Microsoft Copilot for Admins:

https://admin.cloud.microsoft/

Ondrej Vysek

Unlocking Infinite Possibilities Through Technology | SoftwareOne | Microsoft MVP

The Risks We Don’t Fully Understand Yet

What is Microsoft 365 Copilot

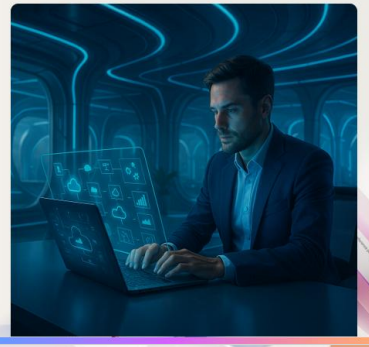
Copilot Control System (CCS)

Microsoft 365 Copilot MAC walkthrough

Data Discovery Configuration

Security Best Practices

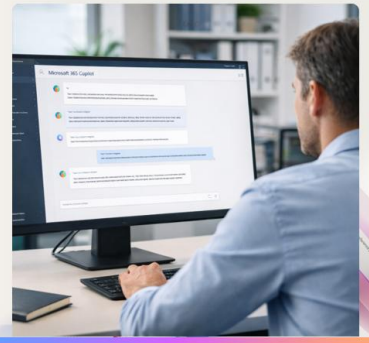
Copilot Data Privacy and Security



Reporting & Monitoring

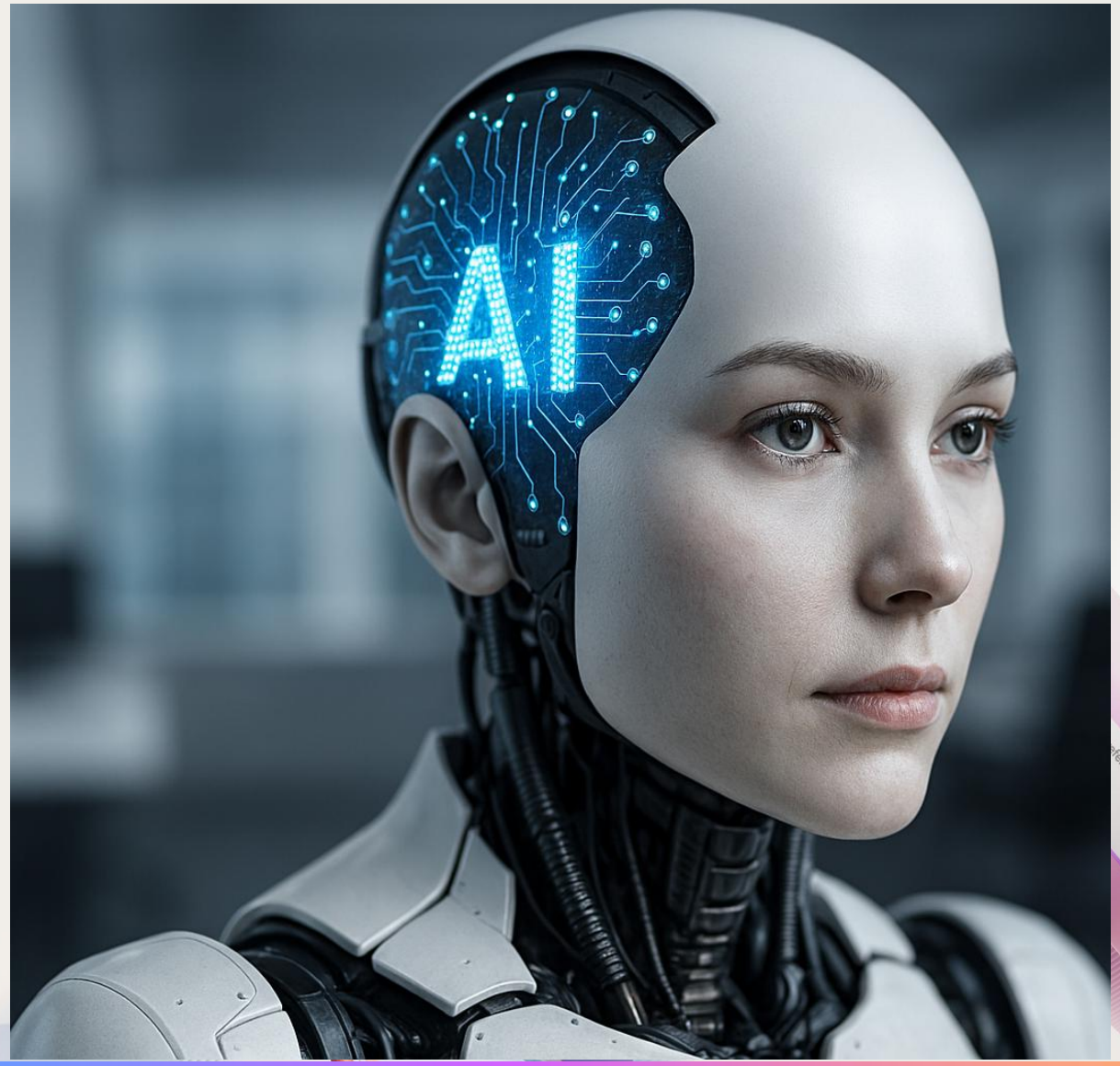
Microsoft 365 Copilot for admin center

Copilot in Microsoft 365 Admin Centers



M365 Copilot Agents

What is Microsoft 365 Copilot



Microsoft 365 Copilot

Copilot Chat

- Secure AI chat and agents with web access
- AI-powered creation (standard access)
- Ability to work with open files in Microsoft 365 apps

- Custom agents based on your data, pay-as-you-go
- Standard access to GPT-5

+

Microsoft 365 Copilot license

- AI chat s Work IQ
- Search with AI
- AI Notebooks
- AI-powered creation (priority access)
- GPT-5 Priority Access
- **Copilot in Microsoft 365 apps**
  Enhanced capabilities and editing directly in the app

- Comprehensive approach to agents
- Pre-built Microsoft agents
- Advanced analysts and research agents for deeper analysis
- Custom agents based on your data
- Advanced management and analytics

Powered by Work IQ

1. Learn about standard and priority access here. 2. Available in Word, Excel, PowerPoint, Outlook, and OneNote. 3. Applies to assistive agents built by you on the Microsoft 365 Copilot agent platform deployed on Microsoft 365 surfaces

Copilot Control System (CCS)

Copilot Control System

Copilot + Agents

Security & Governance

Data security

AI security

Compliance & privacy

Management Controls

Licensing & metering

Customization

Measurement & Reporting

Impact & ROI metrics

Robust prebuilt reports

Custom reporting included

Tools to secure and govern your Copilot use

Address oversharing concerns

- Gain visibility into overshared content
- Remediate excessive permissions
- Prevent Copilot from processing sensitive files

Protect against data loss and insider risks

- Get alerts and reports of risky behavior and AI use
- Protect sensitive files and interactions
- Dynamically apply security policies based on risky actions

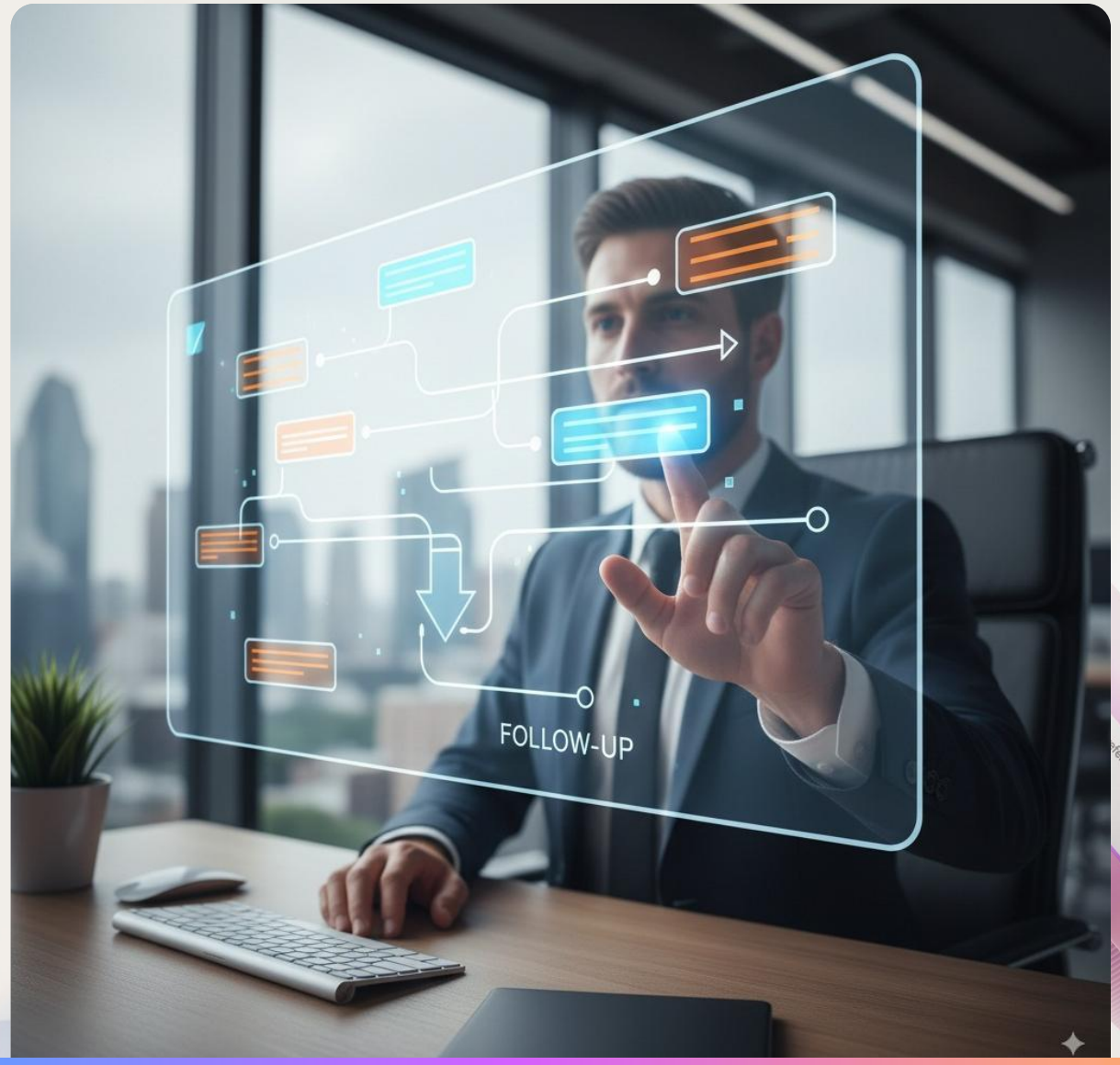
Govern AI use to meet regulations & policies

- Inspect interaction content and audit logs
- Investigate for compliance and ethical violations
- Enforce lifecycle policies and legal holds

Secure

Govern

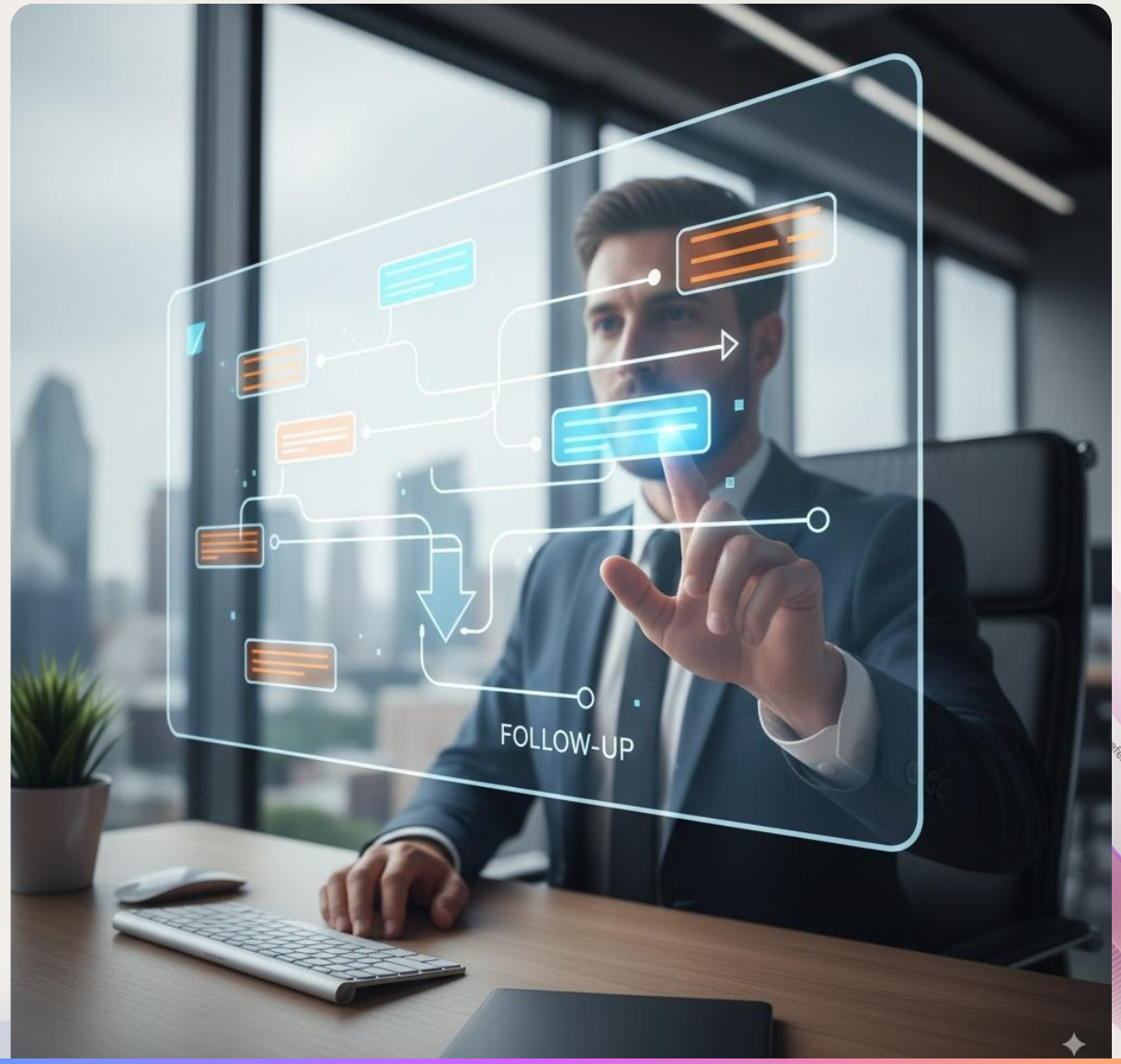
Microsoft 365 Copilot MAC walkthrough



Network requirements

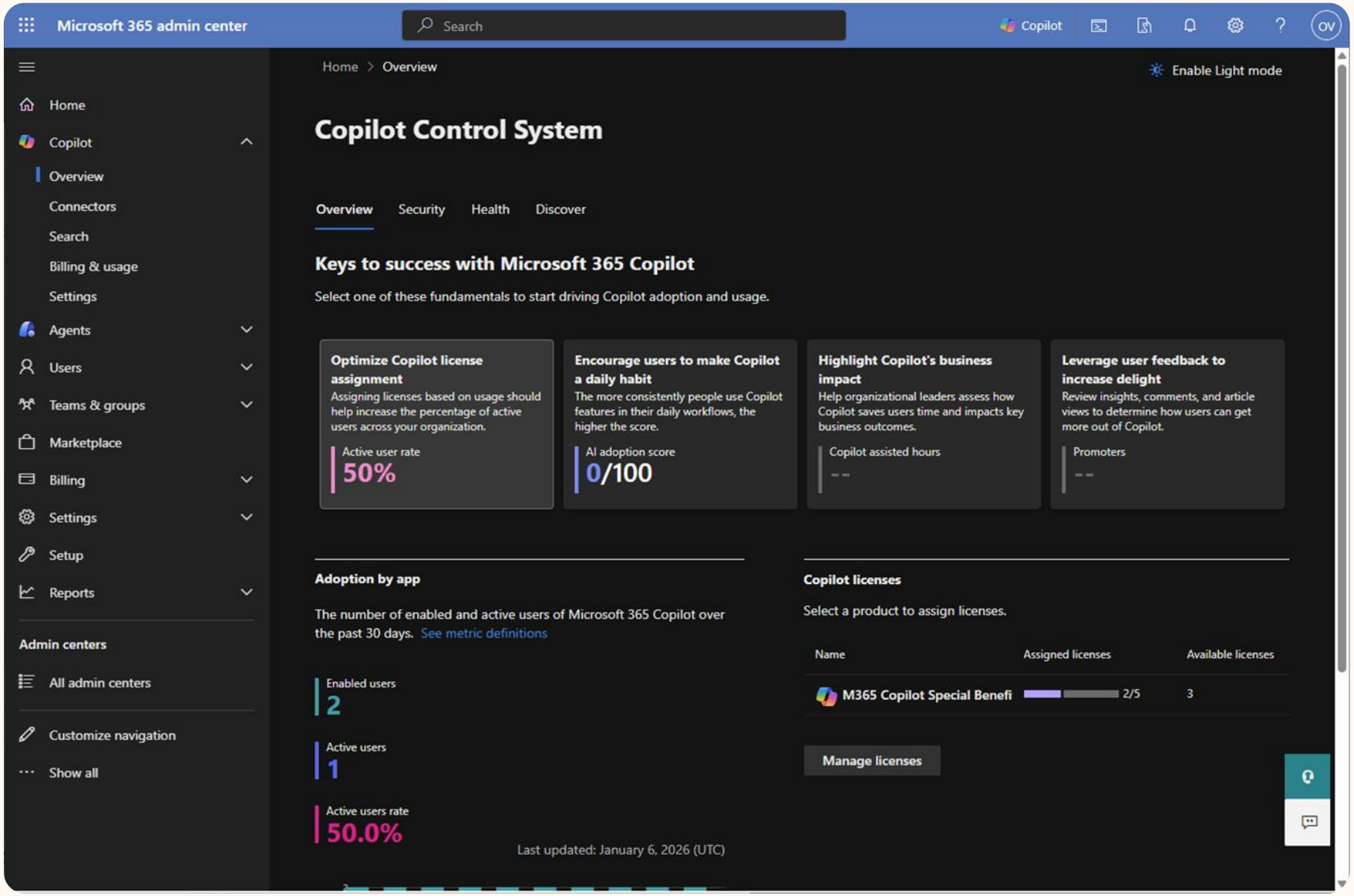
- Most features can be managed in Microsoft 365 admin center (MAC)
- Microsoft doesn't recommend and cannot support attempts to manage Microsoft 365 Copilot Chat and related settings through network-level restrictions
- M365 Copilot is deeply integrated with applications, such network-level restrictions can lead to unpredictable results

[Microsoft 365 URLs and IP address ranges - Microsoft 365 Enterprise]



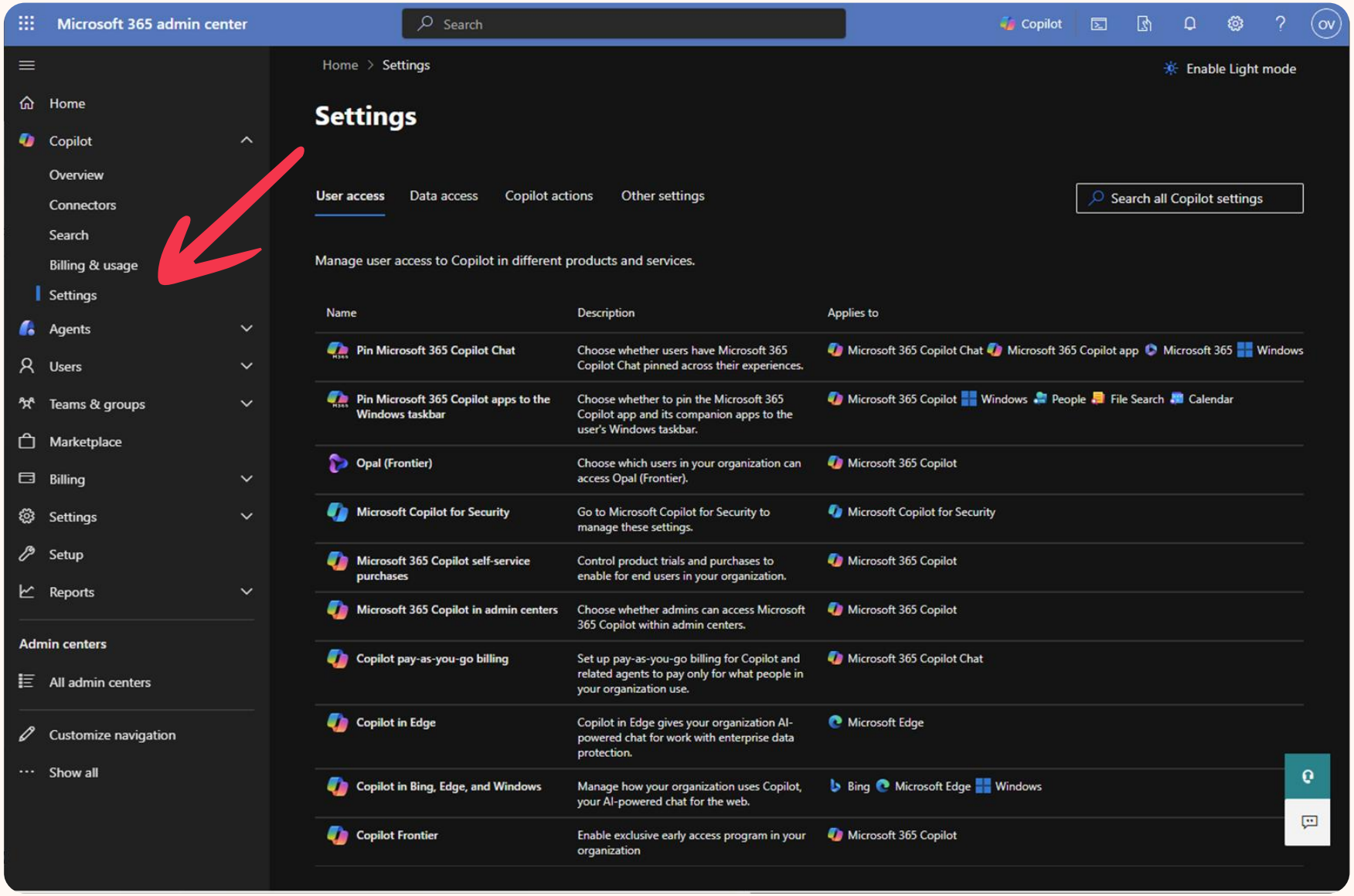
Where to start

- Common Settings under the Copilot Section
- Detailed Agent Settings -> Agent365
- Specialized features are set in the product Admin portals (Defender, Purview, Entra, Power Platform)

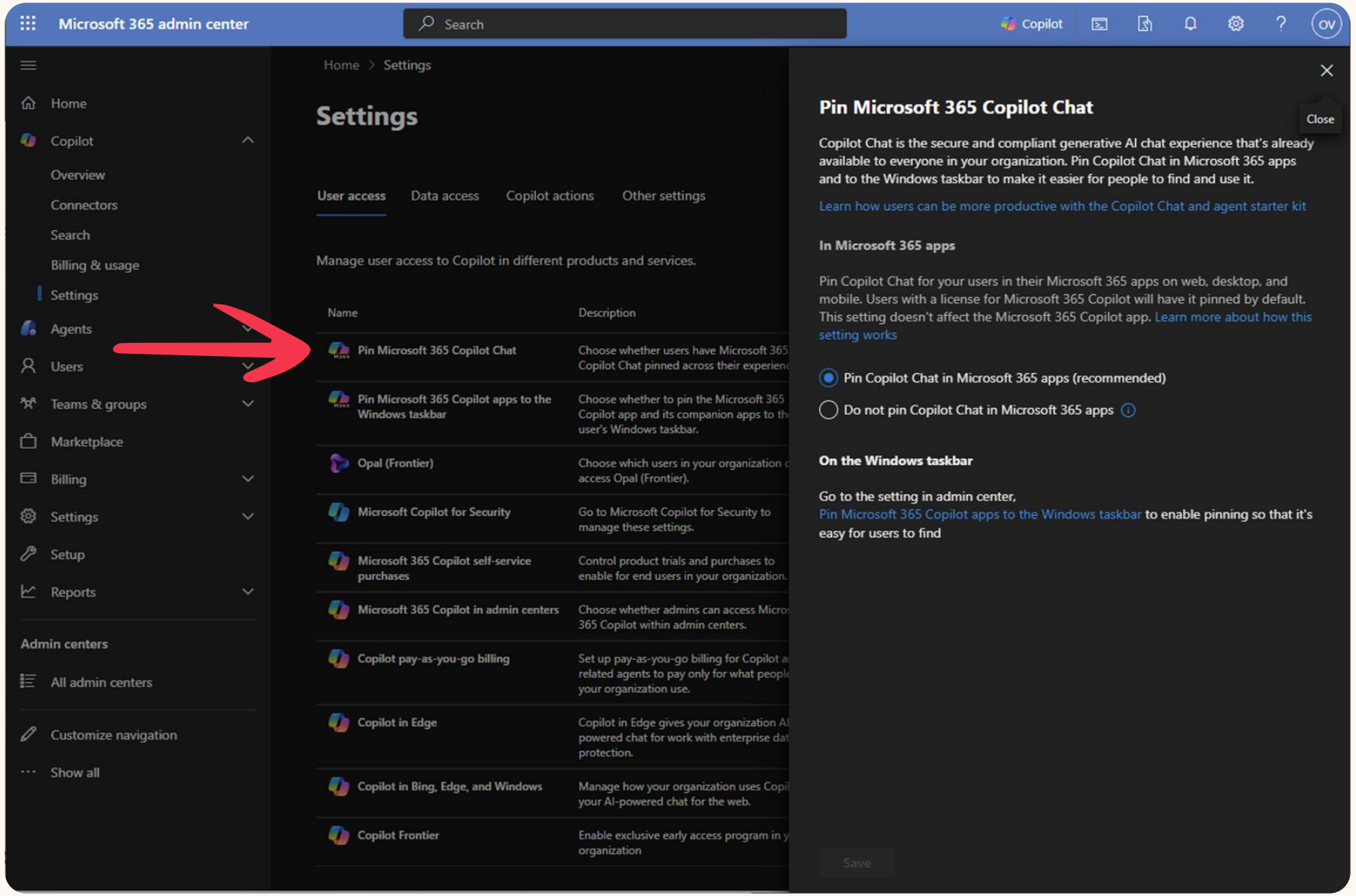


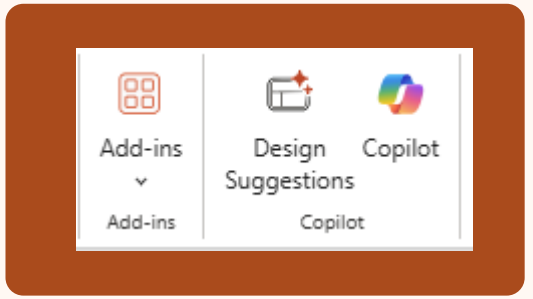
Copilot Settings #1: User Access

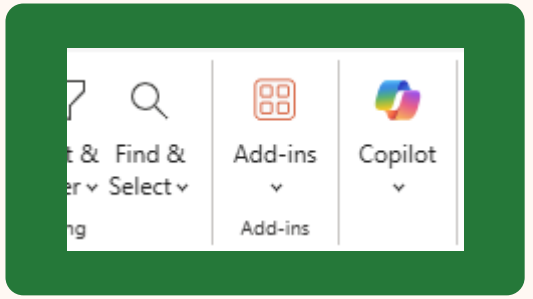
- Common Settings under the Copilot Section

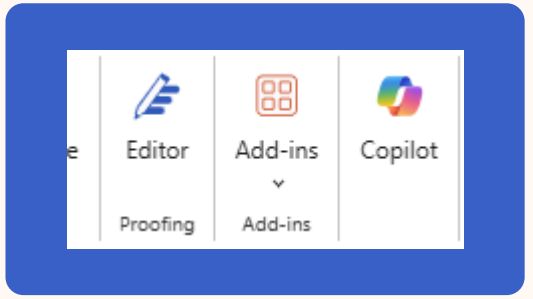


Copilot Settings #1: User Access

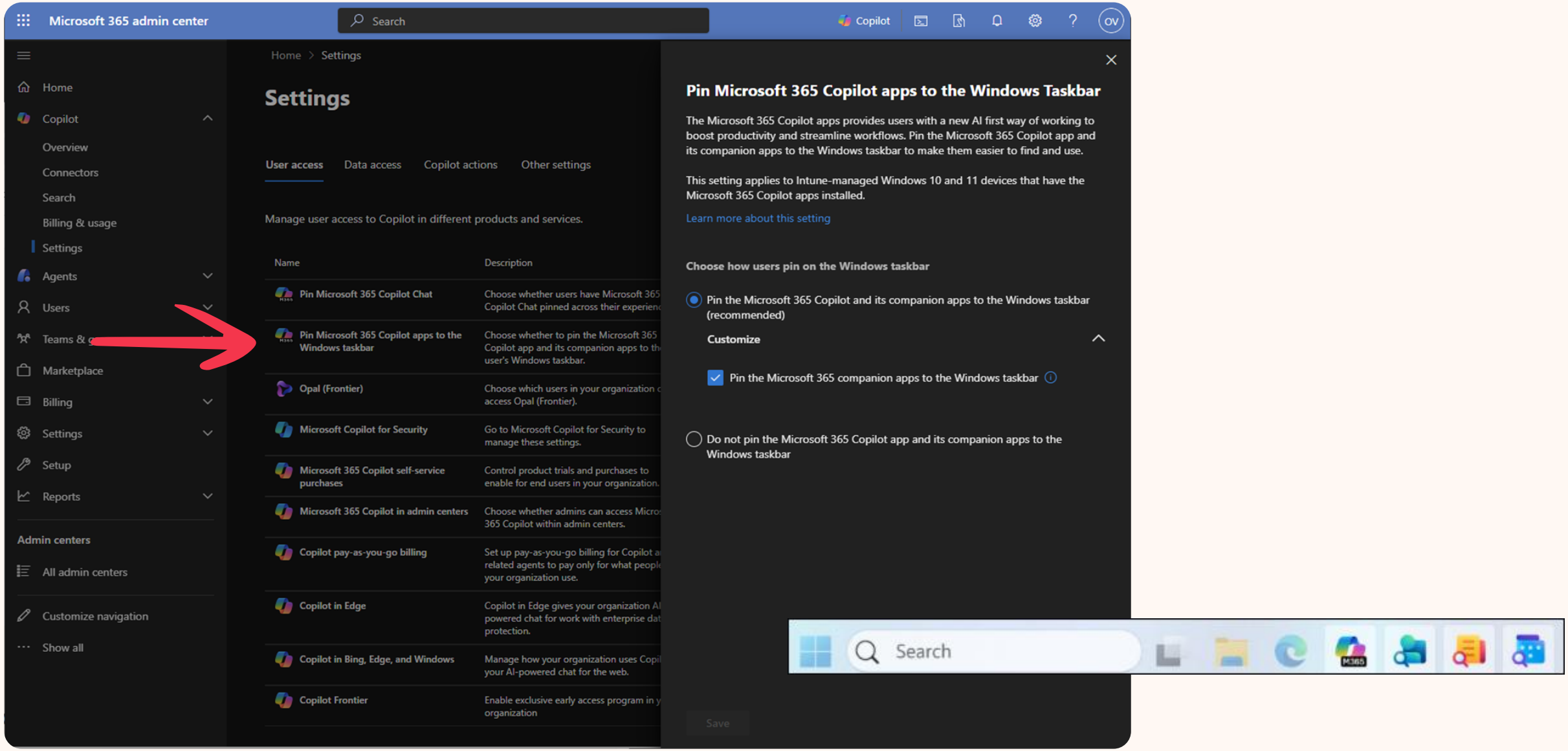




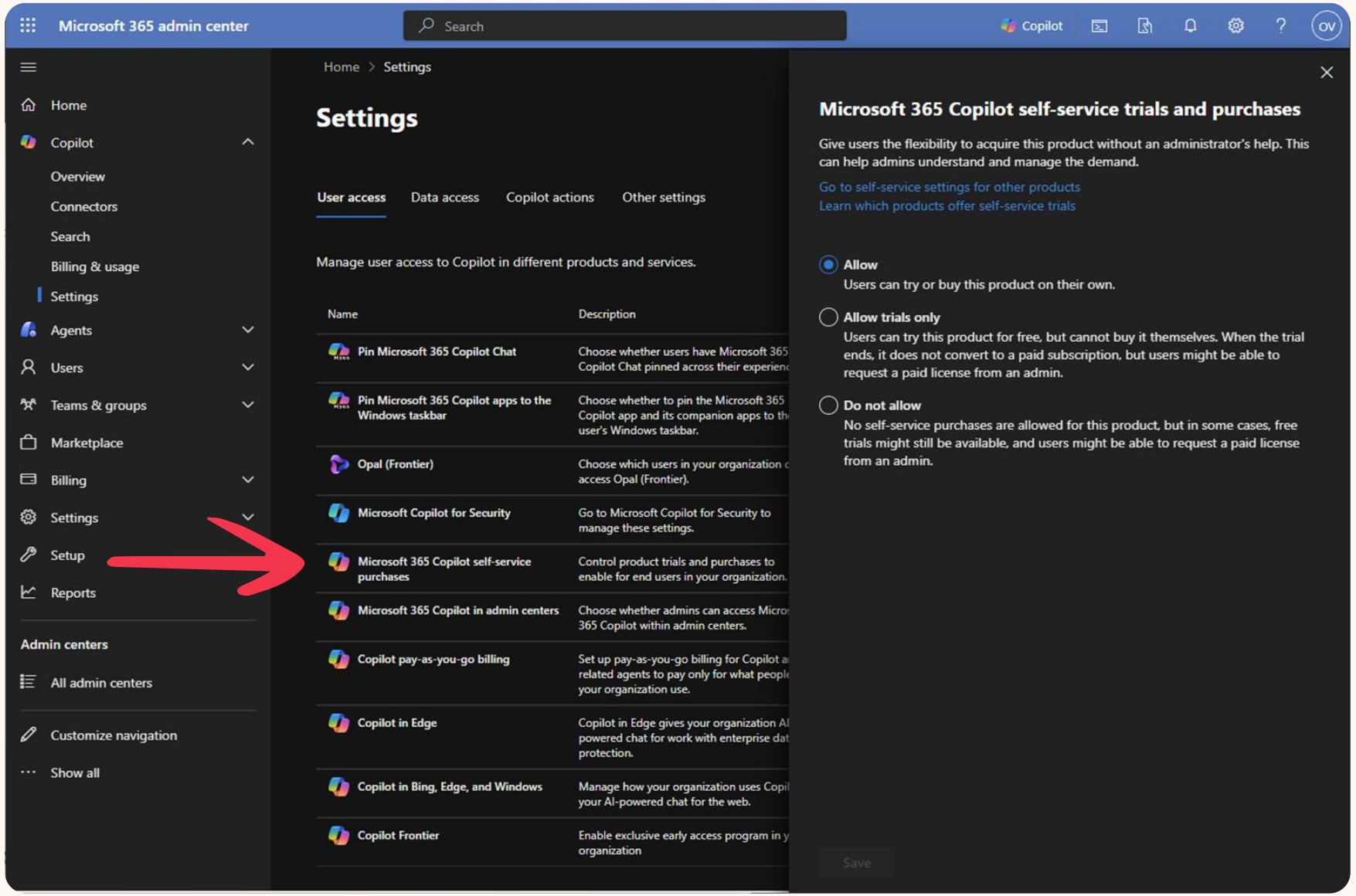




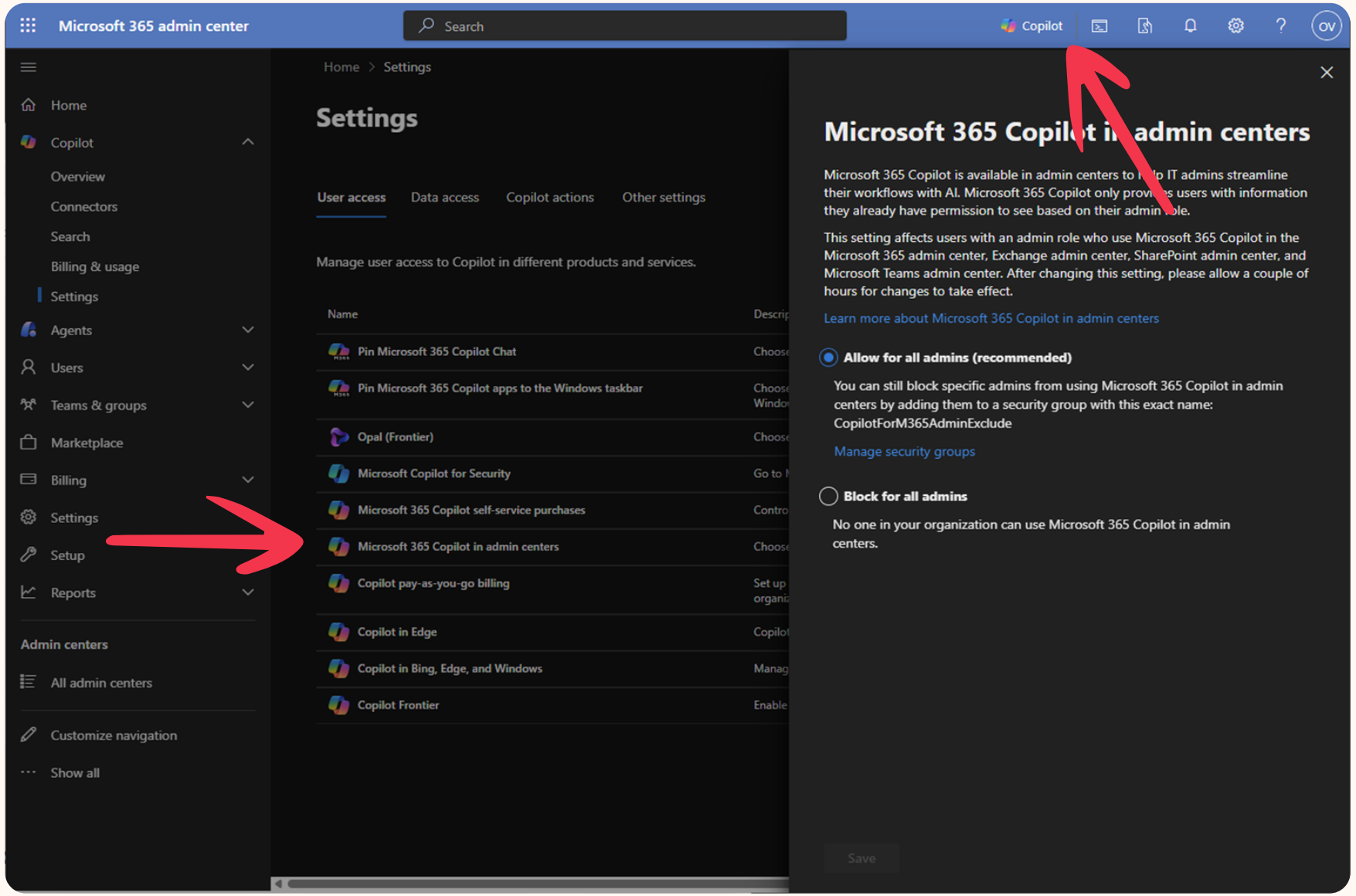
Copilot Settings #1: User Access



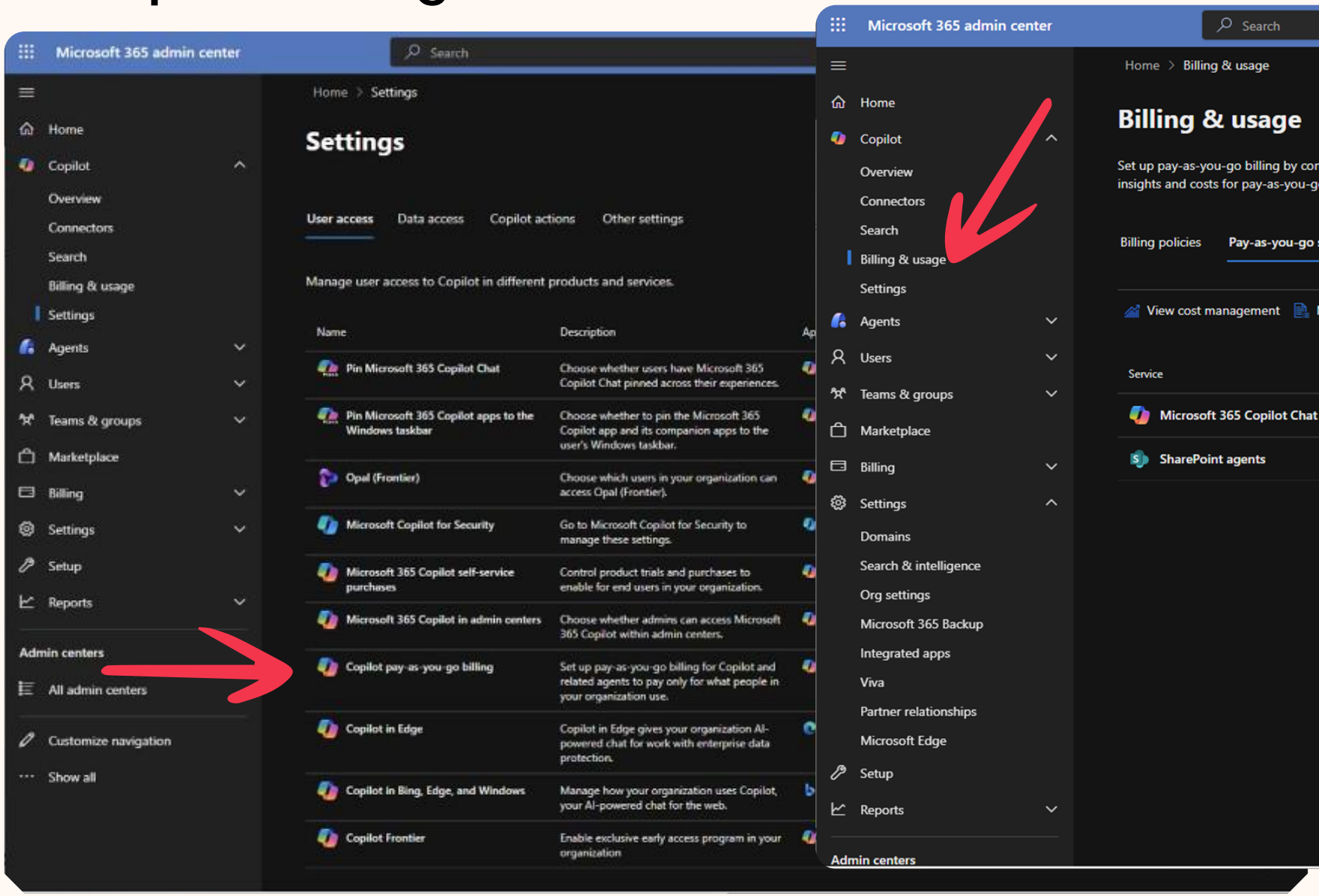
Copilot Settings #1: User Access

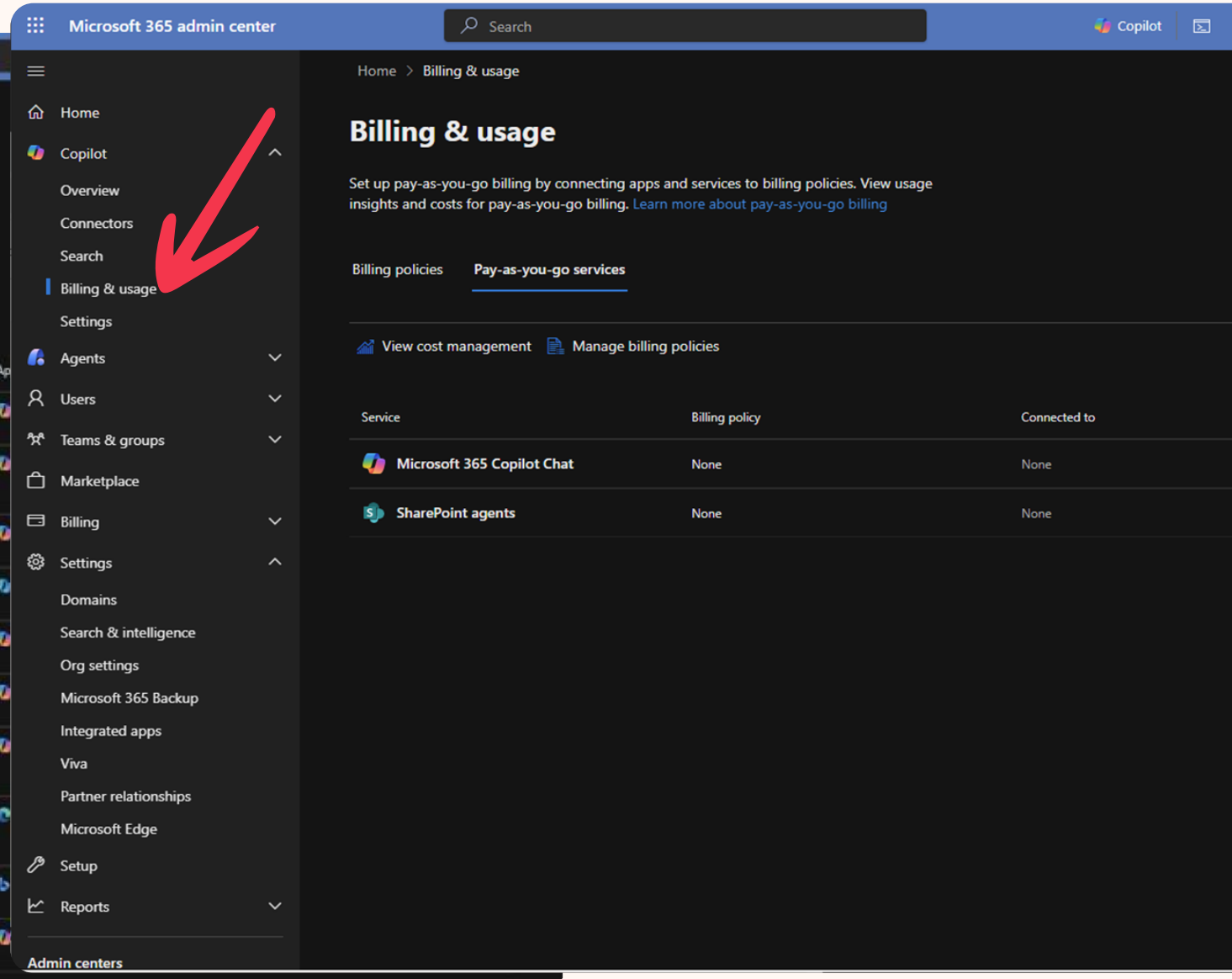


Copilot Settings #1: User Access

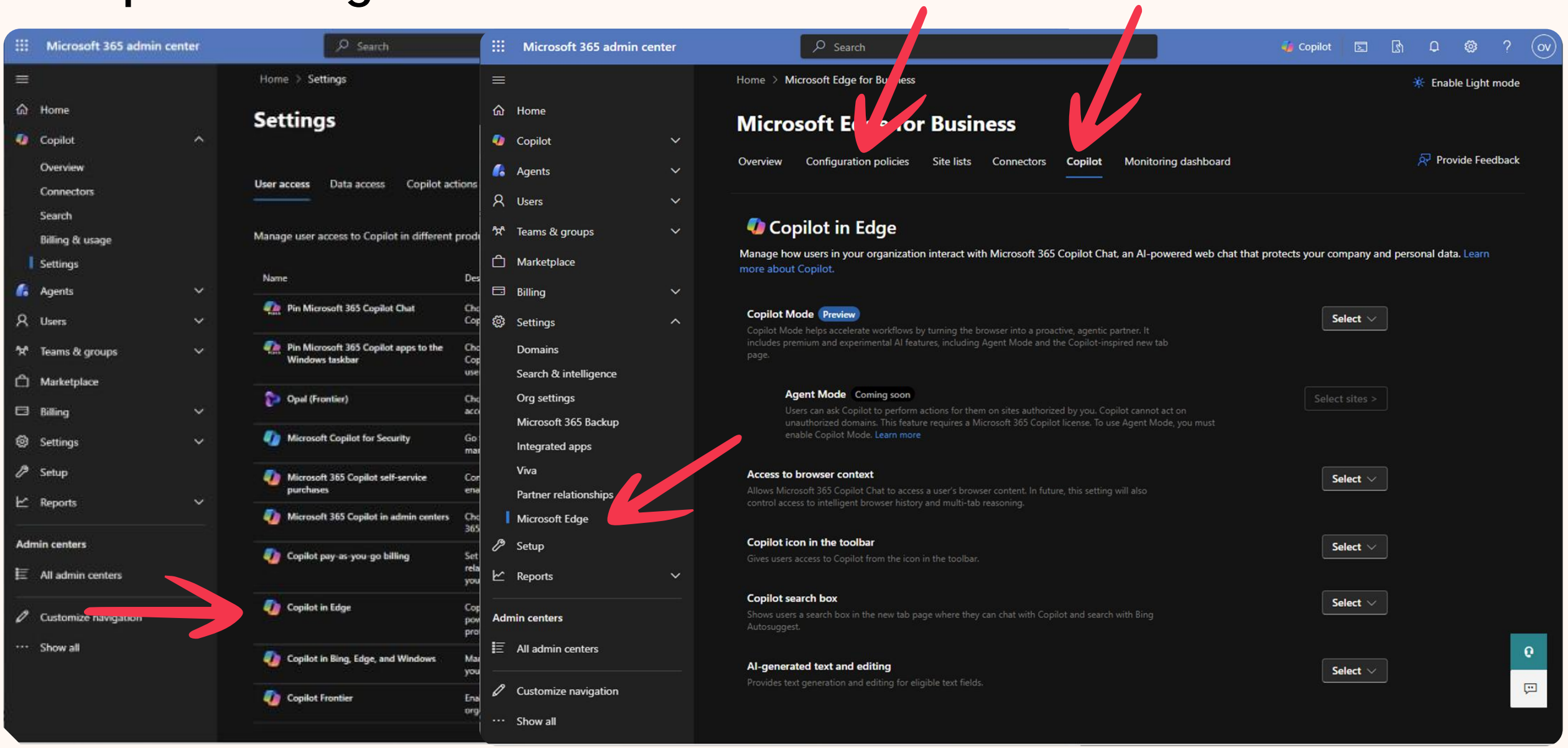


Copilot Settings #1: User Access

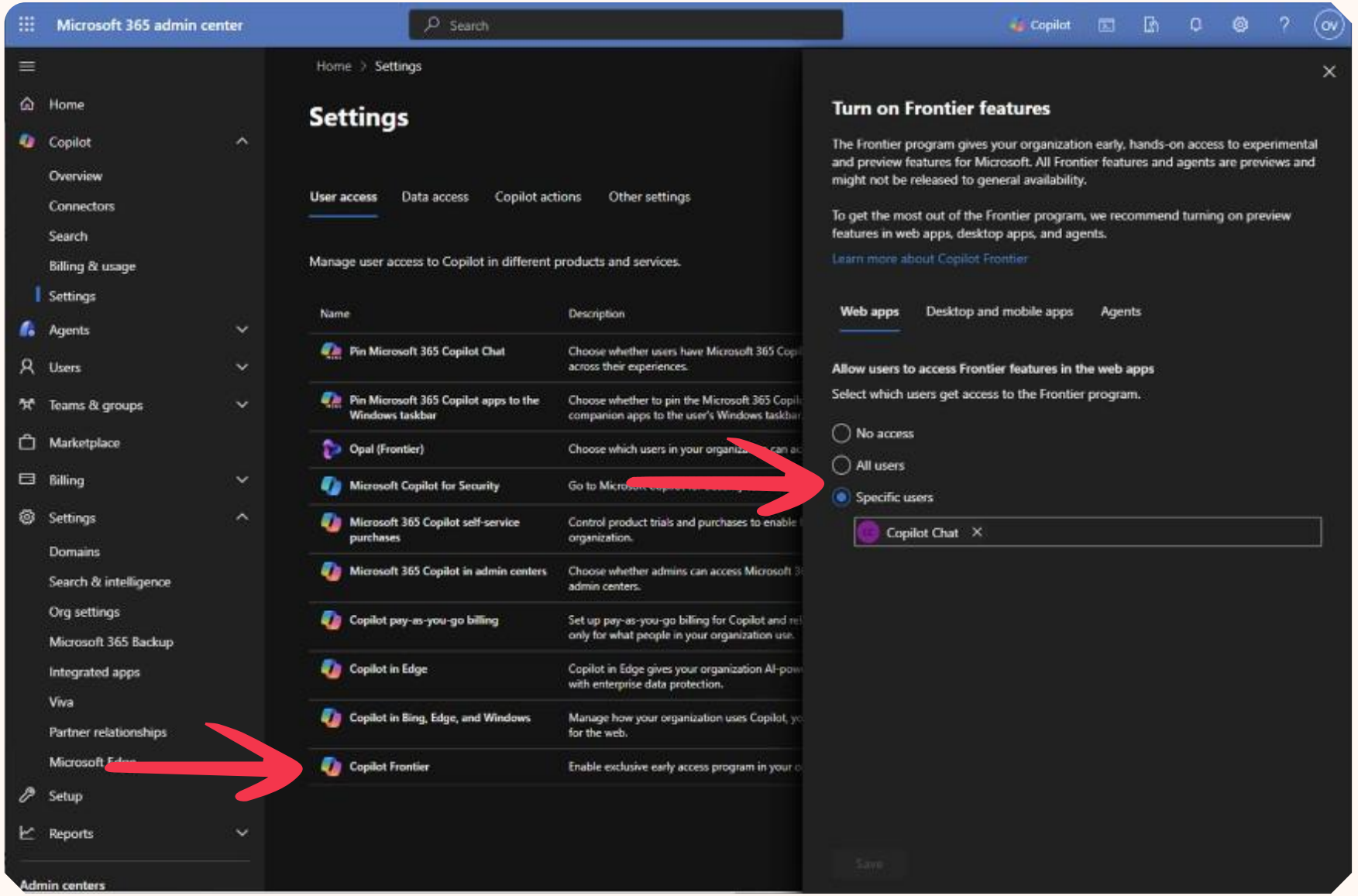




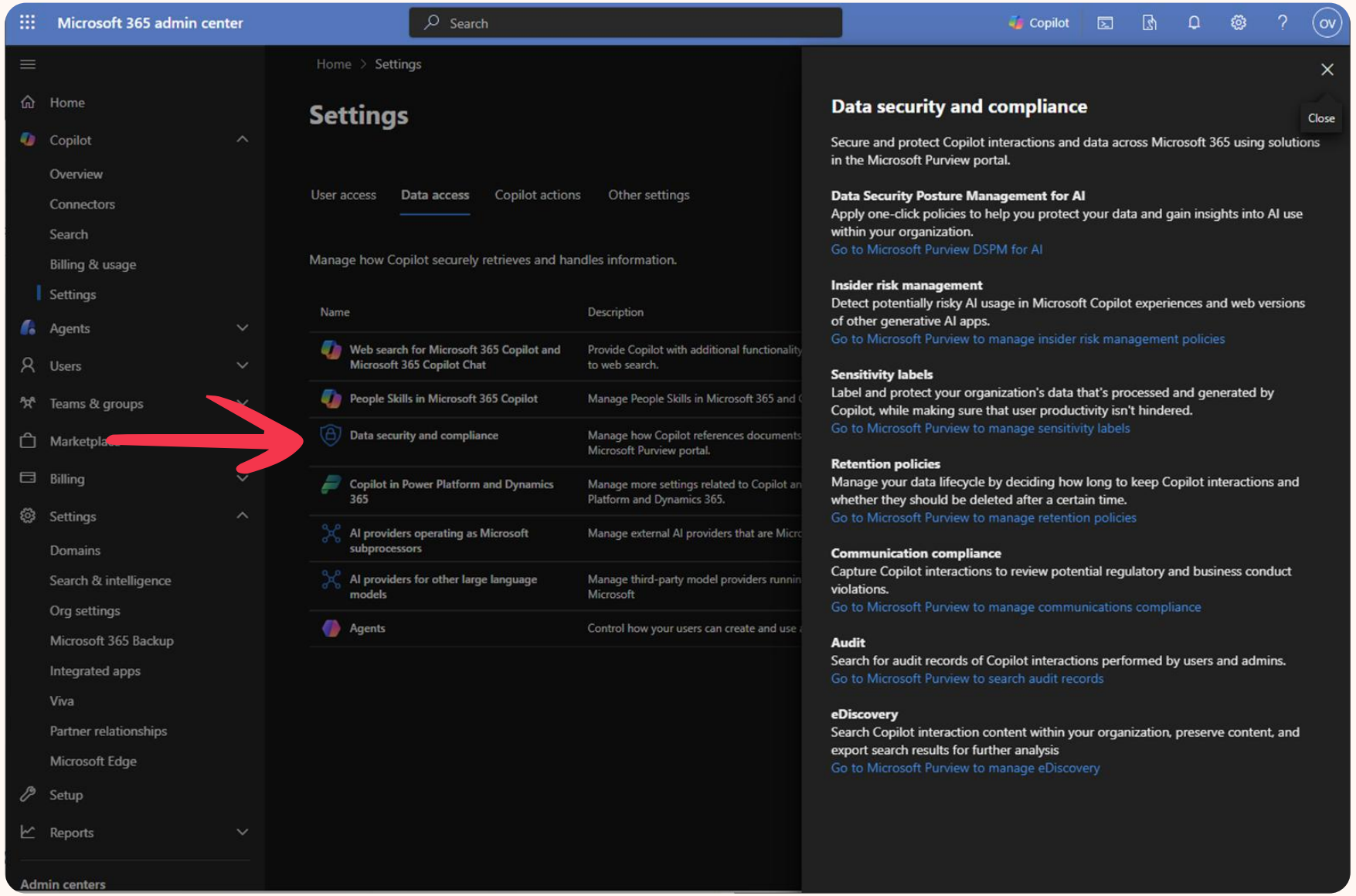
Copilot Settings #1: User Access



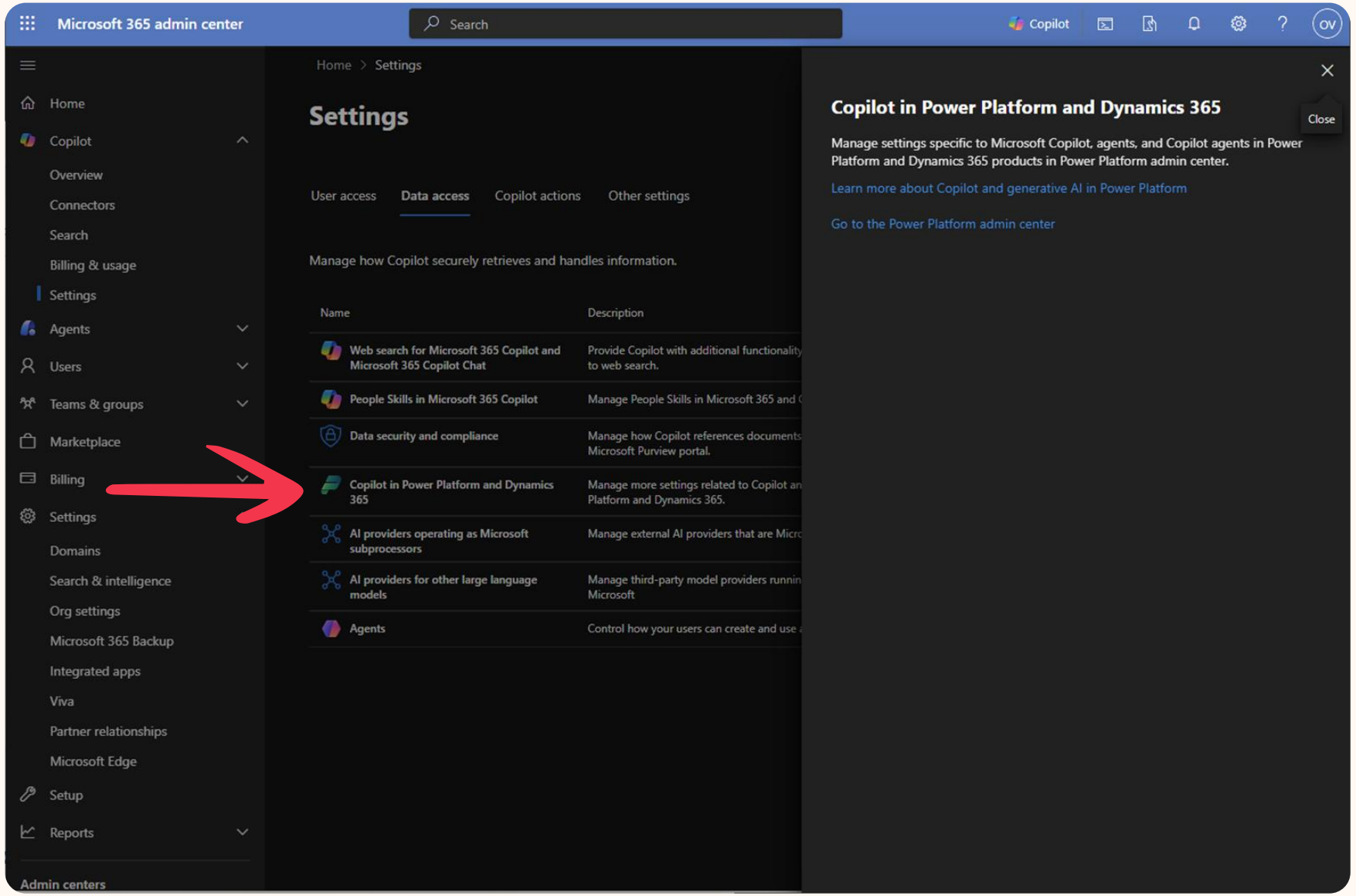
Copilot Settings #1: User Access



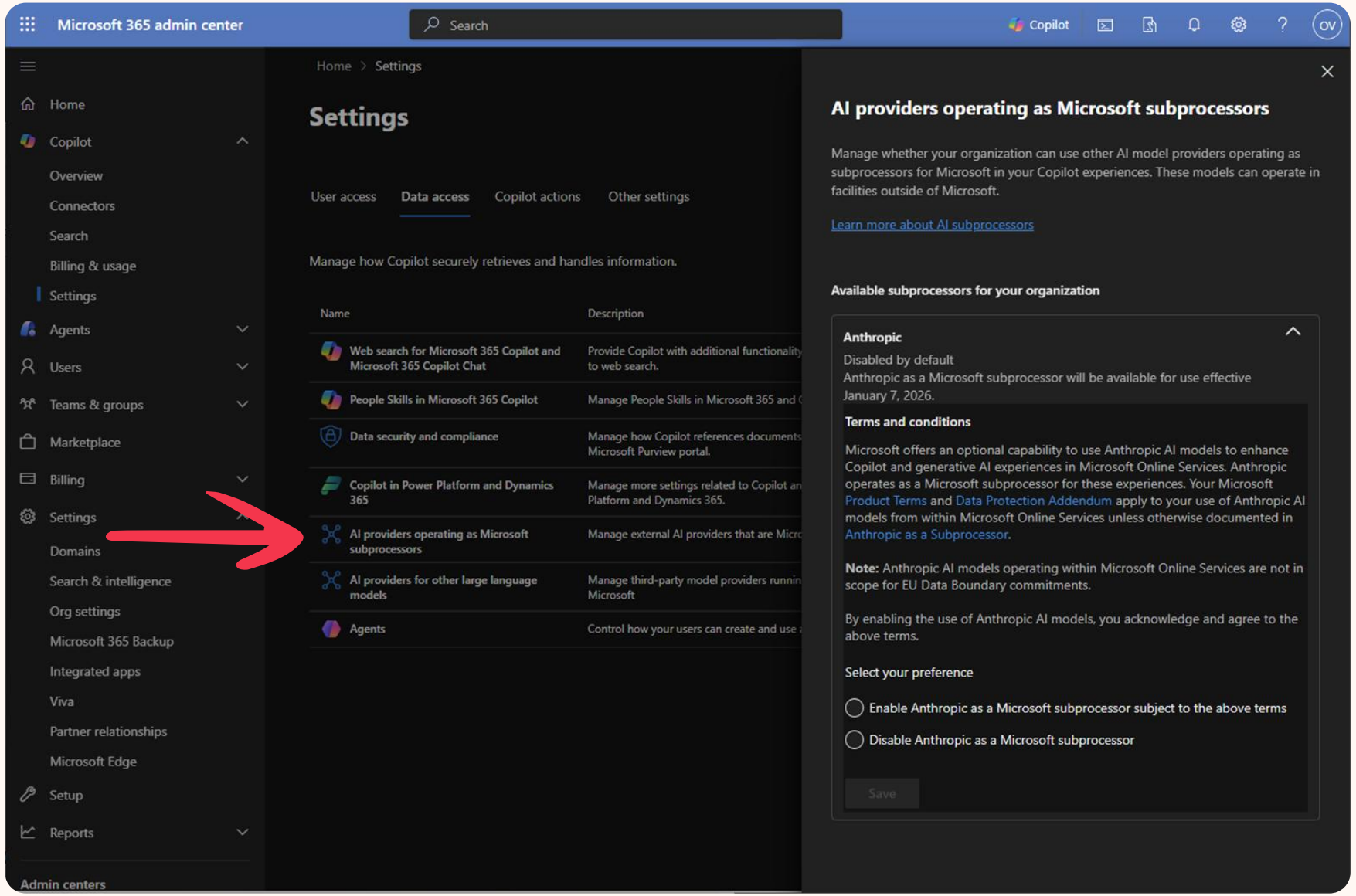
Copilot Settings #2: Data Access – Data Security and Compliance



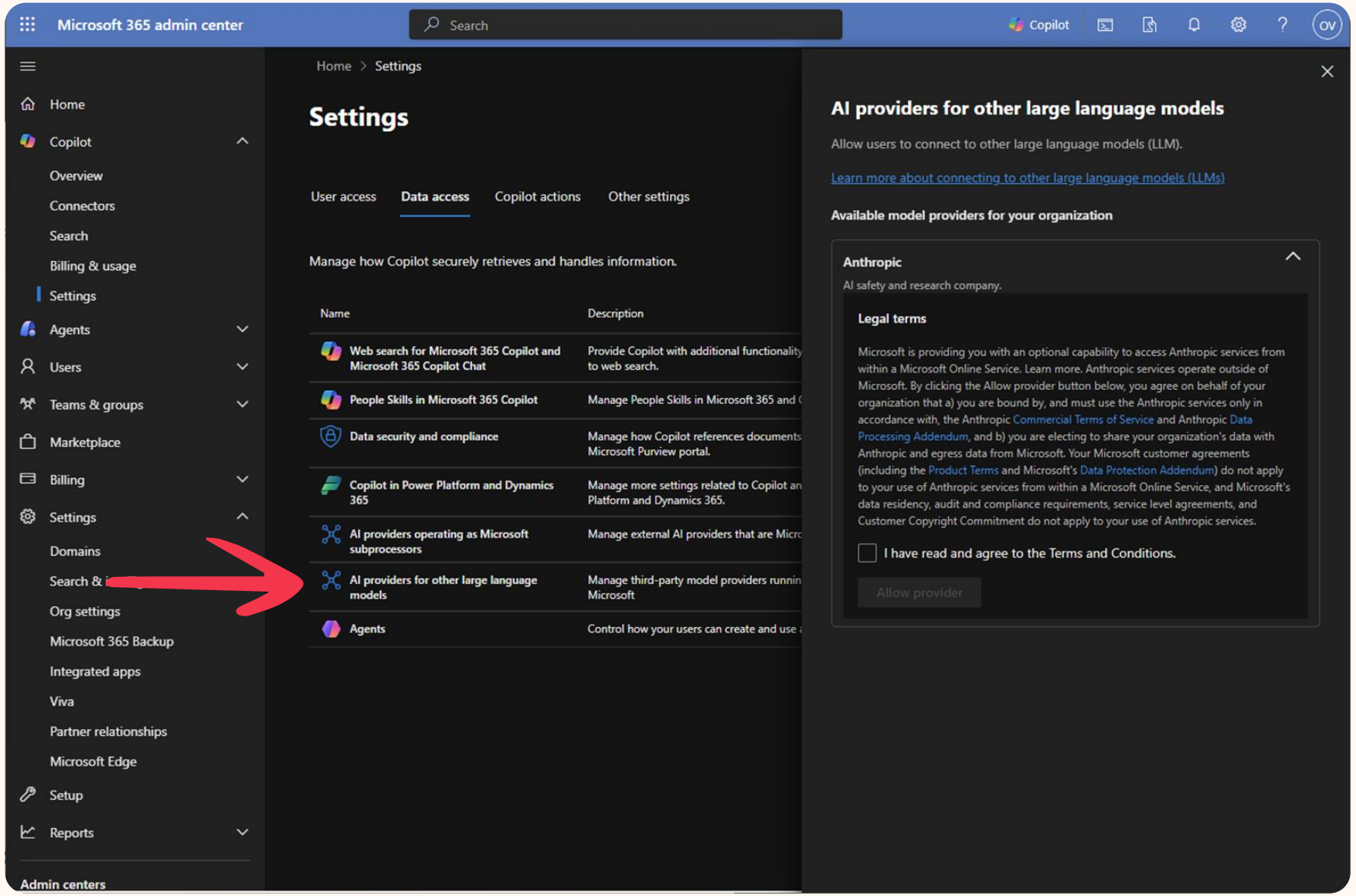
Copilot Settings #2: Data Access - PowerPlatform



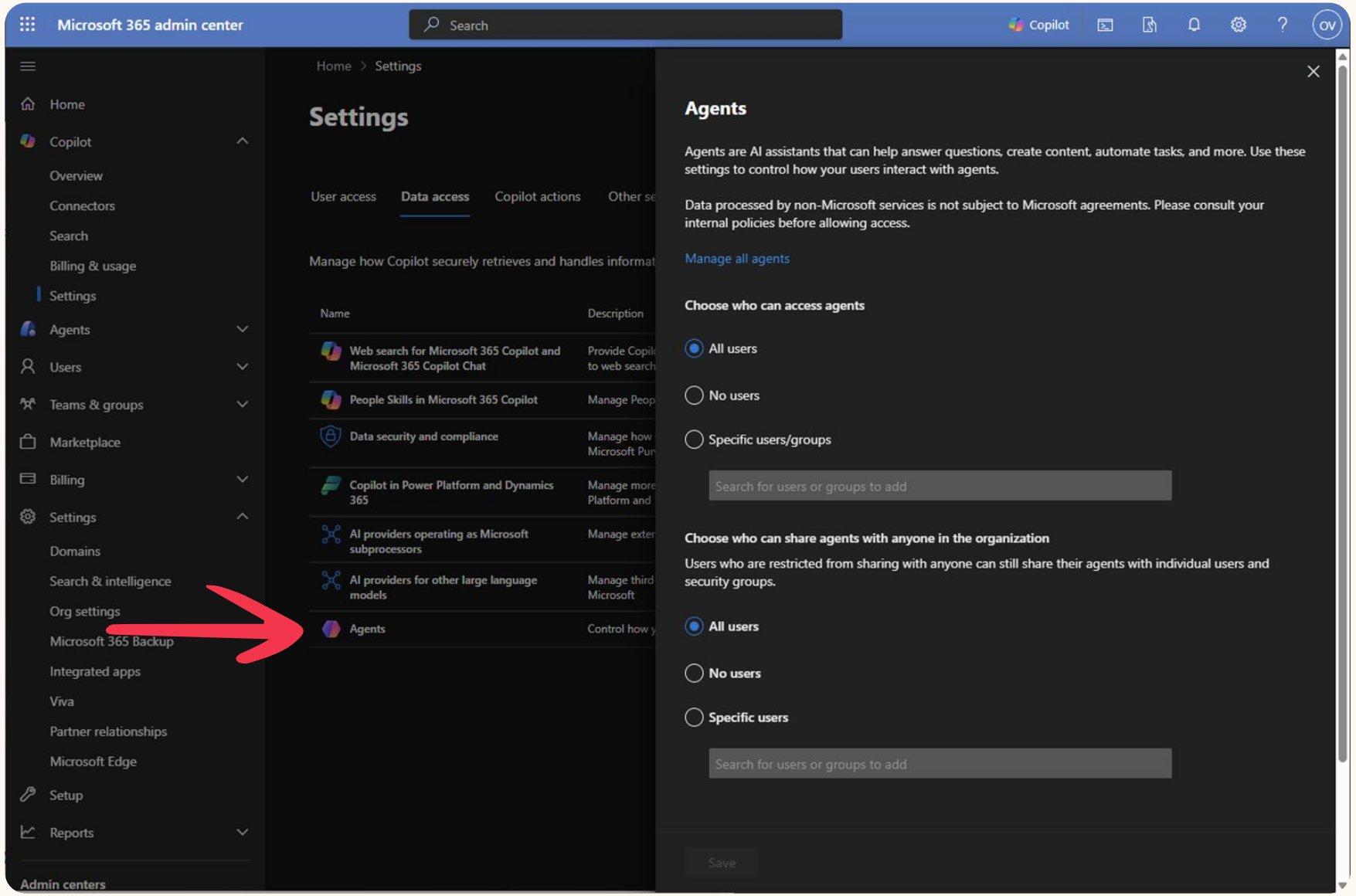
Copilot Settings #2: Data Access – Anthropic subprocessor



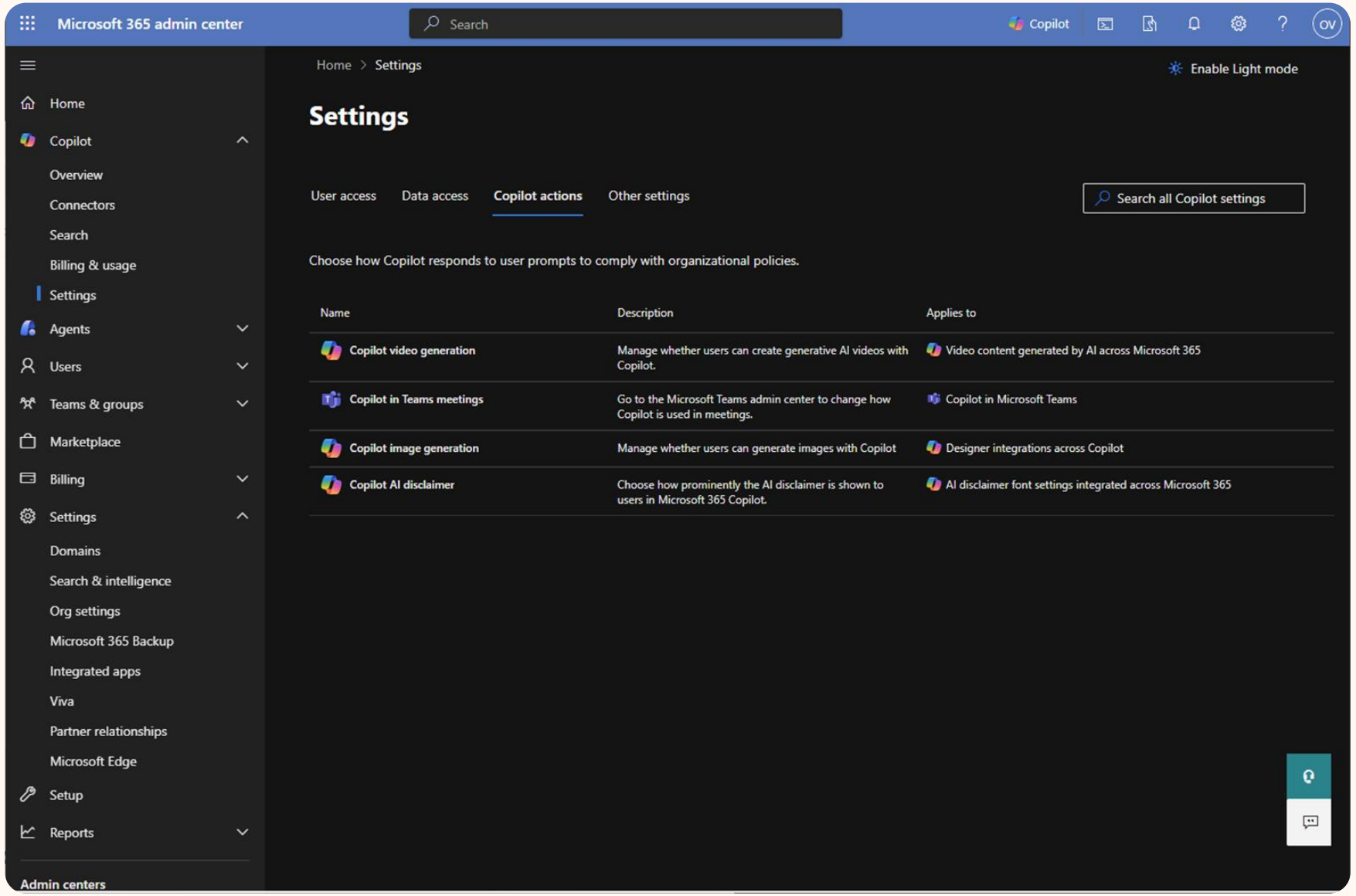
Copilot Settings #2: Data Access – 3rd party model providers



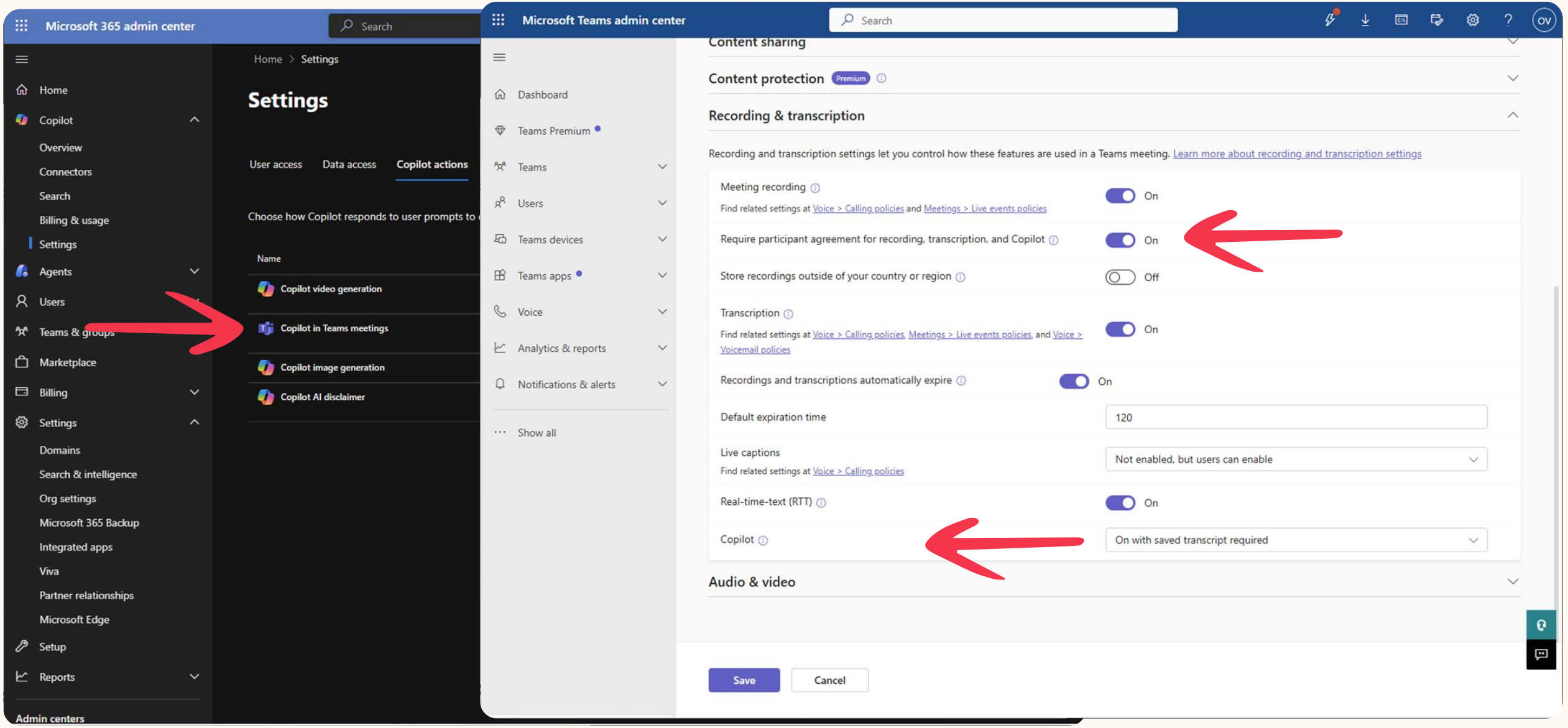
Copilot Settings #2: Data Access – Agents



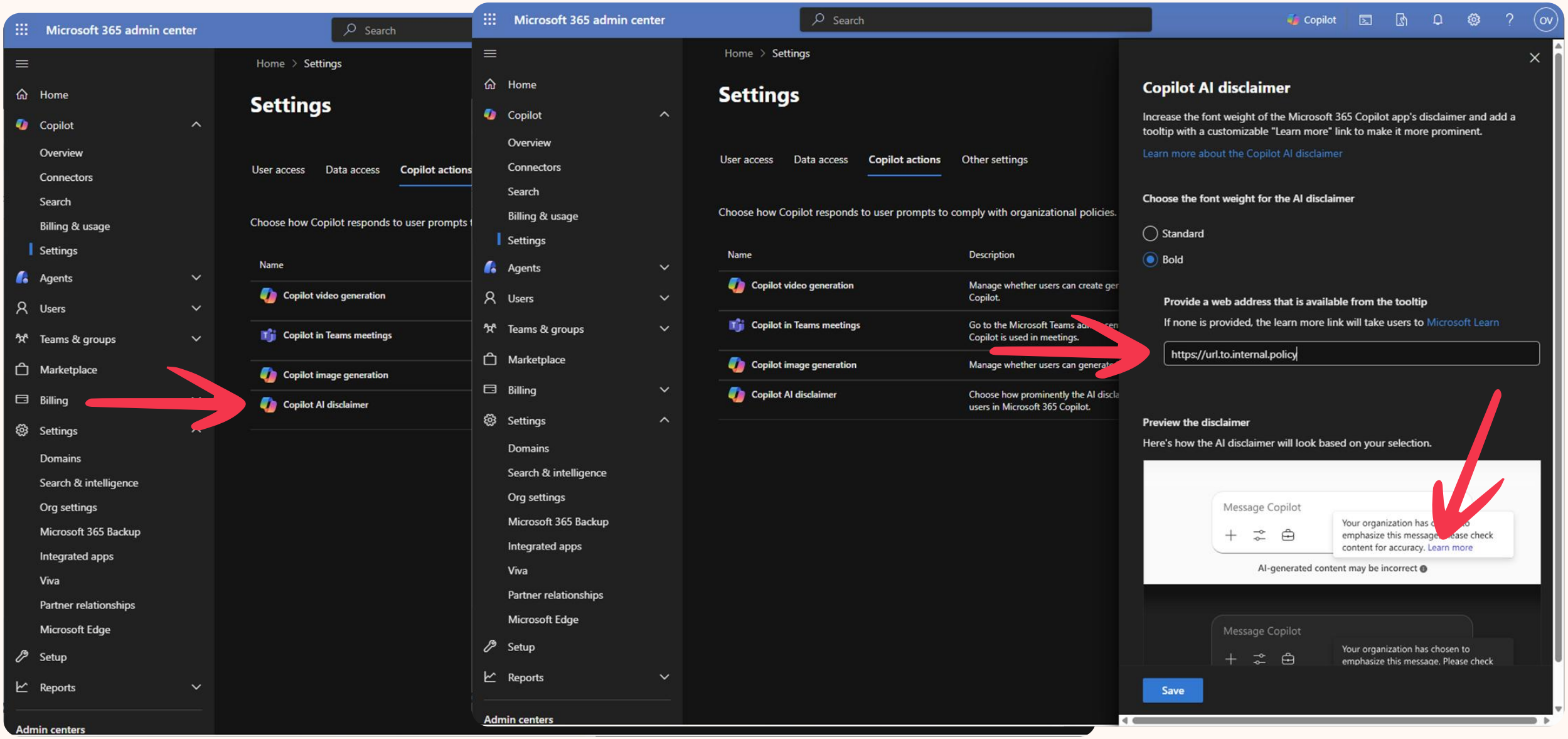
Copilot Settings #3: Copilot Actions



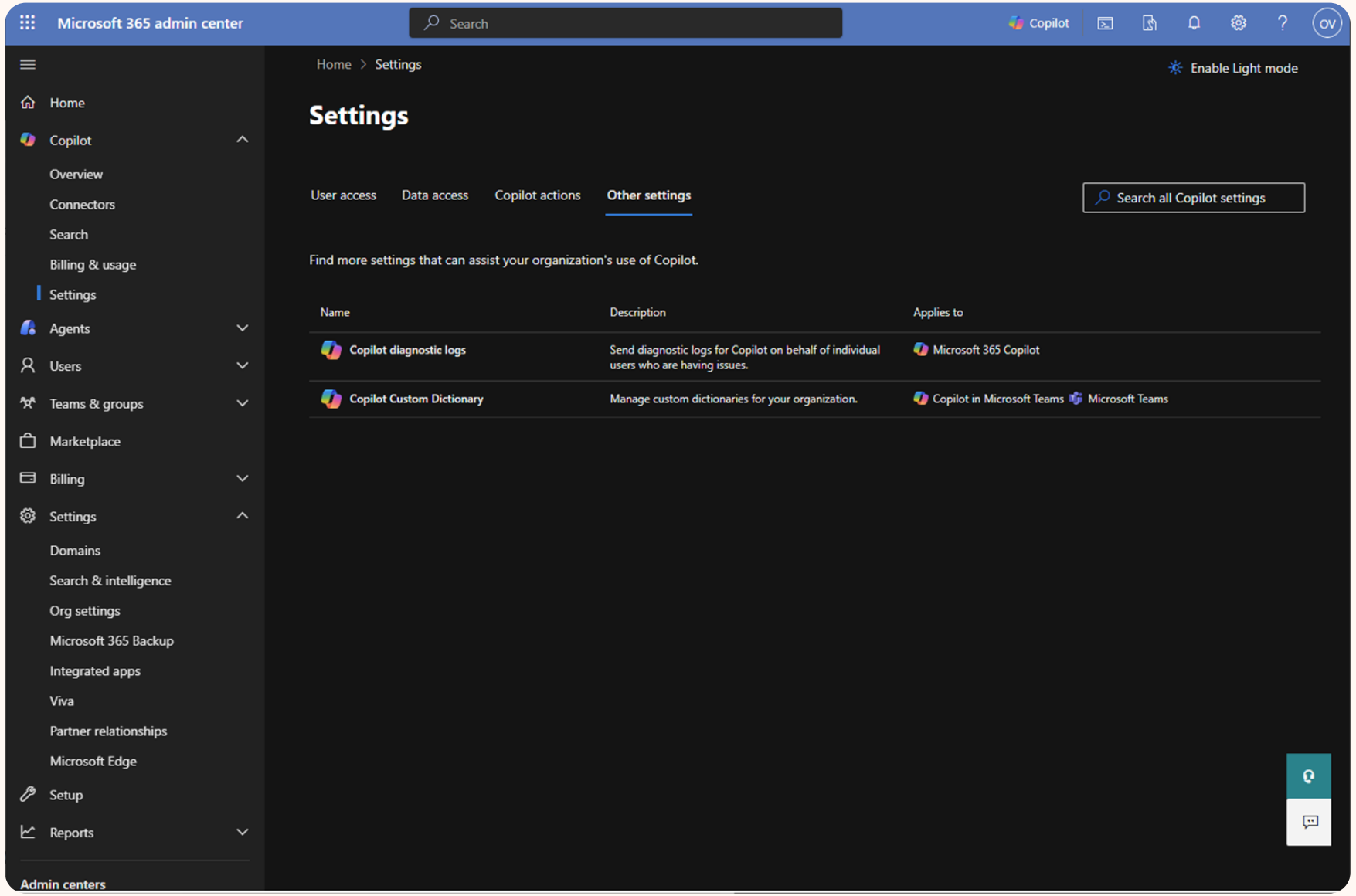
Copilot Settings #3: Copilot Actions - Teams



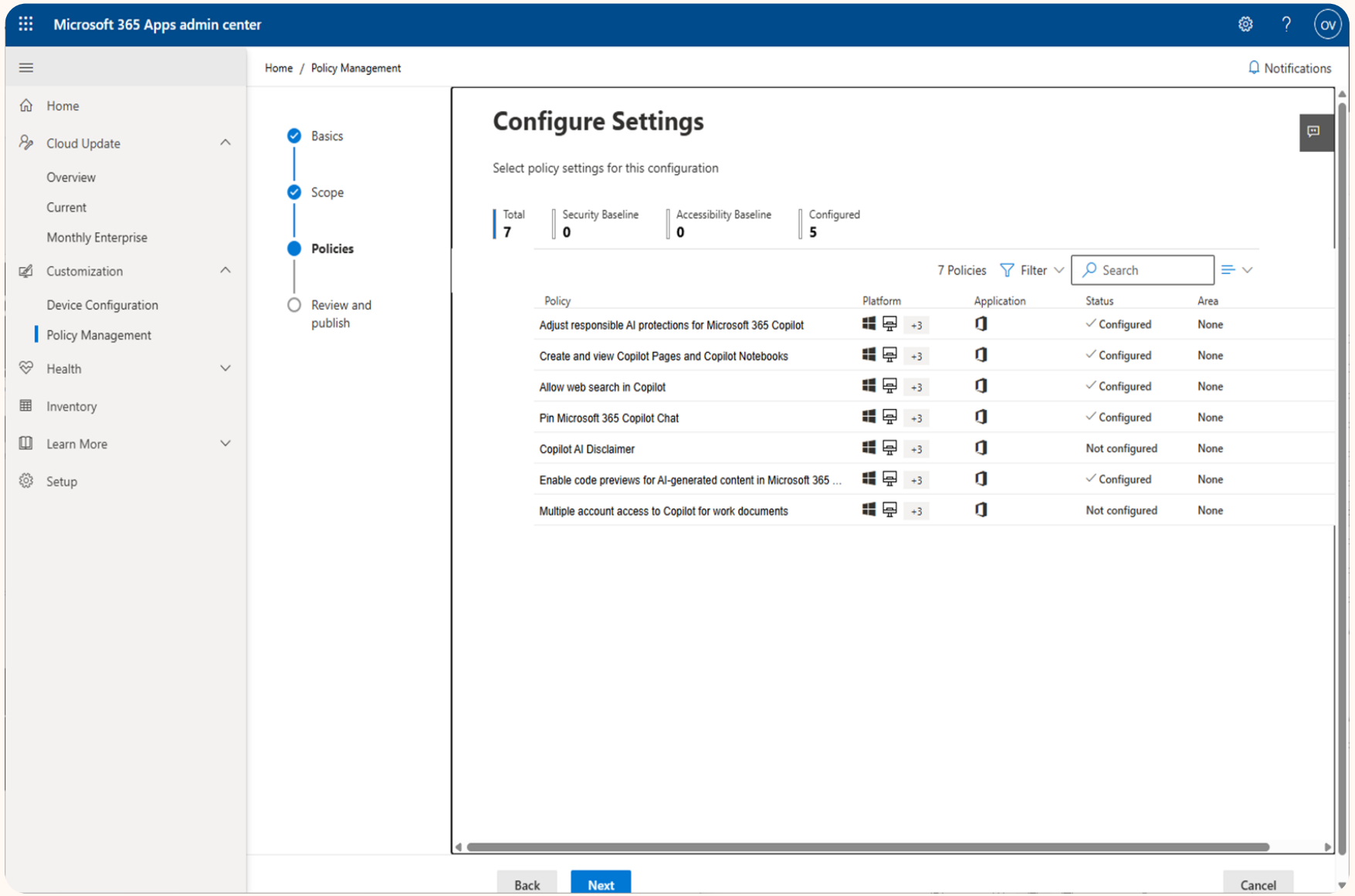
Copilot Settings #3: Copilot Actions - Disclaimer



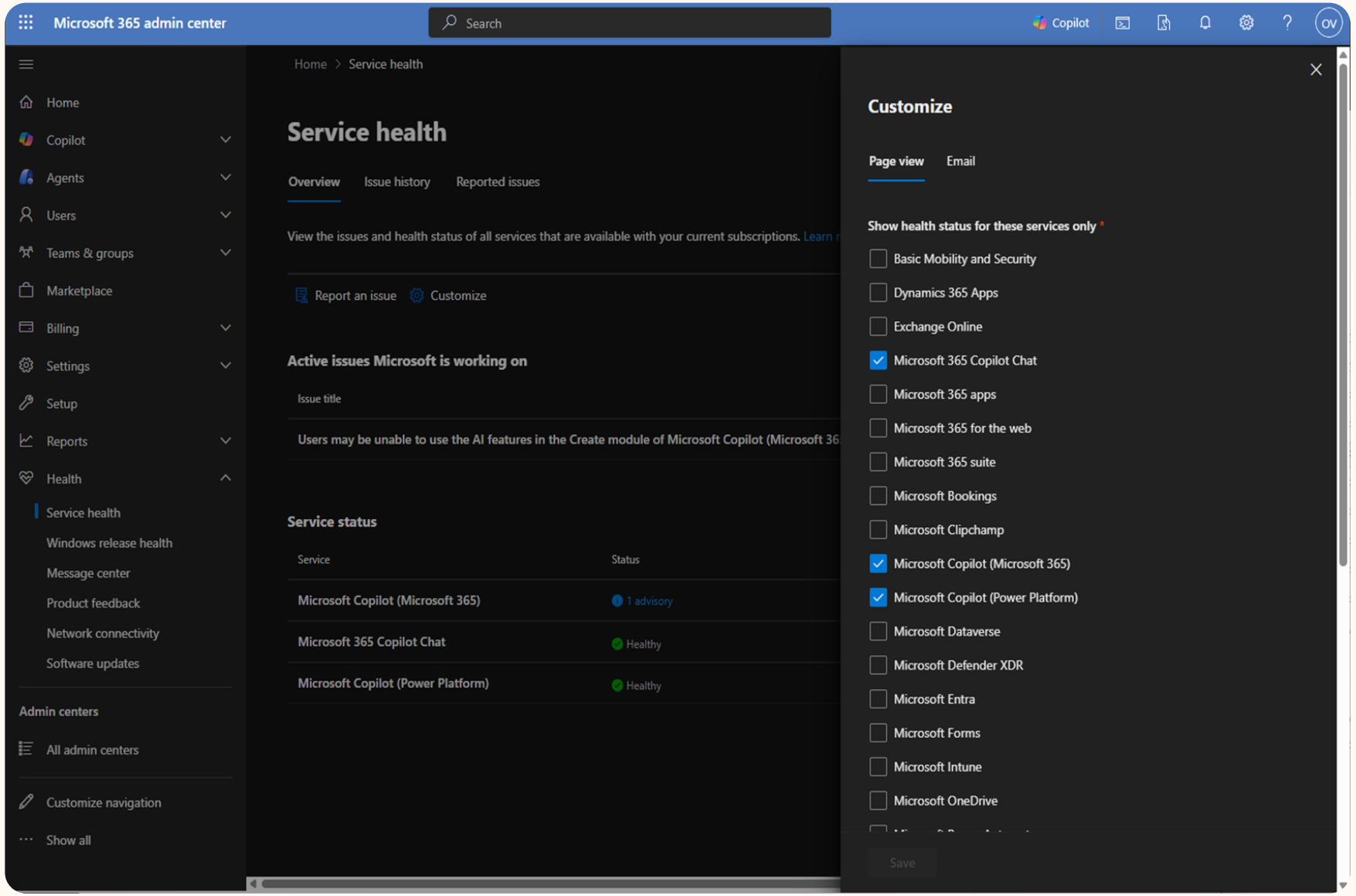
Copilot Settings #4: Other Settings



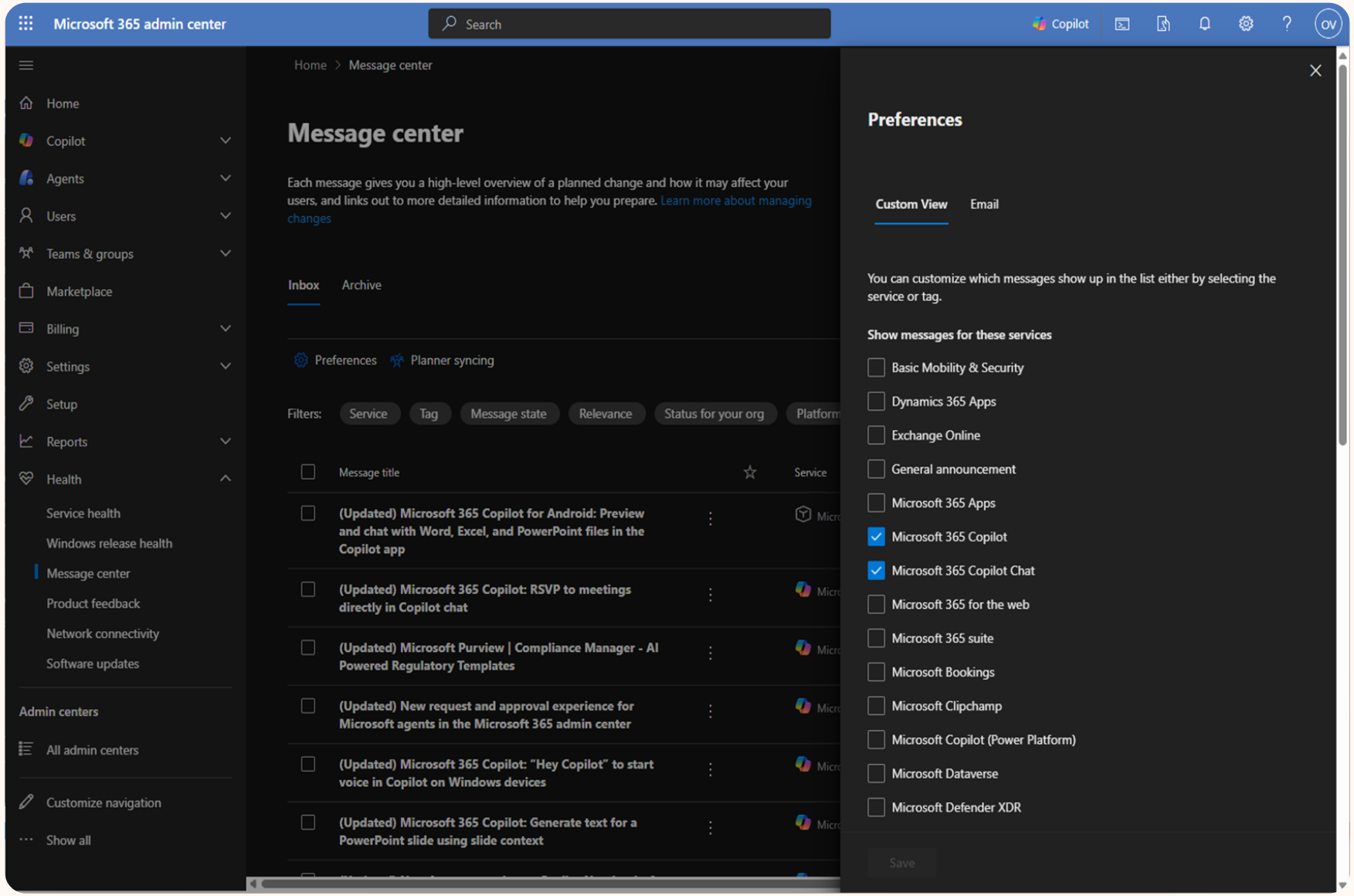
Copilot Settings #5: https://config.office.com



Copilot Settings #6: Service Health



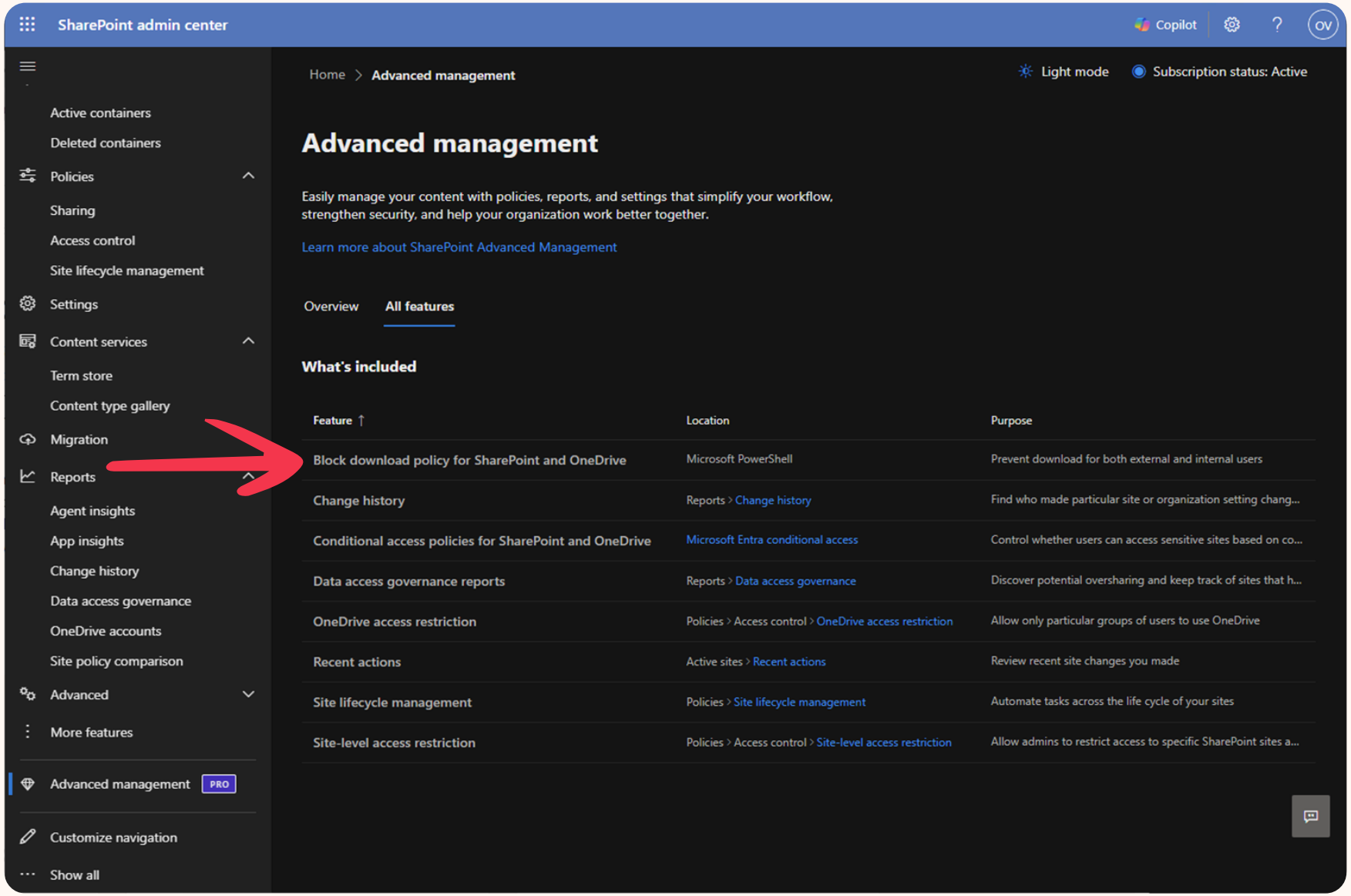
Copilot Settings #6: Message Center



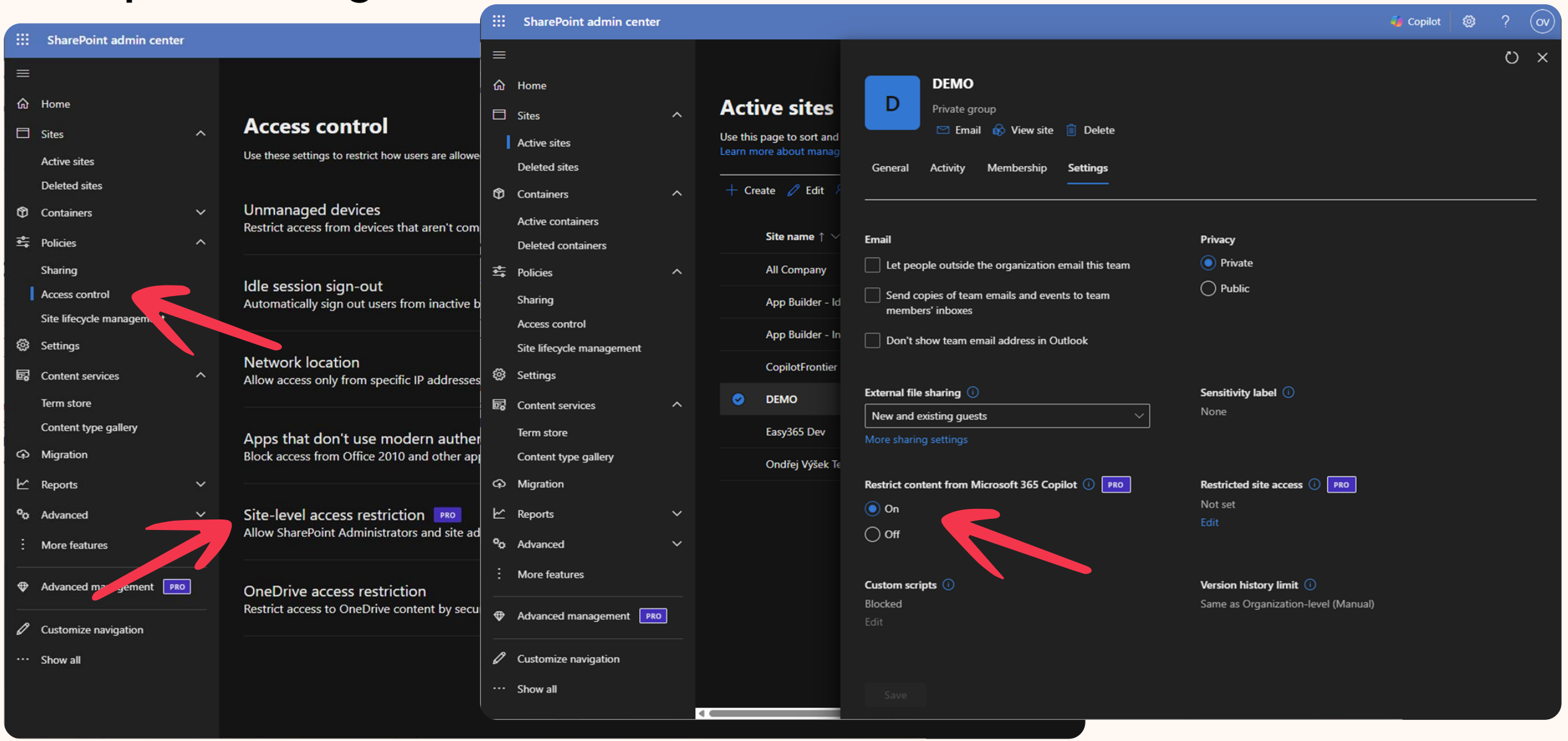
Data Discovery Configuration

Copilot Settings: SharePoint Advanced Managemend

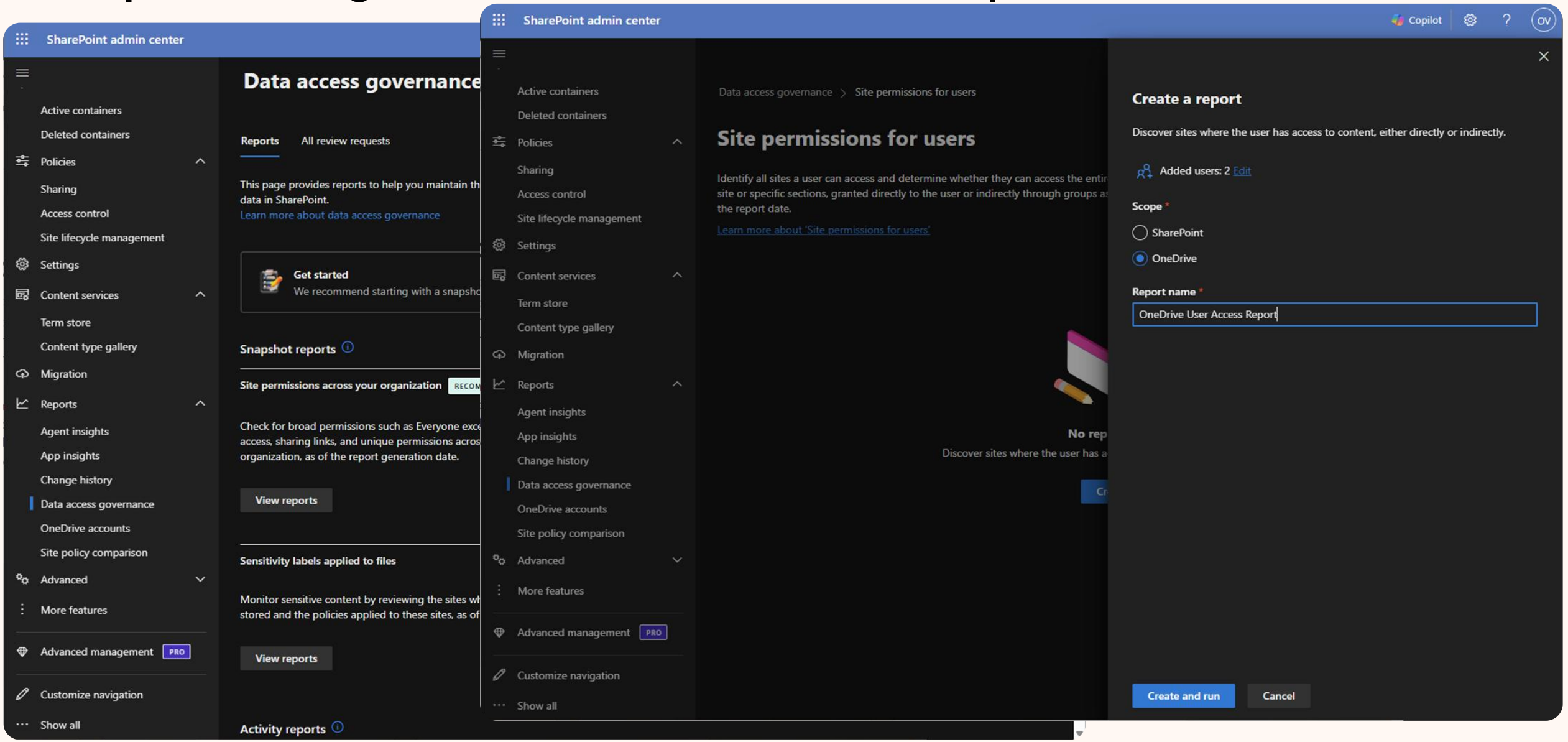
- At least one Copilot License – you have access
- Strong Copilot Readiness toolkit
- Tenant-wide visibility and content insights
- Copilot-ready data governance and quality control



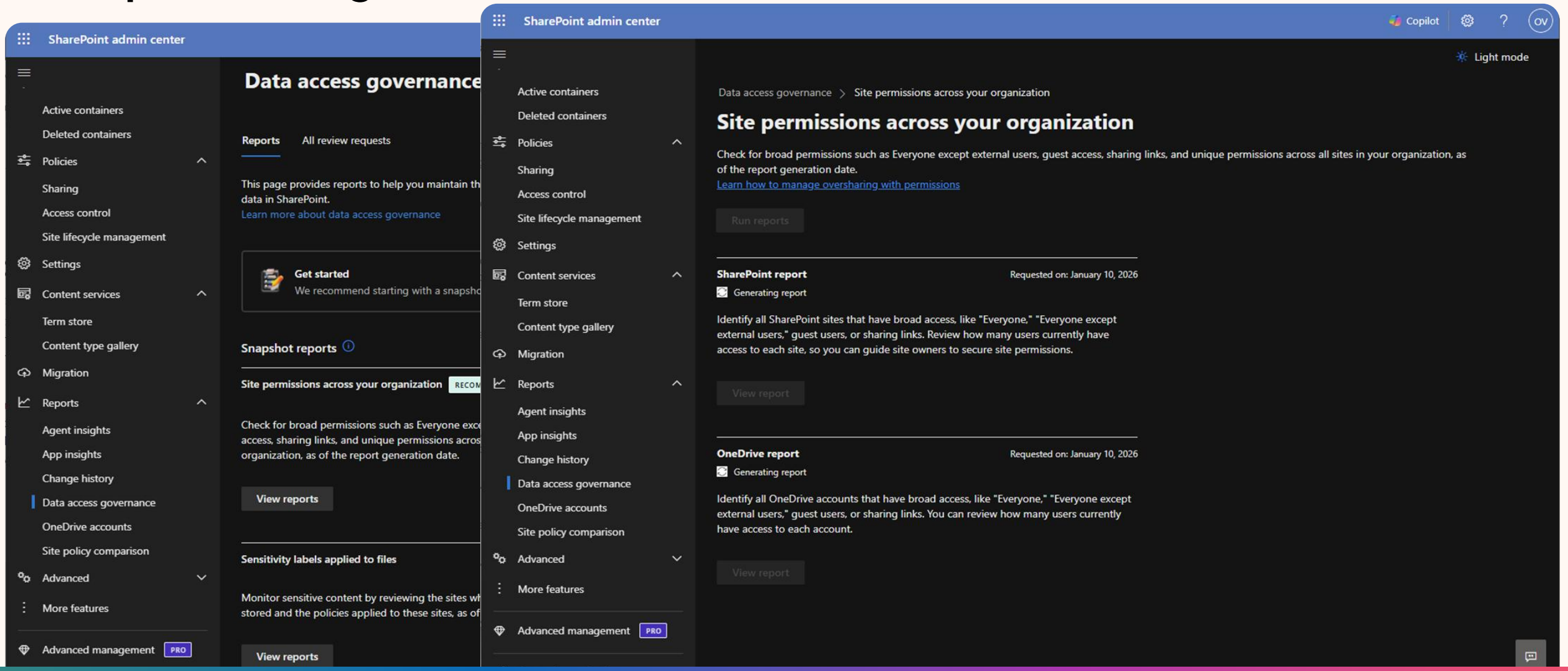
Copilot Settings: SharePoint – Site Level Restrictions



Copilot Settings: SharePoint – User Access Report



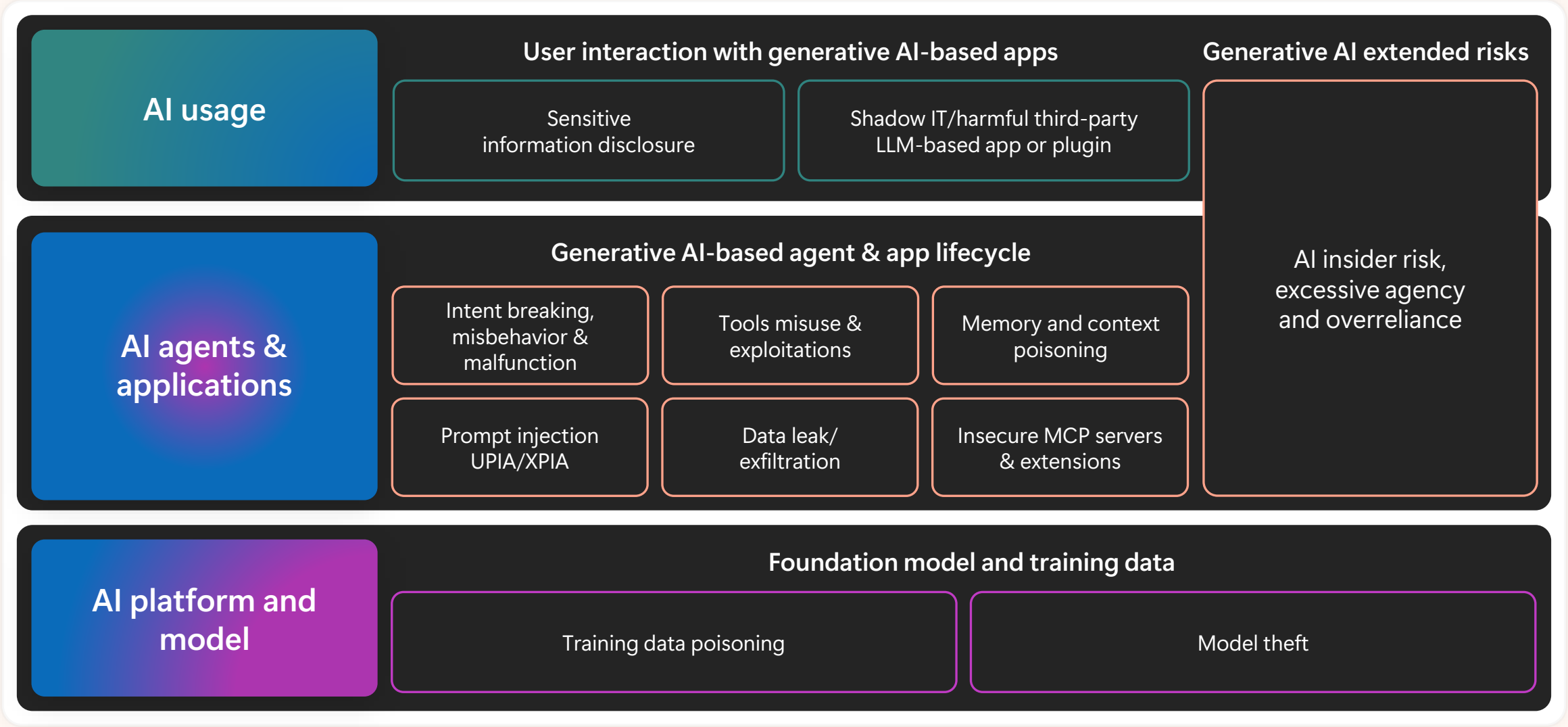
Copilot Settings: SharePoint – Site Permissions



Reports to help identify overshared sites and provide recommended actions to mitigate risks.

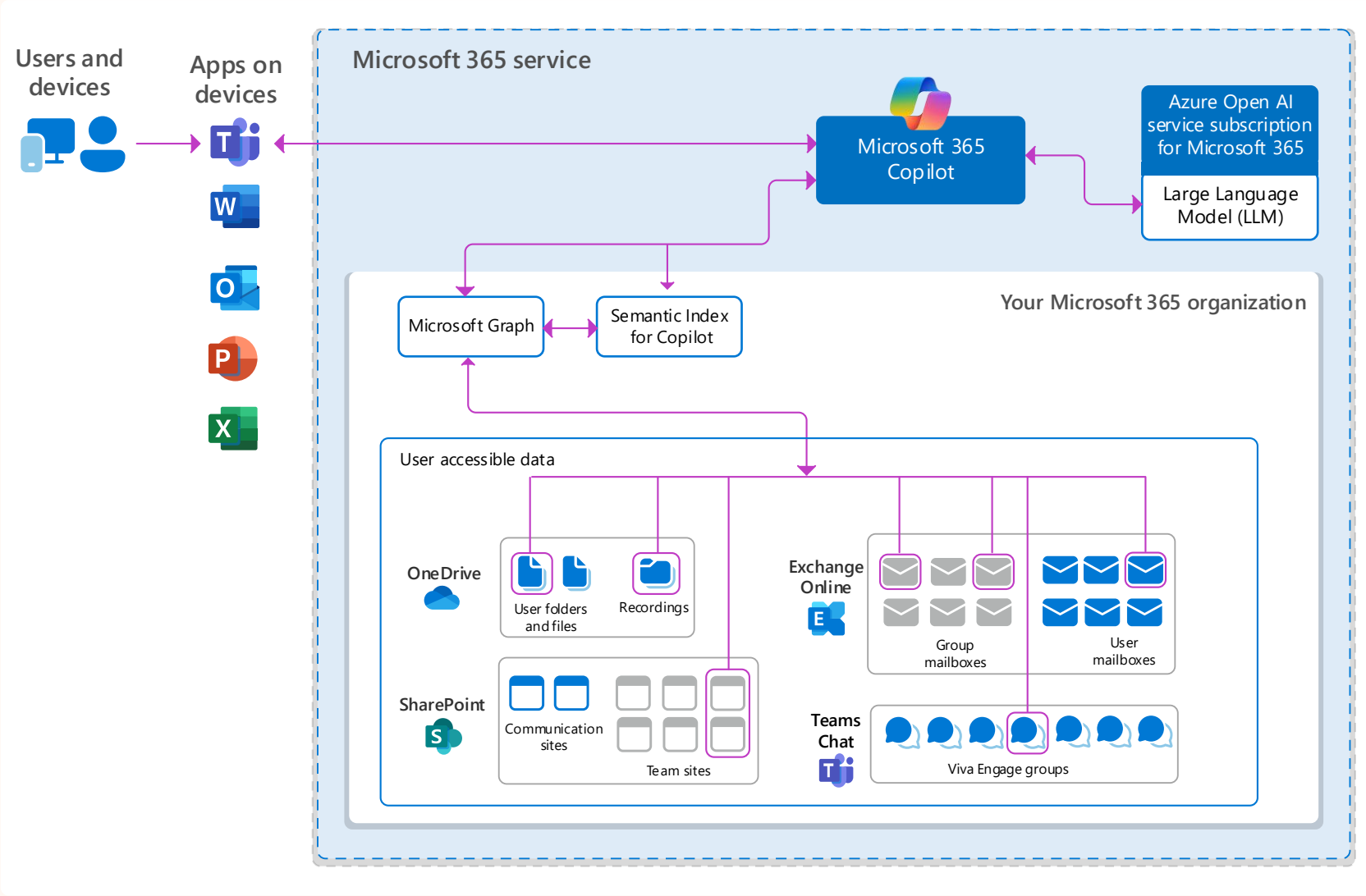
Security Best Practices

Evolving threat map with the rise of (agentic) AI

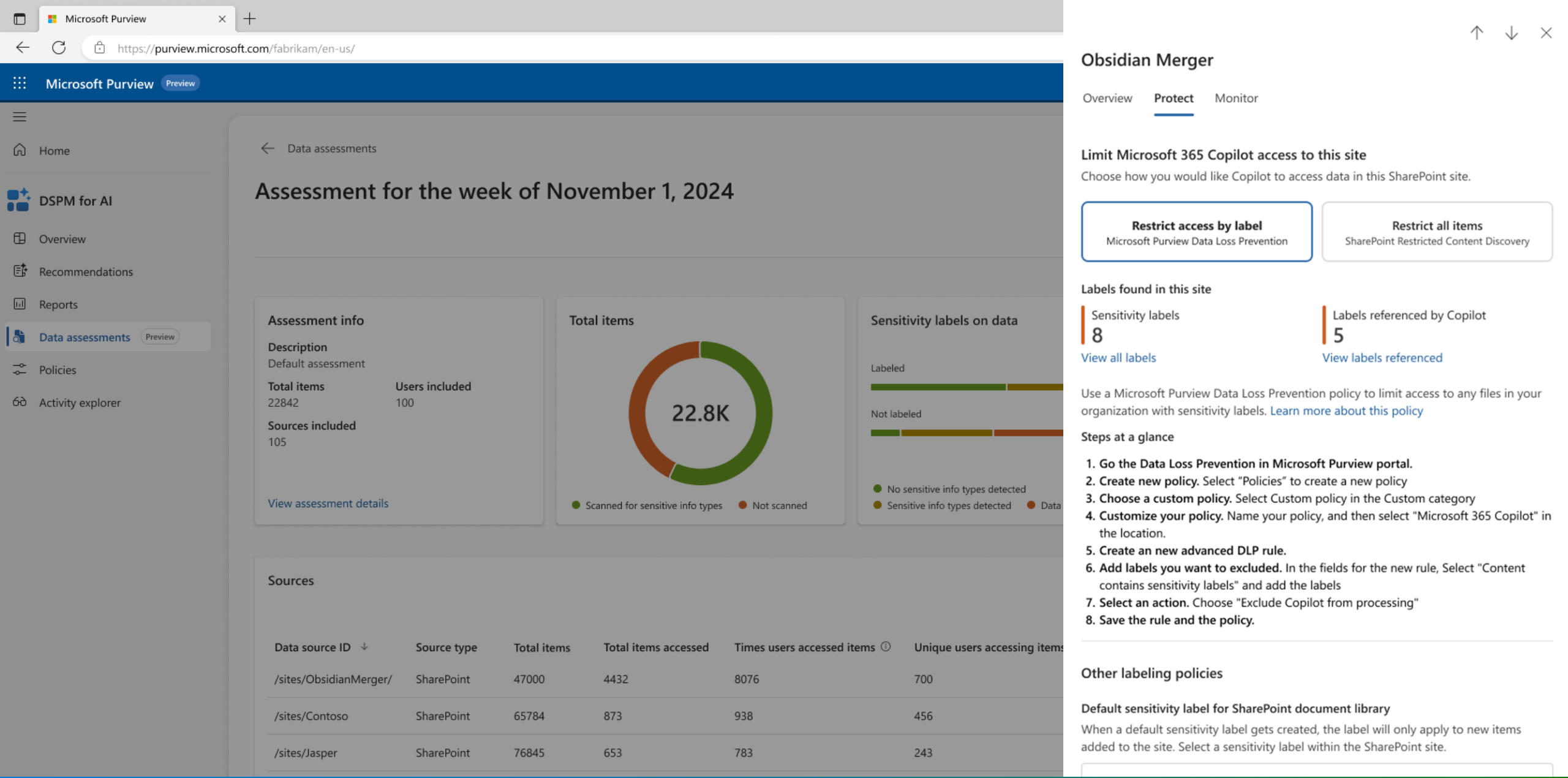


Zero Trust with Microsoft 365 Copilot

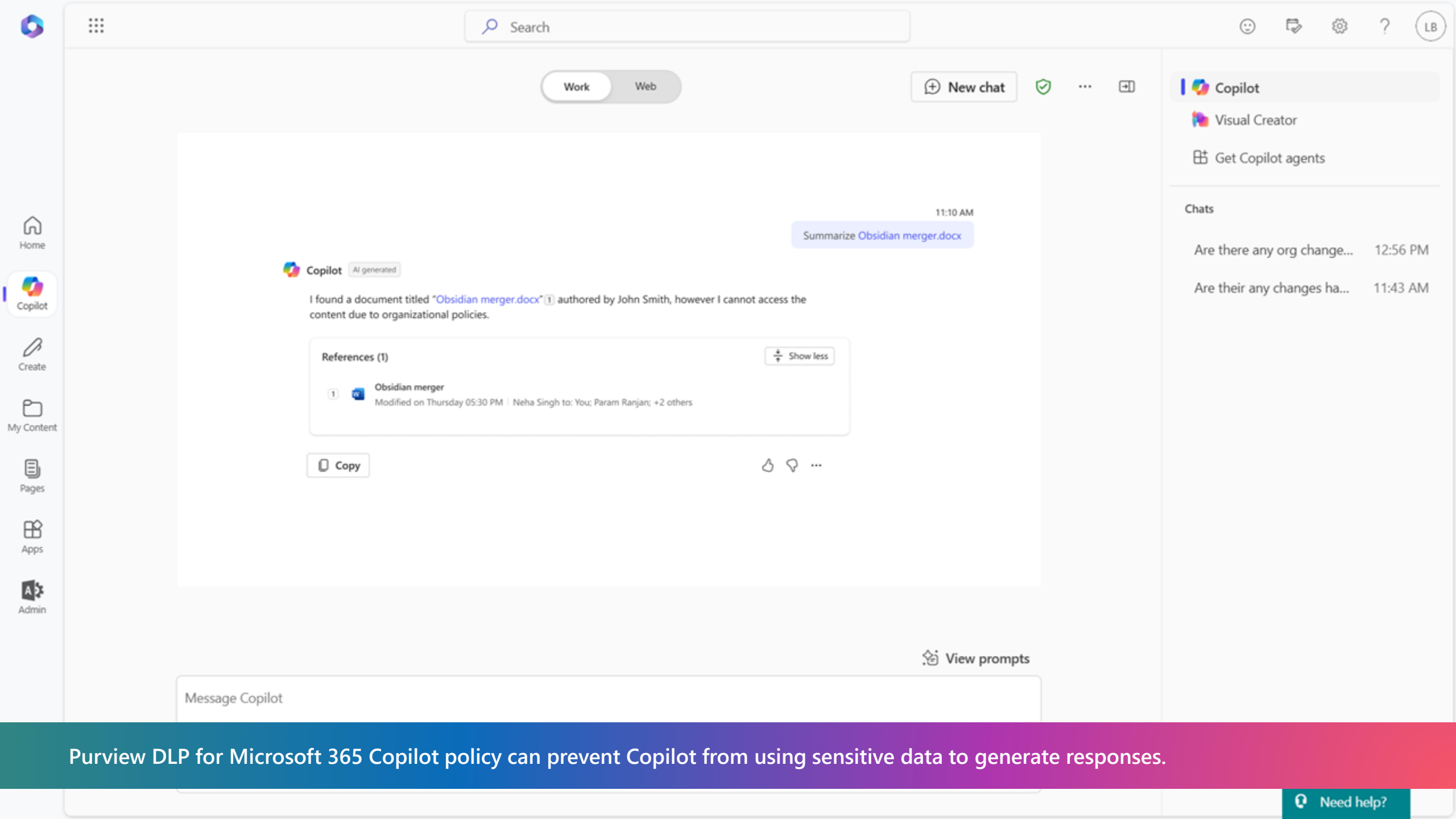
- Data protection
- Identity and access
- App protection
- Device management and protection
- Threat protection
- Secure collaboration with Teams
- User permissions to data



[How do I apply Zero Trust principles to Microsoft 365 Copilot?]



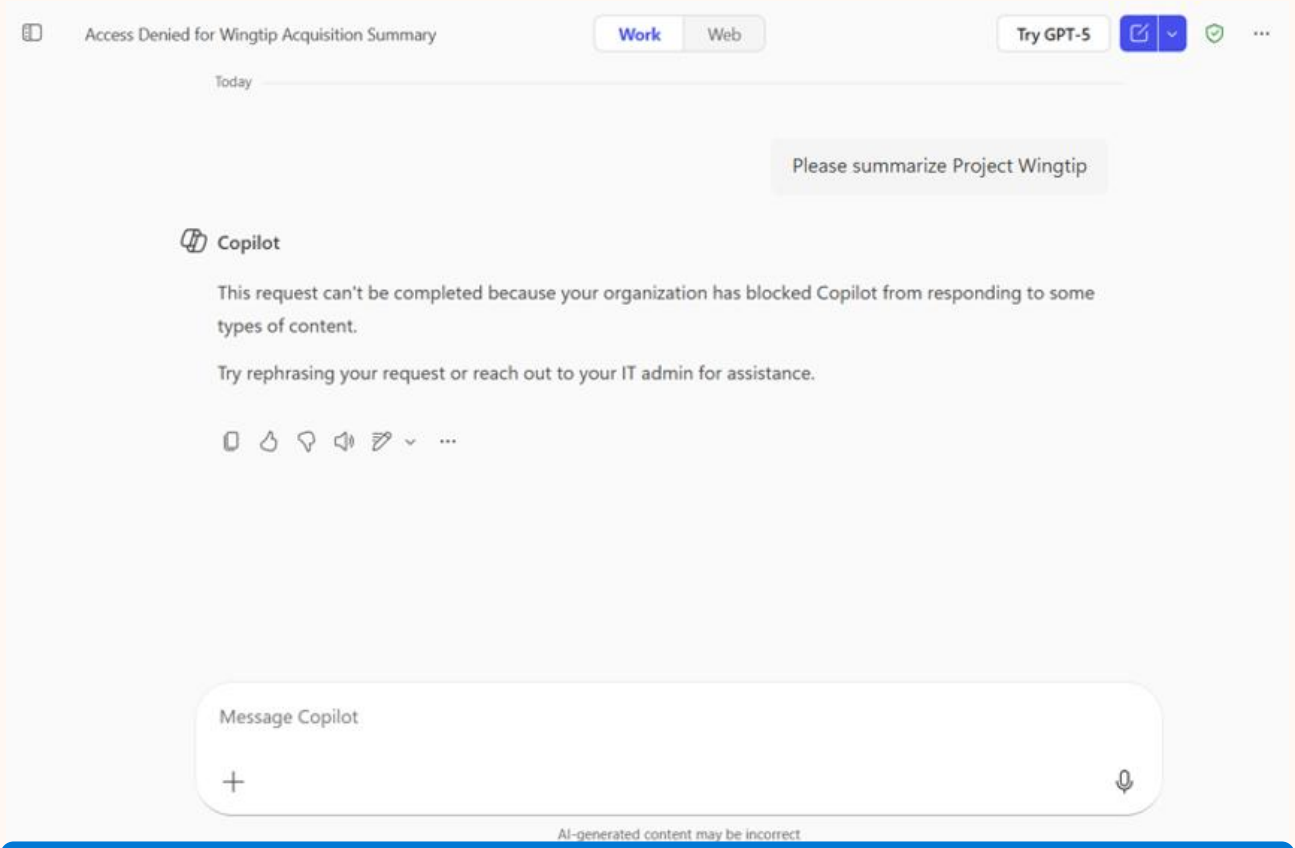
Oversharing assessments help identify overshared sites and content and provide recommended actions to mitigate risks.


Search
LB
Work
Web
New chat
Copilot
Visual Creator
Get Copilot agents
Chats
Are there any org change...
12:56 PM
Are their any changes ha...
11:43 AM
Home
Copilot
Create
My Content
Pages
Apps
Admin
11:10 AM
Summarize Obsidian merger.docx
Copilot
AI generated
I found a document titled "Obsidian merger.docx" 1 authored by John Smith, however I cannot access the content due to organizational policies.
References (1)
Show less
1
Obsidian merger
Modified on Thursday 05:30 PM | Neha Singh to: You; Param Ranjan; +2 others
Copy
View prompts
Message Copilot
Purview DLP for Microsoft 365 Copilot policy can prevent Copilot from using sensitive data to generate responses.
Need help?

Microsoft Purview DLP to safeguard prompts

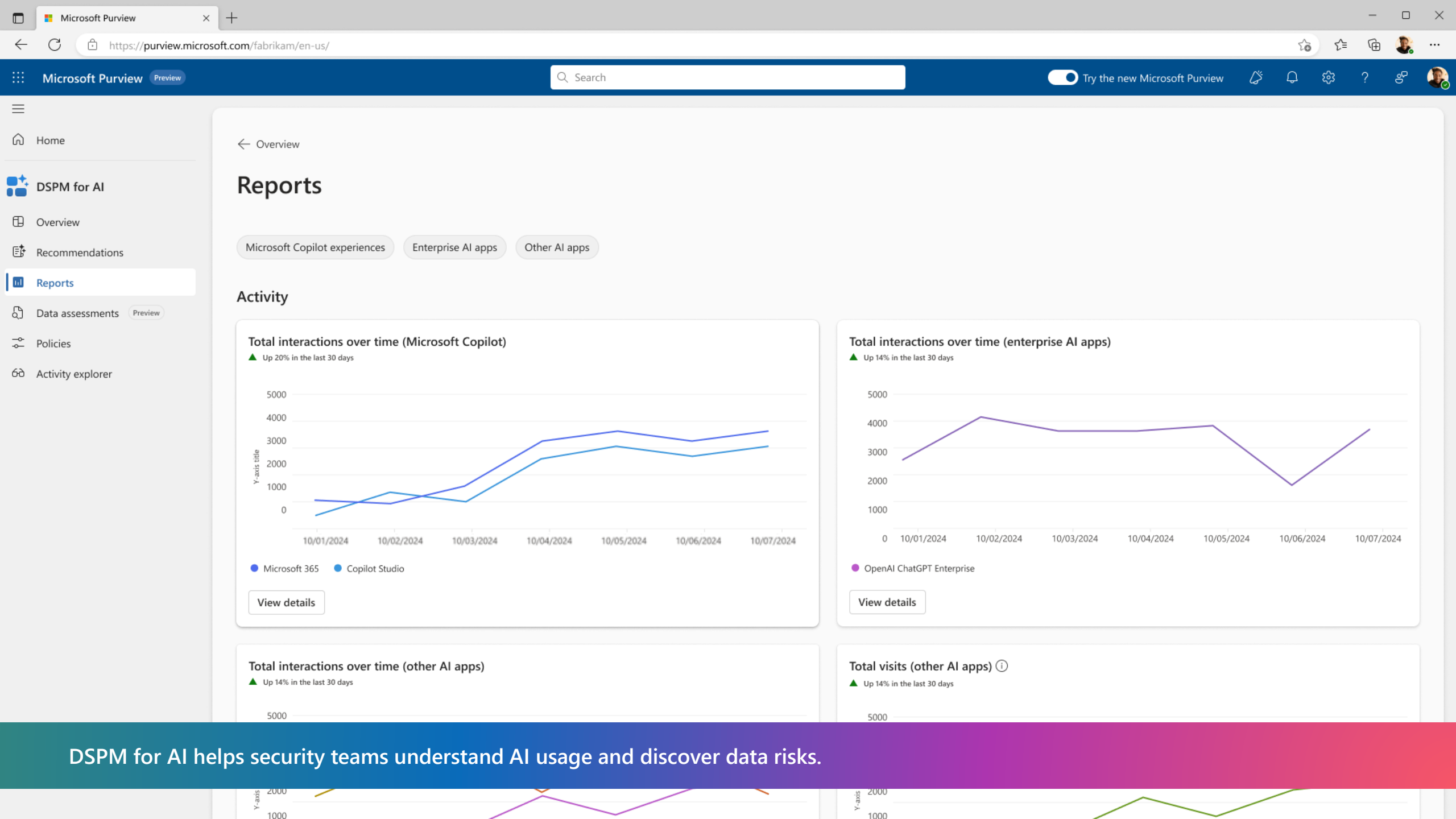
Reduce data leakage and oversharing risks with real-time protection for sensitive data in prompts

- Prevents Copilot from responding to prompts, connecting to internal data sources, and performing web searches, if the prompt contains sensitive data
- Extends to Copilot Chat, M365 Copilot, and agents built in Copilot Studio that are published to Microsoft 365 Channel.



Project Wingtip is on the organization's sensitive information block list

Rollout start to Public Preview Nov 2025

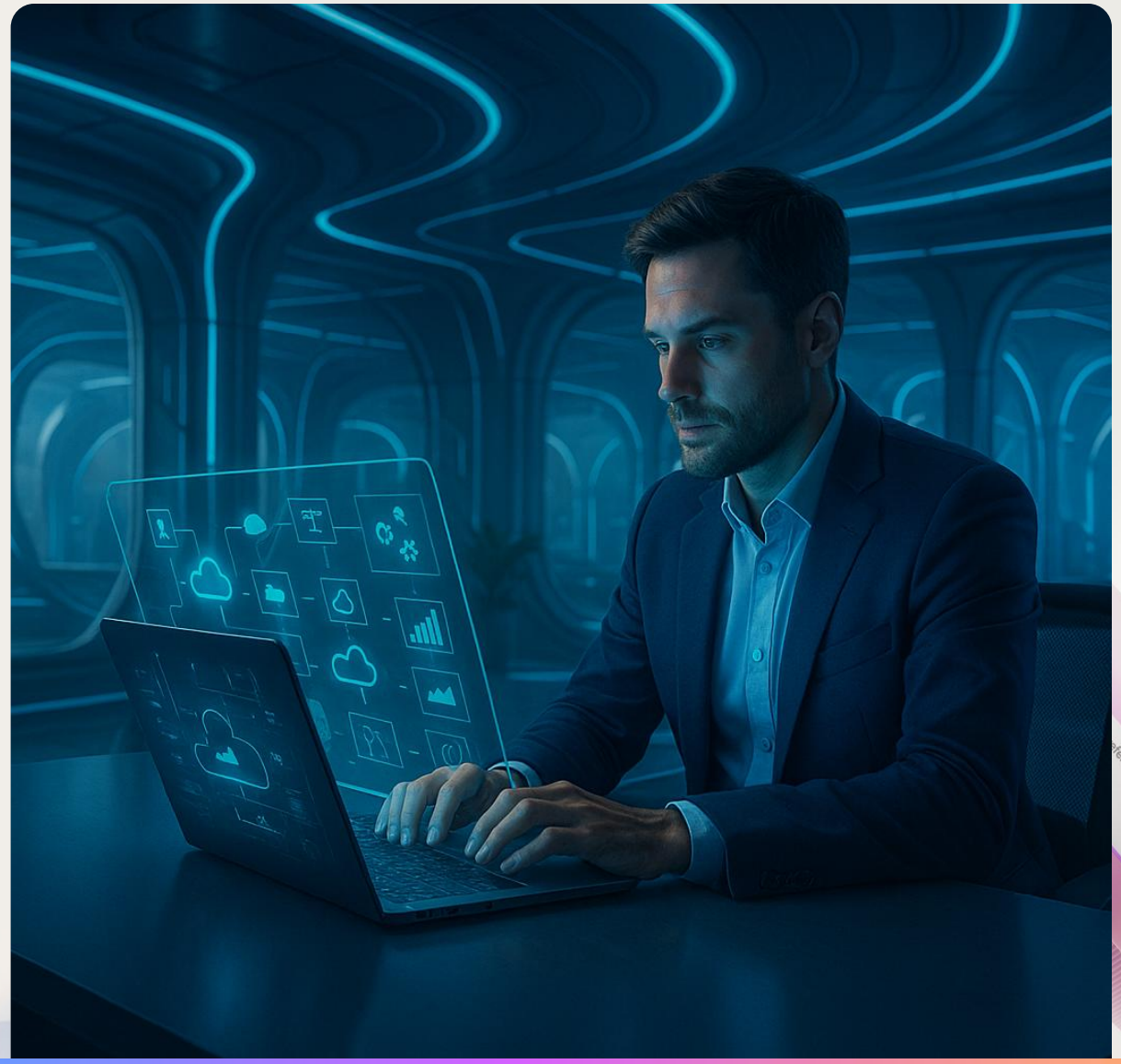

Microsoft Purview
https://purview.microsoft.com/fabrikam/en-us/
Microsoft Purview Preview
Search
Try the new Microsoft Purview
Home
DSPM for AI
Overview
Recommendations
Reports
Data assessments Preview
Policies
Activity explorer
Overview
Reports
Microsoft Copilot experiences
Enterprise AI apps
Other AI apps
Activity
Total interactions over time (Microsoft Copilot)
Up 20% in the last 30 days
5000
4000
3000
2000
1000
0
Y-axis title
10/01/2024
10/02/2024
10/03/2024
10/04/2024
10/05/2024
10/06/2024
10/07/2024
Microsoft 365
Copilot Studio
View details
Total interactions over time (enterprise AI apps)
Up 14% in the last 30 days
OpenAI ChatGPT Enterprise
View details
Total interactions over time (other AI apps)
Up 14% in the last 30 days
Total visits (other AI apps)
Up 14% in the last 30 days
DSPM for AI helps security teams understand AI usage and discover data risks.

Copilot and Purview

Capability or solution in Microsoft Purview	Supported for AI interactions
DSPM for AI (classic) and DSPM (preview)	✓
Auditing	✓
Data classification	✓
Sensitivity labels	✓
Encryption without sensitivity labels	✓
Data loss prevention	✓
Insider Risk Management	✓
Communication compliance	✓
eDiscovery	✓
Data Lifecycle Management	✓
Compliance Manager	✓

https://learn.microsoft.com/en-us/purview/ai-m365-copilot

Copilot Data Privacy and Security



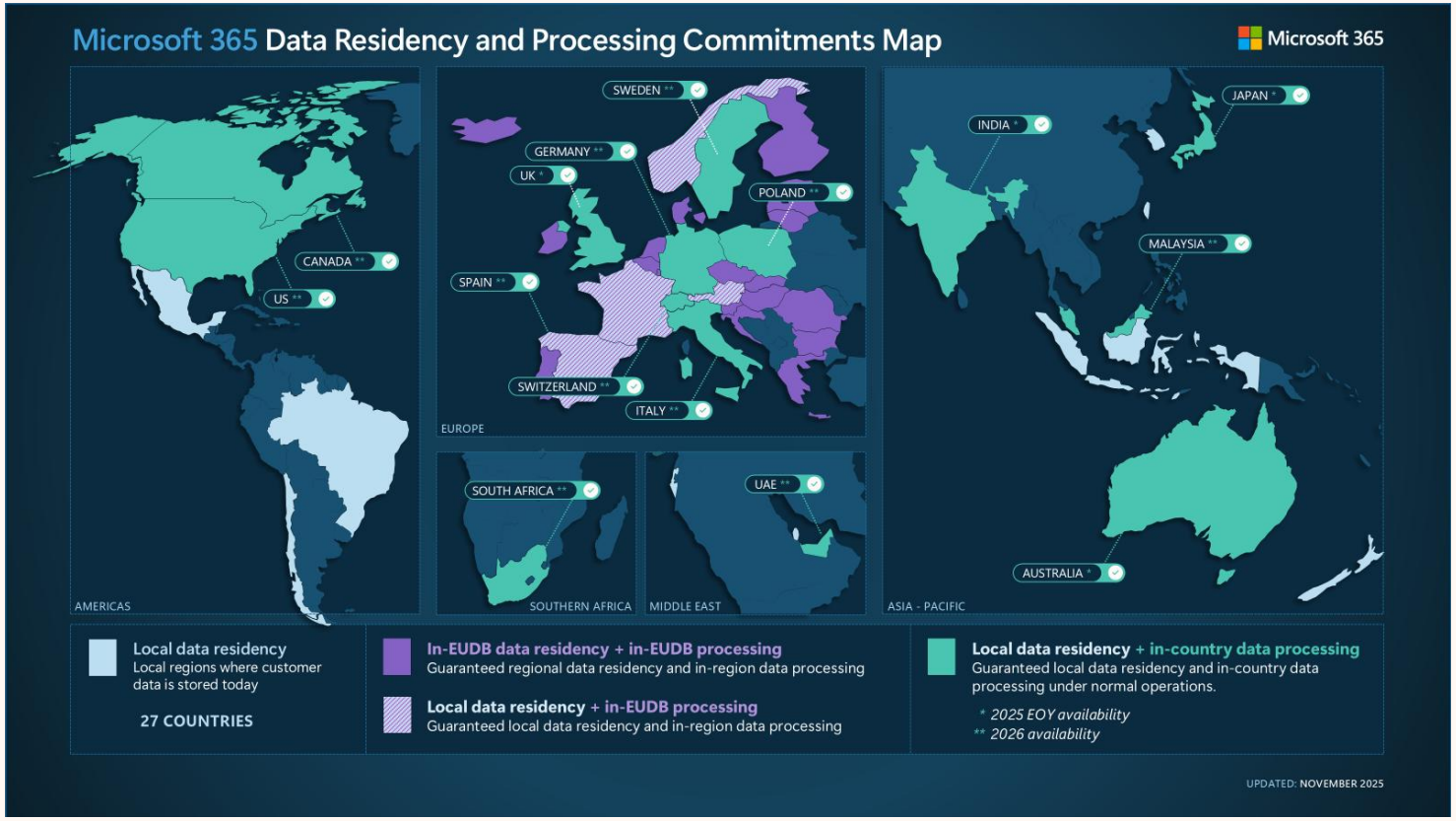
ChatGPT vs Microsoft 365 Copilot Chat

	ChatGPT (Pro)	ChatGPT (Business)	Copilot (Chat & Paid)
Use of data for model training	Data is used unless the user explicitly opts out	Not used. Data may be used for operations, security, and detection	Not used. Data may be used for Microsoft 365 telemetry
Who operates the service	OpenAI	OpenAI	Microsoft
Where the service is operated	Global OpenAI infrastructure. Region not configurable	Global OpenAI infrastructure, no guarantee of a specific region	Azure datacenters in the region of your M365 tenant, within service boundaries
Data residency	Not available. Data may be stored globally	Not available for Business. Data residency only for ChatGPT Ent / Edu	Yes. Governed by Microsoft 365 tenant settings / Preferred Data Location
Security and compliance	Shared multi-tenant OpenAI service	Multi-tenant OpenAI service with data encryption and basic administration	Uses the same identity, encryption, DLP, audit, and compliance controls as M365
Administration and retention	Managed by the end user. Retention governed by OpenAI consumer policies	Managed by workspace admin and users. Retention by OpenAI for Business	Managed by M365 tenant admin. Retention by existing M365 policies

Local Processing for prompts and responses

In-country data handling for secure, compliant Microsoft 365 Copilot experiences

- Process Microsoft 365 Copilot interactions in-country to keep data local and safeguard privacy and integrity.
- Enables compliance for regulated industries by keeping data local and meeting legal requirements.
- Available by end of 2025 customers in Australia, UK, Japan, and India and an additional 11 countries[1] throughout 2026.

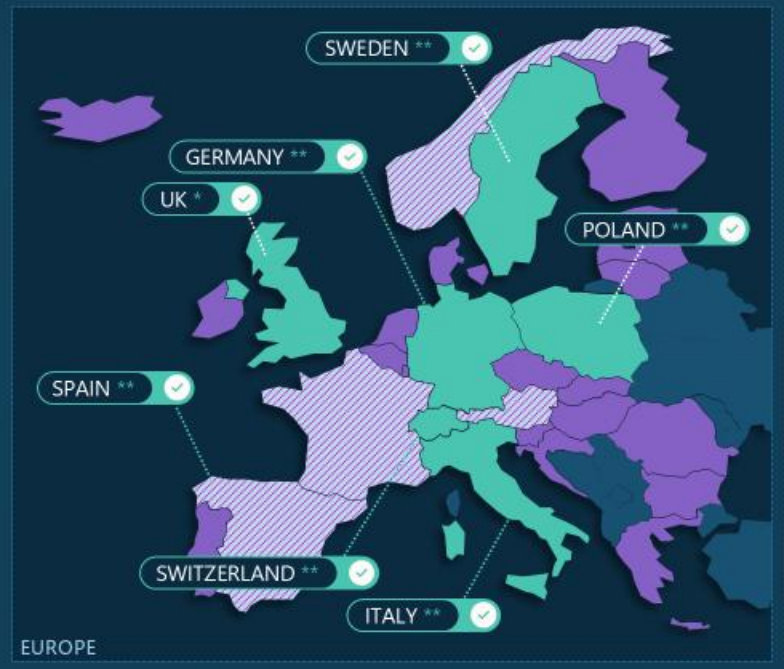


Rollout start Dec 2025

1. UAE, Canada, Germany, Italy, Malaysia, Poland, South Africa, Spain, Sweden, Switzerland, US

Microsoft 365 Data Residency and Processing Commitments Map

Microsoft 365



Local data residency
Local regions where customer data is stored today

27 COUNTRIES

In-EUDB data residency + in-EUDB processing
Guaranteed regional data residency and in-region data processing

Local data residency + in-EUDB processing
Guaranteed local data residency and in-region data processing

Local data residency + in-country data processing
Guaranteed local data residency and in-country data processing under normal operations.

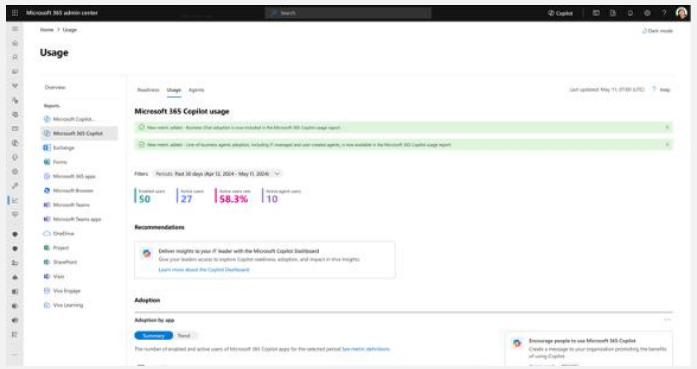
* *2025 EOY availability*
** *2026 availability*

UPDATED: NOVEMBER 2025

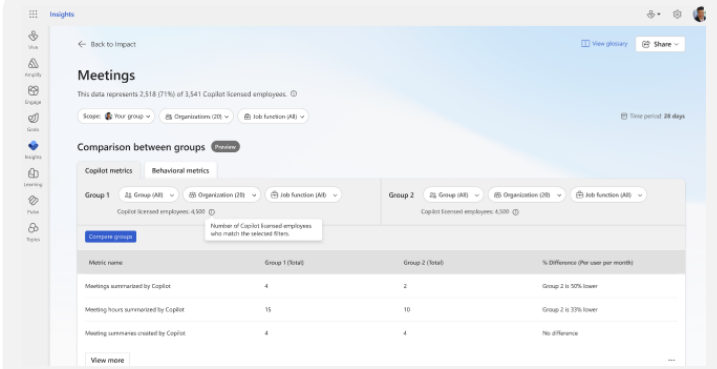
Reporting & Monitoring

Copilot and Agent Analytics

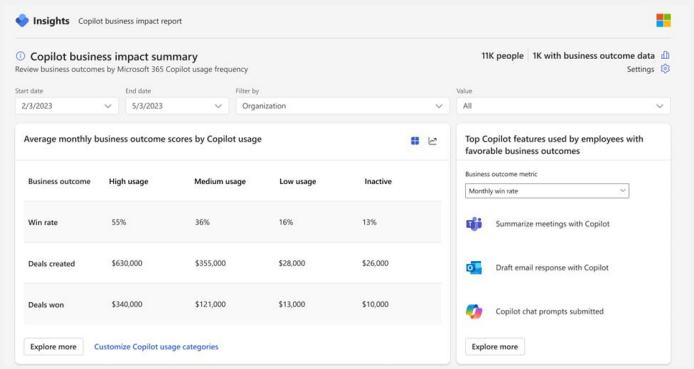
Measure the impact of Copilot and agents on your business



Admin Center



Copilot and Agent Dashboards



Advanced Reporting (Insights)

Usage & Adoption

See Copilot and Agents usage and adoption trends

Impact & Productivity

Explore how AI transforms the way your teams work.

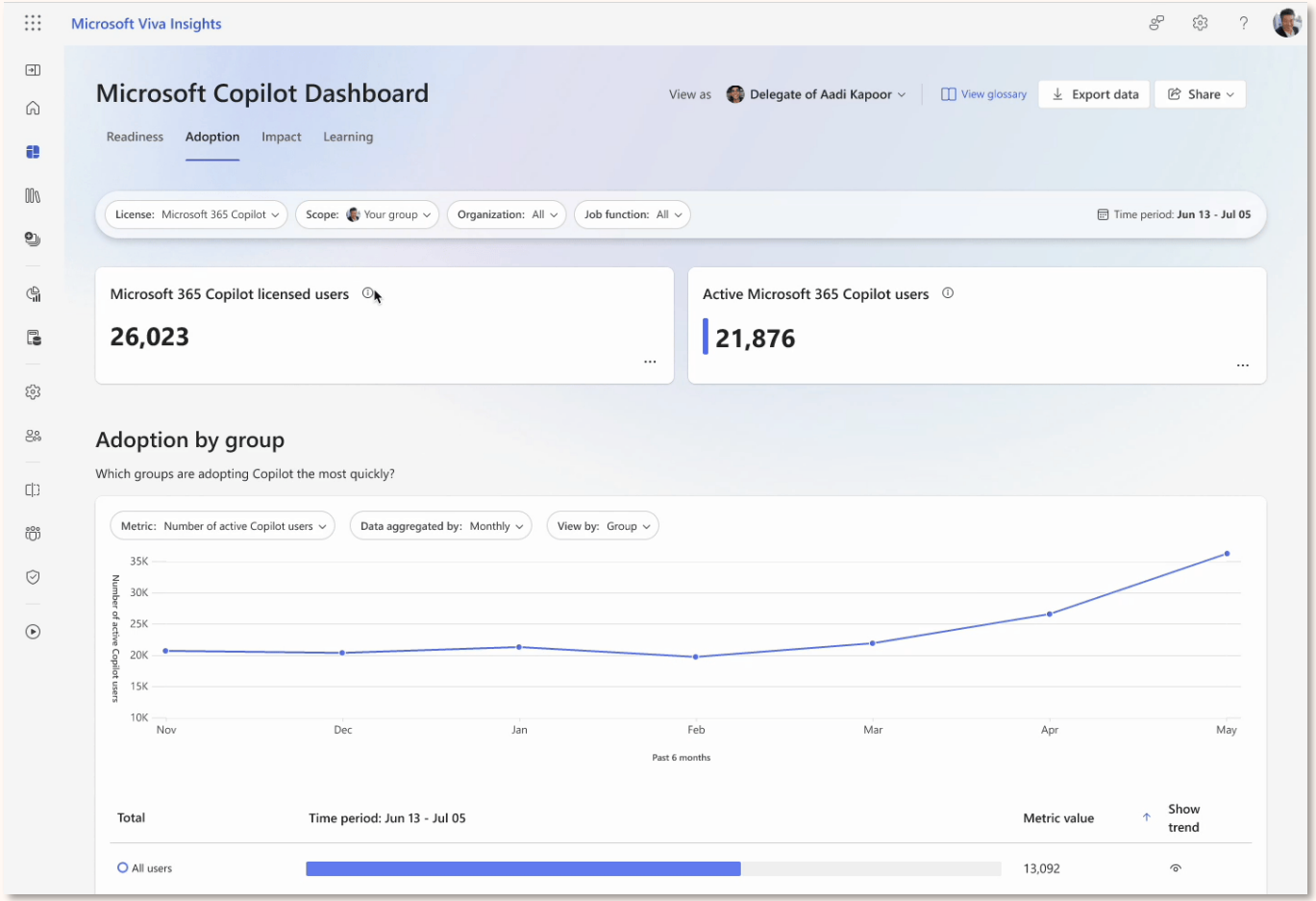
Business value & ROI

Measure the value of Copilot and Agents on your business processes

Copilot Chat reports

Analyze Microsoft 365 Copilot Chat adoption in the Copilot Dashboard

- **View** total users, adoption trends by group, usage intensity, and retention.
- **Understand** how different groups use Copilot Chat across the Microsoft 365 apps.
- **Spot trends and identify top groups** to accelerate adoption by filtering on usage with organizational attributes.



Rollout start to general availability Nov 2025
for customers with 50+ M365 Copilot licenses

Teams Admin Center

Delegate and scale Microsoft Teams administration tasks with dedicated agents

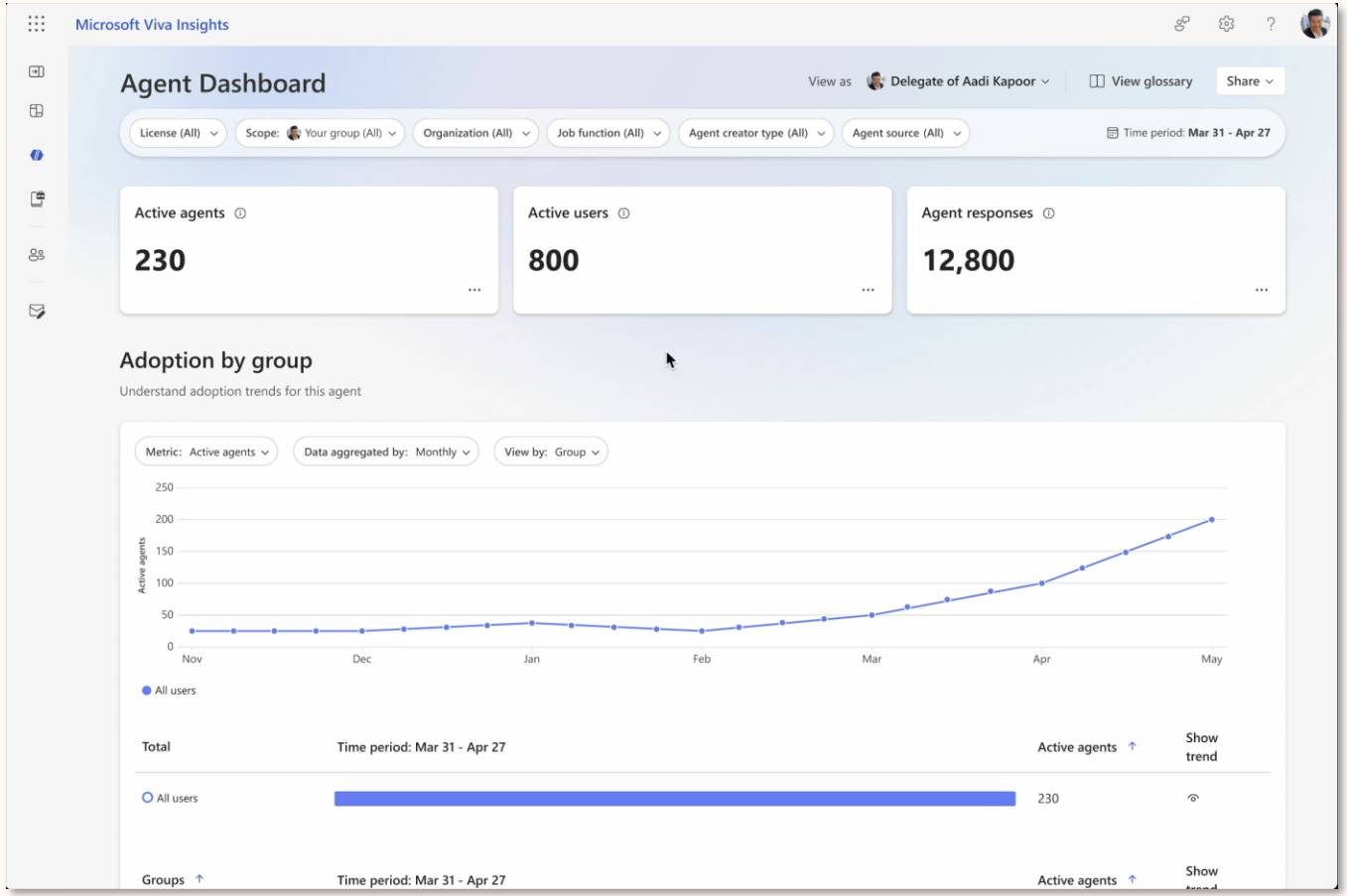
- **Delegate tasks** like meeting monitoring and scale your expertise.
- **Stay in control** while the agents accomplish the tasks autonomously and securely.
- **Focus on what matters most** with intelligent prioritization and remediate issues **proactively**.

Rollout starts to Teams Admin Center (TAP) Nov 2025

Agent Dashboard

Measure the adoption and impact of agents across your organization

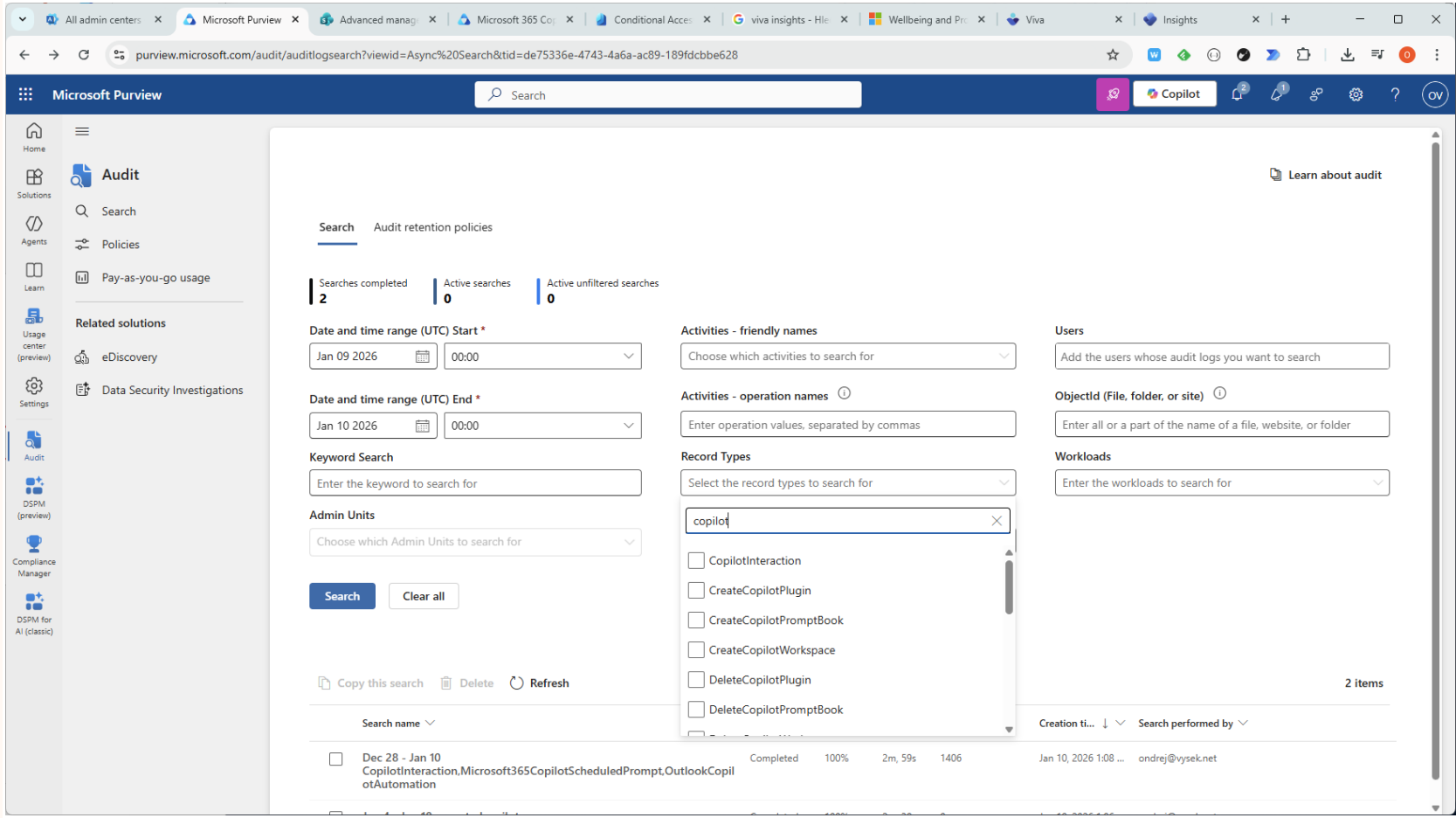
- View **performance metrics for all agents**, including your custom-built agents, Microsoft agents, and third-party agents.
- **Understand agent adoption trends** across teams, functions, and more.
- **Identify** your most popular agents and **dive deeper** into how **specific agents are used**.



Rollout start to Public Preview Jan 2026 Rollout start to worldwide Feb 2026

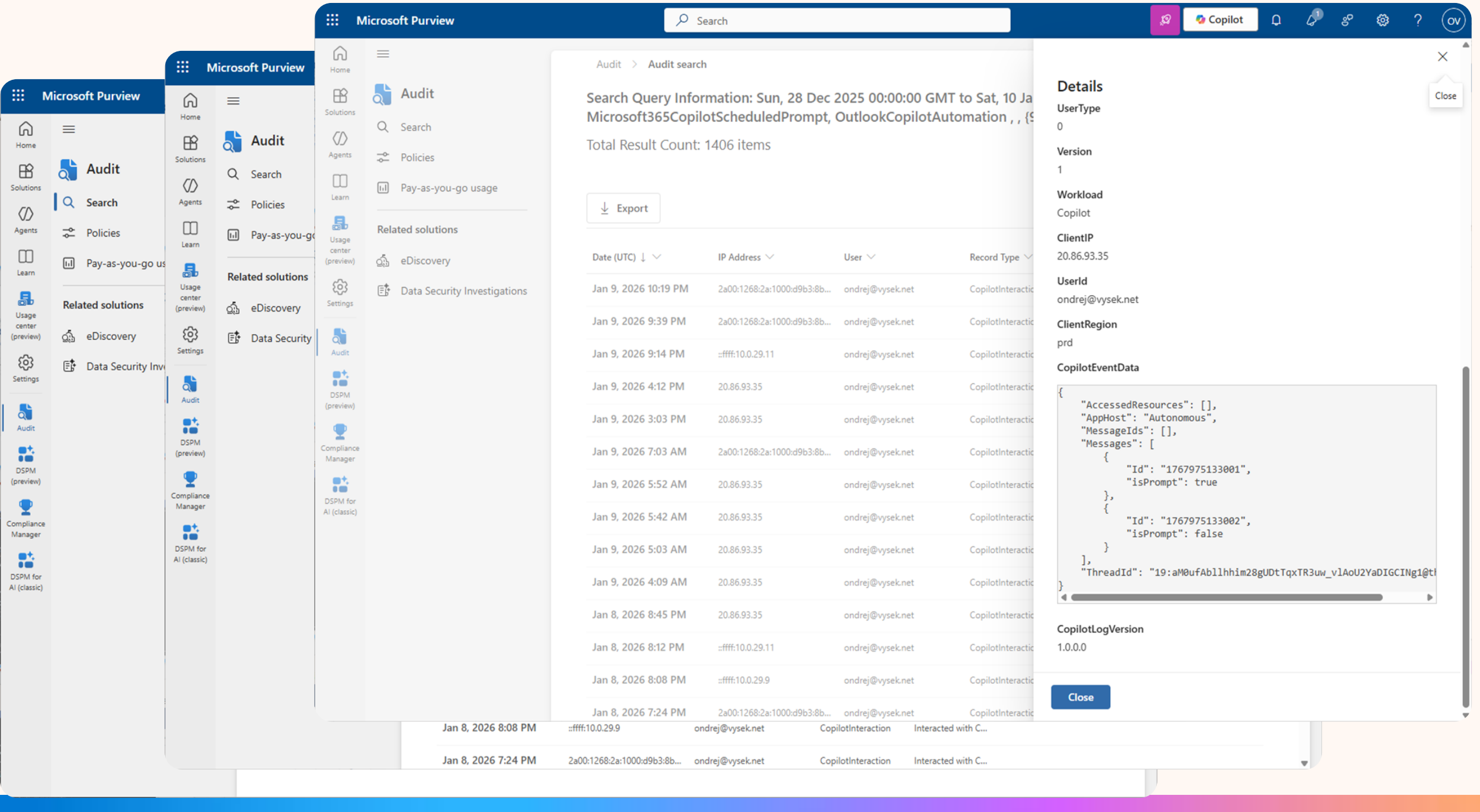
Audit logs for Copilot and AI applications

- Copilot User interaction and admin activities are part of Audit Standard
- Non-Microsoft AI applications are billed pay-as-you-go

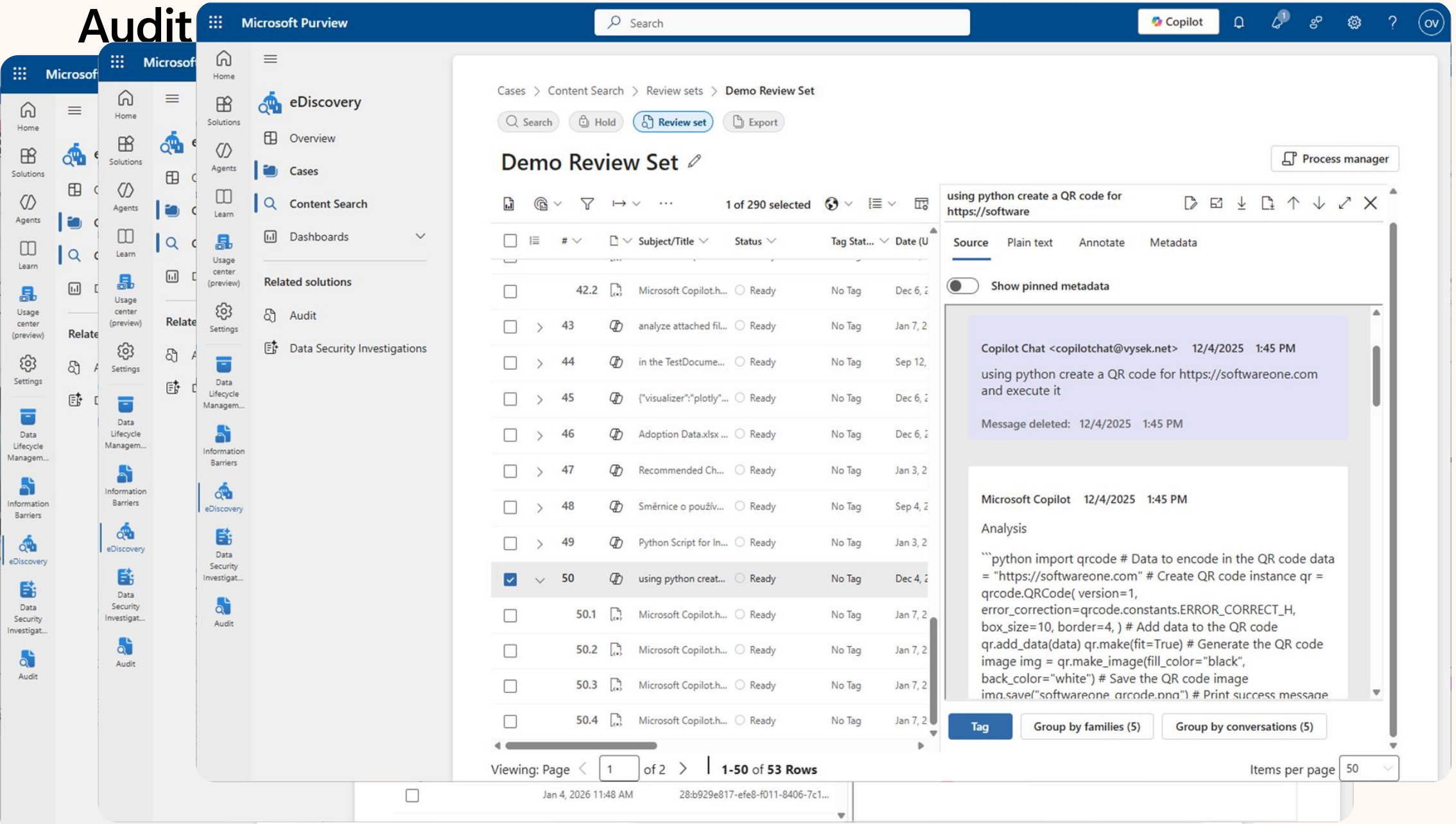


[Audit logs for Copilot and AI applications]

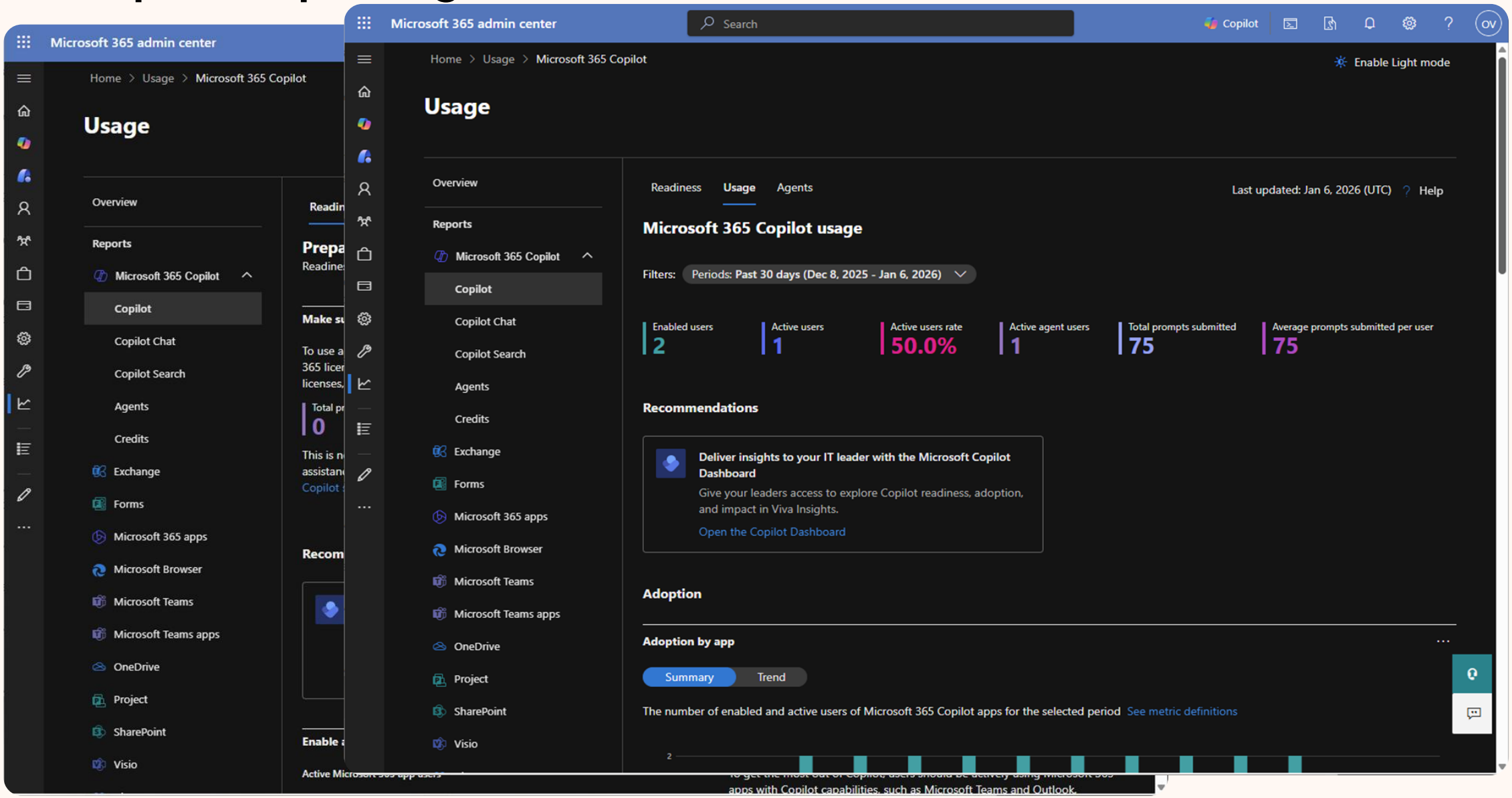
[Auditing solutions in Microsoft Purview]


Microsoft Purview
Search
Copilot
Audit
Search
Policies
Pay-as-you-go usage
Related solutions
eDiscovery
Data Security Investigations
Audit > Audit search
Search Query Information: Sun, 28 Dec 2025 00:00:00 GMT to Sat, 10 Ja
Microsoft365CopilotScheduledPrompt, OutlookCopilotAutomation , , {9
Total Result Count: 1406 items
Export
Date (UTC)
IP Address
User
Record Type
Jan 9, 2026 10:19 PM 2a00:1268:2a:1000:d9b3:8b... ondrej@vysek.net CopilotInteractic
Jan 9, 2026 9:39 PM 2a00:1268:2a:1000:d9b3:8b... ondrej@vysek.net CopilotInteractic
Jan 9, 2026 9:14 PM ::ffff:10.0.29.11 ondrej@vysek.net CopilotInteractic
Jan 9, 2026 4:12 PM 20.86.93.35 ondrej@vysek.net CopilotInteractic
Jan 9, 2026 3:03 PM 20.86.93.35 ondrej@vysek.net CopilotInteractic
Jan 9, 2026 7:03 AM 2a00:1268:2a:1000:d9b3:8b... ondrej@vysek.net CopilotInteractic
Jan 9, 2026 5:52 AM 20.86.93.35 ondrej@vysek.net CopilotInteractic
Jan 9, 2026 5:42 AM 20.86.93.35 ondrej@vysek.net CopilotInteractic
Jan 9, 2026 5:03 AM 20.86.93.35 ondrej@vysek.net CopilotInteractic
Jan 9, 2026 4:09 AM 20.86.93.35 ondrej@vysek.net CopilotInteractic
Jan 8, 2026 8:45 PM 20.86.93.35 ondrej@vysek.net CopilotInteractic
Jan 8, 2026 8:12 PM ::ffff:10.0.29.11 ondrej@vysek.net CopilotInteractic
Jan 8, 2026 8:08 PM ::ffff:10.0.29.9 ondrej@vysek.net CopilotInteractic
Jan 8, 2026 7:24 PM 2a00:1268:2a:1000:d9b3:8b... ondrej@vysek.net CopilotInteractic
Details
UserType
0
Version
1
Workload
Copilot
ClientIP
20.86.93.35
UserId
ondrej@vysek.net
ClientRegion
prd
CopilotEventData
{
"AccessedResources": [],
"AppHost": "Autonomous",
"MessageIds": [],
"Messages": [
{
"Id": "1767975133001",
"isPrompt": true
},
{
"Id": "1767975133002",
"isPrompt": false
}
],
"ThreadId": "19:aM0ufAbllhhim28gUDtTqxTR3uw_vlAoU2YaDIGCINg1@t
}
CopilotLogVersion
1.0.0.0
Close
Jan 8, 2026 8:08 PM ::ffff:10.0.29.9 ondrej@vysek.net CopilotInteraction Interacted with C...
Jan 8, 2026 7:24 PM 2a00:1268:2a:1000:d9b3:8b... ondrej@vysek.net CopilotInteraction Interacted with C...

Audit


Microsoft Purview
Search
Copilot
Home
Solutions
Agents
Learn
Usage center (preview)
Settings
Data Lifecycle Managem...
Information Barriers
eDiscovery
Data Security Investigat...
Audit
eDiscovery
Overview
Cases
Content Search
Dashboards
Related solutions
Audit
Data Security Investigations
Cases > Content Search > Review sets > Demo Review Set
Search
Hold
Review set
Export
Demo Review Set
Process manager
1 of 290 selected
using python create a QR code for https://software
Source
Plain text
Annotate
Metadata
Show pinned metadata
Copilot Chat <copilotchat@vysek.net> 12/4/2025 1:45 PM
using python create a QR code for https://softwareone.com and execute it
Message deleted: 12/4/2025 1:45 PM
Microsoft Copilot 12/4/2025 1:45 PM
Analysis
```python import qrcode # Data to encode in the QR code data = "https://softwareone.com" # Create QR code instance qr = qrcode.QRCode( version=1, error_correction=qrcode.constants.ERROR_CORRECT_H, box_size=10, border=4, ) # Add data to the QR code qr.add_data(data) qr.make(fit=True) # Generate the QR code image img = qr.make_image(fill_color="black", back_color="white") # Save the QR code image
Subject/Title
Status
Tag Stat...
Date (U
42.2 Microsoft Copilot.h... Ready No Tag Dec 6, 2
43 analyze attached fil... Ready No Tag Jan 7, 2
44 in the TestDocume... Ready No Tag Sep 12,
45 {"visualizer":"plotly"... Ready No Tag Dec 6, 2
46 Adoption Data.xlsx ... Ready No Tag Dec 6, 2
47 Recommended Ch... Ready No Tag Jan 3, 2
48 Směrnice o použív... Ready No Tag Sep 4, 2
49 Python Script for In... Ready No Tag Jan 3, 2
50 using python creat... Ready No Tag Dec 4, 2
50.1 Microsoft Copilot.h... Ready No Tag Jan 7, 2
50.2 Microsoft Copilot.h... Ready No Tag Jan 7, 2
50.3 Microsoft Copilot.h... Ready No Tag Jan 7, 2
50.4 Microsoft Copilot.h... Ready No Tag Jan 7, 2
Tag
Group by families (5)
Group by conversations (5)
Viewing: Page 1 of 2
1-50 of 53 Rows
Items per page 50
Jan 4, 2026 11:48 AM
28:b929e817-efe8-f011-8406-7c1...
```

Copilot Reporting: Basics



Advanced Copilot analysis with Viva Insights

Viva Insights customers can use **analyst workbench** capabilities to dive deeper with custom reports, including incorporating data from other relevant sources.

For a limited time only, Copilot for Microsoft 365 customers will be eligible for a promotional offer that will provide access to all of Viva Insights, including Copilot Dashboard, as well as access to advanced insights and manager and leader insights.

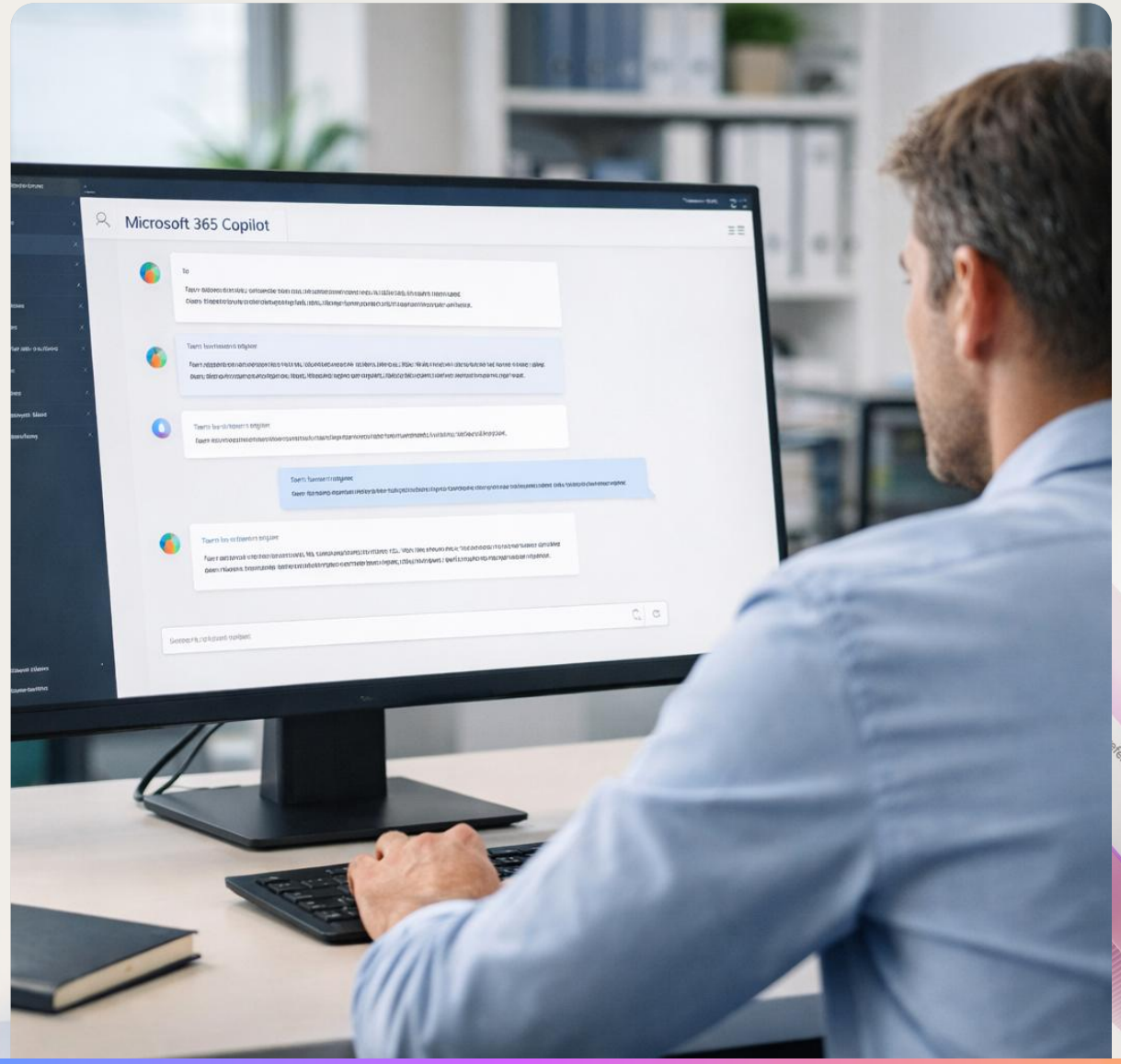
Copilot Dashboard features and capabilities		License requirement		
		Microsoft or Office 365	Copilot for Microsoft or Office 365*	Viva Insights**
Readiness	Tenant level visibility into Copilot eligibility, licensing, and activation status.	●	●	●
	Microsoft 365 app usage and supporting research to help assess potential impact.	●	●	●
Adoption	Visibility into adoption trends, such how many people are using Copilot, in which apps, and in what ways.		●	●
	Apply scopes and filters to adoption trend reports for deeper organizational views.		●	●
	Tailorable advanced capabilities to create custom reports for additional visibility into adoption trends.			●
Impact	Understand the impact of using key Copilot features on key metrics and workplace behaviors.		●	●
	Apply scopes and filters to compare Copilot usage and key workplace metrics between groups of Copilot users and between Copilot users and non-Copilot users.		●	●
	Tailorable advanced capabilities to create custom reports for additional visibility into Copilot impact and return on investment.			●
Sentiment	Tenant level visibility into employee feedback about the value and benefits of Copilot.		●	●
	Visibility into how Copilot user sentiment differs across teams (heatmap).			●
Learning	Research and best practices to help throughout the AI journey.	●	●	●
Egress	Ability to export Copilot data via Microsoft 365 Reporting Graph APIs.		●	●
	Ability to export Copilot data via Viva Insights Analyst Workbench.			●

* Copilot Dashboard will be included in the Copilot for M365 SKU/service plan (Starting FY25 Q1)

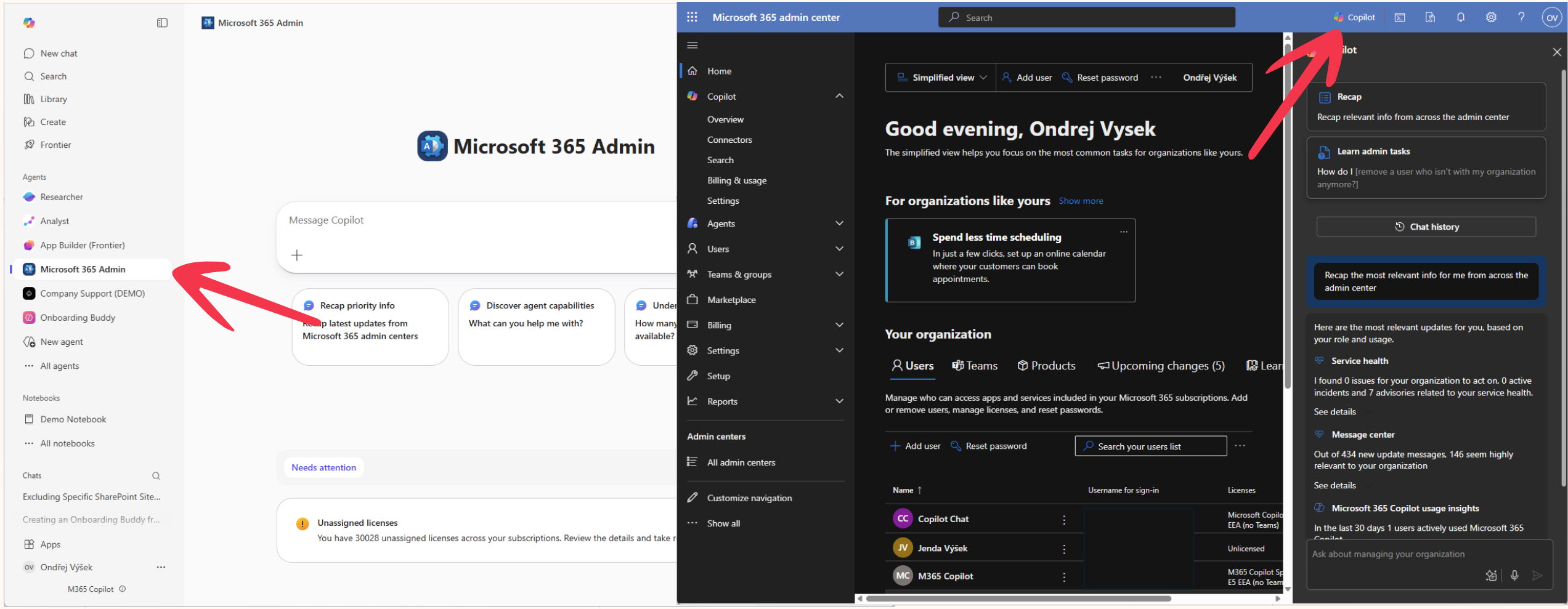
** Viva Insights, Workplace Analytics and Employee Feedback, or Viva Suite SKUs

Microsoft 365 Copilot for admin center

[Copilot in Microsoft 365 Admin Centers]



Copilot for admins in Microsoft 365 admin centers



Copilot for admins – Sample prompts (read only)

Recap

- Recap relevant info from across the admin center

Get Help

- How do I view Copilot usage across my organization?
- How do I restore a deleted user?
- How do I set up multifactor authentication?

Service Health

- Show me the health of Teams?
- Are there any service issues right now?

Licensing Information

- Show me users without a Copilot license?
- How many Copilot licenses are available?
- What available licenses I have - format table

Search

- Show me users in Australia with an assigned Teams license?
- Identify all groups in my organization with an owner.
- Show me all the users who are not using Copilot in the last 30 days.

Teams

- Search and return a list of all policies where the meeting recording is turned Off.
- Analyze the call quality of for their meeting with Meeting ID. Were there any quality issues?
- List the most common quality issues in meetings for the last 30 days.

SharePoint

- Find sites with external sharing on

M365 Copilot Agents

AI agents are **software systems** that use AI to pursue goals and complete tasks on behalf of users.

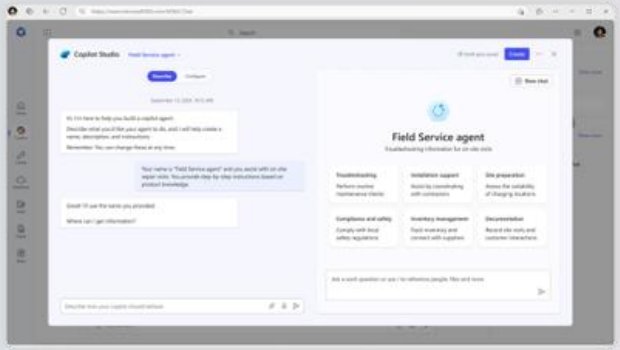
The Set-and-Forget approach is not the right one; AI agents need to be monitored and maintained.

A range of tools for agent creation

No code

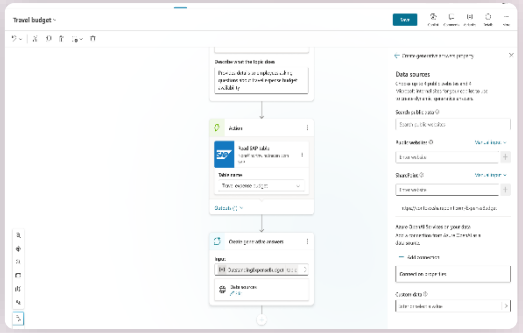
Pro code

For end users



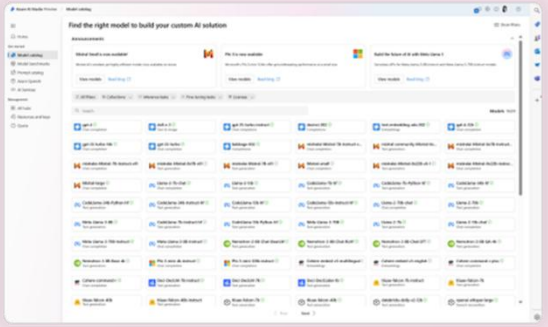
Copilot Studio
Lite

For makers



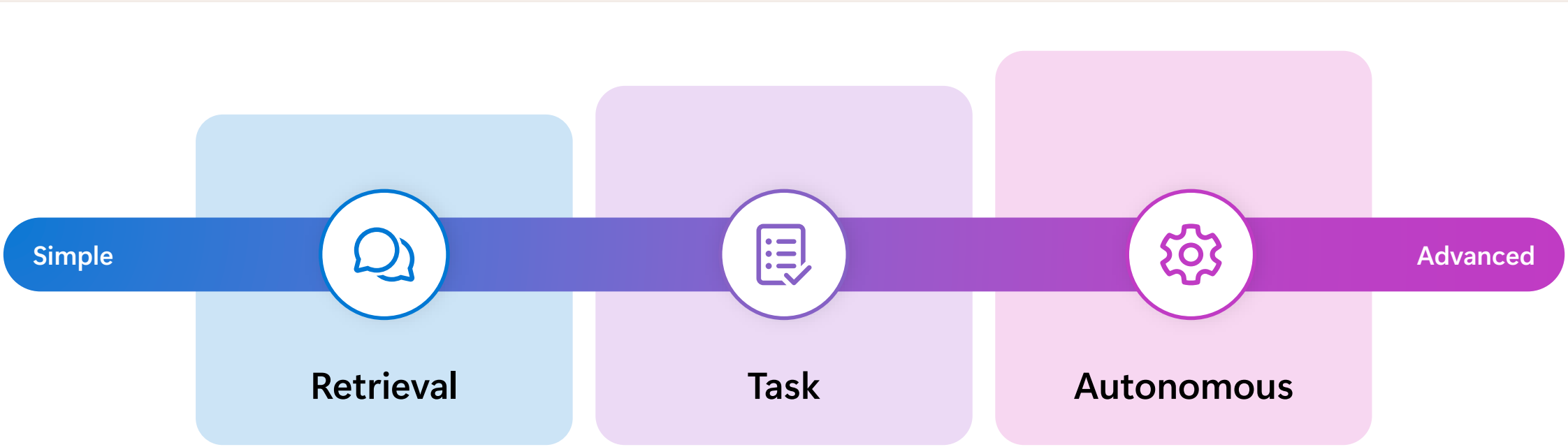
Copilot Studio
Full

For developers



VS Code, Copilot Studio,
Azure AI Foundry

View agent starters and scenarios based the level of agent complexity. Ranging from Simple → Advanced.



Agents vary complexity and capabilities depending on your need

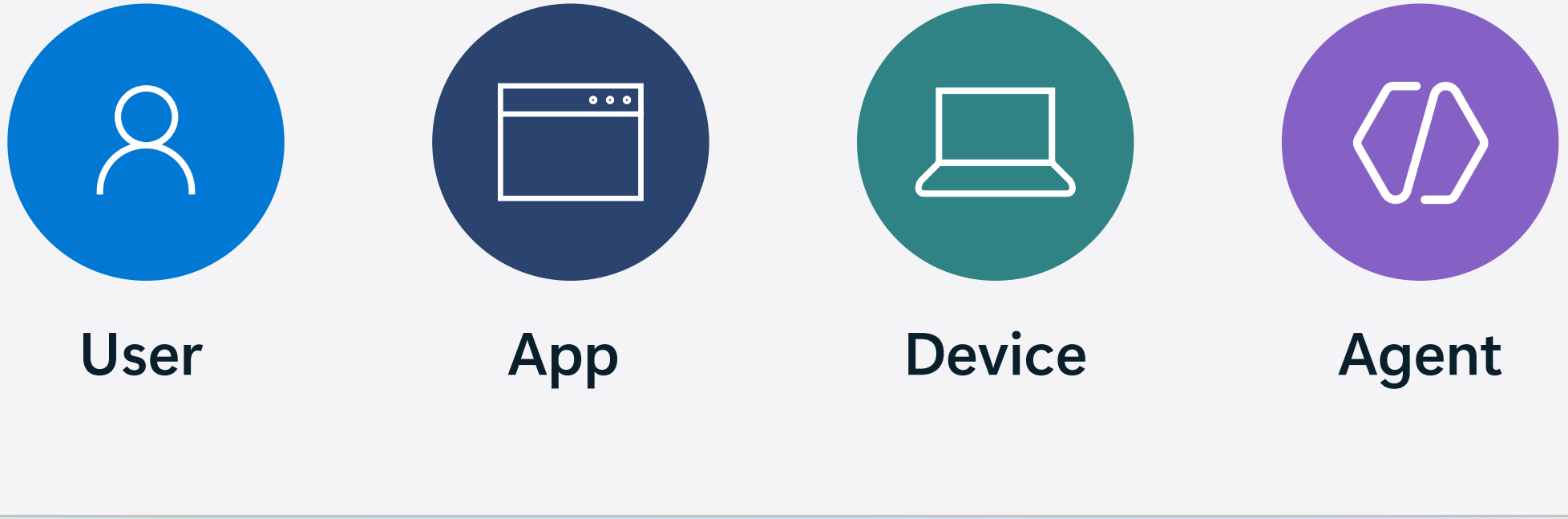
Simple agents can be made in the Copilot Studio lite version in Copilot Chat + M365 Copilot

Advanced agents need to be made in the Copilot Studio full version

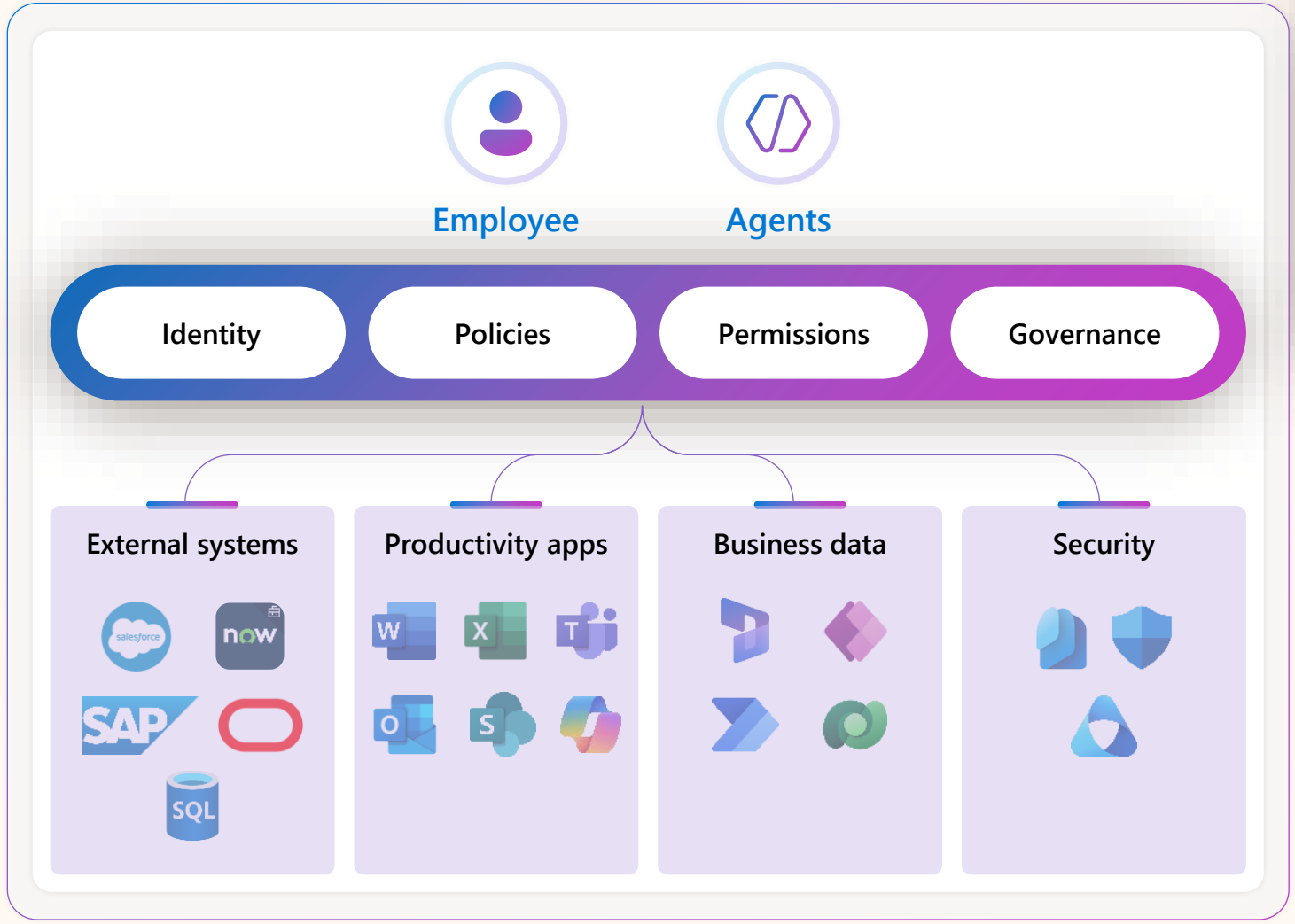
Microsoft Agent 365

The control plane for agents

Agents are a new type of identity



Microsoft 365 for employees, Agent 365 for agents



Unlock agent productivity – Extend the tools you already use to secure & enable people

Every agent gets

- An identity
- Access to productivity tools, systems and data

IT gets

- Total observability and visibility
- Control, security and governance

Microsoft Agent 365

The same Microsoft's management, security, and productivity solutions are tailor-made for your agents.

Microsoft Defender

Extend comprehensive security posture and advanced threat protection to agents.

Microsoft Entra

Protect agent identities, and secure their access to any app or resource, from anywhere.

Microsoft Purview

Manage, protect and govern data that agents use and create across your entire organization.

Work IQ

Enable agents to use your organization's unique data and context to seamlessly join workflows and effectively complete tasks.

Microsoft 365

Enable agents to access and work in Word, Outlook, Excel and other productivity apps.

Microsoft Power Apps

Enable agent workflows with access to Power Apps and power Automate.

Microsoft Power BI

Enable agents to create analytics and Power BI dashboards to support collaboration.

Microsoft 365 Admin Center

Centralized hub to manage users, apps, and settings securely across your Microsoft 365 environment.

Home
Copilot
Agents
Overview
All agents
Tools
Settings
Users
Devices
Teams & groups
Marketplace
Billing
Setup
Customize navigation
Show all

Agent 365 overview

Last updated: Nov 14, 2025 (Last 30 days)

Track agent usage across your org over the last 30 days and take steps to improve impact. Adjust settings, manage access, and help teams unlock more value while staying aligned with governance goals.

Agent inventory — Explore all agents

26,350 ↑ 28% this week

Total agents in your org

Active users

58,293 ↑ 12% this week

Unique users interacting with agents

Time saved with agents

45,208 ↑ 6% this week

Hours saved by using agents

Agent analytics

Agent publishers

Created by your organization

Shared by creator	14.6k
Used only by creator	4k
Published by your org	6.8k

Created by external partners

Microsoft	154
Workday	36
Other	710

Agent platforms

Copilot Studio (lite)	11k
Copilot Studio (full)	10.4k
Microsoft Foundry	3.7k
Workday	14
ServiceNow	6
Windows 365	5
Manus	1

Active users over time

Trending agents by active users

Claims Processing Agent	10,992
Contract intelligence	8,146
Researcher	7,392
Incident resolution	6,100
Manus	583

Top actions for you

Pending requests for agents

3 +2 this week

Open requests to add specific agents

Staffing Genie Agent — Nov 17, 2025

Agent risks

6 +3 this week

Agents with security risks

Comms agent — 2 risks

Ownerless agents

8 -4 this week

Agents without a creator or business owner

DataBridge — Nov 16, 2025

Agents with exceptions

100 +10 this week

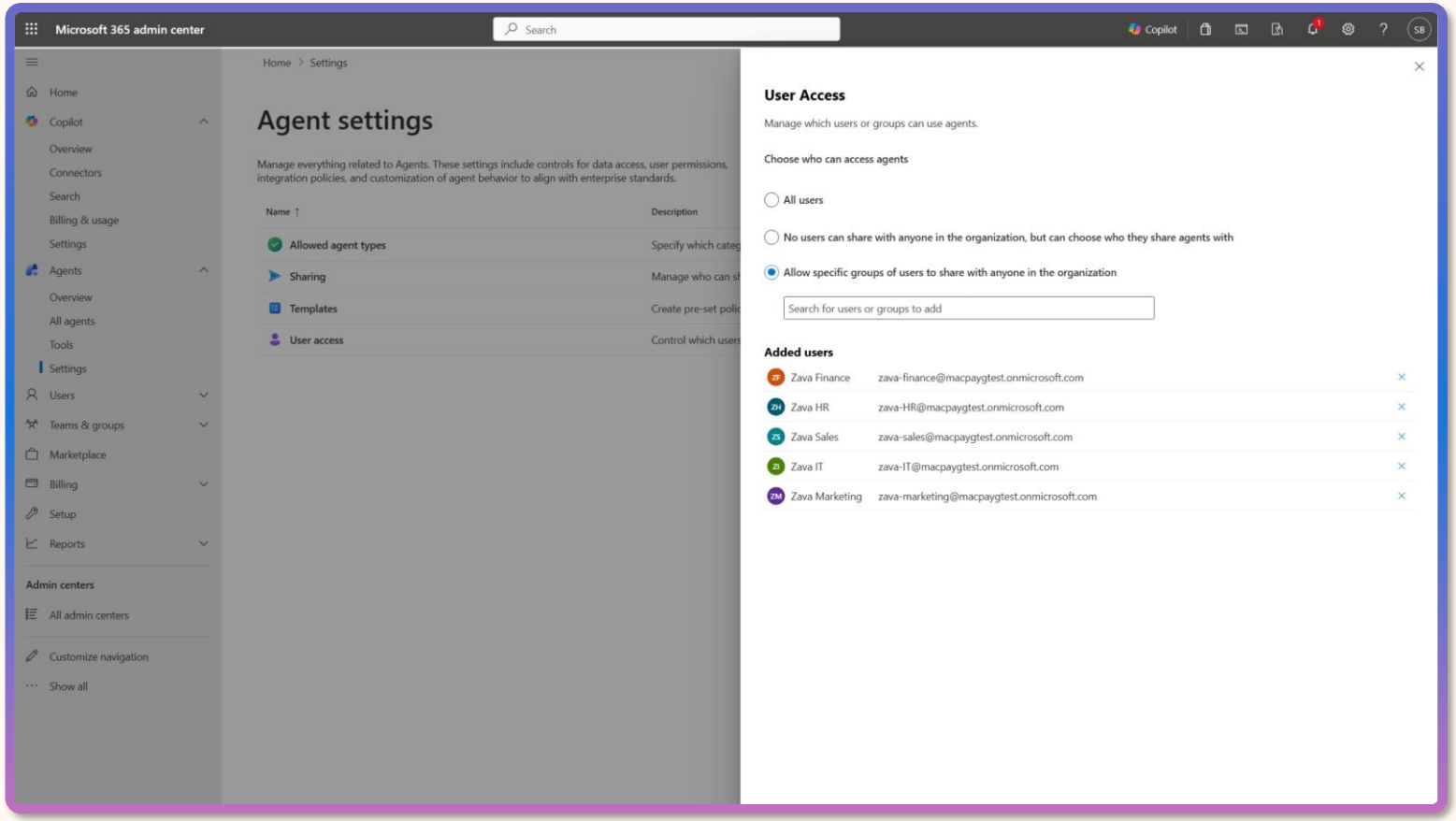
Agents needing your input to complete tasks

Insights Hub — 65%

Access control settings

Agent 365

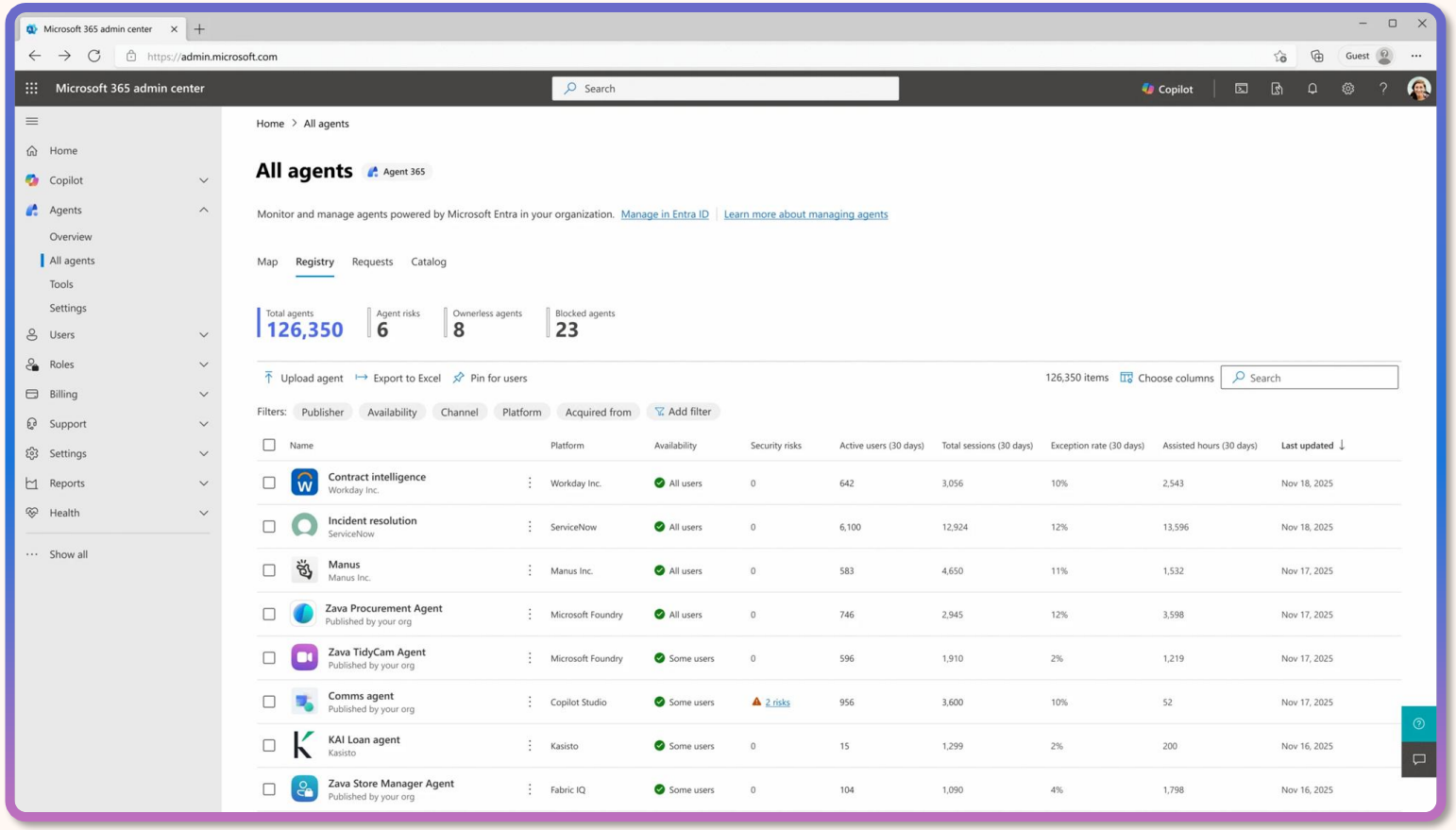
- Set guardrails for who creates, onboards, and manages agents.
- Choose how broad agents can be shared.
- Manage agents and limit their access only to the resources they need.



Product images subject to change

Single agent registry
Agent 365

- Start with a single registry for all agents.
- Quarantine unsanctioned agents to block discovery and connections.
- Use the Agent Store for easy agent discovery in Microsoft 365 Copilot and Teams.



Product images subject to change

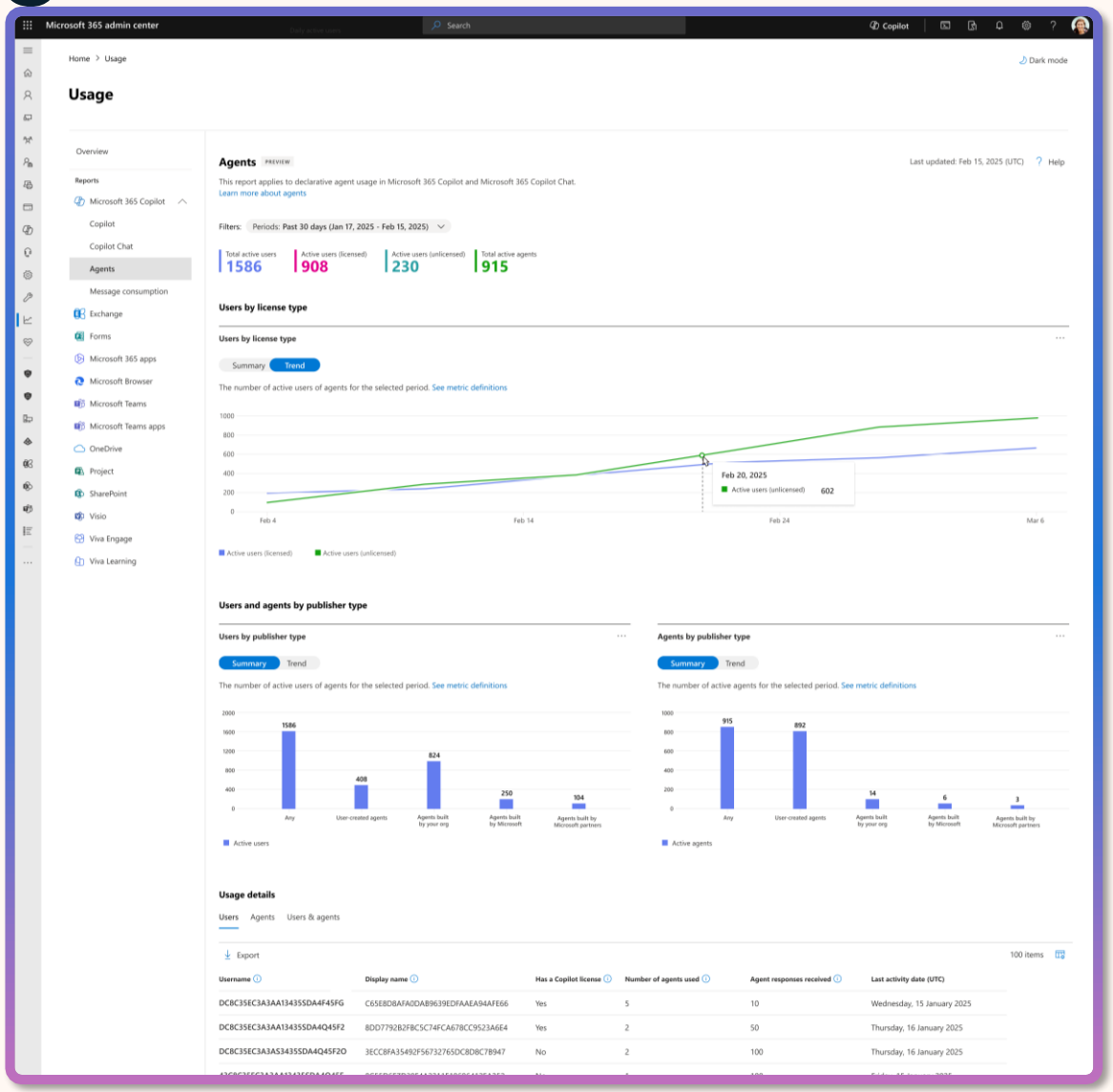
Agent observability & usage

Agent 365

Admins can gain insights to guide agent management and adoption strategy.

Sample metrics:

- Total active users & agents
- Active users and agents by publisher type
- Line-level consumption details per user, agent, billing policy, and user-agent pair
- High-consumption alerts to prevent over-spending



Product images subject to change

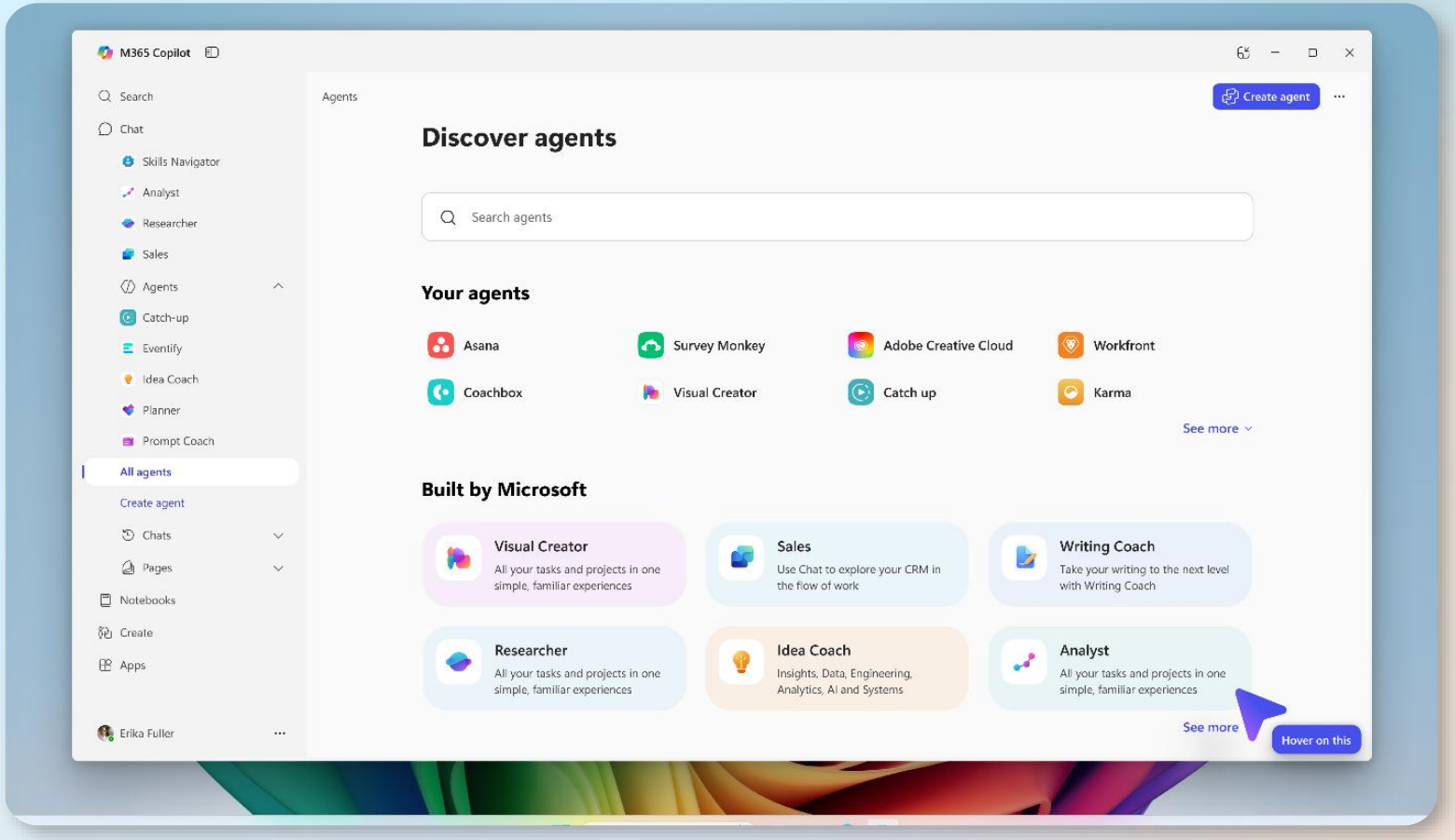
Agent Store

Agent Store is an agent marketplace featuring agents from **Microsoft, partners and customer organizations**. You can also share agents with colleagues via Copilot Chat or other Microsoft 365 Copilot endpoints to boost collaboration.

All agents, whether developed by Microsoft or partners, undergo **strict validation processes to meet enterprise standards for functionality, security, and compliance**.

IT admins have full visibility and control over how agents are deployed in their organization.

Consider which 3rd party agents will be available to users



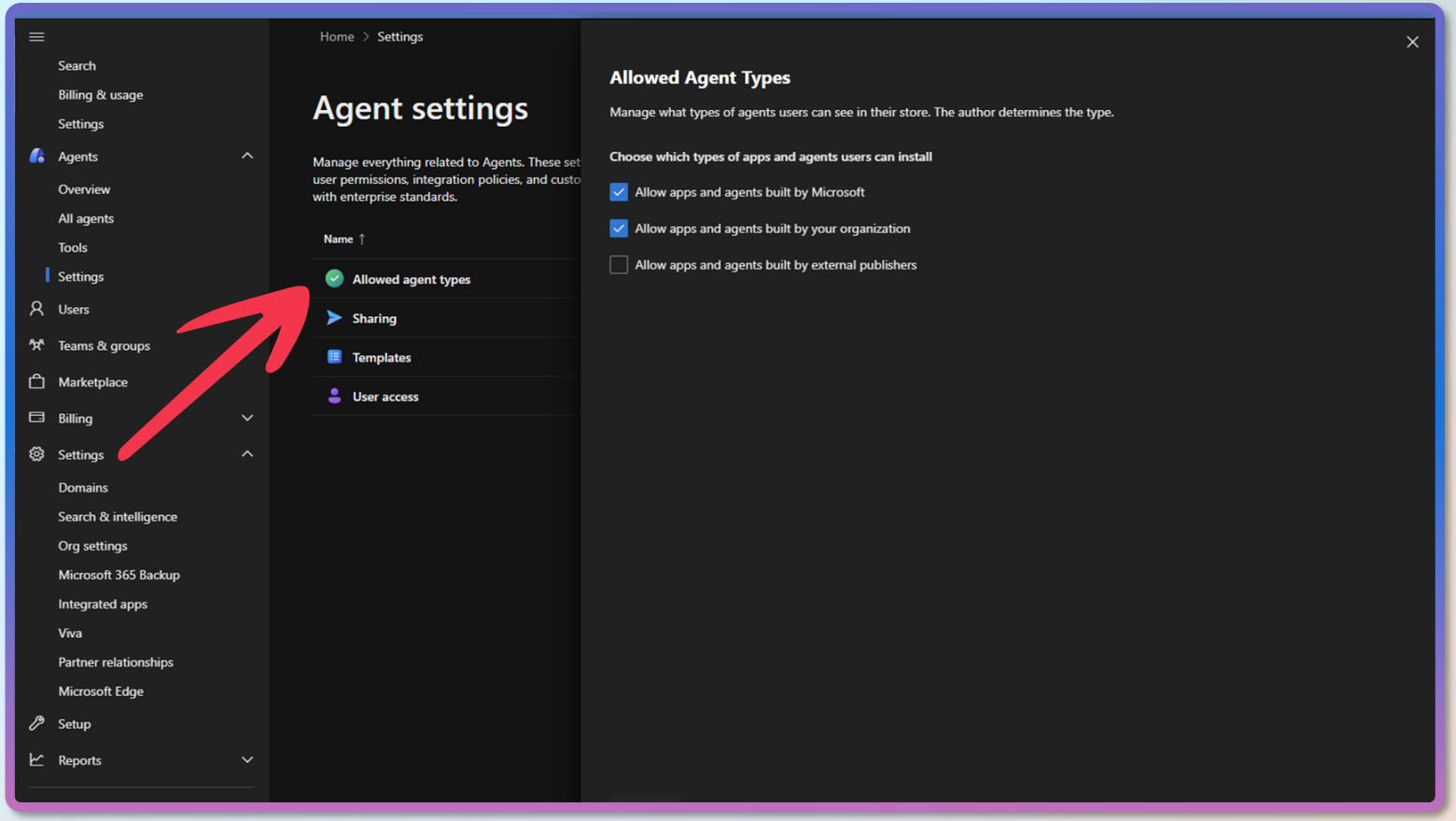
Agent Store

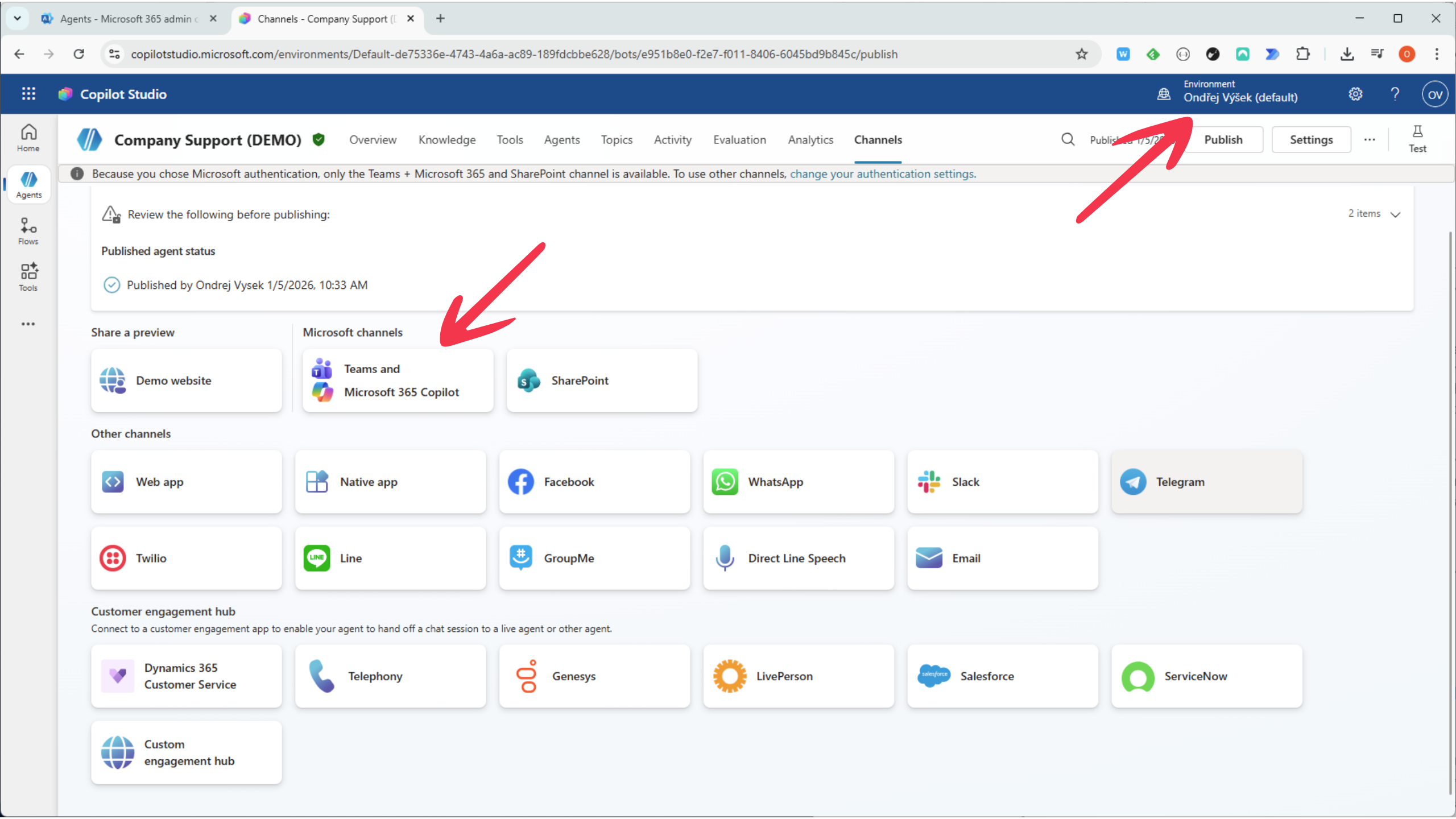
Agent Store is an agent marketplace featuring agents from **Microsoft, partners and customer organizations**. You can also share agents with colleagues via Copilot Chat or other Microsoft 365 Copilot endpoints to boost collaboration.

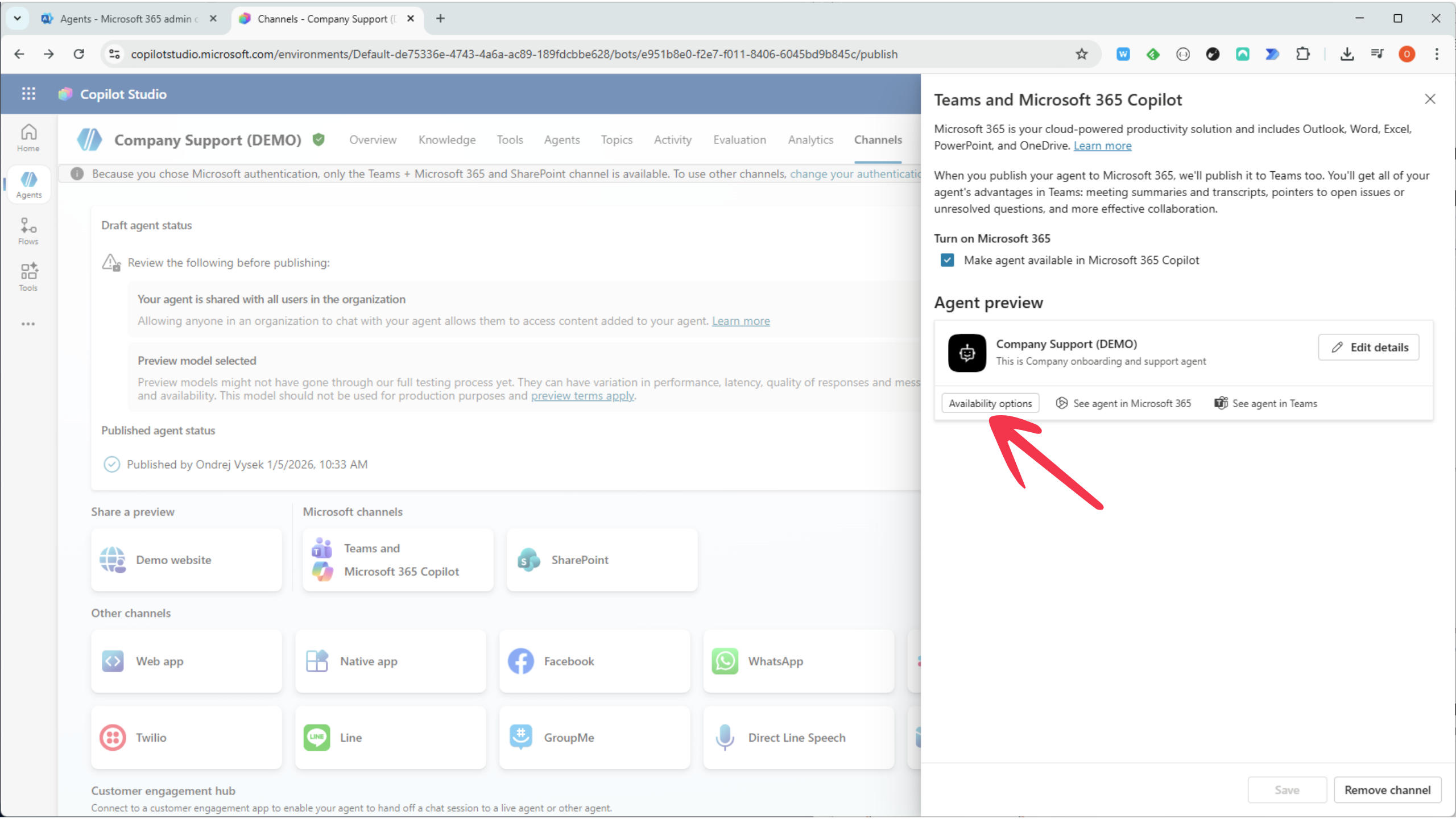
All agents, whether developed by Microsoft or partners, undergo **strict validation processes to meet enterprise standards for functionality, security, and compliance**.

IT admins have full visibility and control over how agents are deployed in their organization.

Consider which 3rd party agents will be available to users




Agents - Microsoft 365 admin
Channels - Company Support
copilotstudio.microsoft.com/environments/Default-de75336e-4743-4a6a-ac89-189fdcbbe628/bots/e951b8e0-f2e7-f011-8406-6045bd9b845c/publish
Copilot Studio
Environment
Ondřej Výšek (default)
Company Support (DEMO)
Overview
Knowledge
Tools
Agents
Topics
Activity
Evaluation
Analytics
Channels
Publish
Settings
Test
Home
Agents
Flows
Tools
Because you chose Microsoft authentication, only the Teams + Microsoft 365 and SharePoint channel is available. To use other channels, change your authentication settings.
Review the following before publishing:
2 items
Published agent status
Published by Ondrej Vysek 1/5/2026, 10:33 AM
Share a preview
Demo website
Microsoft channels
Teams and Microsoft 365 Copilot
SharePoint
Other channels
Web app
Native app
Facebook
WhatsApp
Slack
Telegram
Twilio
Line
GroupMe
Direct Line Speech
Email
Customer engagement hub
Connect to a customer engagement app to enable your agent to hand off a chat session to a live agent or other agent.
Dynamics 365 Customer Service
Telephony
Genesys
LivePerson
Salesforce
ServiceNow
Custom engagement hub


Agents - Microsoft 365 admin
Channels - Company Support
copilotstudio.microsoft.com/environments/Default-de75336e-4743-4a6a-ac89-189fdcbbe628/bots/e951b8e0-f2e7-f011-8406-6045bd9b845c/publish
Copilot Studio
Home
Agents
Flows
Tools
Company Support (DEMO)
Overview
Knowledge
Tools
Agents
Topics
Activity
Evaluation
Analytics
Channels
Because you chose Microsoft authentication, only the Teams + Microsoft 365 and SharePoint channel is available. To use other channels, change your authenticatic
Draft agent status
Review the following before publishing:
Your agent is shared with all users in the organization
Allowing anyone in an organization to chat with your agent allows them to access content added to your agent. Learn more
Preview model selected
Preview models might not have gone through our full testing process yet. They can have variation in performance, latency, quality of responses and mess
and availability. This model should not be used for production purposes and preview terms apply.
Published agent status
Published by Ondrej Vysek 1/5/2026, 10:33 AM
Share a preview
Demo website
Microsoft channels
Teams and
Microsoft 365 Copilot
SharePoint
Other channels
Web app
Native app
Facebook
WhatsApp
Twilio
Line
GroupMe
Direct Line Speech
Customer engagement hub
Connect to a customer engagement app to enable your agent to hand off a chat session to a live agent or other agent.
Teams and Microsoft 365 Copilot
Microsoft 365 is your cloud-powered productivity solution and includes Outlook, Word, Excel, PowerPoint, and OneDrive. Learn more
When you publish your agent to Microsoft 365, we'll publish it to Teams too. You'll get all of your agent's advantages in Teams: meeting summaries and transcripts, pointers to open issues or unresolved questions, and more effective collaboration.
Turn on Microsoft 365
Make agent available in Microsoft 365 Copilot
Agent preview
Company Support (DEMO)
This is Company onboarding and support agent
Edit details
Availability options
See agent in Microsoft 365
See agent in Teams
Save
Remove channel

Agents - Microsoft 365 admin c | Channels - Company Support ([

copilotstudio.microsoft.com/environments/Default-de75336e-4743-4a6a-ac89-189fdcbbe628/bots/e951b8e0-f2e7-f011-8406-6045bd9b845c/publish

Copilot Studio

Home
Agents
Flows
Tools

Company Support (DEMO)

Overview | Knowledge | Tools | Agents | Topics | Activity | Evaluation | Analytics | Channels

Because you chose Microsoft authentication, only the Teams + Microsoft 365 and SharePoint channel is available. To use other channels, change your authenticatic

Draft agent status

Review the following before publishing:

Your agent is shared with all users in the organization

Allowing anyone in an organization to chat with your agent allows them to access content added to your agent. Learn more

Preview model selected

Preview models might not have gone through our full testing process yet. They can have variation in performance, latency, quality of responses and mess and availability. This model should not be used for production purposes and preview terms apply.

Published agent status

Published by Ondrej Vysek 1/5/2026, 10:33 AM

Share a preview

Demo website

Microsoft channels

Teams and Microsoft 365 Copilot

SharePoint

Other channels

Web app

Native app

Facebook

WhatsApp

Twilio

Line

GroupMe

Direct Line Speech

Customer engagement hub

Connect to a customer engagement app to enable your agent to hand off a chat session to a live agent or other agent.

Teams and Microsoft 365 Copilot

Get a link

Users you select can open your agent in Microsoft Teams with this link. Manage sharing

Copy link

Download a file

Use your downloaded file to add your agent to the Microsoft Teams or Microsoft 365 store. Learn more

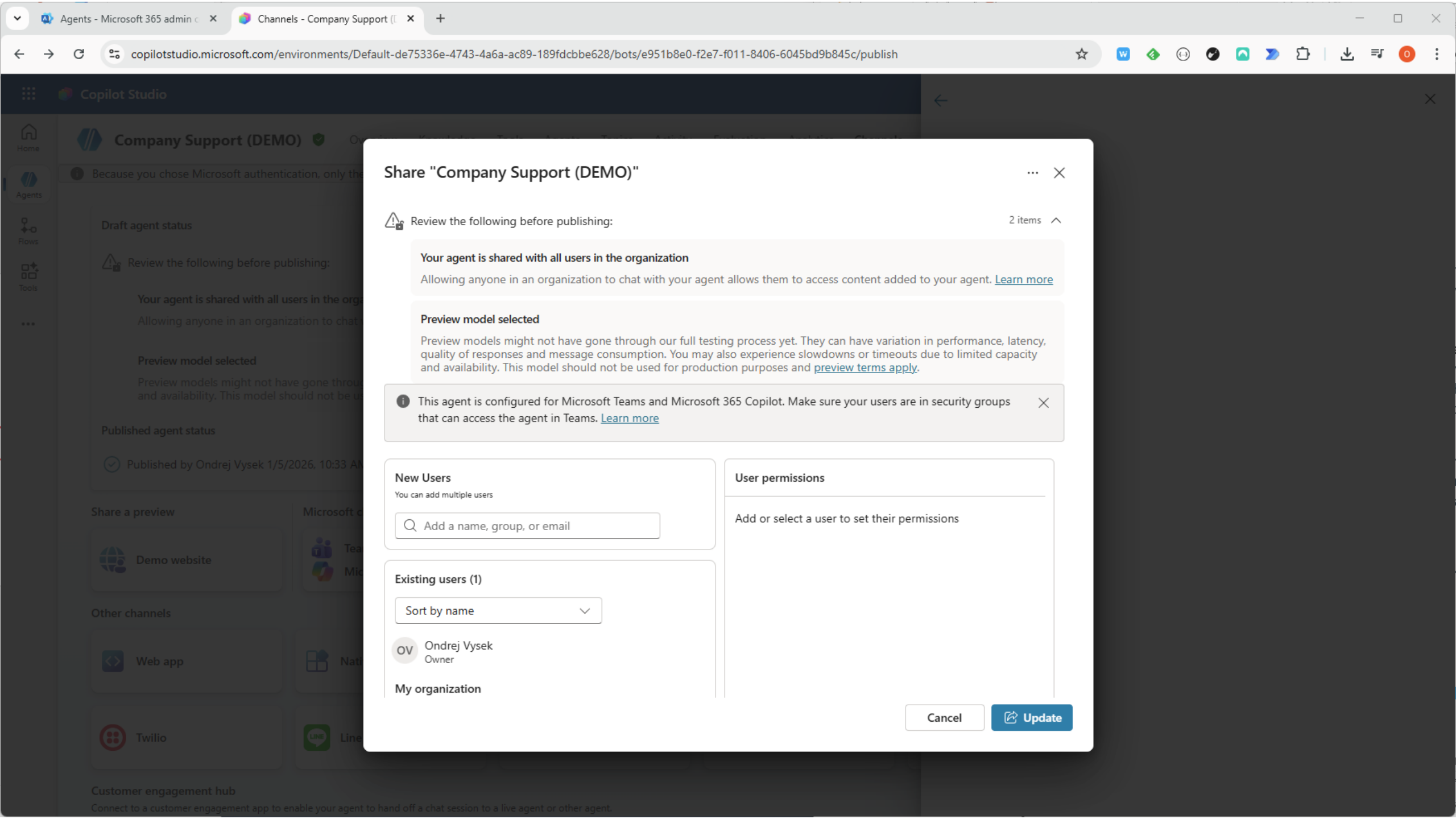
Download .zip

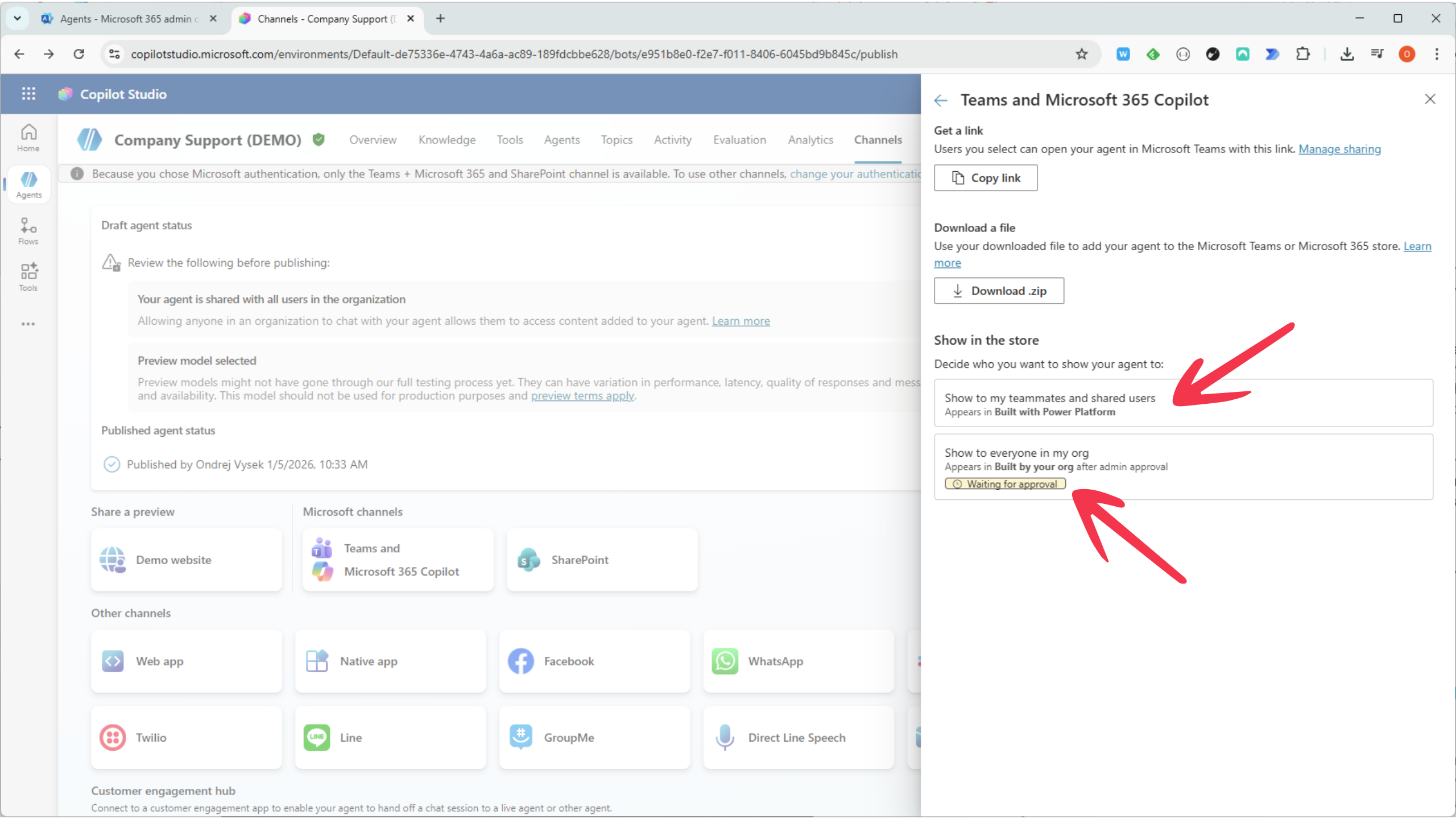
Show in the store

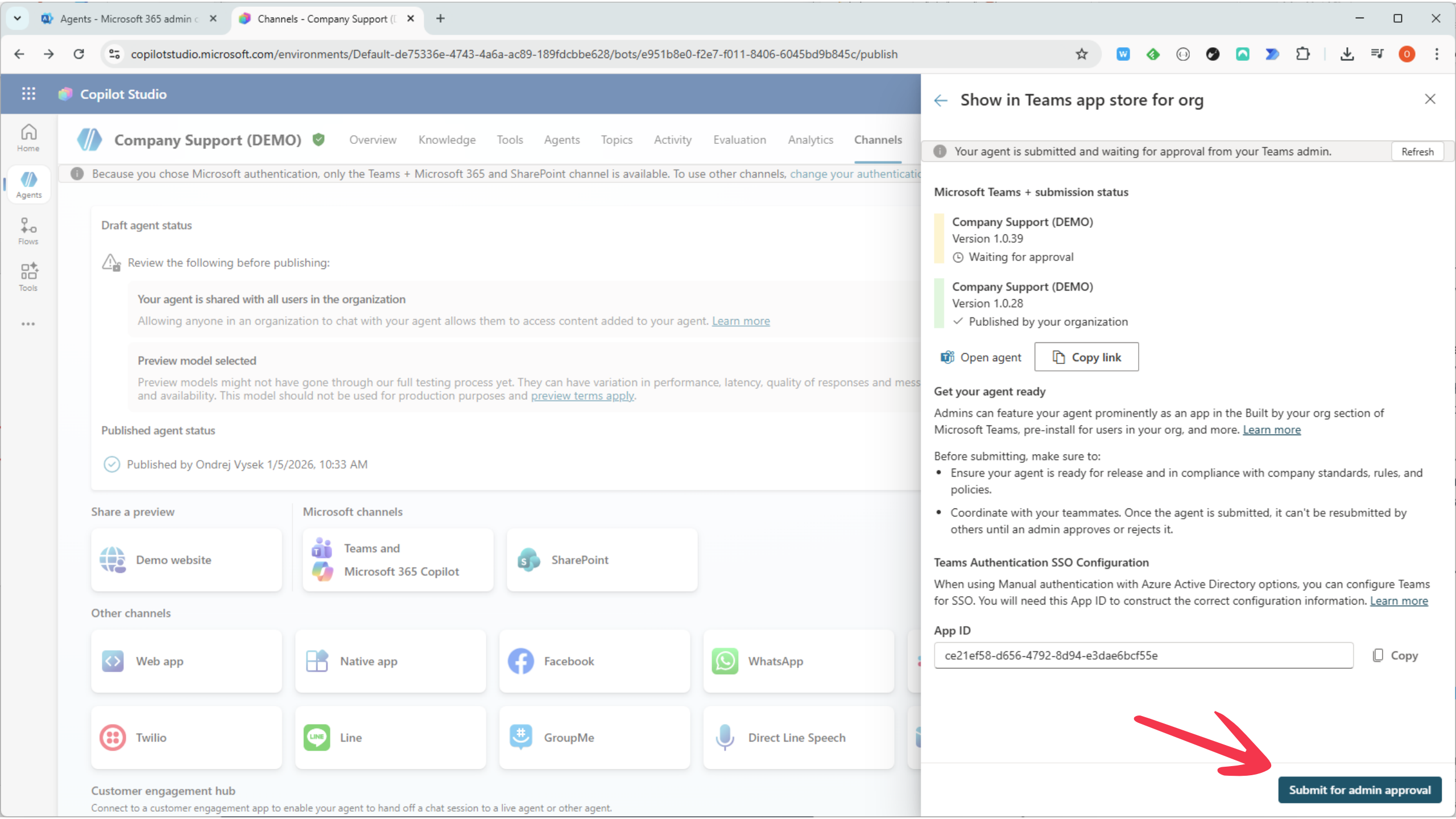
Decide who you want to show your agent to:

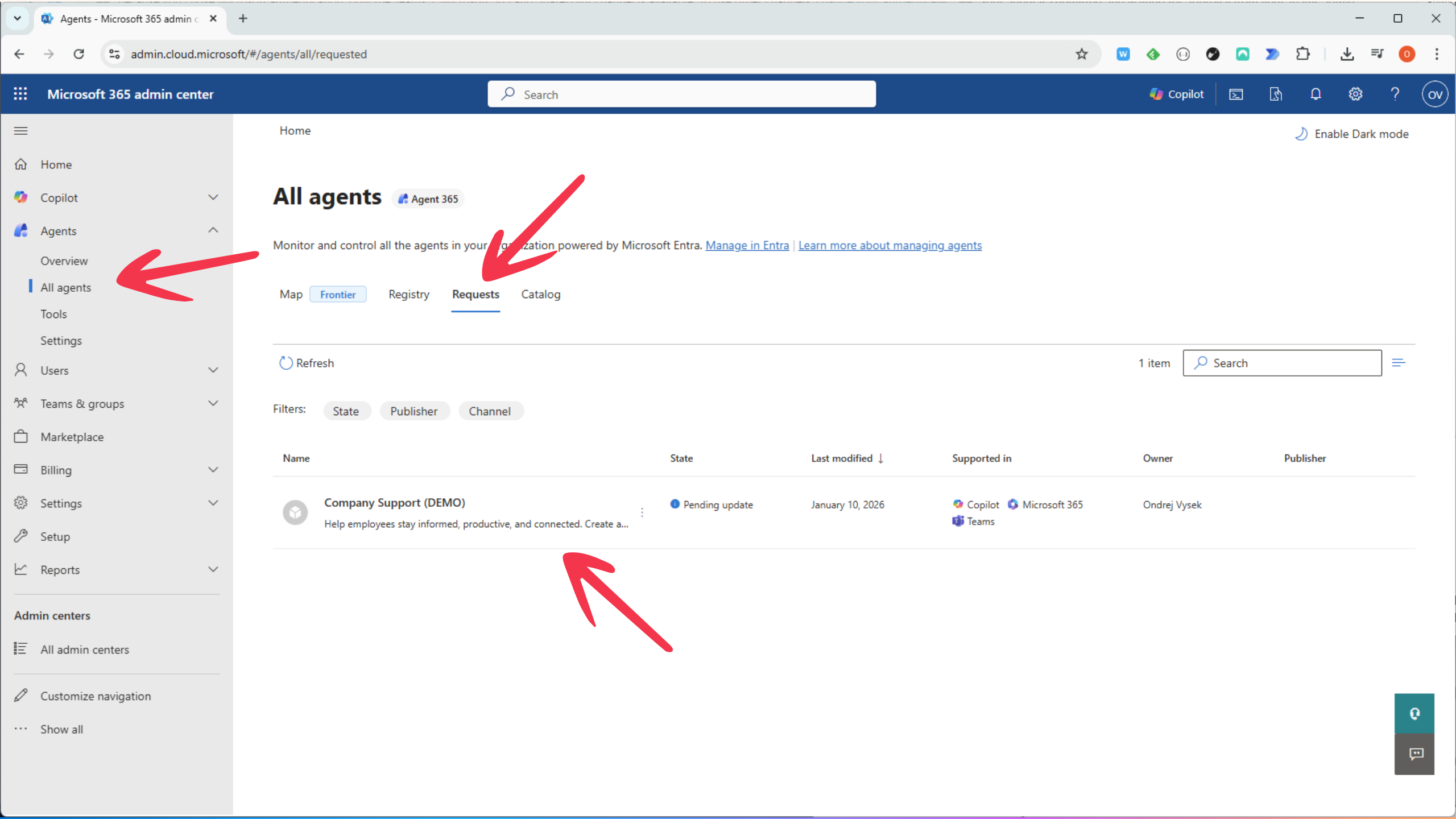
Show to my teammates and shared users
Appears in **Built with Power Platform**

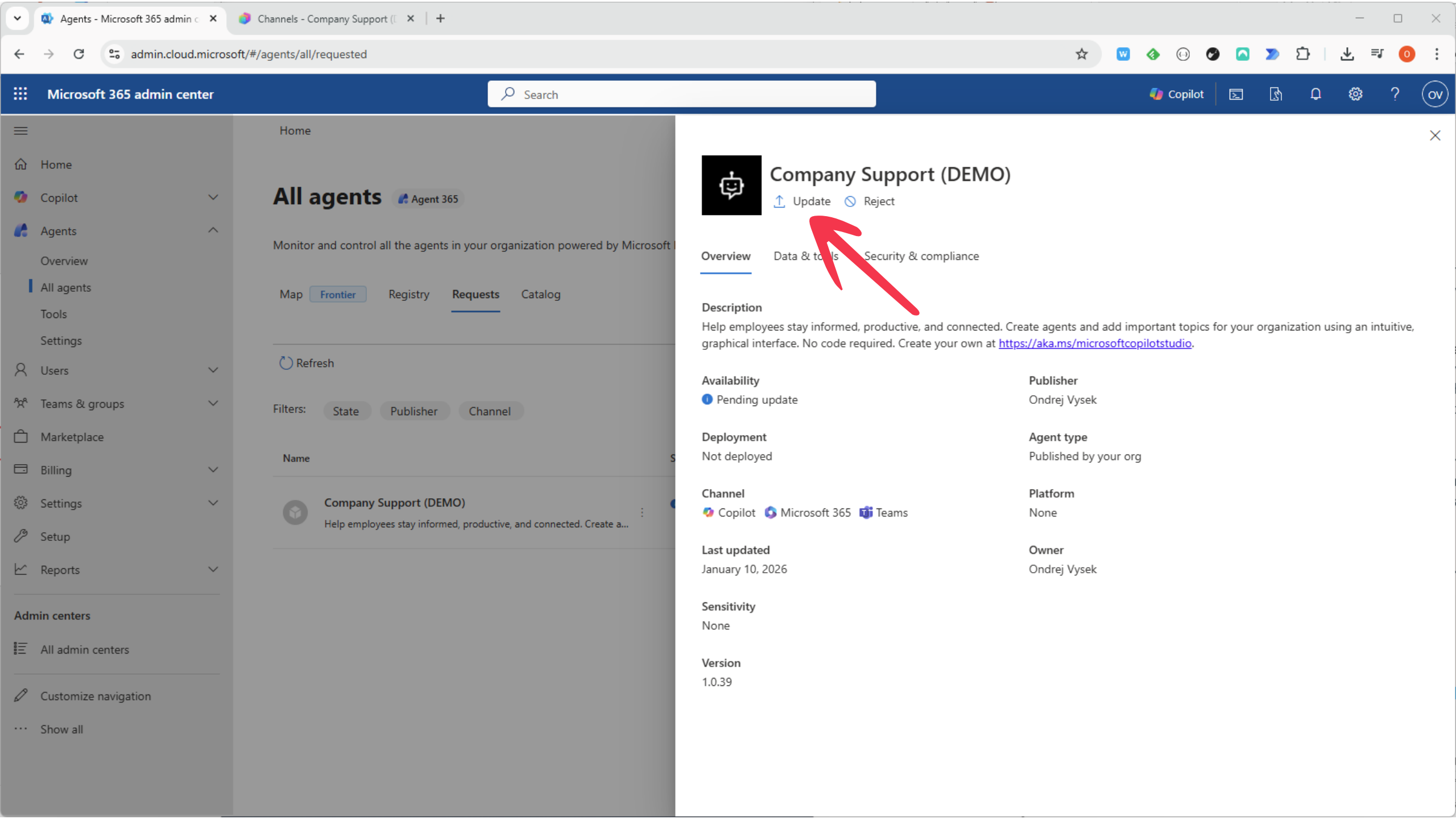
Show to everyone in my org
Appears in **Built by your org** after admin approval
Waiting for approval

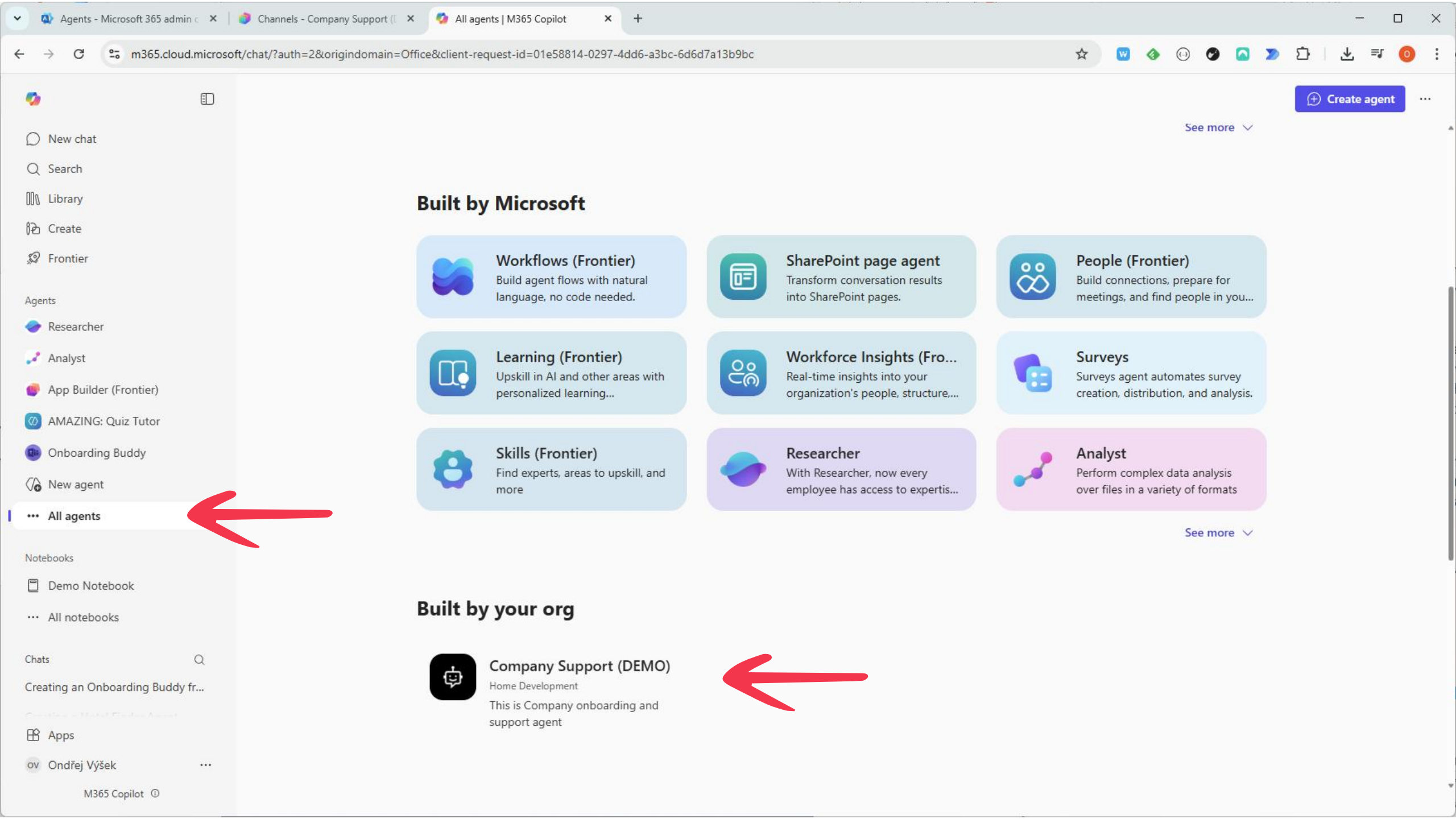

Agents - Microsoft 365 admin
Channels - Company Support
copilotstudio.microsoft.com/environments/Default-de75336e-4743-4a6a-ac89-189fdcbbe628/bots/e951b8e0-f2e7-f011-8406-6045bd9b845c/publish
Copilot Studio
Company Support (DEMO)
Share "Company Support (DEMO)"
Review the following before publishing:
2 items
Your agent is shared with all users in the organization
Allowing anyone in an organization to chat with your agent allows them to access content added to your agent. Learn more
Preview model selected
Preview models might not have gone through our full testing process yet. They can have variation in performance, latency, quality of responses and message consumption. You may also experience slowdowns or timeouts due to limited capacity and availability. This model should not be used for production purposes and preview terms apply.
This agent is configured for Microsoft Teams and Microsoft 365 Copilot. Make sure your users are in security groups that can access the agent in Teams. Learn more
New Users
You can add multiple users
Add a name, group, or email
Existing users (1)
Sort by name
OV
Ondrej Vysek
Owner
My organization
User permissions
Add or select a user to set their permissions
Cancel
Update
Draft agent status
Published agent status
Published by Ondrej Vysek 1/5/2026, 10:33 A
Share a preview
Demo website
Other channels
Web app
Twilio
Customer engagement hub
Connect to a customer engagement app to enable your agent to hand off a chat session to a live agent or other agent.


Agents - Microsoft 365 admin
Channels - Company Support
copilotstudio.microsoft.com/environments/Default-de75336e-4743-4a6a-ac89-189fdcbbe628/bots/e951b8e0-f2e7-f011-8406-6045bd9b845c/publish
Copilot Studio
Home
Agents
Flows
Tools
Company Support (DEMO)
Overview
Knowledge
Tools
Agents
Topics
Activity
Evaluation
Analytics
Channels
Because you chose Microsoft authentication, only the Teams + Microsoft 365 and SharePoint channel is available. To use other channels, change your authenticatic
Draft agent status
Review the following before publishing:
Your agent is shared with all users in the organization
Allowing anyone in an organization to chat with your agent allows them to access content added to your agent. Learn more
Preview model selected
Preview models might not have gone through our full testing process yet. They can have variation in performance, latency, quality of responses and mess
and availability. This model should not be used for production purposes and preview terms apply.
Published agent status
Published by Ondrej Vysek 1/5/2026, 10:33 AM
Share a preview
Demo website
Microsoft channels
Teams and
Microsoft 365 Copilot
SharePoint
Other channels
Web app
Native app
Facebook
WhatsApp
Twilio
Line
GroupMe
Direct Line Speech
Customer engagement hub
Connect to a customer engagement app to enable your agent to hand off a chat session to a live agent or other agent.
Teams and Microsoft 365 Copilot
Get a link
Users you select can open your agent in Microsoft Teams with this link. Manage sharing
Copy link
Download a file
Use your downloaded file to add your agent to the Microsoft Teams or Microsoft 365 store. Learn more
Download .zip
Show in the store
Decide who you want to show your agent to:
Show to my teammates and shared users
Appears in Built with Power Platform
Show to everyone in my org
Appears in Built by your org after admin approval
Waiting for approval


Agents - Microsoft 365 admin
Channels - Company Support
copilotstudio.microsoft.com/environments/Default-de75336e-4743-4a6a-ac89-189fdcbbe628/bots/e951b8e0-f2e7-f011-8406-6045bd9b845c/publish
Copilot Studio
Home
Agents
Flows
Tools
Company Support (DEMO)
Overview
Knowledge
Tools
Agents
Topics
Activity
Evaluation
Analytics
Channels
Because you chose Microsoft authentication, only the Teams + Microsoft 365 and SharePoint channel is available. To use other channels, change your authenticatic
Draft agent status
Review the following before publishing:
Your agent is shared with all users in the organization
Allowing anyone in an organization to chat with your agent allows them to access content added to your agent. Learn more
Preview model selected
Preview models might not have gone through our full testing process yet. They can have variation in performance, latency, quality of responses and mess
and availability. This model should not be used for production purposes and preview terms apply.
Published agent status
Published by Ondrej Vysek 1/5/2026, 10:33 AM
Share a preview
Demo website
Microsoft channels
Teams and
Microsoft 365 Copilot
SharePoint
Other channels
Web app
Native app
Facebook
WhatsApp
Twilio
Line
GroupMe
Direct Line Speech
Customer engagement hub
Connect to a customer engagement app to enable your agent to hand off a chat session to a live agent or other agent.
Show in Teams app store for org
Your agent is submitted and waiting for approval from your Teams admin.
Refresh
Microsoft Teams + submission status
Company Support (DEMO)
Version 1.0.39
Waiting for approval
Company Support (DEMO)
Version 1.0.28
Published by your organization
Open agent
Copy link
Get your agent ready
Admins can feature your agent prominently as an app in the Built by your org section of Microsoft Teams, pre-install for users in your org, and more. Learn more
Before submitting, make sure to:
Ensure your agent is ready for release and in compliance with company standards, rules, and policies.
Coordinate with your teammates. Once the agent is submitted, it can't be resubmitted by others until an admin approves or rejects it.
Teams Authentication SSO Configuration
When using Manual authentication with Azure Active Directory options, you can configure Teams for SSO. You will need this App ID to construct the correct configuration information. Learn more
App ID
ce21ef58-d656-4792-8d94-e3dae6bcf55e
Copy
Submit for admin approval


Agents - Microsoft 365 admin
admin.cloud.microsoft/#/agents/all/requested
Microsoft 365 admin center
Search
Copilot
Home
Enable Dark mode
Home
Copilot
Agents
Overview
All agents
Tools
Settings
Users
Teams & groups
Marketplace
Billing
Settings
Setup
Reports
Admin centers
All admin centers
Customize navigation
Show all
All agents
Agent 365
Monitor and control all the agents in your organization powered by Microsoft Entra. Manage in Entra | Learn more about managing agents
Map
Frontier
Registry
Requests
Catalog
Refresh
1 item
Search
Filters:
State
Publisher
Channel
Name
State
Last modified
Supported in
Owner
Publisher
Company Support (DEMO)
Help employees stay informed, productive, and connected. Create a...
Pending update
January 10, 2026
Copilot
Microsoft 365
Teams
Ondrej Vysek

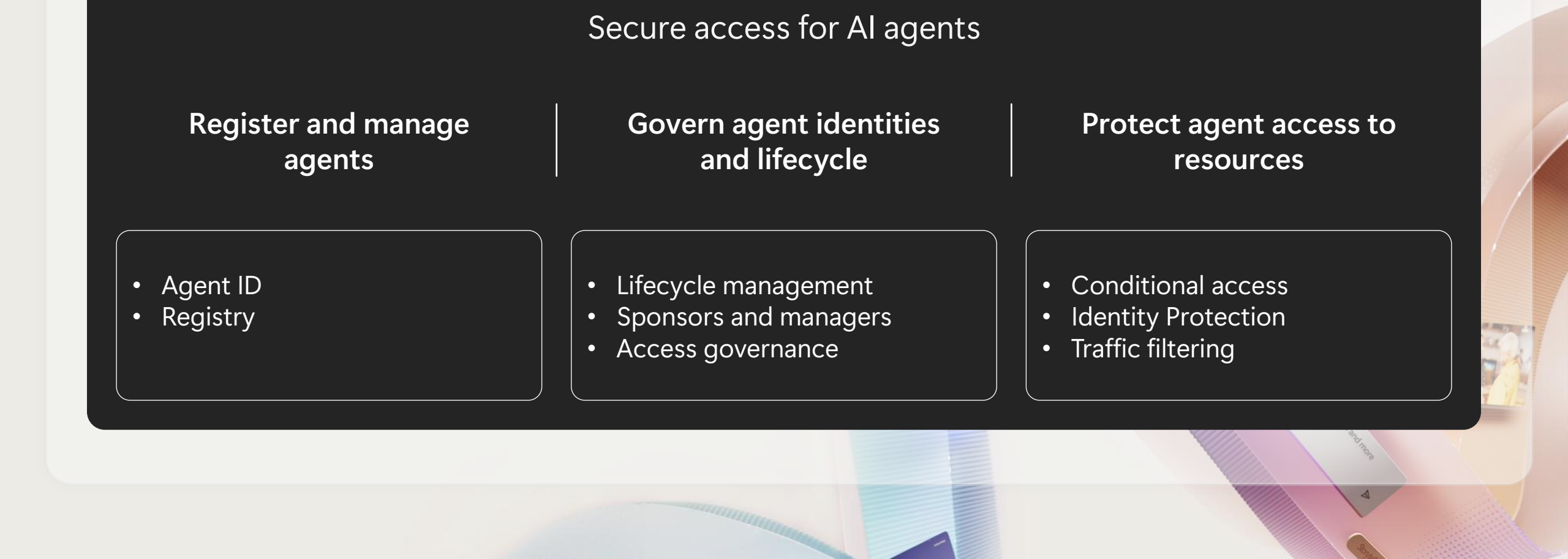

Agents - Microsoft 365 admin
Channels - Company Support
admin.cloud.microsoft/#/agents/all/requested
Microsoft 365 admin center
Search
Copilot
Home
Copilot
Agents
Overview
All agents
Tools
Settings
Users
Teams & groups
Marketplace
Billing
Settings
Setup
Reports
Admin centers
All admin centers
Customize navigation
Show all
Home
All agents
Agent 365
Monitor and control all the agents in your organization powered by Microsoft
Map
Frontier
Registry
Requests
Catalog
Refresh
Filters:
State
Publisher
Channel
Name
Company Support (DEMO)
Help employees stay informed, productive, and connected. Create a...
Company Support (DEMO)
Update
Reject
Overview
Data & tools
Security & compliance
Description
Help employees stay informed, productive, and connected. Create agents and add important topics for your organization using an intuitive, graphical interface. No code required. Create your own at https://aka.ms/microsoftcopilotstudio.
Availability
Pending update
Publisher
Ondrej Vysek
Deployment
Not deployed
Agent type
Published by your org
Channel
Copilot
Microsoft 365
Teams
Platform
None
Last updated
January 10, 2026
Owner
Ondrej Vysek
Sensitivity
None
Version
1.0.39


Agents - Microsoft 365 admin
Channels - Company Support
All agents | M365 Copilot
m365.cloud.microsoft/chat/?auth=2&origindomain=Office&client-request-id=01e58814-0297-4dd6-a3bc-6d6d7a13b9bc
New chat
Search
Library
Create
Frontier
Agents
Researcher
Analyst
App Builder (Frontier)
AMAZING: Quiz Tutor
Onboarding Buddy
New agent
All agents
Notebooks
Demo Notebook
All notebooks
Chats
Creating an Onboarding Buddy fr...
Apps
Ondřej Výšek
M365 Copilot
Create agent
See more
Built by Microsoft
Workflows (Frontier)
Build agent flows with natural language, no code needed.
SharePoint page agent
Transform conversation results into SharePoint pages.
People (Frontier)
Build connections, prepare for meetings, and find people in you...
Learning (Frontier)
Upskill in AI and other areas with personalized learning...
Workforce Insights (Fro...
Real-time insights into your organization's people, structure,...
Surveys
Surveys agent automates survey creation, distribution, and analysis.
Skills (Frontier)
Find experts, areas to upskill, and more
Researcher
With Researcher, now every employee has access to expertis...
Analyst
Perform complex data analysis over files in a variety of formats
See more
Built by your org
Company Support (DEMO)
Home Development
This is Company onboarding and support agent

Microsoft Entra Agent ID

Secure access for AI agents

Register and manage agents	Govern agent identities and lifecycle	Protect agent access to resources
• Agent ID • Registry	• Lifecycle management • Sponsors and managers • Access governance	• Conditional access • Identity Protection • Traffic filtering

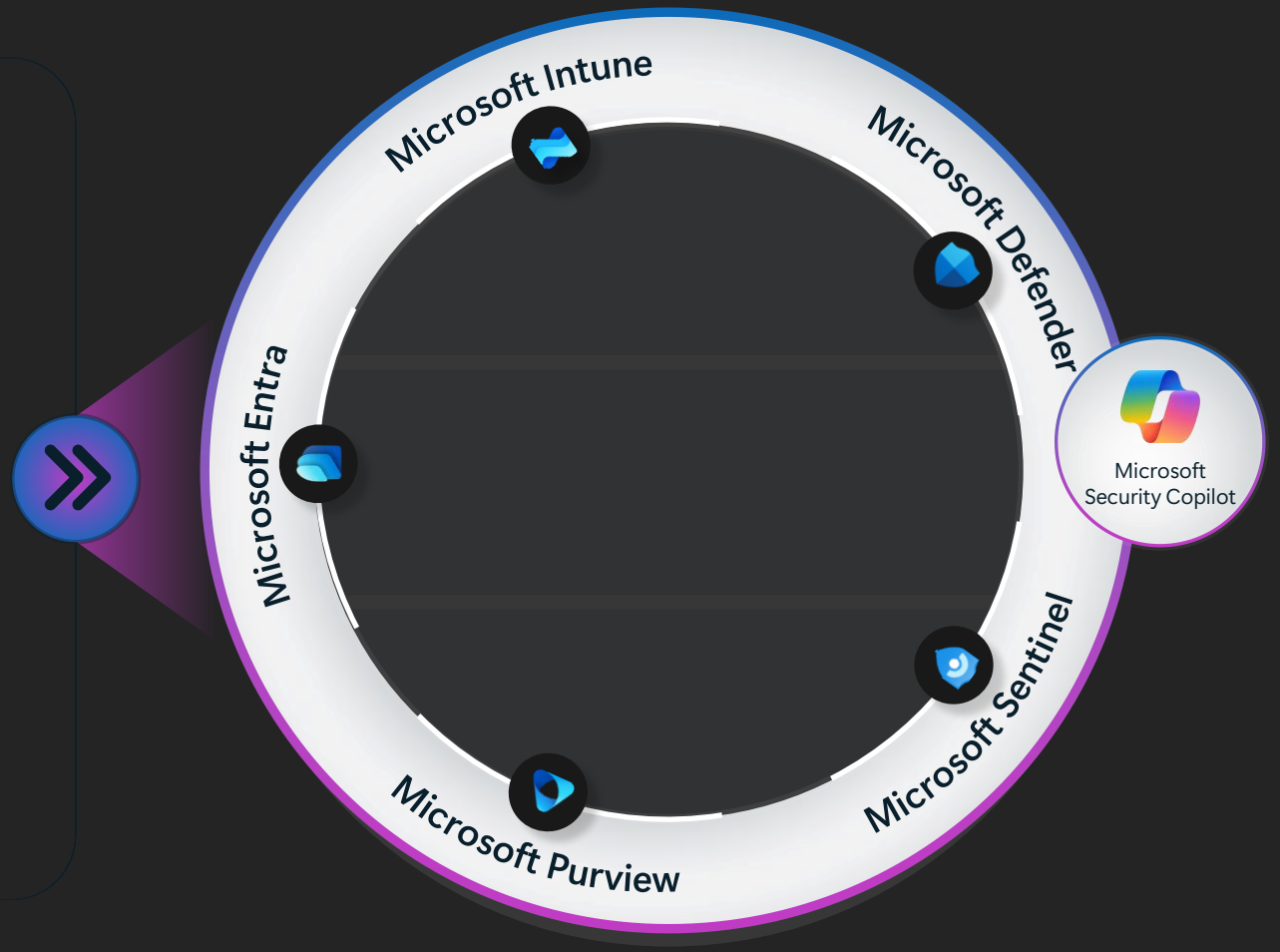


How Microsoft Entra manages agent identity and access

Get a directory of your AI agents
Natively integrated with Copilot Studio and Microsoft Foundry

Control agent access to resources
Adaptive access and permissions management

Protect and govern agent identities
Prevent agent compromise and manage lifecycle



Home
Entra agents
Favorites
Entra ID
Overview
Users
Groups
Devices
Agent ID
Enterprise applications
App registrations
Roles & admins
Identity Protection
Conditional Access
Authentication
External Identities
Custom security attributes
Certificate authorities
Cross-tenant synchronization
Microsoft Entra Connect
Domains
Custom branding
Mobility
Monitoring & health
Identity governance

Agent ID | Overview

Entra ID

Overview
All agent identities
Agent registry
Agent collections

Activity
Audit logs
Sign-in logs

Search for agent identities by name or object ID

Got feedback?

Agents in your tenant

6,053 ↑ 31% Last 7 days

Gain full visibility into agent identities in your tenant, and secure them by default with policies and lifecycle controls. Learn more

View all agent identities

Recently created
Created in last 30 days
74 ↑ 17% View

Unmanaged
No owners or sponsors
29 ↓ 24% View

Active
Enabled for access
5,016 View

No identities
Agents without identities
141 View

Types of agents

Breakdown of different types of agents in the tenant

Agent identities (Non-users) 4,011 View
Agent identities (Users) 892 View
Agents with service principals 1,009 View
Agents with no identities 141 View

Agent blueprints

Blueprints are parent templates that power agent identities in your tenant.

Agent blueprints
342 ↑ 28%

View all

Recently created blueprints

SA Sales Agent blueprint	13 agent identities
Finance agent	124 agent identities
OP Orion Pulse	69 agent identities

Agent collections overview

Automatically or manually-created groups of agents in your tenant.

Global
1210 agents

Custom
122 agents

Quarantined
0 agents

View all

Home
Entra agents
Favorites
Entra ID
Overview
Users
Groups
Devices
Agent ID
Enterprise applications
App registrations
Roles & admins
Identity Protection
Conditional Access
Authentication
External Identities
Custom security attributes
Certificate authorities
Cross-tenant synchronization
Microsoft Entra Connect
Domains
Custom branding
Mobility
Monitoring & health
Identity governance

Agent ID | Agent registry

Entra ID

Overview
All agent identities
Agent registry
Agent collections

Activity
Audit logs
Sign-in logs

Refresh Columns

Search by name or object ID

Add filter

Showing 6,053 items

Name	Registry ID	Platform	Has Agent ID	Source ID	
Image Recognition Agent	jpig5qtp-hr5o-iq9s-me2r-le4t2n4p6...	PixelNova AI	No	default_055beb02-87cc-48e1-b4ab-7...	
Inventory Management Agent	58b744c1-e3b9-4205-8016-dbc9194...	Adatum	No	ab9c6ad5-9da3-4610-bd2f-7db8de2c...	View more
Procurement & logistics	microsoftCopilotStudio_055beb02-87...	Copilot Studio	Yes	default_bd1aeecb-6e88-41aa-90ab-e3...	
Content Generation Agent	10314218-d641-48aa-aa2c-e9e2ea6a...	BrightMind Systems	No	default_b0e53276-403b-49dd-9720-c...	
HR Actions	microsoftAzureFoundry_088beb02-8...	Microsoft Foundry	Yes	783beb02-87cc-48e1-b4ab-784889ed...	View more
Deal advisor	microsoftCopilotStudio_055beb02-87...	Copilot Studio	Yes	default_982beb02-87cc-48e1-b4ab-78...	
Conditional Access Optimization Agent	becef3a5-8a8b-4b6b-87b5-bace1fb5...	Security Copilot	Yes	376f8eee-0fc8-4345-9f82-6e3bcea65...	View more
Manus	0a52a0fb-5b3b-4ebc-b231-5cc98f7b...	Manus AI	Yes	95deb0cd-6d3d-441d-9ace-5b1c5be3...	
HR self-servicve	microsoftCopilotStudio_055beb02-87...	Copilot Studio	Yes	default_675ref02-87cc-48e1-b4ab-784...	View more
Finance optimizer	microsoftCopilotStudio_055beb02-87...	Copilot Studio	Yes	default_426117dc-2180-4057-9939-ae...	View more
Zava Assist	microsoftAzureFoundry_088beb02-8...	Microsoft Foundry	Yes	2900dfd4-b521-480b-8125-79293609...	
Sales Forecasting Agent	84e24f35-b1f9-4e39-b700-bbae2cc6...	FutureCast Labs	No	default_055beb02-87cc-48e1-b4ab-7...	
Genspark Super	41d8d132-7546-4b9c-8589-f2a5d16...	Genspark	Yes	d6f078d6-feeb-4dd3-933d-e87573bc...	View more
Test HR 123	microsoftCopilotStudio_055beb02-87...	Copilot Studio	Yes	default_055beb02-87cc-48e1-b4ab-78...	View more
Customer Assist	e97c3dc4-17c0-4236-a0e1-3451cc86...	Kasisto	Yes	7a065927-bbc7-4aa2-b4ae-429d8582...	
Stock monitor	microsoftCopilotStudio_055beb02-87...	Copilot Studio	Yes	default_055beb02-87cc-48e1-b4ab-78...	

Home
Entra agents
Favorites
Entra ID
Overview
Users
Groups
Devices
Agent ID
Enterprise applications
App registrations
Roles & admins
Identity Protection
Conditional Access
Authentication
External Identities
Custom security attributes
Certificate authorities
Cross-tenant synchronization
Microsoft Entra Connect
Domains
Custom branding
Mobility
Monitoring & health
Identity governance

Agent ID | All agent identities

Entra ID

Overview
All agent identities
Agent registry
Agent collections

Activity
Audit logs
Sign-in logs

Disable | Download | Refresh | Columns | View agent blueprints

Search by name or object ID | Status: All | Add filter

Showing 5,912 items

Name	Status	Created on	Object ID
HR Self-Service Agent	Active	10/14/2025	a5ab672c-af21-484e-8dc8-93104c7ee003
Zava Assist	Active	10/13/2025	ee83c249-c54d-4888-b27b-103dd9a842de
Procurement & logistics	Active	10/13/2025	15139328-96c2-4058-b936-eb2ff4698556
Finance optimizer	Active	10/13/2025	c5988f7c-0533-4ce1-9f69-d344217e806a1
Conditional Access Optimization Agent	Active	10/10/2025	1f7531a6-2568-4ea7-b2a3-8cf80223e5bb
Stock monitor	Active	10/10/2025	2964b7a6-20d7-4dfe-9be5-b13e0a2ac832...
HR Actions Agent	Active	10/10/2025	d41234e9-9988-47da-9724-d51cdb99fd9d...
Manus Agent	Active	10/10/2025	cb889b16-54bf-4db1-a5de-07629904252f...
Deal advisor	Active	10/10/2025	8a061d40-75b7-4cd6-b1de-872d989ec8e8...
Genspark Super	Active	10/10/2025	d3813e44-21f5-4a9e-bd26-e932e1fa62b4...
Customer Assist	Active	10/09/2025	acedf255-393d-4796-9a8c-e7625bd36440...
NowAssist	Active	10/09/2025	6770647e-1ce6-464a-ae31-3dc4308fbce4...
Glean	Active	10/09/2025	b4fc7b68-d937-4d4d-9fd9-56e3912d2eb4...
Test HR 123	Active	09/19/2025	f1611e33-2b9b-4c8f-bdf0-79831faec0294
Genie Space	Disabled	09/19/2025	bcc40574-8e66-46d6-bb9f-81b4353829e4
Stock monitor	Disabled	09/19/2025	7ecae9f7-5613-4697-bb47-8c263449dcfe...

Home
Entra agents
Favorites
Entra ID
Overview
Users
Groups
Devices
Agent ID
Enterprise applications
App registrations
Roles & admins
Identity Protection
Conditional Access
Authentication
External Identities
Custom security attributes
Certificate authorities
Cross-tenant synchronization
Microsoft Entra Connect
Domains
Custom branding
Mobility
Monitoring & health
Identity governance

HR-Self-Service Agent | Overview

Agent identity

Overview
Custom security attributes

Access
Owners and sponsors
Agent identity's access

Activity
Audit logs
Sign-in logs

Disable | Got feedback?

HR-Self-Service Agent

Agent identity

Answers HR policy questions, initiates HR cases when needed.

Status	: Active
Sponsors	: Lawrence Gilbertson
Owners	: -
Blueprint ID	: cb889b16-54bf-4db1-a5de-07629904255
Object ID	: a5ab672c-af21-484e-8dc8-93104c7ee003
Agent blueprint	: HR Self-Service Agent Blueprint
Created on	: 10/14/2025

Agent identity's access

View

View the permissions, roles and resources that this agent has access to

Permissions	Entra roles
4	0

Policies & ID Governance

Useful links to policies and ID Governance features for this agent identity

CA policies	View
Access packages	View

Home
Agents
Favorites
Entra ID
Overview
Users
Groups
Devices
Agent identities
Enterprise apps
App registrations
Roles & admins
Delegated admin partners
Domain services
Conditional Access
Multifactor authentication
Identity Secure Score
Authentication methods
Password reset
Custom security attributes
Certificate authorities
External Identities
Cross-tenant synchronization
Entra Connect

Policies

New policy | New policy from template | Upload policy file | What if | Refresh | Preview features | Got feedback?

Microsoft Entra Conditional Access policies are used to apply access controls to keep your organization secure. Learn more

Conditional Access Optimization Agent

Policies created: 6
Policy suggestions: 20
Manage agent

Microsoft-managed policies

Policies created: 4

User created policies

Policies created: 74

Search | Add filter | Actors: Agents (Preview) | Reset filters

4 out of 84 policies found

Policy name	Created by	State	Alert	Creation date	Modified date
Allow HR approved agents to access resources	USER	On		11/6/2025, 11:55:57 AM	11/7/2025, 5:56:28 PM
EB - Test Risky Agent Block	USER	Report-only		10/16/2025, 7:39:11 PM	10/16/2025, 7:42:08 PM
High Risk Agents Template	USER	Off		10/23/2025, 3:38:44 PM	11/7/2025, 5:56:57 PM
Review all high risk agents from accessing all resources	CONDITIONAL ACCESS OPTIMIZATION AGENT	Report-only		10/27/2025, 3:48:50 PM	11/7/2025, 5:57:20 PM

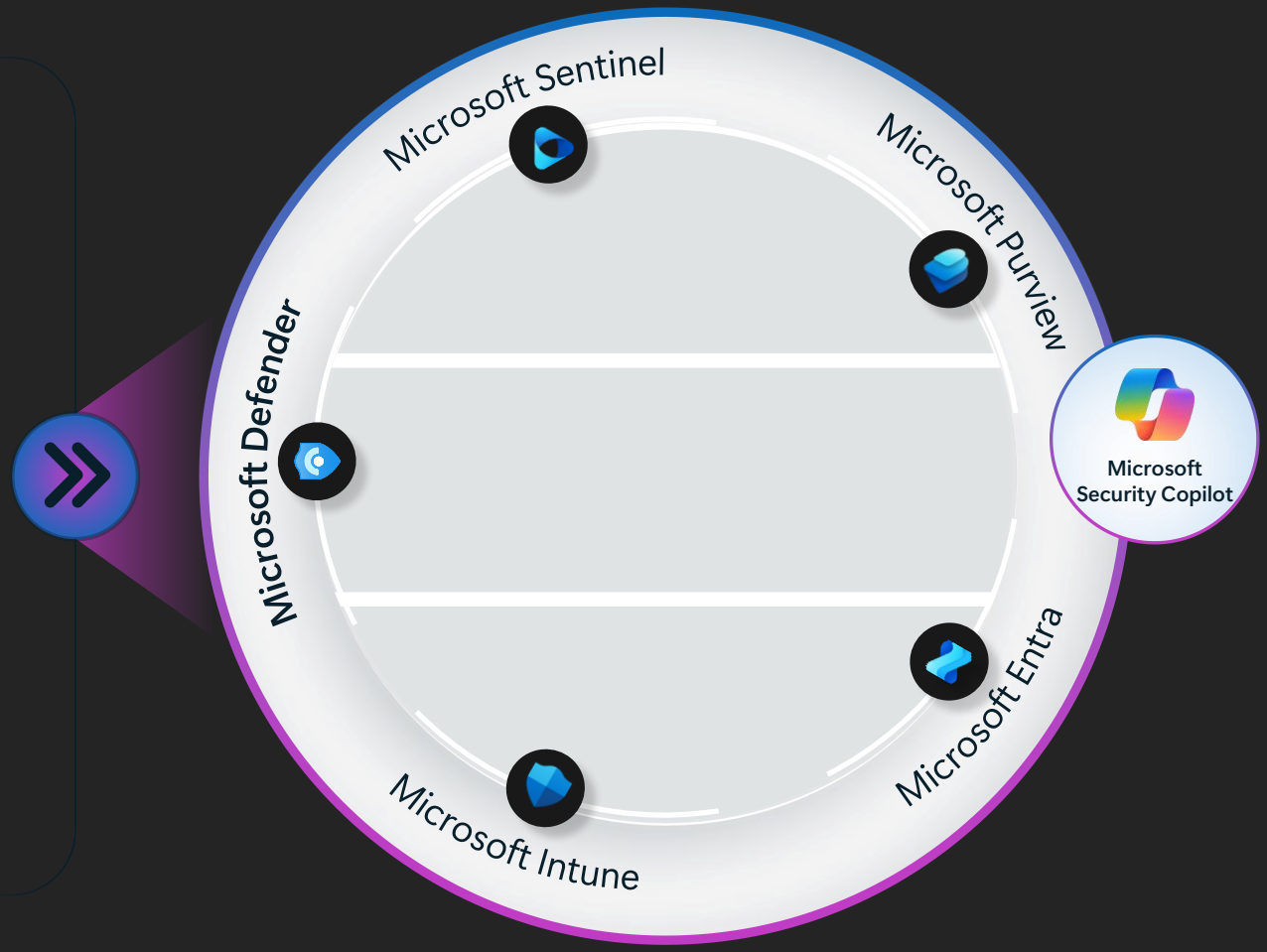
Defend against emerging AI threats + vulnerabilities

Discover and prevent risks
Defender - AI Security Posture Management
Azure AI Foundry - Red Teaming

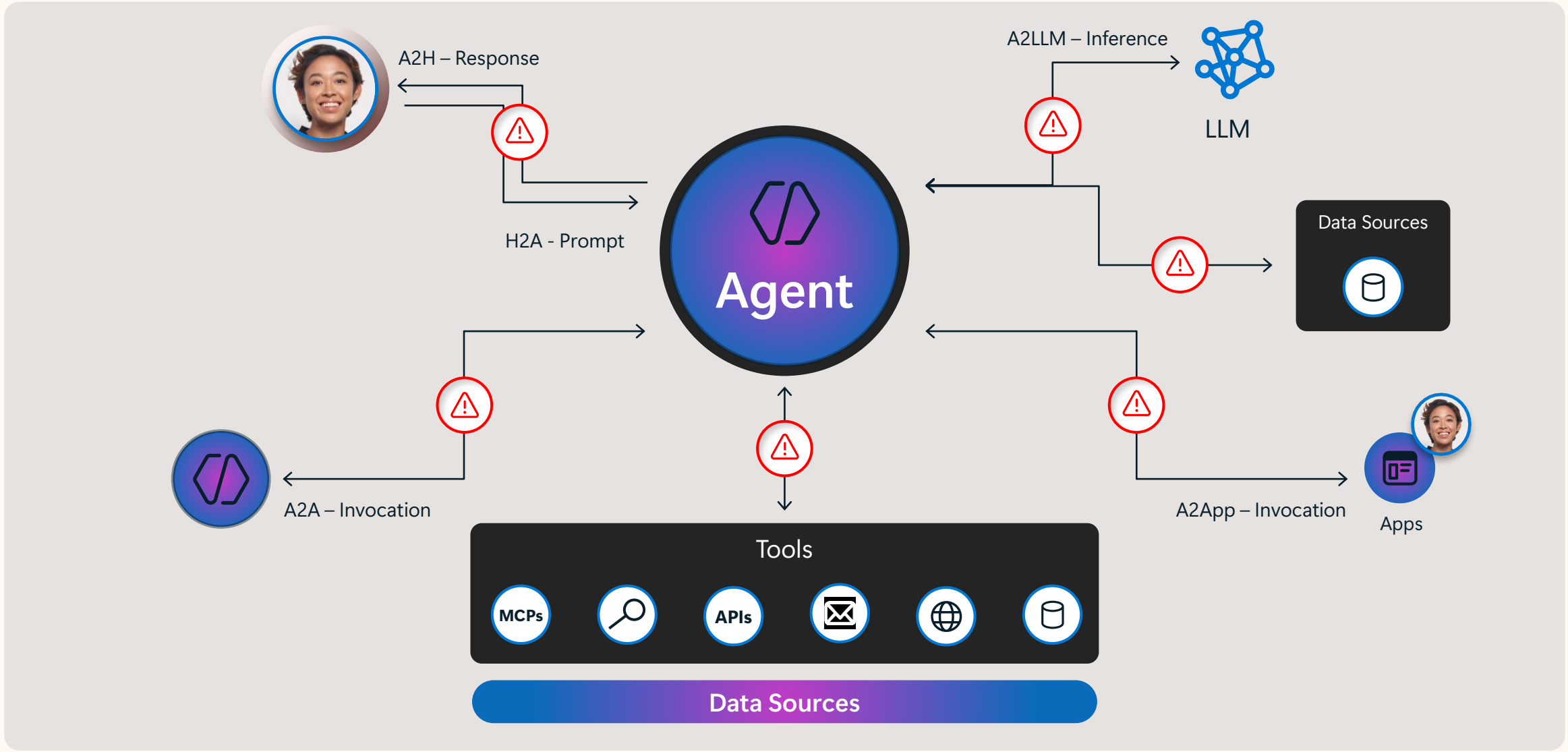
Defend and block AI threats
Defender for Cloud, Defender XDR
Azure AI Foundry - Content Safety Prompt Shields

Gain complete attack visibility
Defender for Cloud

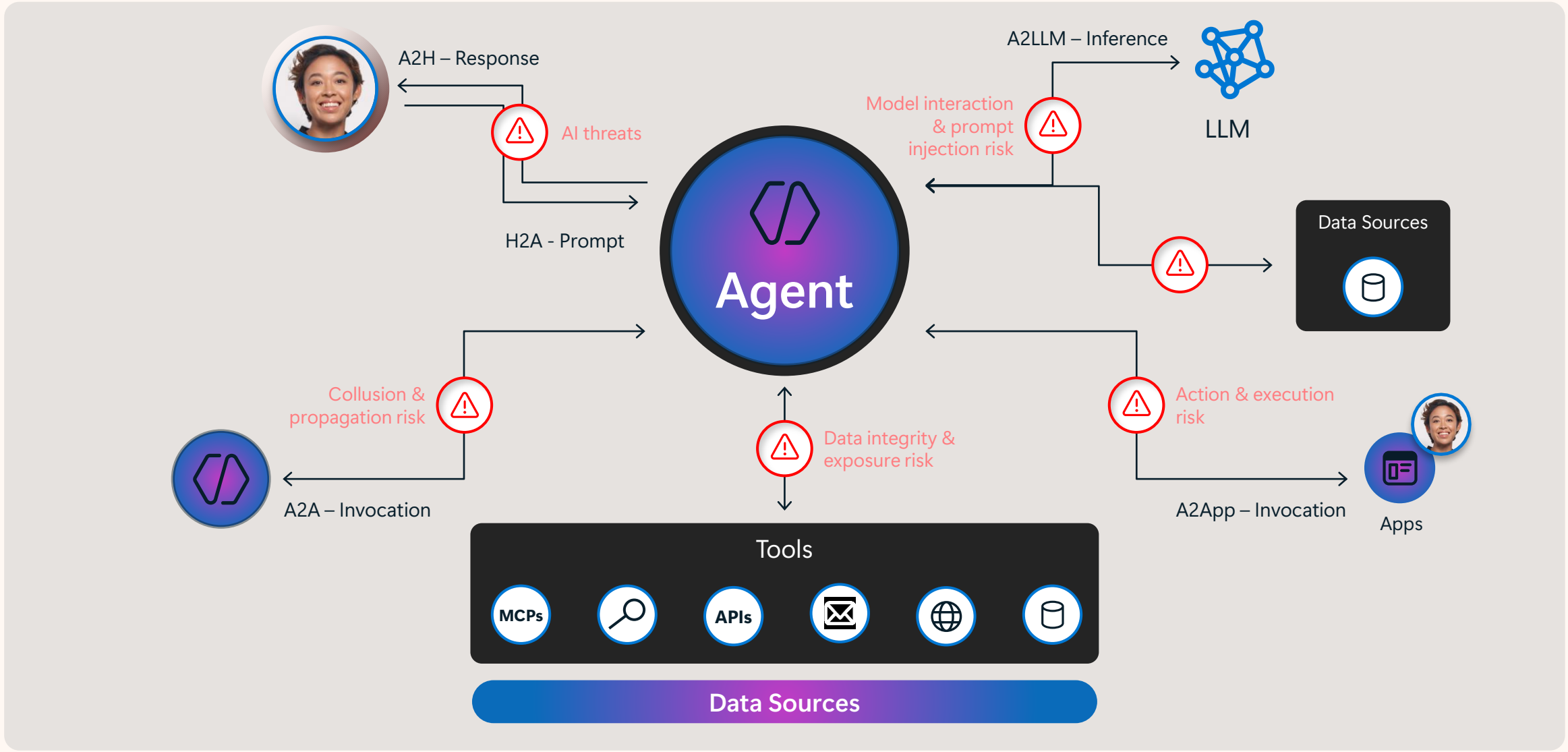
Enforce identity guardrails
Microsoft Entra - risk-based conditional access



Agents need same protection as users and more



Agents need same protection as users and more



Home
Exposure management
Investigation & response
Threat intelligence
Assets
Devices
Identities
Applications
Cloud infrastructure
AI Agents
Microsoft Sentinel
Identities
Endpoints
Email & collaboration
Cloud apps
Cloud infrastructure
Security Copilot
Agents
Security Store
Cases

AI Agents

All (551) | Azure AI Foundry (142) | Copilot Studio (409)

Security Posture for Agents

This feature is currently in preview and included with your Microsoft Defender CSPM license at no extra cost. Licensing requirements might change when the fea
you'll be notified should you wish to re-enable it under the new license.

Last 7 days

Discovered agents -2%
142

Agents requiring attention +400%
5

Refresh | Export

Filter set:

Account: Any | Project: Any | Model: Any | Deployment: Any | Agent Name: Any | Add filter

Agent name	Status	ID	Creation time	Deployment	Account
[redacted] Covered	Published	asst_D5FvPArwjVOj4GOmsuDjR4Kx	Oct 16, 2025, 1...	gpt-4.1	d4ai-foundry
Agent780 Covered	Published	asst_e1ITVCx9xPCAYCWdcjenMIcR	Nov 3, 2025, 7:...	gpt-4.1	foundry145
Agent217 Covered	Published	asst_ZAbVJB0S6YysIoSRARwEUIDr	Nov 3, 2025, 7:...	gpt-4.1	foundry145
Agent629 Covered	Published	asst_cRFtoC50JXG83e1H1FTLO075	Oct 30, 2025, 8...	gpt-4.1	foundry145
Agent487 Covered	Published	asst_IdE1svKmaGephqFUa21ErkAK	Oct 19, 2025, 5...	gpt-4.1	foundry145
coordinator					

Contoso Assist

Covered | Published | Platform: Azure AI Foundry

Open agent page | Go hunt | View on map

Agent info

ID
asst_D5FvPArwjVOj4GOmsuDjR4Kx

Name
coordinatorAgent

Creation time
Oct 16, 2025, 1:26 PM

Account
d4ai-foundry

Project
D4AI-Foundry/Dev-project

Deployment
gpt-4.1

Model
gpt-4.1 version 2025-04-14

Attack paths
18

Risk factors
Grounded With Sensitive Data

Recommendations

2 Recommendations

Critical: 0 | High: 0 | Medium: 0 | Low: 2

Home
Exposure management
Investigation & response
Incidents & alerts
Incidents
Alerts
Hunting
Actions & submissions
Partner catalog
Threat intelligence
Assets
Microsoft Sentinel
Identities
Endpoints
Email & collaboration
Cloud apps
Cloud infrastructure
Security Copilot
Agents
Security Store

Attack on Contoso Assist Agent

Copilot | Manage incident | Tasks

High | Active | Unassigned | Agents | CriticalAsset

Attack story | Alerts (3) | Activities | Assets (2) | Investigations (0) | Evidence and Response (3) | Summary | Similar incidents (1)

Alerts

Play attack story | Unpin all | Show all

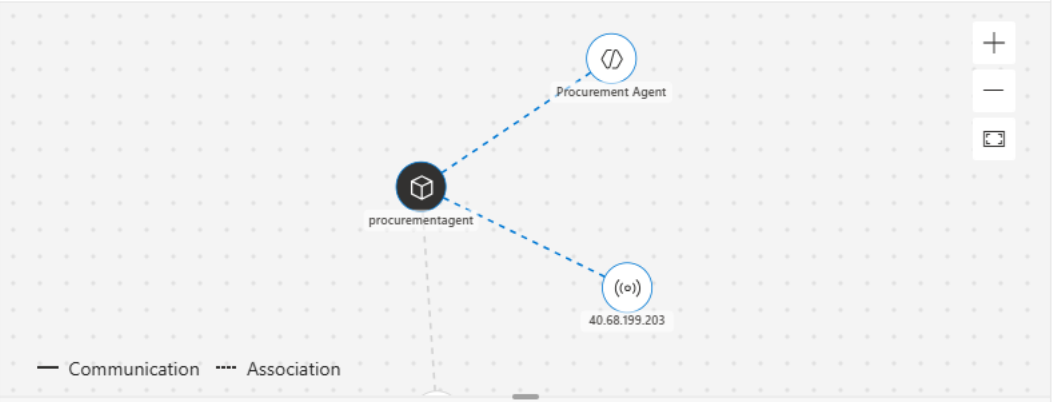
Nov 6, 2025 4:02 AM New
A user phishing attempt was detected on an AI agent (Preview)
procurementagent

Nov 6, 2025 10:03 AM New
A Jailbreak attempt was blocked on an AI agent (Preview)
procurementagent

Nov 9, 2025 2:19 PM New
DLP policy (Exfiltration to external recipient blocked) matched for email with subject (Procurement details for Orion)
Abbi Atkins

Incident graph

Layout | Group similar nodes



A user phishing attempt was detected on an... | A Jailbreak attempt was blocked on an AI a...

What happened

There was 1 blocked attempt of a Jailbreak attack on AI agent Procurement Agent on an Azure AI Foundry project procurementagent. A Jailbreak attack is also known as User Prompt Injection Attack (UPIA). It occurs when a malicious user manipulates the system prompt, and its purpose is to bypass a generative AI's large language model's safeguards in order to exploit sensitive data stores or to interact with privileged functions. Learn more at https://aka.ms/RAI/jailbreak. The attempts on your AI Agent were using direct prompt injection techniques and were detected by Azure Responsible AI Content Filtering. To get detailed information on the prompt injection attempts, refer to the 'Supporting evidence events' section in the Azure Portal.

This alert is triggered by MDC detection
View alert page in MDC

Activities

Activity details | Related activities

Back to incident details

A Jailbreak attempt was blocked on an AI agent (Preview)

Medium | Unknown | New

Open alert page | Manage alert

Details | Recommendations

INSIGHT

Quickly classify this alert

Classify alerts to improve alert accuracy and get more insights about threats to your organization.

Classify alert

Alert state

Classification	Assigned to
Not Set	Unassigned
Set Classification	

Alert details

Alert ID	Category
dc4cd5e5ae-2bab-	Privilege escalation

Wrap-up

And btw, there is a lot more, e.g., Power Platform, Viva Analytics, MCP servers,...

1. Copilot is more than just AI chat - It's a comprehensive ecosystem that spans productivity, security, governance, and automation.

2. Copilot Agents are the future of scalable IT - With Agent 365 and Copilot Studio, but admins have control.

3. Security and compliance are built-in, not bolted on - Tools like Microsoft Purview, Entra, and Defender ensure Copilot usage aligns with Zero Trust.

4. Oversharing is the #1 risk - Use DSPM for AI and oversharing assessments to identify and mitigate data exposure.

5. Insights drive adoption and ROI - The Copilot Dashboard and Viva Insights help measure usage, impact, and business value.

Q & A

Ondrej Vysek

Unlocking Infinite Possibilities Through Technology | SoftwareOne | Microsoft MVP

Microsoft Copilot for Admins:

https://admin.cloud.microsoft/

Ondrej Vysek

Unlocking Infinite Possibilities Through Technology | SoftwareOne | Microsoft MVP