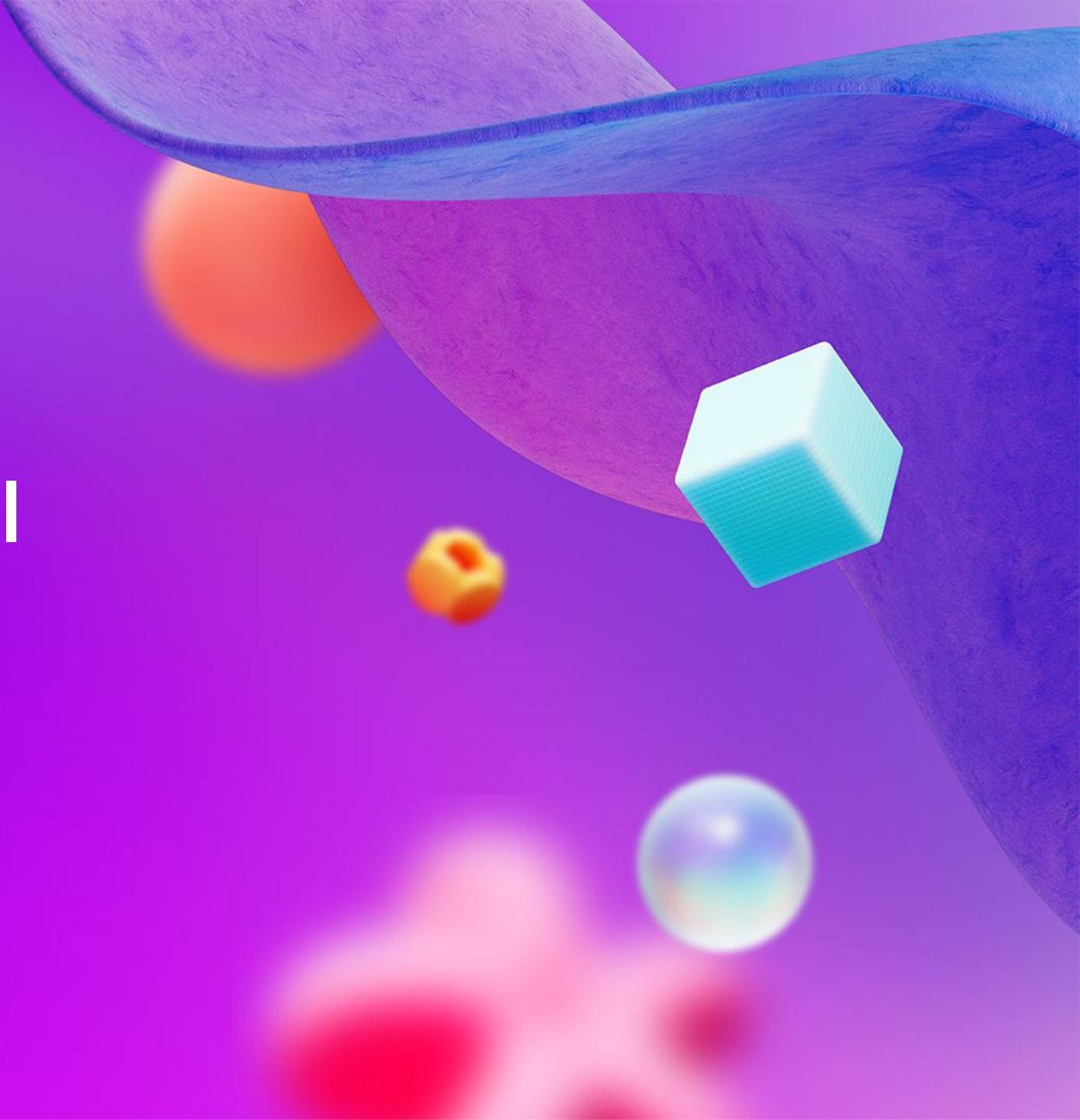
Ensure your data is accessible and usable wherever you need it across any Microsoft experience.



# Demo: On-Premises Connector



# Demo: 3<sup>rd</sup> Party AI tool discovery



# Get in touch.

+852 2751 2800

[info.hk@softwareone.com](mailto:info.hk@softwareone.com)

Unit 1203, NEO, 123 Hoi Bun Road, Kwun Tong  
Kowloon, Hong Kong

