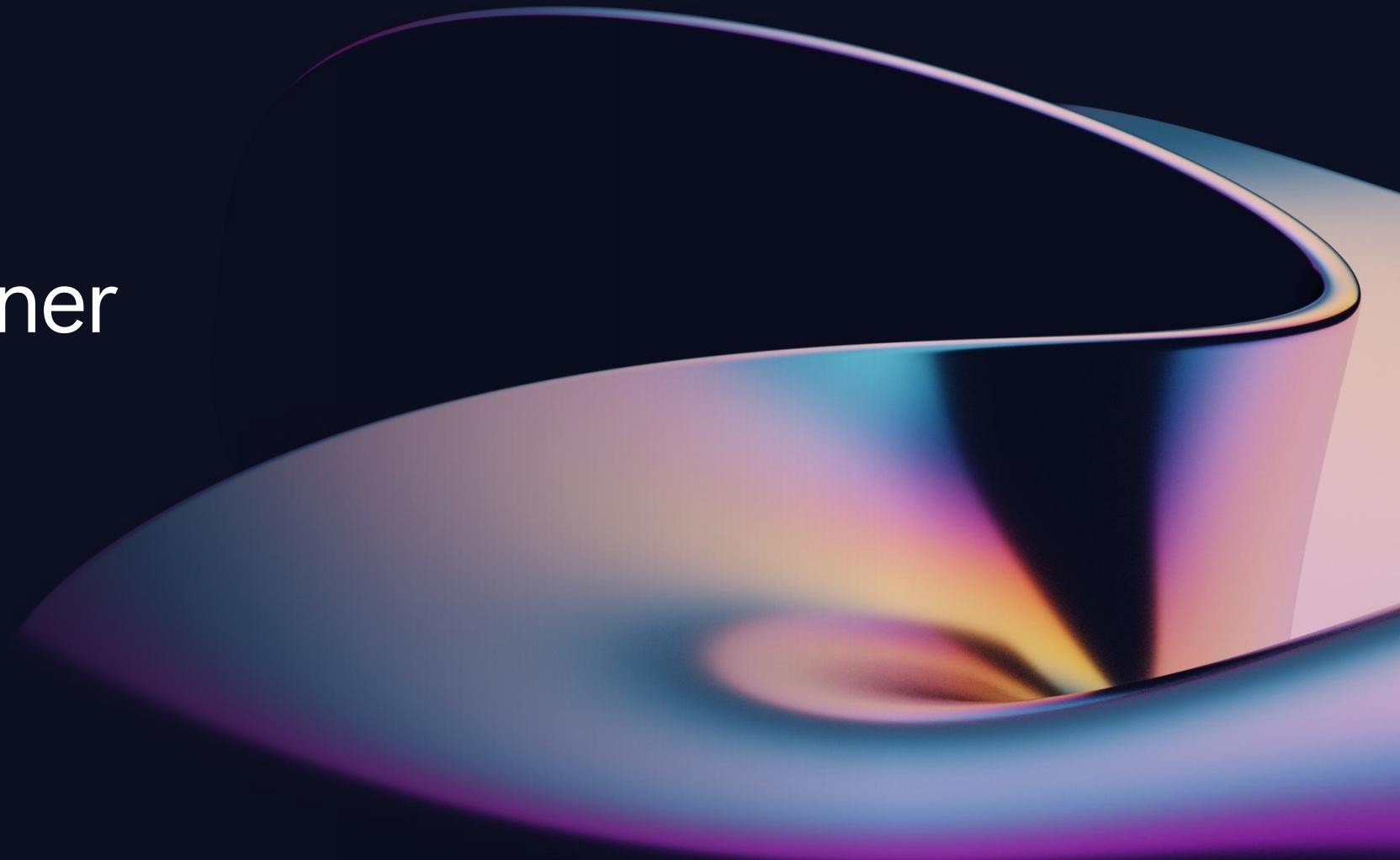




# Microsoft AI Partner Training Day





You are here

# The AI Partner Training Day

SALES AND TECHNICAL  
ENABLEMENT TRACKS



## Sales Excellence

Driving sales success with Microsoft AI

## Technical Deep Dive

Build Apps with Azure AI

## Technical Overview

Microsoft Copilot and AI Stack

• Sales • — Technical —

# Presenters



Presenter 1



Presenter 2



Procter 1



Procter 2

# T3: Agenda

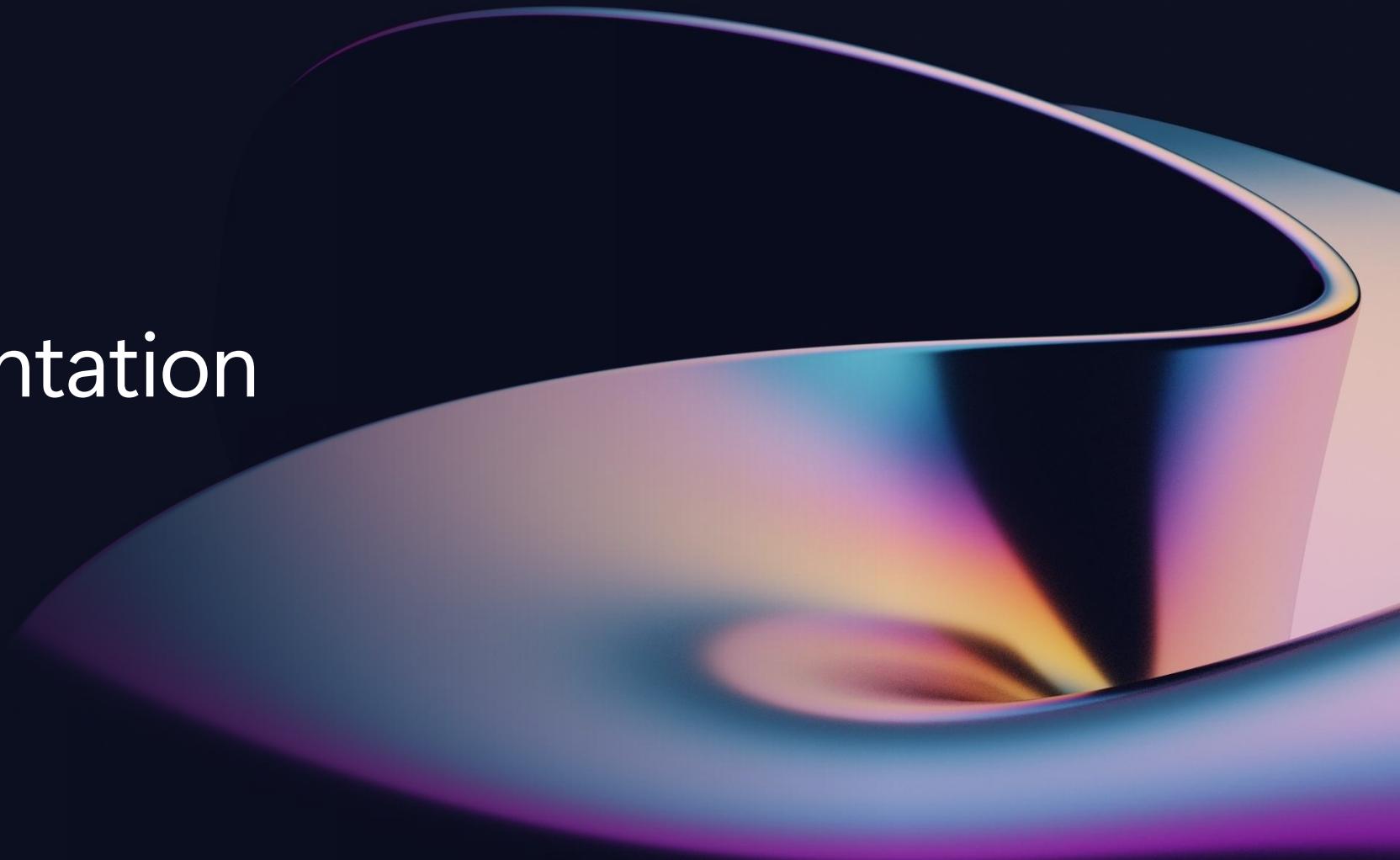
Timing	Session	Duration
10:45-11:30	Copilot Implementation Essentials	45 mins
11:30-12:45	Workshop: Build and customize agents with Copilot Studio	75 mins
<b>12:45-13:30</b>	<b>Lunch Break</b>	<b>45 mins</b>
13:30-14:15	Extending Microsoft 365 Copilot and maximizing the potential of your Teams app with AI	45 mins
14:15-15:00	The foundation of generative AI in Azure	45 mins
15:00-15:45	Securing AI applications on Azure	45 mins
<b>15:45-16:00</b>	<b>Break</b>	<b>15 mins</b>
16:00-17:00	Workshop: Build your first agent with Azure AI Agent Service	60 mins
17:00-18:15	NVIDIA Inference Microservices and NIM Agent Blueprints	75 mins
18:15-19:00	Networking	45min



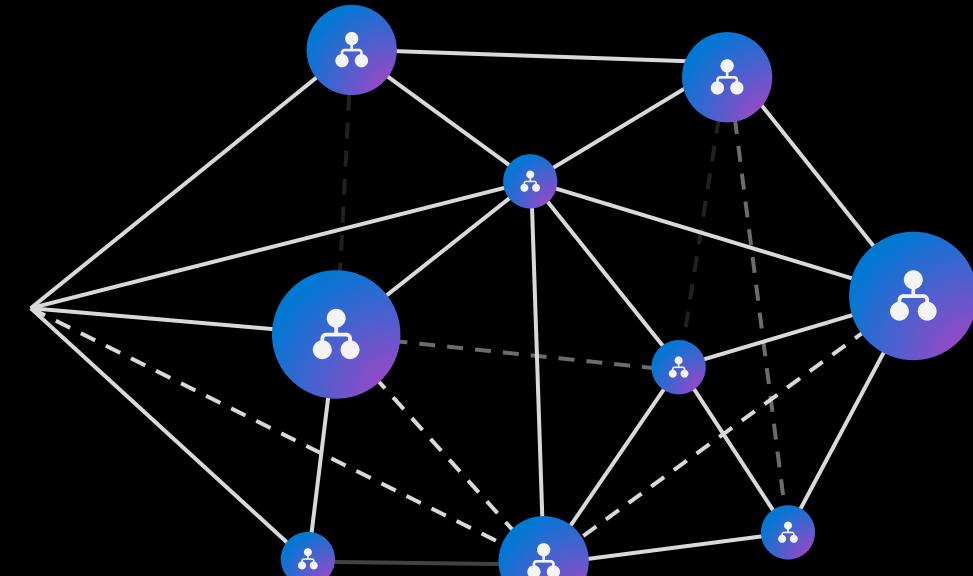
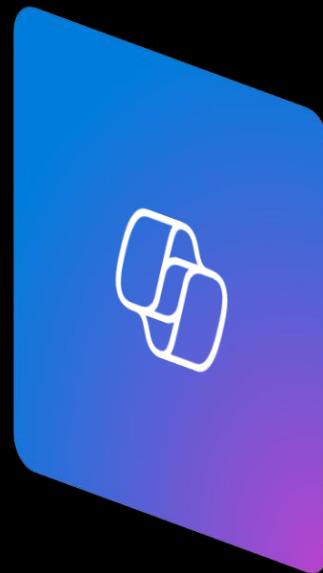
Microsoft AI Partner Training Day

Track 3

# Copilot implementation essentials



# Copilot is the UI for AI



# Microsoft 365 Copilot

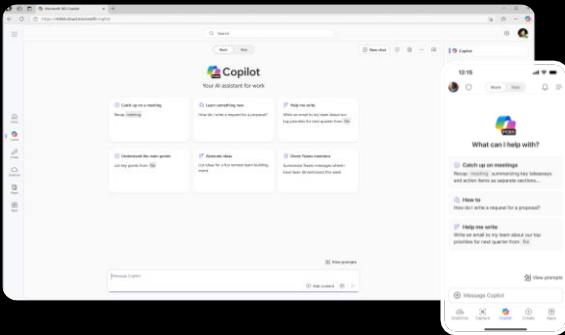


## Microsoft 365 Copilot

- 1 Consistent UI for AI
- 2 Integrated in the tools millions use every day
- 3 Platform for agents and extensibility
- 4 Enterprise-grade security, privacy, and compliance
- 5 Flexible purchasing and deployment options
- 6 Measure AI impact and business value



# Introducing Microsoft 365 Copilot Chat



## Chat

Free AI chat -- powered by GPT 4o and grounded in the web

+

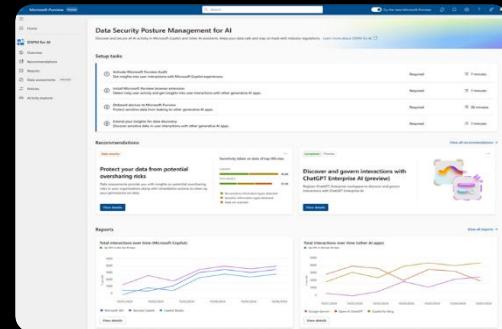
## Agents

Integrated into the chat experience and paid for on a consumption basis

+

## IT Controls

Enterprise Data Protection and management





# Microsoft 365 Copilot

Your personal AI assistant

\$30

## Copilot Chat

Free, secure AI chat



## Chat

Work scope

## Copilot in Microsoft 365 apps

Teams, Outlook, Word, Excel, PowerPoint

## Agents

## Copilot Control System

## Copilot Analytics

# The journey to becoming AI powered

## Leadership

Develop leadership capabilities to leverage AI for business outcomes

- ✓ Foundational learning
- ✓ Business strategy
- ✓ AI Council creation
- ✓ Providing clarity and prioritization

## Human change

Manage the human transformation through robust user enablement programs

- ✓ Invest in the employee experience
- ✓ Improve the culture
- ✓ Authentically integrate feedback

## Technical skills

Build and iterate technical skills to deliver on business results

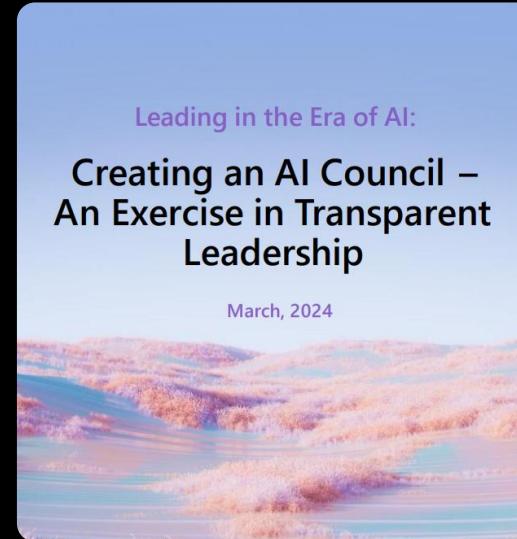
- ✓ Provide access to training and experts
- ✓ Manage and mitigate risk
- ✓ Improve service management process

Responsible AI principles

# Leverage AI for business outcomes



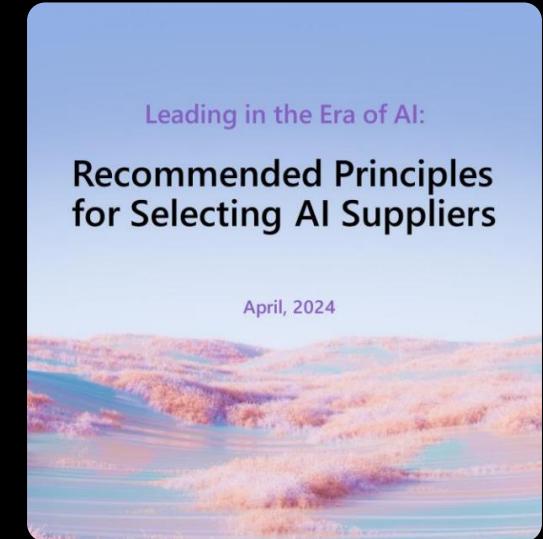
Get tips for your AI journey with actionable guidance from early adopters with the [Business Leader's guide for AI adoption](#).



Explore practical guidance for aligning AI strategy with business goals and mitigating risk with the [Leading in the Era of AI: Creating an AI Council – An Exercise in Transparent Leadership](#) whitepaper.



Learn about building trust and putting human connections first to get the most from AI with the whitepaper [Leading in the Era of AI: It's not about AI – It's about trust](#).



Read how those you enlist to support your success will guide it to the next horizon of business expansion with the [Leading in the Era of AI: Recommended Principles for Selecting AI Suppliers](#) whitepaper.

# Microsoft 365 Copilot

## Implementation summary

### 1 Get ready

Select initial departments for rollout with the [Scenario Library](#). Target a critical mass of users for rapid impact.

- Identify your success team
- Be intentional with assignment and concentrate seats

### 2 Onboard & engage

Lay the foundation for an intelligent progression of AI skills with [Copilot Lab](#).

- Deploy training and Champion programs, engagement community
- Make ongoing training the standard

### 3 Deliver impact

Review success measures with the [Copilot Dashboard](#) and the [User survey kit](#).

- Quantify impact including growth, cost savings and employee benefits
- Build momentum with success stories and knowledge sharing

### 4 Extend & optimize

Extend to new scenarios and transform business processes.

- Identify new high value functional and cross-org scenarios
- Recognize and reward success

User enablement



Technical readiness

Perform the Microsoft Microsoft 365 Copilot [Optimization Assessment](#)

- Address data security, governance, and data access questions
- Build shared Copilot implementation plan with User Enablement team

Prepare Microsoft 365 for AI deployment with the [Setup Guide](#)

- Ensure appropriate Data Security controls are in place
- If needed, deploy updates and additional Microsoft 365 apps

Mature AI management skills through improved IT service delivery

- Establish service management plan
- Review Admin usage reports and the [Copilot Dashboard](#) to analyze user retention and engagement

Provide insights on service health and optimization opportunities

- Design, build, and publish plugins to deliver unique experiences
- Build your own copilots

Microsoft is here to help accelerate your Copilot journey with expert-led services

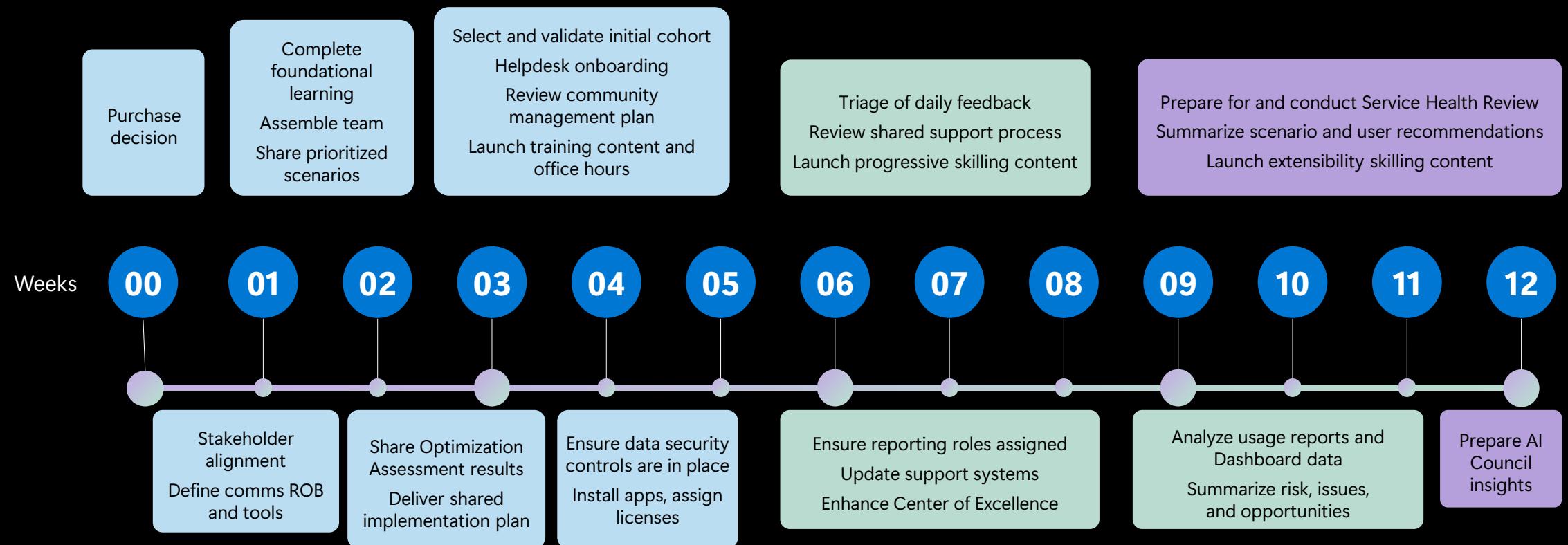
# Implementation project summary

First 30 days

30-60 days

Recurring tasks

## Shared milestone view



# Be intentional with seat assignments and define success criteria



## Copilot brings AI value across lines of business

1 Review which departments have the highest Microsoft 365 usage data, starting with Teams meetings and PowerPoint.

2 Concentrate licenses across entire teams or departments to start.

3 Use the **Scenario Library** to identify top use cases and the key metrics you would like to improve in that functional area.

### All roles

Improve meetings
Content creation
Manage daily agenda
Summarize information
Generate ideas

### HR

Cost per hire
Employee turnover
Compliance risk reduction
Benefit usage
Onboarding time

### Marketing

Leads created
Brand value
Cost per lead

### Operation

Customer retention
Product time to market
Supply chain efficiencies

### IT

Outstanding support tickets
Application downtime
Departmental spending

### Sales

Number of opportunities
Close rate
Revenue per sale
Customer retention
Time to close

### Finance

Accelerate cash flow
Spend on ERP system
Risk reduction
Departmental spending
Departmental spending

# Prepare Tenant for Agents

## Journey to Copilot

# IT Admin access controls for Copilot agents

## Power Platform Admin Center

Developer and resource access

### Agent & connector catalog

- Admins control whether developers can publish from Copilot Studio when AI features are enabled

### Management and monitoring

- Admins control which connectors and API endpoints are allowed in Power Platform environments

### Developer access

- Admins control who has developer permissions in a Power Platform environment

## Microsoft 365 Admin Center

Agent access, publishing, deployment and measurement

### Agent & connector catalog

- Admins can review agents and publish to tenant catalog
- Admins are notified about new agents awaiting review via Teams notifications
- Admins can review API endpoint of any Copilot agent
- Developers are notified about admin decision on approval of requested apps

### Management and monitoring

- Admins can apply tenant postures for 1P/3P/LOB apps with agents
- Admins can manage agents at an app level for user access and pre-installation
- Admins can view agent usage

### User access

- Admins can manage who can upload a package with agents for personal use (planned) Available now in Teams Admin Center
- Admins can review and consent to AAD SSO permission for actions via API endpoints

## Teams Admin Center (TAC)

### User access

- Admin can manage who can upload and use custom apps

## SharePoint Advanced Management (SAM)

### User access

- Admins can manage who can create and use SharePoint agents
- Admins can restrict access to SharePoint sites to specific users to isolate agent access
- Admins can apply content permissions policies to ensure users have access to appropriate content

## Microsoft Purview Portal

Security and governance controls

### Discover

- Admins can secure, govern, and identify risks in the use of AI applications with DSPM for AI
- Admins can view prompts and responses in activity explorer

### Protect

- MIP: Honor View/Extract usage rights for any content encrypted
- MIP: Cite sensitivity labels in Copilot output
- MIP: Sensitivity labels for files references in prompts/responses
- MIP: Conversation labeled with most restrictive sensitivity label

### Govern

- Admins can Audit AI prompts and responses
- Admins can preserve, collect, analyze, review, export AI interactions
- Admins can set retention and deletion policies for AI interactions
- Admins can detect business or regulatory violations in AI interactions

General Availability: May 2025

# Pin Copilot Chat to the navigation bar



To enable people in your organization to use Copilot Chat and agents, you can pin Copilot to the navigation bar of Teams, Outlook and Microsoft 365 Copilot app.

Pinning Copilot Chat is a key step to encouraging people in your organization to use Copilot Chat and agents by conveniently accessing it in these apps

As a global administrator or AI administrator, you can access this setting in the [Microsoft 365 admin center](#) by navigating to

- **Copilot > Settings > Pin Copilot.**
- Select **Pin Microsoft Copilot (recommended by Microsoft).**

Learn more about how to pin Copilot Chat through the Copilot settings in the Microsoft 365 admin center [here](#).

The screenshot shows the Microsoft 365 admin center interface. On the left, there's a navigation sidebar with options like Home, Copilot, Users, Devices, Teams & groups, Billing, Settings, and Setup. The main content area is titled 'Copilot' and contains sections for 'About Copilot' and 'What's new in Copilot'. Below these are tabs for Overview, Health, Discover, and Settings, with 'Settings' being the active tab. The main pane lists various Copilot-related items, such as 'Copilot agent consumption meter', 'Copilot diagnostic logs', 'Copilot for Sales', etc., each with a brief description and a 'Manage' link. To the right of this list is a detailed configuration panel for 'Pin Microsoft 365 Copilot Chat'. It includes a heading, a description, a 'Learn more about how this setting works' link, and two radio button options: 'Pin Copilot Chat to the navigation bar (recommended)' (unchecked) and 'Do not pin Copilot Chat to the navigation bar' (checked). There's also a checkbox for 'Allow users to be asked whether they want to pin it'. At the bottom of this panel is a 'Save' button.

# Set access permissions for Copilot Studio authors



For individual users who will need to create and manage agents, you will need:

- 1) a Copilot Studio tenant license for your organization, and
- 2) a Copilot Studio User License for individual users who need access to create and manage agents.

Copilot Studio licenses can be acquired through the [Microsoft 365 admin center](#). Learn more about Copilot Studio license assignment [here](#).

The screenshot shows the Microsoft 365 Admin Center interface. On the left, there's a sidebar with various icons. The main area is titled "Active users". A user named "Adele Vance" is selected, shown in a detailed view on the right. The "Licenses and apps" tab is active. Adele Vance has three Microsoft 365 E5 (no Teams) licenses assigned. There are sections for "Licenses (3)" and "Apps (107)". A blue "Save changes" button is at the bottom right.

**Active users**

Add a user Multi-factor authentication Refresh Delete user

Display name ↑	Username
Adele Vance	adelev@M365CPI82048
Adil Eli	AdilE@M365CPI82048
Amber Rodriguez	AmberR@M365CPI820
Automate Bot	AutomateB@M365CPI82048
Billie Vester	BillieV@M365CPI82048
Catie Jordan	cjtan@M365CPI82048
Conf Room Adams	Adams@M365CPI82048
Conf Room Baker	Baker@M365CPI82048
Conf Room Crystal	Crystal@M365CPI8204
Conf Room Hood	Hood@M365CPI82048
Conf Room Rainier	Rainier@M365CPI8204
Conf Room Stevens	Stevens@M365CPI820

**Adele Vance**

Change photo

Reset password Block sign-in Delete user

Account Devices Licenses and apps Mail OneDrive

Select location \* United States

Licenses (3)

Microsoft 365 E5 (no Teams) Microsoft Copilot Studio Microsoft Power Automate Microsoft Teams Enterprise Microsoft Teams Premium

Apps (107)

Save changes

# Configure Copilot agent consumption meter



Create a billing plan in the Power Platform admin center. You can reach Power Platform licensing from **Copilot > Settings** in the Microsoft 365 admin center and select 'Go to Power Platform billing configuration to enable consumption support'.

The screenshot shows the Microsoft 365 Admin Center interface. The left sidebar has 'Copilot' selected under the 'Copilot' category. The main content area is titled 'Copilot' and contains a sub-section titled 'Copilot agent consumption meter configuration'. It includes a brief description: 'Enable your users to do more with agents in Microsoft 365 Copilot Chat with consumption meters.' Below this are links to 'Learn more about pay-as-you-go setup' and 'Go to Power Platform billing configuration to enable consumption support'. The 'Copilot agent consumption meter configuration' section lists several items:

Name ↑	Description
Copilot agent consumption meter configuration	Setup and configure Microso
Copilot diagnostic logs	Send diagnostic logs for Cop
Copilot in Bing, Edge, and Windows	Manage how your organizati
Copilot in Edge	Copilot in Edge gives your or
Copilot in Teams meetings	Go to the Microsoft Teams ac
Data security and compliance	Manage how Copilot referen
Extensions	Choose who can use Copilot
Pin Copilot	Choose whether users have C
Web search for Microsoft 365 Copilot and Microsoft Copilot	Provide Copilot with addition

A 'Start' button is located at the bottom right of the configuration pane.

# Create a pay-as-you-go billing plan – can decrement MACC



In the navigation pane, select **Licensing**

In the **Licensing** pane, select **Pay-as-you-go plans**. The **Billing plans** page is displayed.

Select **New billing plan**.

Select Microsoft 365 Copilot Chat to create a billing plan, turn on pay-as-you-go billing, and provision a default Power Platform environment for Copilot Chat

- Provide a name for your new billing Plan
- Select an Azure subscription
- Specify a resource group with that subscription

The screenshot shows the Power Platform admin center interface. In the left navigation pane, under the **Licensing** section, the **Pay-as-you-go plans** option is selected. The main content area is titled **Billing plans** and contains the following information:

A pay-as-you-go plan is a group of one or more environments that you can configure to bill to Azure.

**Active**

Name ↓	Status	Azure subscription name	Resource group	Products	Region	Created on
M365BillingPlan	Provisioning	NeptuneE2E	-	Dataverse, Copil...	United States	1/2/2025
M365BillingPlan1	Enabled	NeptuneE2E	M365BillingPlan1	Dataverse	United States	1/2/2025

At the top of the **Billing plans** page, there is a button labeled **+ New billing plan** with a cursor pointing at it. Other buttons include **Refresh list**, **See details**, **Edit**, and **Download report**. A search bar labeled **Search plans** is also present.

# Review message capacity and consumption



You can monitor usage from the Licensing pane, under Products, and Copilot Studio, where you are provided with details in the Messages capacity tab for both prepaid as well as pay-as-you-go consumption for the current month.

The screenshot shows the Power Platform admin center interface. On the left, there's a navigation sidebar with various options like Home, Actions, Manage, Monitor, Security, Deployment, Licensing (which is selected), Copilot, and Support. At the bottom of the sidebar is an 'Admin centers' link. The main content area is titled 'Licensing' and shows 'Licenses'. It has tabs for 'Summary' (which is selected) and 'Environments'. Under 'Capacity summary', it shows 'Pay-as-you-go messages' with 1 Billing plan and 32000 Total messages. To the right, there's a table for 'Prepaid capacity' and another section for 'Capacity consumption by product' which shows M365 Copilot Chat using 150000 Prepaid and 32000 Pay-as-you-go messages. A cursor arrow is pointing at the Pay-as-you-go bar in the capacity consumption chart.

License type	Category	Purchased	Assigned	Consumed
Capacity	Messages capacity	200000	150000	150000
Capacity (Legacy)	Sessions capacity	0	0	0
Manage capacity				

# Copilot Technical Essentials

Journey to Copilot

Get ready

# Perform the Microsoft 365 Copilot Optimization Assessment

## Optimization Assessment

The assessment is designed to understand your current licensing profile, your collaboration tools, sensitive data handling, and security controls implemented today in your organization, helping you identify a clear path to deploying Microsoft 365 Copilot. The assessment consists of 26 questions and takes about 30 minutes to complete.

- Complete the Microsoft Microsoft 365 Copilot Optimization Assessment
- Understand current licensing
- Understand identity management
- Understand current collaboration tools
- Understand current data locations
- Uncover opportunities to implement data security measures and improve data security posture to optimize user experience with Microsoft 365 Copilot

[aka.ms/Copilot/OptimizationAssessment](https://aka.ms/Copilot/OptimizationAssessment)

The screenshot shows the results page of the Microsoft Copilot for Microsoft 365 Optimization Assessment. It features a header with the Microsoft Copilot logo and the title "Microsoft Copilot for Microsoft 365 Optimization Assessment Results". Below the header, there is a message of thanks for completing the assessment, followed by a summary of the organization's potential to take advantage of Copilot for Microsoft 365. The page includes three main performance metrics: "Blockers Identified" (0), "Microsoft 365 Copilot-ready users in your organization" (67%, 5000 of 7500), and "Customer Baseline" scores for "Organizational Profile Readiness" (90%, 19/16) and "Productivity Tool Readiness" (80%, 16/20). A note at the bottom explains the organizational readiness score. On the right, there is a section titled "Copilot for Microsoft 365 Deployment Path" with a "Best in Class" badge and a note about the deployment path being part of the overall technical readiness guidance.

**Microsoft Copilot for Microsoft 365 Optimization Assessment Results**

Thank you for taking the time to complete the Copilot for Microsoft 365 Optimization Assessment. You've taken an important step to understand how far along your organization is in adopting AI. This report highlights the foundational elements you already have to help your organization prepare for its digital transformation journey and take full advantage of Copilot for Microsoft 365.

The answers you provided in the Copilot Optimization Assessment give us your Optimization Scores, which reflects your organization's potential ability to take advantage of Copilot for Microsoft 365 to help increase employee productivity and security posture.

**Customer Baseline**

Organizational Profile Readiness	90%	19/16
Productivity Tool Readiness	80%	16/20

Your organizational readiness score relates to your ability to drive adoption of Copilot for Microsoft 365 through effective organizational sponsorship and awareness of the capabilities of generative AI solutions.

**Blockers Identified** 0  
This score reflects any primary blockers to overcome to get ready for Copilot for Microsoft 365 and the new era of AI.

**Microsoft 365 Copilot-ready users in your organization** 67%  
5000 of 7500

**Copilot for Microsoft 365 Deployment Path**  
**Best in Class**

The Copilot deployment path is part of the overall technical readiness guidance developed to help customers get started with their Copilot deployments quickly and continue to optimize their data security along the way.

# Address internal oversharing concerns for M365 Copilot deployment

	Pilot (Optional)	Deploy	Operate
Activities	<ul style="list-style-type: none"><li>Identify most popular sites &amp; assess oversharing</li><li>Grant Copilot access to popular, low risk sites</li><li>Turn on proactive audit and protection</li></ul>	<ul style="list-style-type: none"><li>Discover oversharing risks</li><li>Restrict sensitive info from Copilot access and/or processing</li><li>Increase site privacy</li></ul>	<ul style="list-style-type: none"><li>Further reduce risk and simplify oversight</li><li>Further secure sensitive data</li><li>Improve Copilot responses</li></ul>
Outcomes	<p>Deploy copilot to sub-set of users with up to 100 sites</p>	<p>Copilot fully deployed in your organization</p>	<p>Continuous improvement of data security practices</p>
Effort*	<p>2–4 days</p>	<p>2–4 weeks</p>	<p>More than one month</p>

\*Suggested efforts should be reviewed into timelines based on your tenant size and organizational complexity

Last updated December 10, 2024

# 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.

## Pre-requisites

- 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, chats they are part of, emails they send and receive, calendars they have access to, etc.
- Files that are shared with and accessed by users.
- Content from users' frequently visited sites.

Access this [blog](#) for more info

# Restricted SharePoint Search user notification

Microsoft 365

Search

Your organization's admin has restricted Copilot from accessing certain SharePoint sites. This limits the content Copilot can search and reference when responding to your prompts. [Learn more](#)

New chat ...

  
Copilot

**What's new?**  
What's the latest from person , organized by emails, chats, and files?

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

**Get calendar info**  
When's my next meeting with person ?

**Understand quickly**  
Provide a comprehensive summary of my emails about <placeholder>the FY24 Sales Report</placeholder>

**Help me write**  
Write an email to my team about our top priorities for next quarter from file

**Prep for that meeting**  
Help me prepare for meeting

OK, what can I help with? Try one of the examples or enter your own prompt.

[View prompts](#)

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

Need help?

# Microsoft 365 Copilot is the AI assistant you can trust

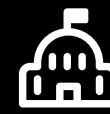


## Security

Honors your existing permissions

Persistent label inheritance and DLP policies

Risk-based conditional access and endpoint management



## Governance & Compliance

Ramp your data preparedness for AI

Detect and investigate non-compliant usage

Guided assistance to remain compliant with AI regulations



## Privacy

You control your data

You control your data location

Enterprise Data Protection

Your Microsoft 365 security, governance, compliance, and privacy policies

# Problem summary

Microsoft 365 Copilot (Copilot)'s ability to leverage information available to employees has raised concerns for organizations about overshared permissions

If oversharing risks aren't addressed, they could lead to



Access to information beyond what the user needs for their role



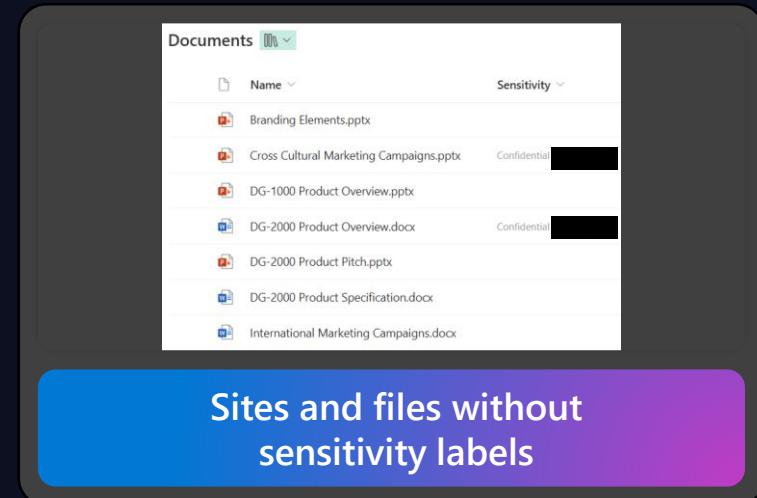
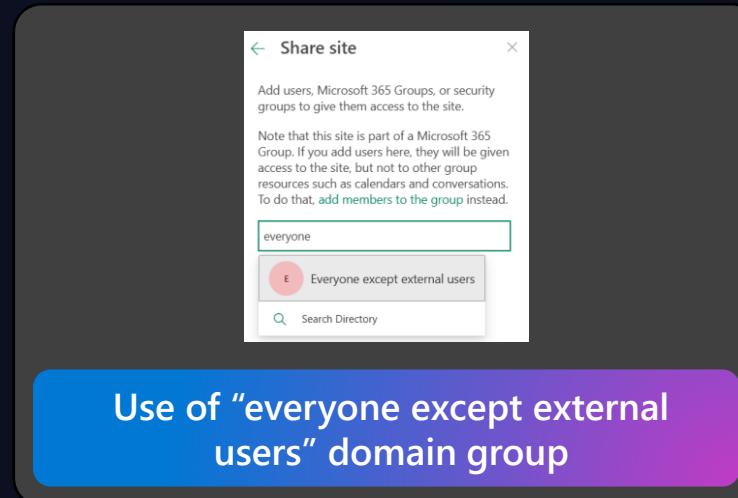
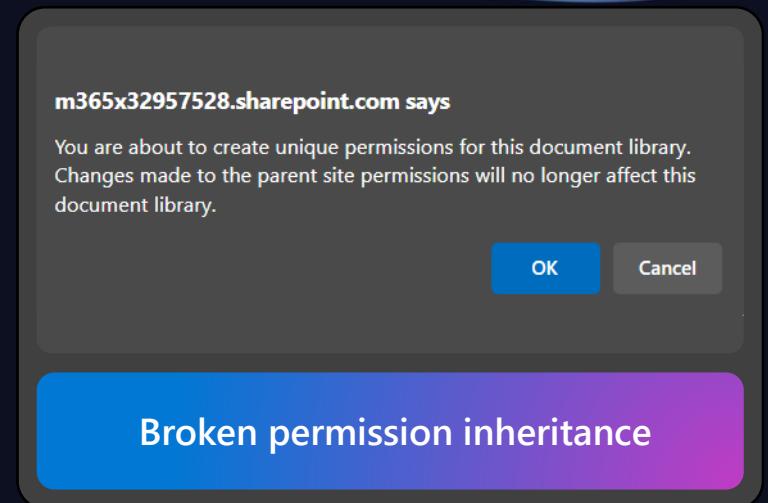
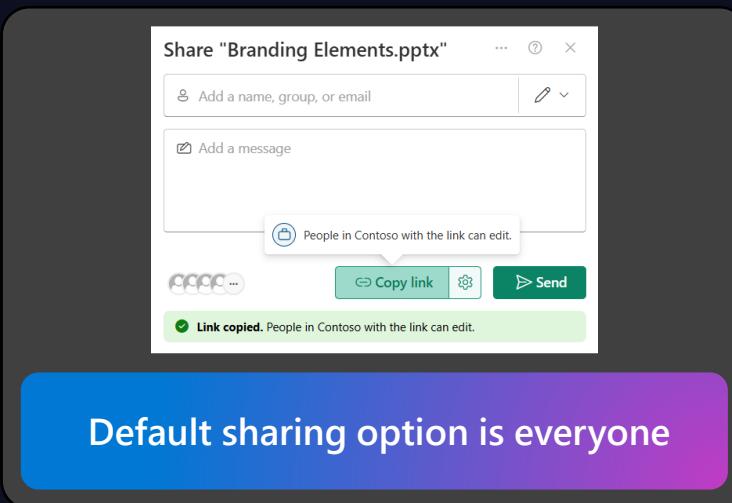
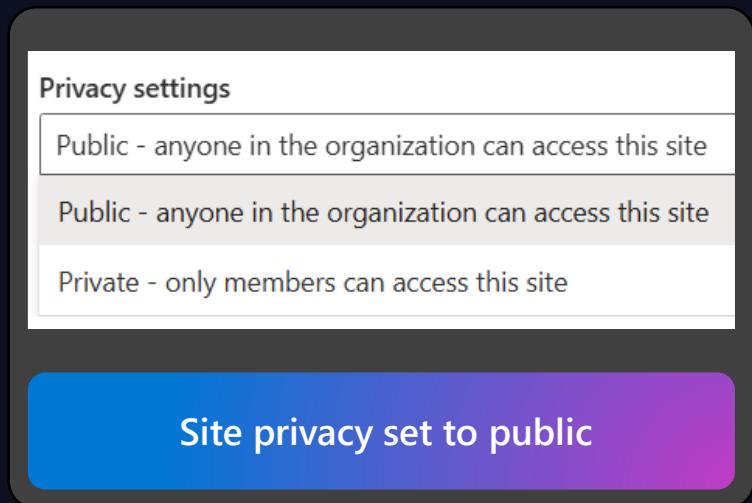
Inappropriate sharing of content



Out of date or irrelevant responses

By addressing these risks, organizations can ensure that information is shared appropriately and securely

# Common causes of Copilot oversharing in SharePoint



# Data protection tools used by Microsoft 365 Copilot

Microsoft SharePoint

Microsoft Purview classifications

Microsoft Entra Conditional Access policies

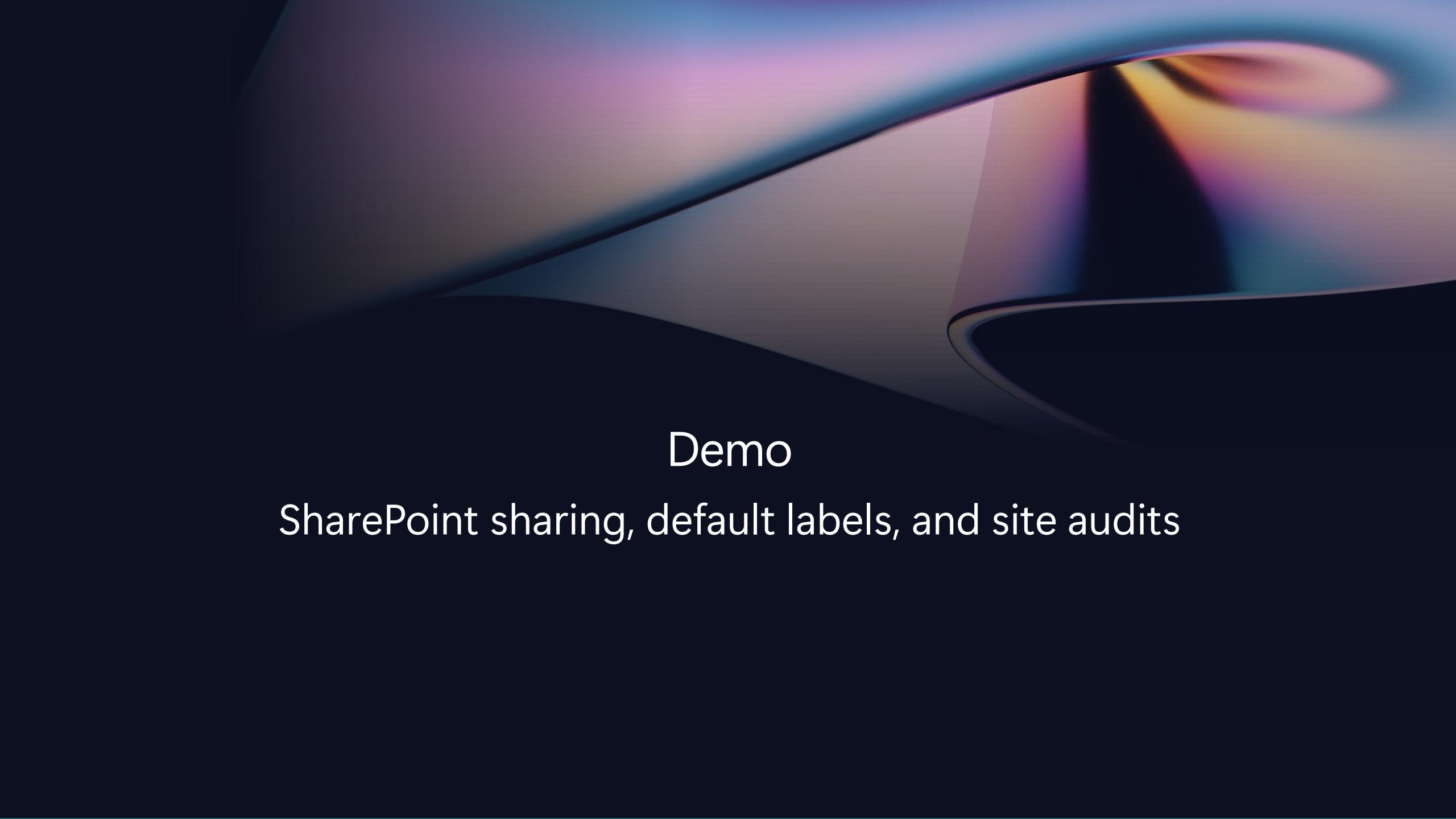
Microsoft Entra Privileged Identity Management (PIM)

Microsoft Entra ID Governance

Microsoft Defender for Cloud App Security

Microsoft Intune





# Demo

SharePoint sharing, default labels, and site audits



## Leadership

Public group Not following 20 members

Executive FY Goals

+ New

Upload

Sync

Add shortcut to OneDrive

Pin to Quick access

Automate

...

All Documents



Leadership accountability...

Leadership team

Shared with us

Recycle bin

Edit

[Return to classic SharePoint](#)

## Documents

Name

Modified

Modified By

+ Add column

Executive FY Goals.pptx

July 12, 2023

Megan Bowen

Far East Region Support.xlsx

July 12, 2023

Patti Fernandez

New Litware-Contoso Partnership.docx

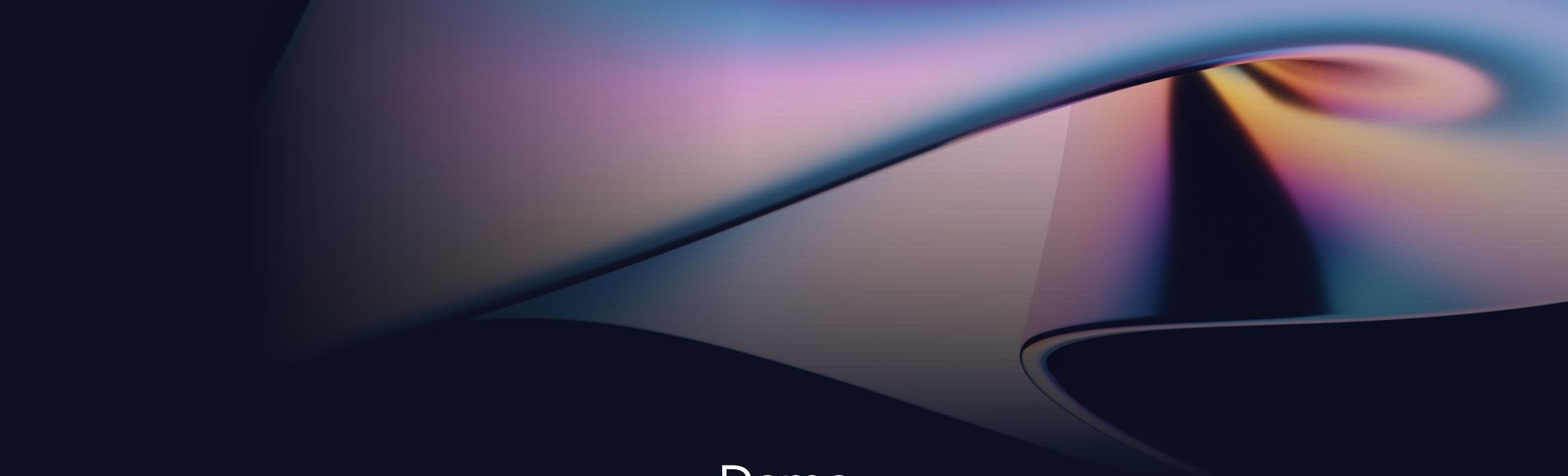
July 12, 2023

Megan Bowen

Strategic Objectives.pptx

July 12, 2023

Megan Bowen



## Demo

How Copilot respects classified content and can  
automatically apply labels

Draft with Copilot

Draft a confirmation using the terms from [Contoso Purchase agreement for Mark 8 quadcopters.docx](#)

96/2000

Generate

Reference a file

# Address internal oversharing concerns in Microsoft 365 Copilot

## LEGEND

1 – Copilot and SharePoint Adv. Mgt.

2 – OE3/ME3

Realize value quickly with Copilot by reviewing potential content sharing risks and optionally enabling Restricted SharePoint Search to address risk to enable full Copilot deployment

Select services are included in your FastTrack benefit. Other critical services are available thru Microsoft Unified or our Partner Ecosystem

Phase	Pilot (Optional)	Deploy	Operate
Effort	2–4 days	2–4 weeks	1+ months
Deployment steps	<p><b>1. Identify the most popular sites &amp; assess oversharing</b></p> <ul style="list-style-type: none"> <li>Export the top 100 most used sites from SPO admin center</li> <li>Run SAM permission state report<sup>1</sup></li> <li>Use Purview Content Explorer to view which sites contain sensitive information types (SITs)<sup>2</sup></li> </ul> <p><b>2. Grant Copilot access to popular, low risk sites</b></p> <ul style="list-style-type: none"> <li>Cross reference the report results from SAM and Purview Content Explorer with the top 100 used sites to identify up to 100 sites to be allowed for Copilot discovery<sup>1,2</sup></li> <li>Optionally enable Restricted SharePoint Search (RSS) for up to 100 sites identified<sup>1</sup></li> </ul> <p><b>3. Turn on proactive audit and protection</b></p> <ul style="list-style-type: none"> <li>Turn Off EEEU (everyone except external users) at the tenant level<sup>2</sup></li> <li>Turn on Audit and view Copilot interaction activity reports and charts<sup>1,2</sup></li> <li>Turn on oversharing SPO Purview DLP policy in simulation mode to detect anyone sharing links for labeled and unlabeled data<sup>2</sup></li> </ul>	<p><b>1. Discover oversharing risks</b></p> <ul style="list-style-type: none"> <li>Use permission state report with SITs to flag sites and files that are potentially overshared (Includes: EEEU, company shared links)<sup>1</sup></li> <li>Identify Copilot agent insights &amp; take actions<sup>1</sup></li> </ul> <p><b>2. Restrict sensitive info from Copilot access and/or processing</b></p> <ul style="list-style-type: none"> <li>Initiate Access Review for all sites that are overshared<sup>1</sup></li> <li>Apply restricted access control (RAC) on business-critical sites<sup>1</sup></li> <li>Exclude critical sites from Copilot reasoning over them<sup>1</sup></li> </ul> <p><b>3. Increase site privacy</b></p> <ul style="list-style-type: none"> <li>Publish labels to Office apps, Container/Sites, Outlook for manual data protection by user<sup>2</sup></li> <li>Use site labels to limit access to org-wide sharing by marking sites as 'Private' and giving access only to site members<sup>2</sup></li> <li>Turn on enforce-mode oversharing SPO DLP policy to restrict access to sensitive data exposure &amp; starting remediating them<sup>2</sup></li> <li>Disable RSS (if enabled) to allow full Copilot experience<sup>1</sup></li> </ul>	<p><b>1. Further reduce risk and simplify oversight</b></p> <ul style="list-style-type: none"> <li>Routinely run the SAM site lifecycle management policy's site ownership policy and review the ownerless sites and assign owners<sup>1</sup></li> <li>Automate SAM permission state report to maintain permissions hygiene<sup>1</sup> <ul style="list-style-type: none"> <li>Automate permission reports and actions to maintain permission hygiene<sup>1</sup></li> <li>Regularly review oversharing reports and restrict access as needed<sup>1</sup></li> <li>Proactively avoid oversharing by applying RAC at site provisioning<sup>1</sup></li> <li>Periodically review inactive sites and take necessary action<sup>1</sup></li> <li>Control site provisioning by allowing creation for users that complete training<sup>1</sup></li> <li>Use change history to identify site changes that may cause oversharing<sup>1</sup></li> </ul> </li> <li>Continuously manage all your oversharing DLP alerts via the Microsoft Purview Portal<sup>2</sup></li> </ul> <p><b>2. Further secure sensitive data</b></p> <ul style="list-style-type: none"> <li>Reduce risk by remediating alerts for overshared documents from the SPO DLP policy and applying sensitive labels<sup>2</sup></li> </ul> <p><b>3. Improve Copilot responses</b></p> <ul style="list-style-type: none"> <li>Setup retention/deletion policies for SharePoint to reduce data surface<sup>2</sup></li> <li>Identify inactive sites, then restrict access or delete<sup>1</sup></li> </ul>

Guidance assumes Copilot technical prerequisites in place: Technical enablement of core services (Teams, SharePoint, Exchange), Office Applications deployed (modern Outlook recommended) and on current or monthly update channel

Learn how to use the features in the blueprint and how these features impact Microsoft 365 Copilot: <https://aka.ms/E3PrepareYourDataForCopilot>

Last updated December 10, 2024

# Address internal oversharing concerns in Microsoft 365 Copilot

LEGEND

1 – Copilot and SharePoint Adv. Mgt.

2 – OE3/ME3

Realize value quickly with Copilot by reviewing potential content sharing risks and optionally enabling Restricted SharePoint Search to address risk to enable full Copilot deployment

Select services are included in your FastTrack benefit. Other critical services are available thru Microsoft Unified or our Partner Ecosystem

Phase	Pilot (Optional)	Deploy	Operate
Effort	2–4 days	2–4 weeks	1+ months
Deployment steps	<p><b>1. Identify the most popular sites &amp; assess oversharing</b></p> <ul style="list-style-type: none"> <li>Export the top 100 most used sites from SPO admin center</li> <li>Run SAM permission state report<sup>1</sup></li> <li>Run the Purview DSPM for AI Data assessments to gain visibility into all data at risk of Copilot access, pivoted on labels and sensitive information types<sup>3</sup></li> </ul> <p><b>2. Grant Copilot access to popular, low risk sites</b></p> <ul style="list-style-type: none"> <li>Cross reference the report results from SAM and Purview DSPM for AI with the top 100 used sites to identify up to 100 sites to be allowed for Copilot discovery<sup>1,3</sup></li> <li>Optionally enable Restricted SharePoint Search (RSS) for up to 100 sites identified<sup>1</sup></li> </ul> <p><b>3. Turn on proactive audit and protection</b></p> <ul style="list-style-type: none"> <li>Turn Off EEEU (everyone except external users) at the tenant level<sup>2</sup></li> <li>Turn on Purview Audit and view Copilot interaction activity reports and charts<sup>1,2,3</sup></li> <li>Turn on proactive analysis for sensitive data handling with prompts and responses with Purview Communications Compliance<sup>3</sup></li> <li>Turn on oversharing SPO Purview DLP policy in simulation mode to detect anyone sharing links for labeled and unlabeled data<sup>2</sup></li> </ul>	<p><b>1. Discover oversharing risks</b></p> <ul style="list-style-type: none"> <li>Use DAG permission state report with SITs to flag sites and files that are potentially overshared (Includes: EEEU, company shared links)<sup>1</sup></li> <li>Identify Copilot agent insights &amp; take actions<sup>1</sup></li> <li>Create customized Purview DSPM for AI Data assessments to scale out data security actions, pivoted on labels and sensitive information types<sup>3</sup></li> </ul> <p><b>2. Restrict sensitive info from Copilot access and/or processing</b></p> <ul style="list-style-type: none"> <li>Initiate SAM Access Review for all sites that are overshared<sup>1</sup></li> <li>Apply SAM restricted access control (RAC) on business-critical sites<sup>1</sup></li> <li>Exclude critical sites from Copilot reasoning over them with SAM Restricted Content Discovery (RCD)<sup>1</sup></li> <li>Publish sensitivity labels with Purview Information Protection to Office apps, Container/Sites, Outlook for manual data protection by user<sup>2</sup></li> <li>Exclude Copilot from summarizing sensitive content via sensitivity labels<sup>3</sup></li> </ul> <p><b>3. Increase site privacy</b></p> <ul style="list-style-type: none"> <li>Use site sensitivity labels to limit access to org-wide sharing by marking sites as 'Private' and giving access only to site members<sup>2</sup></li> <li>Apply default site library sensitivity labels to protect new and modified unlabeled documents<sup>3</sup></li> <li>Turn on enforce-mode oversharing SPO Purview DLP policy to restrict access to sensitive data exposure &amp; starting remediating them<sup>2</sup></li> <li>Disable RSS (if enabled) to allow full Copilot experience<sup>1</sup></li> </ul>	<p><b>1. Further reduce risk and simplify oversight</b></p> <ul style="list-style-type: none"> <li>Routinely run the SAM site lifecycle management policy's site ownership policy and review the ownerless sites and assign owners<sup>1</sup></li> <li>Automate SAM permission state report to maintain permissions hygiene<sup>1</sup> <ul style="list-style-type: none"> <li>Automate permission reports and actions to maintain permission hygiene<sup>1</sup></li> <li>Regularly review oversharing reports and restrict access as needed.<sup>1</sup></li> <li>Proactively avoid oversharing by applying RAC at site provisioning.<sup>1</sup></li> <li>Periodically review ownerless sites and take necessary action<sup>1</sup></li> <li>Control site provisioning by allowing creation for users that complete training<sup>1</sup></li> <li>Use change history to identify site changes that may cause oversharing<sup>1</sup></li> </ul> </li> <li>Routinely run Purview DSPM for AI Data assessments to scale out data security actions, pivoted on labels and sensitive information types<sup>3</sup></li> <li>Continuously manage all your oversharing Purview DLP alerts via incidents with Microsoft Defender XDR incident queue<sup>2</sup></li> <li>View risky user activity in context of oversharing Purview DLP incidents<sup>3</sup></li> </ul> <p><b>2. Further secure sensitive data</b></p> <ul style="list-style-type: none"> <li>Automatically label new documents and prevent them from oversharing with run time auto-labeling policy, starting with client-side policies and extend to service-side policies<sup>3</sup></li> <li>Reduce risk by remediating alerts for overshared documents from the SPO Purview DLP policy by applying sensitive labels and disabling anyone access<sup>2</sup></li> </ul> <p><b>3. Improve Copilot responses</b></p> <ul style="list-style-type: none"> <li>Setup Purview retention/deletion policies for SharePoint to reduce data surface<sup>2</sup></li> <li>Identify inactive sites with SAM, then restrict access or delete<sup>1</sup></li> </ul>

Guidance assumes Copilot technical prerequisites in place: Technical enablement of core services (Teams, SharePoint, Exchange), Office Applications deployed (modern Outlook recommended) and on current or monthly update channel

Learn how to use the features in the blueprint and how these features impact Microsoft 365 Copilot: <https://aka.ms/E5PrepareYourDataForCopilot>

Last updated December 10, 2024

# Onboard & engage: Setup guides

## Set up Microsoft 365 Copilot

01

Quick start – This guide helps you accelerate Copilot for M365 onboarding, with step-by-step guidance to fulfill the core requirements for Microsoft 365 Copilot. New features include Restricted SharePoint

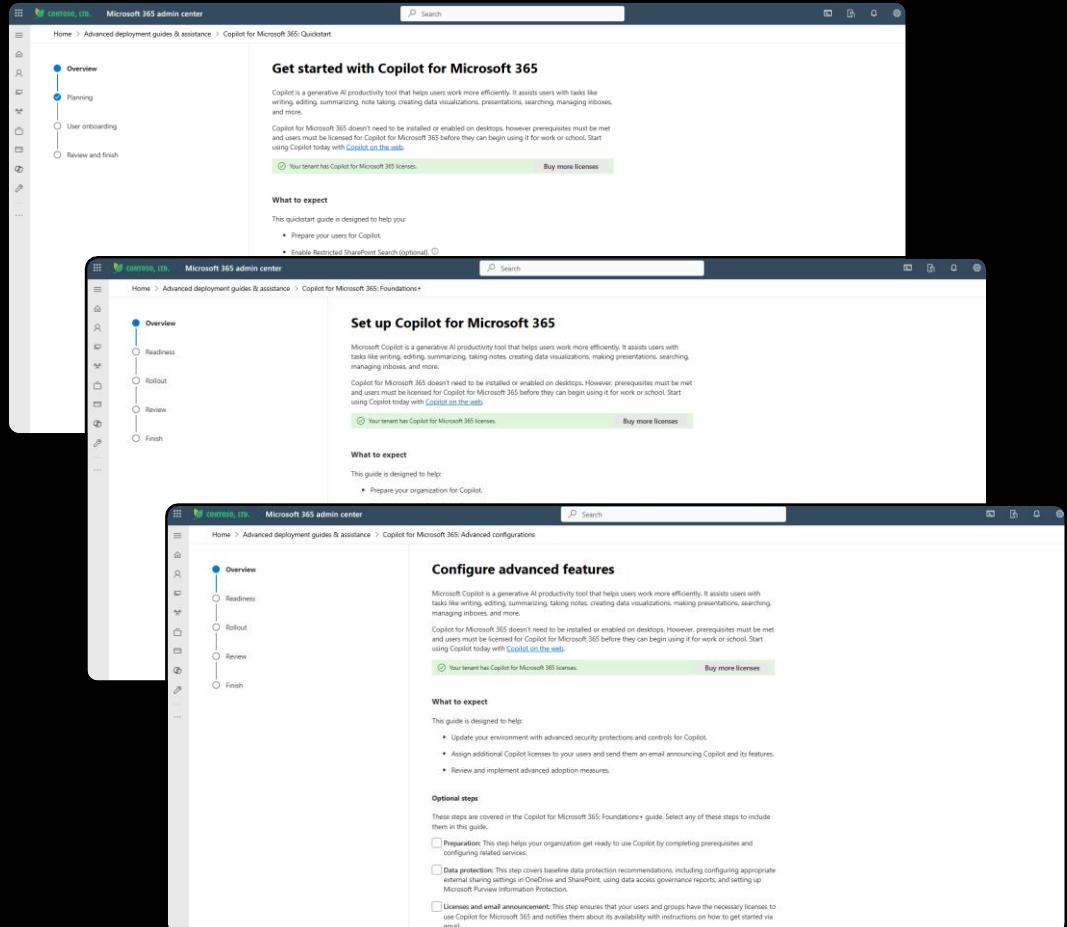
02

Foundations+ – This guide is the next step in your customer's Copilot onboarding process and includes core recommendations to support Copilot readiness and full-scale adoption.

03

Advanced Configurations – Advanced configurations provide best in class security, privacy, and data protection recommendations for Microsoft 365 E5.

These guides may be completed individually or in sequence, so administrators can choose the path that best suits their organization's needs.



# Choosing the right Microsoft 365 Apps update channel strategy



Copilot Ready!

## Current Channel (CC)

General-purpose devices, any type and size organization

## Monthly Enterprise Channel (MEC)

General-purpose apps, large enterprises

## Semi-Annual Enterprise Channel (SAEC)

*Copilot not supported*



### Benefits of monthly channels

- **70%** of helpdesk claims eliminated
- **Security** features 6+ months faster
- **Performance** increases (~15% vs SAEC\*, ~50% vs Office 2019)
- Increased **quality** – 6+ months faster fixes
- Higher end user **satisfaction** (NPS +~3%)



### Proof

- **75%** of businesses run monthly updates today

Forrester Total Economic Impact (TEI) Key Findings

<https://aka.ms/M365AppsTEIStudy>

# Leverage App Assure if you encounter in application compatibility issue moving to a monthly update channel!

## Microsoft's Microsoft 365 Copilot application compatibility promise

Microsoft is committed to ensuring your apps work when moving to Monthly Enterprise Channel to take advantage of Microsoft 365 Copilot. If you encounter any issues, App Assure will help you remediate them!



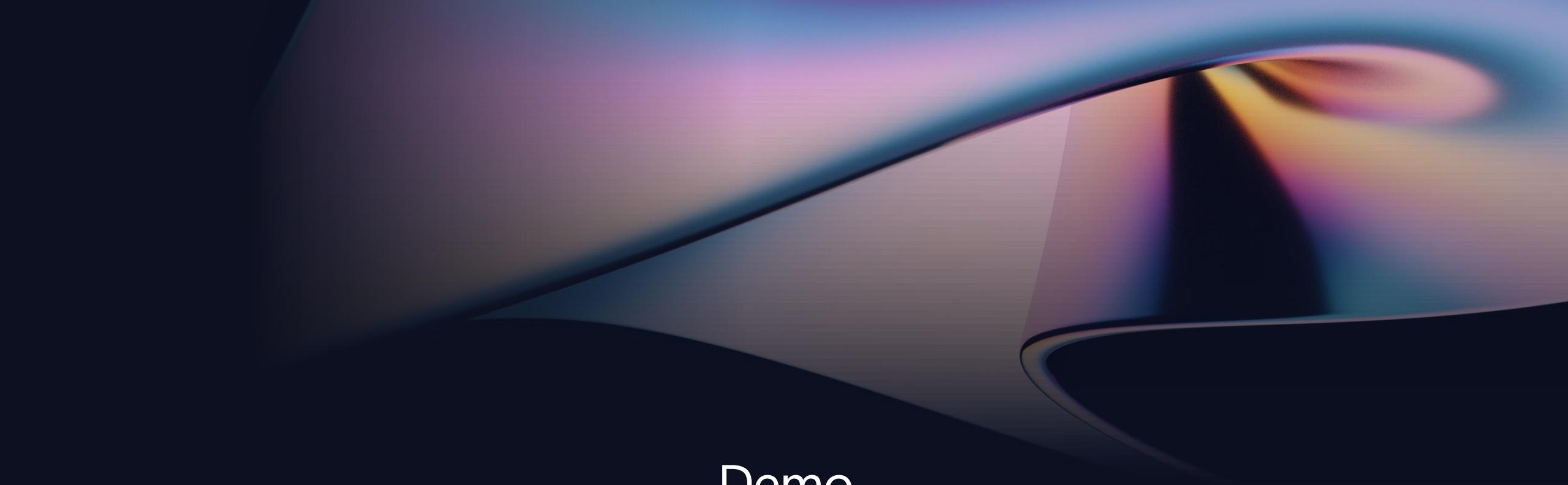
Help customers troubleshoot root cause and resolve app compatibility issues



Included as part of your license, this service is at no additional cost



Customers get a direct line of communication to Microsoft product engineering teams



# Demo

## Admin controls for Microsoft 365 Copilot

Enable Dark mode



Home

Users



Teams &amp; groups



Marketplace



Billing



Copilot



Settings

Setup

... Show all

Home &gt; Copilot

# Copilot



Manage everything related to Copilot. View insights about how people are using and learning about Copilot, assign licenses, find training, change settings, and more.

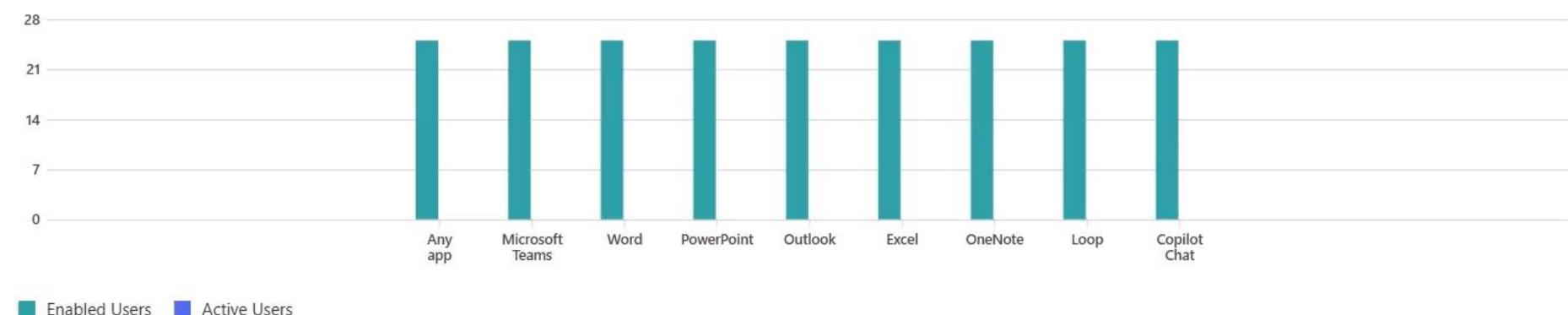
[Overview](#) [Settings](#)

## Reports

### Adoption by app



Adoption status of Copilot for Microsoft 365 over the past 30 days. See [metric definitions](#)



Enabled Users Active Users

[Learn more in Usage](#)

### License assignment

Assign a license to individual users or multiple users, as well as reassign licenses to other

### Copilot info from the Message center

Review the most relevant messages about the latest Copilot features, changes, and

Help &amp; support

Give Feedback

# User Enablement

Journey to Copilot

# Evaluate your user enablement capabilities



Invest in a healthy **champions team**, who will provide peer learning and support during the AI journey



Leverage in-product experiences to create a culture of **continuous learning** and deliver training in the flow of work



Ensure a vibrant **community of practice** for ongoing user engagement and skill building

# Viva Features for Copilot Adoption and Measurement

Product capabilities to drive Copilot adoption through Viva

Measurement		Communications			Skilling	
Viva Insights	Viva Glint	Viva Pulse	Viva Goals	Viva Amplify	Viva Engage	Viva Learning
						
Copilot Dashboard	Copilot Impact Survey	Copilot Adoption OKR Template	Copilot Campaign in a Box	Copilot Adoption Community	Copilot Academy	
<ul style="list-style-type: none"><li>Tenant level visibility into activation, adoption, and user sentiment*</li><li>Assess potential impact*</li><li>Scopes and filters for deeper organizational views</li><li>Analyze and compare metrics between user cohorts</li><li>Advanced tools for custom analysis</li></ul>	<p><b>Phase 1:</b> Copilot Impact Survey to capture user sentiment</p> <p><b>Phase 2:</b> User Pulse sentiment data included in Dashboard (Q3 FY24)</p> <p><b>Phase 3:</b> Integrate Pulse sentiment with benchmark data (Q4 FY24)</p>	<ul style="list-style-type: none"><li>OKR import template prepopulated</li><li>Faster time to configuration for driving clarity and transparency of Copilot investment</li></ul>	<ul style="list-style-type: none"><li>Ready to send weekly communications to Engage Employee across multiple communication channels to create awareness on Copilot capabilities to accelerate adoption</li></ul>	<ul style="list-style-type: none"><li>Copilot Adoption Community creation*</li><li>Templatized onboarding steps, suggested content &amp; members</li><li>External community to connect change managers across orgs &amp; copilot SME</li><li>Intelligent Q&amp;A</li></ul>	<ul style="list-style-type: none"><li>Copilot Learning Courses via MS Learn and Microsoft 365 Trainings*</li><li>Out-of-the-box structured learning environment for targeted Copilot upskilling with Copilot Academy</li></ul>	

# Functional scenario guidance

Utilize our interactive scenario library to start the conversation with business users about their pain points, opportunities, and ideas.

[aka.ms/Copilot/ScenarioLibrary](https://aka.ms/Copilot/ScenarioLibrary)

## Scenarios by persona

### Microsoft Copilot Scenario Library

Becoming AI powered means transforming scenarios across your organization. Use our guidance by department and individual scenario to get inspired, empower your workforce and realize value from your Microsoft Copilot investment.

Everyone can start with the free version of Microsoft Copilot on the web or mobile to assist with everyday tasks – for examples, check out the “Microsoft Copilot only” scenarios.

Copilot for Microsoft 365 builds on this by connecting with your work data and is available in the apps you use every day. You can take Copilot even further with Copilot Studio and other Copilot extensions to streamline business processes.

[Start using Microsoft Copilot >](#)

#### Functional scenarios

[Customer Service](#)

[Finance](#)

[Human Resources](#)

[Information Technology](#)

[Legal](#)

[Marketing](#)

[Marketing Communications](#)

[Operations](#)

[Sales](#)

[Looking for](#)



# Build your Community of Practice with Viva Engage

## Connect and empower employees

Create a community in Viva Engage to generate excitement, share learning, and support Copilot Champions and experts.

Give employees a place to:

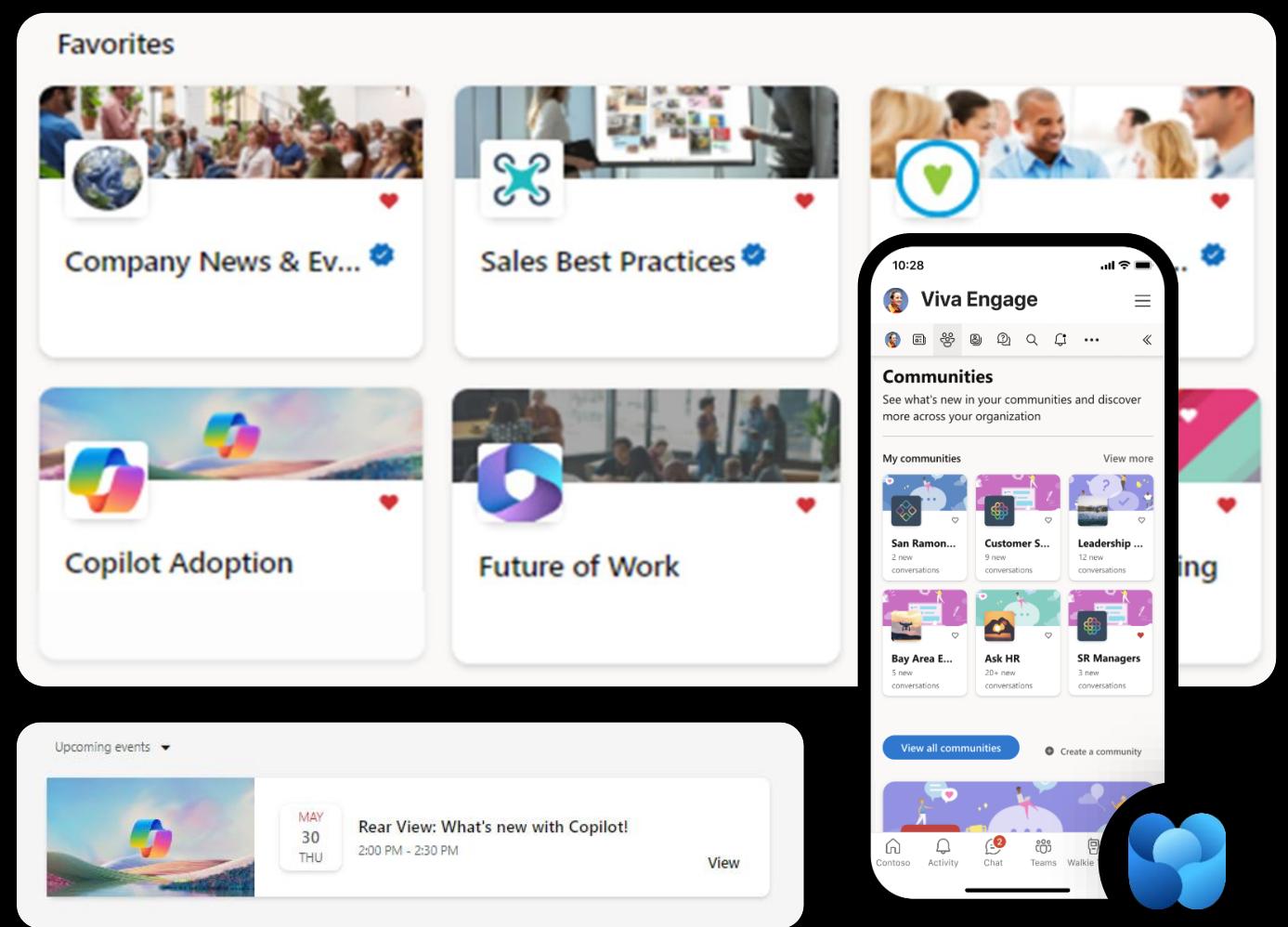
- Share best practices, such as prompts.
- Share success stories of Copilot saving time and driving productivity.
- Access company announcements on AI usage, direction, and mission.
- Facilitate peer to peer learning and Champion engagement.

Get ready

Onboard & engage

Deliver impact

Extend & optimize





# Objective: Land and expand Microsoft 365 Copilot awareness and AI skill centric vision for employees



## Awareness

- Land AI transformation vision.
- Tailor content by audience, scenario, persona, and usage journey.
- Copilot Champions launch.
- Internal testing for some.



## Engagement

- Deliver strategic engagements by org and role.
- Ongoing partner and employee education.
- Showcase successes via #CopilotStories.
- Conduct ongoing feedback surveys.



## Measurement

- Usage, support, and health metrics inform baseline for enablement journey.
- Drive listening systems engagement.
- Improve employee guidance.
- Identify additional scenarios for AI transformation.



## Management

- Improve the experience from employee feedback.
- Deliver integrated service roadmaps.
- Iterate messages and tactics bi-monthly.
- Provide employee insights signals in Service Health Review.

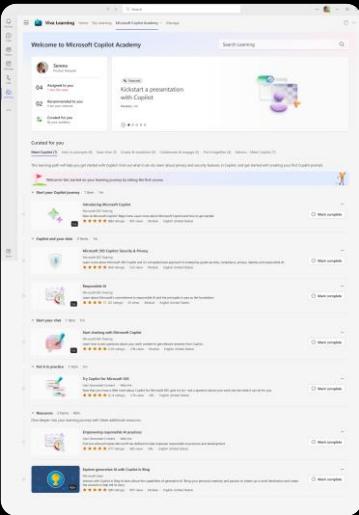
Land the message

Support the change

Analyze and adjust

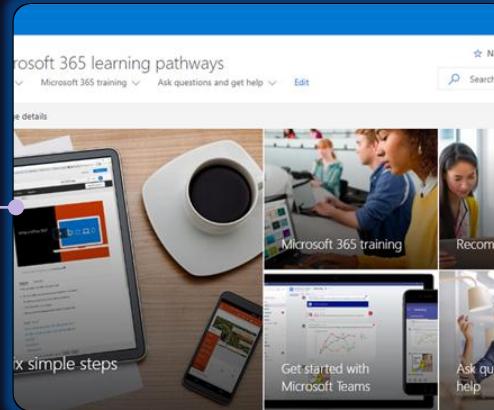
Improve the experience

# Microsoft 365 Copilot skilling experiences



## Microsoft Copilot Academy

- Centralized location to help with the basics of Copilot learning and upskilling, pulling the best content from available free Microsoft sources.
- Structured content in easily consumable learning paths curated by Microsoft experts.
- Develop your AI interaction skills from your Viva Learning app in Teams or webapp.



## Microsoft Learn

- Free, on-demand training content for skill development.
- Step-by-step exercises guiding learners through common Copilot prompts and use cases.

## Copilot Lab

- Free location to meet, learn about, and test the capabilities of Copilot.
- Improve your prompt engineering skills in an interactive hands-on environment.

Downloadable assets for customization available at [adoption.microsoft.com/copilot](https://adoption.microsoft.com/copilot)

# Measuring Value and Extending your AI Scenarios

Journey to Copilot

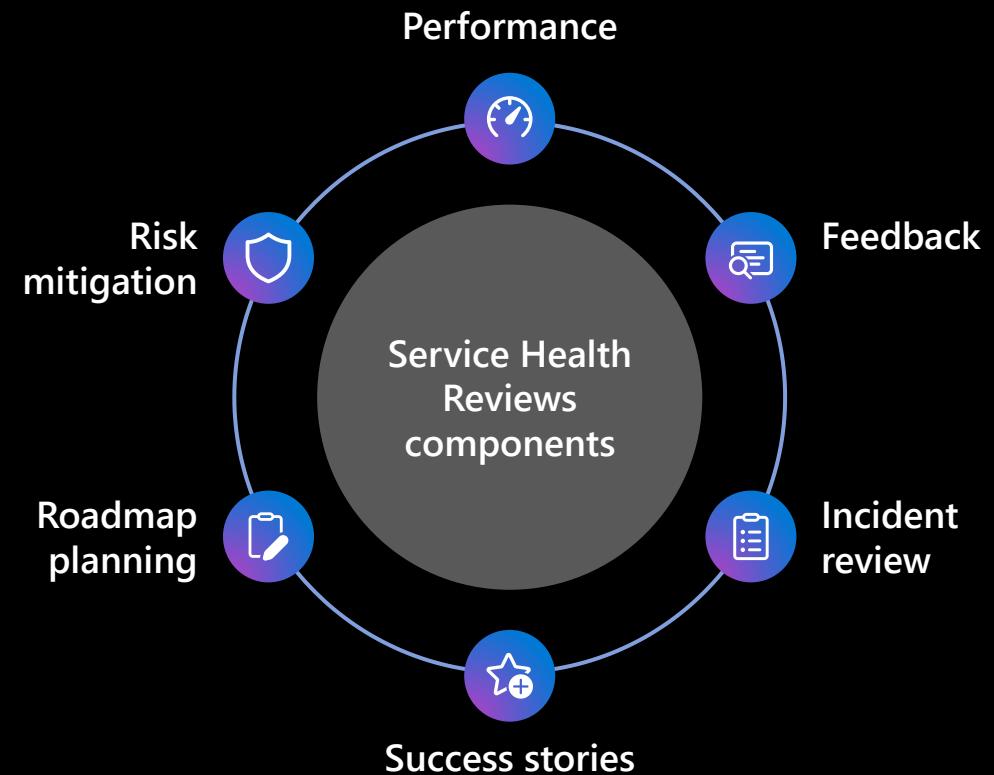
# Deliver impact: Establish service management plan

## Establish forum for continuous service improvement

Establishing a service management plan empowers IT and User Enablement teams to:

- 01 Periodically review health and business value of the AI transformation journey.
- 02 Conduct periodic assessments of governance, security, and user enablement practices.
- 03 Identify opportunities for expansion and further optimization of key Microsoft Copilot for Microsoft 365 user experiences.

- Access the [admin documentation](#) for the latest technical requirements, policies and reporting.
- Join [the Copilot community](#) to connect with experts and community members.
- Participate in Copilot Ask Microsoft Anything [events](#).





# Deliver impact: Access usage reports

## Interpret the Microsoft 365 admin center usage report

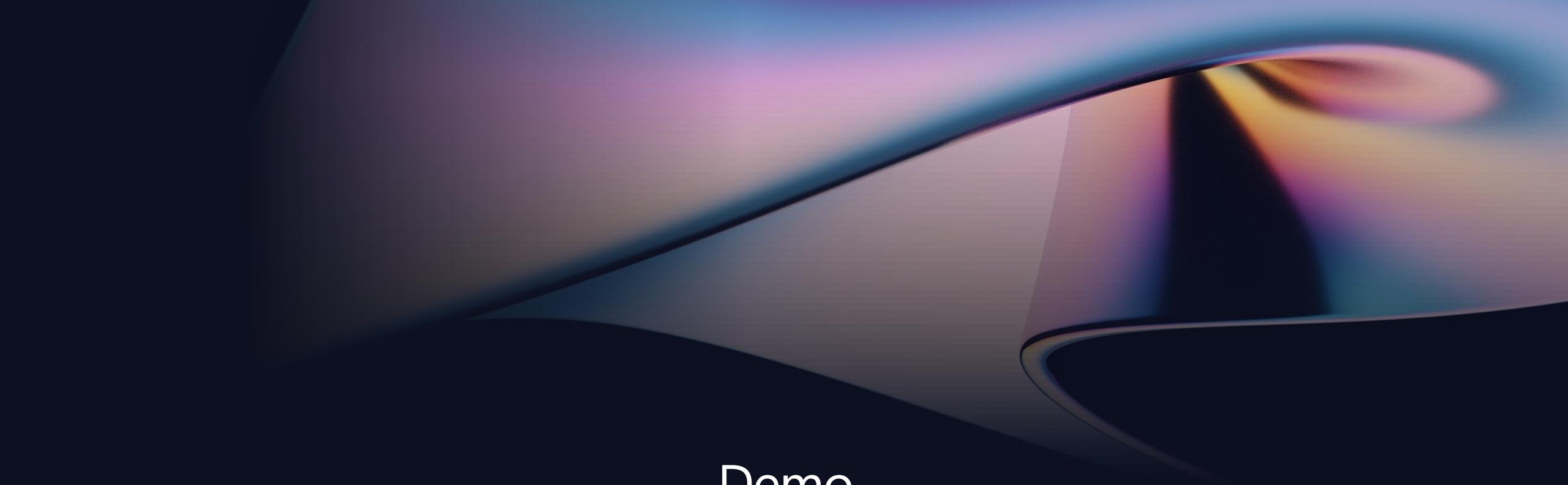
The Microsoft 365 Copilot usage report includes two sections: Readiness and Usage.

In the **Readiness section**, you can view a summary of users who are in a strong position to get value from Microsoft 365 Copilot.

In the **Usage section**, you can view a summary of Microsoft 365 Copilot adoption with visibility into users' last Microsoft 365 Copilot activity.

Interpret the Readiness section by analyzing assigned and available Copilot licenses, how many users are technically eligible, and how many are in a strong position to get value from Microsoft 365 Copilot.

If needed, you can export the report data into an Excel .csv file by selecting the Export link. This exports the Microsoft 365 Copilot last activity data of all users and enables your identified report readers to do simple sorting, filtering, and searching for further analysis.



Demo

Copilot reporting in the Microsoft 365 admin center

Microsoft 365 Admin Center X +

https://admin.microsoft.com

Microsoft 365 admin center

Search for users, groups, settings, and actions

Copilot | Dark mode

Home > Copilot

## Copilot

Manage everything related to Copilot. View insights about how people are using and learning about Copilot, assign licenses, find training, change settings, and more.

Overview Settings Discover

### Reports

#### Adoption by app

Adoption status of Copilot for Microsoft 365 over the past 30 days. See metric definitions

Summary Trend Apps: All ▾

App	Enabled users	Active users
Any app	~2500	~1800
Microsoft Teams	~2500	~1800
Copilot chat	~2500	~1800
Outlook	~2500	~1600
Word	~2500	~1400
PowerPoint	~2500	~1200
Excel	~2500	~1000
OneNote	~2500	~700
Loop	~2500	~400

Enabled users   Active users

Learn more in Usage

#### Help article views

People in your organization have viewed these topics about Copilot frequently over the last 30 days. Review these topics to see if they indicate trending interests that you could share with everyone.

# Extend & optimize



Shared  
activity



## Explore

### Identify new high value scenarios

- Gather data from service health reviews
- Prioritize via AI Council and leadership engagement
- Skill/acquire talent for extensibility opportunities



## Expand

### Understand Copilot Studio capabilities

- Build, automate and administer copilots
- Select extensibility scenarios

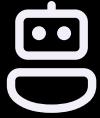


## Extend

### Scale Copilot users and skills

- Extend throughout organization
- Identify high value user cohorts for advanced skill building
- Optimize usage patterns

# Copilot hub & community



**Copilot hub on**  
[adoption.microsoft.com/copilot](https://adoption.microsoft.com/copilot)  
Enablement and usage guidance for  
Microsoft Copilot

The landing page for Copilot for Microsoft 365 features a large image of a laptop displaying a presentation slide with a play button. The slide has a blue and purple design with the word 'Copilot' at the top. Below the image, there are three main sections: 'Explore the Copilot Success Kit', 'Learn how Copilot works', and 'Join the Copilot community'. Each section includes a brief description and a 'View the kit', 'Learn now', or 'Join now' button.



Ask questions and get answers in our  
community  
[aka.ms/M365CopilotCommunity](https://aka.ms/M365CopilotCommunity)

The community hub for Copilot for Microsoft 365 shows a banner with the text 'Copilot for Microsoft 365' and 'Welcome to the Copilot for Microsoft 365 community. Your hub for the latest news, live events, and discussions on Copilot for Microsoft 365.' Below the banner, there's a section for help and learning with a link to the Microsoft Copilot Adoption hub. At the bottom, there are statistics: 9,629 members, 4 spaces, 746 discussions, and 30 blog articles.

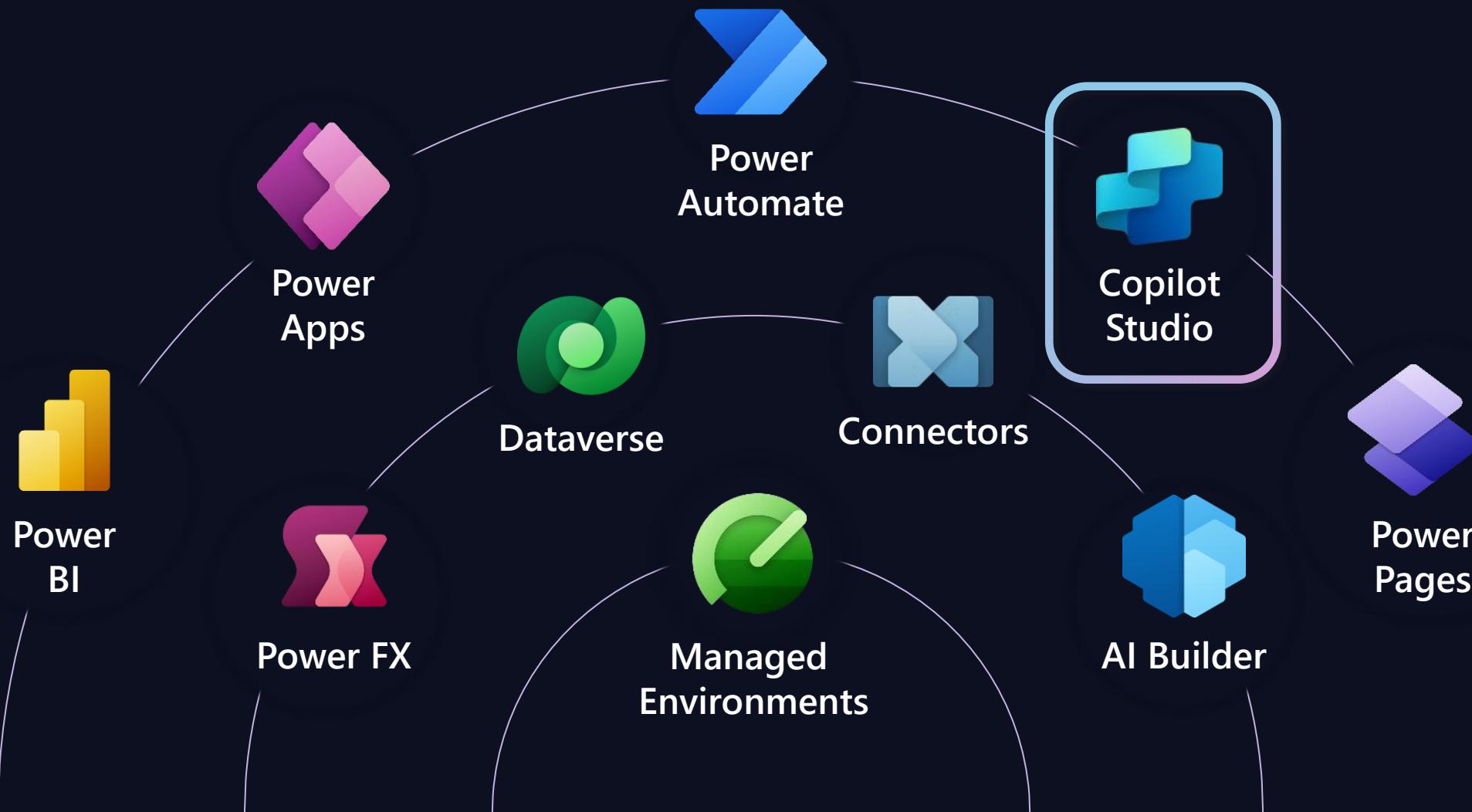


**Build and customize agents  
with Microsoft Copilot Studio**



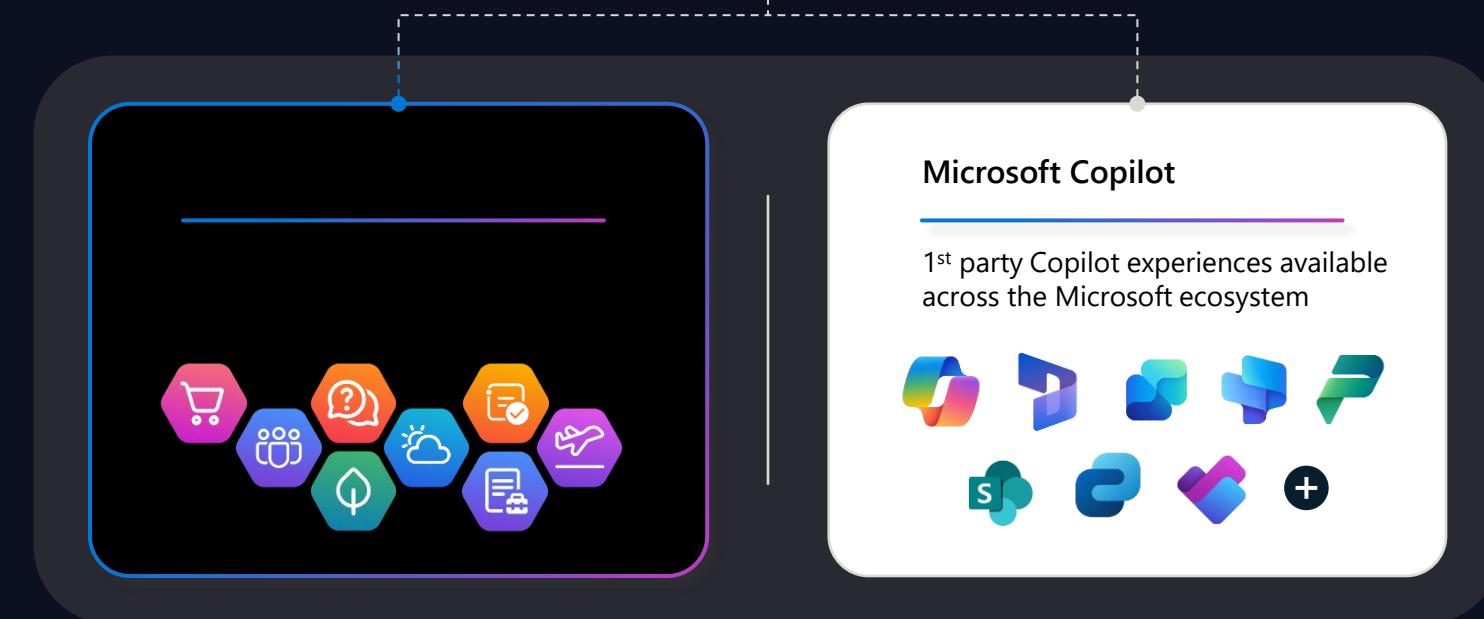
# Microsoft Power Platform

AI-Enabled Low-Code Platform



# What is a copilot?

Intelligent AI assistants that use generative AI and large language models to assist humans with complex cognitive tasks.



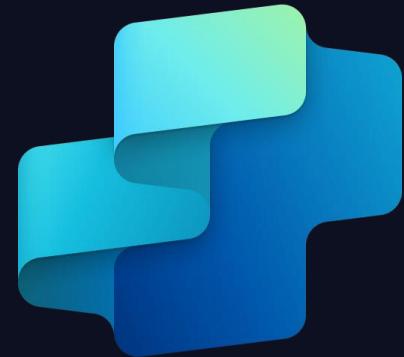


# Microsoft Copilot Studio

## Your copilot, your way

Copilot Studio is an end-to-end conversational AI product for **building your own copilots or extending Microsoft Copilot** with generative AI, large language models and **your data**.

The screenshot shows the Microsoft Copilot Studio web interface. At the top, there's a search bar and a navigation menu with options like Home, Create, Copilots, and Library. The main area has a heading "Describe your copilot to create it" with a text input placeholder "Use everyday words to describe what your copilot should do...". Below this is a "Recent" section listing two copilots: "Copilot for Microsoft 365" and "Copilot for Sales". There's also a "Start with a template" section featuring various AI-generated copilot templates such as Approval Manager, Job Craft, Organization Navigator, Safe Travels, Store Operations, Sustainability Insights, Weather, Website Q&A, Quick start: Create and deploy a copilot, Documentation, Responsible AI FAQs, Extend your copilots with plugins and extension, Quick start: Use Generative AI in a copilot, Support community, Try Copilot Agents, and Security and governance in Copilot Studio.



## Copilot Studio solutions for every industry

### Customer service

Resolve 14% more customer issues per hour



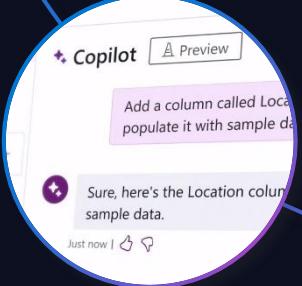
### Security operations

Respond to threats in minutes, not hours



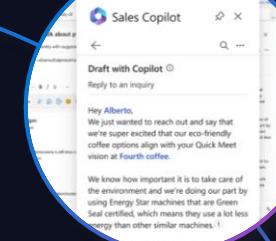
### Data & IT pros

Create workflows in half the time



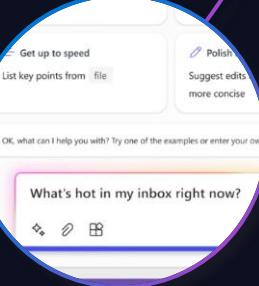
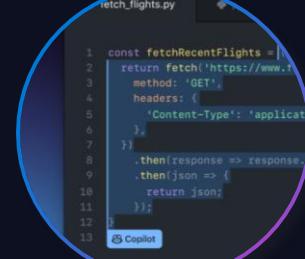
### Sales

Streamline the process of checking and answering emails



### Software developers

Code 55% faster



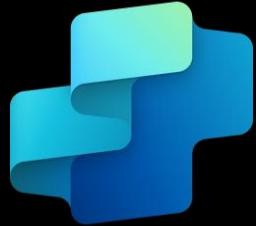
### Knowledge workers

Complete tasks 37% quicker

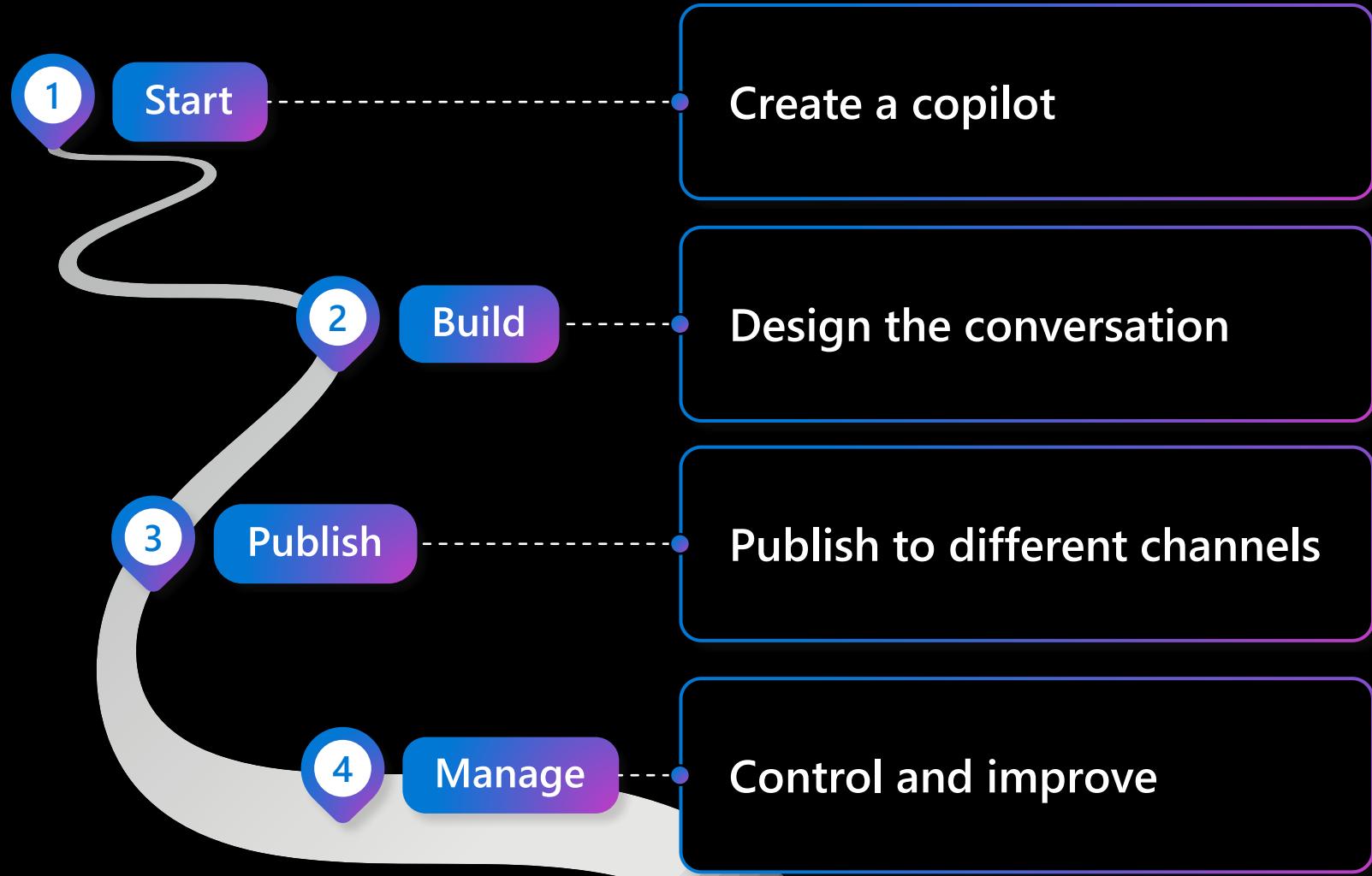


# Create powerful custom copilots

- ✓ Build and test together
- ✓ Design personalized, responsive interactions
- ✓ Boost your conversations
- ✓ Handle complex queries
- ✓ Continuous self learning and improvement

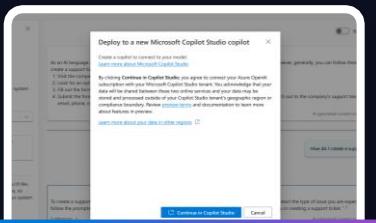


# How to build a custom copilot

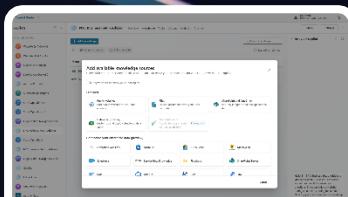




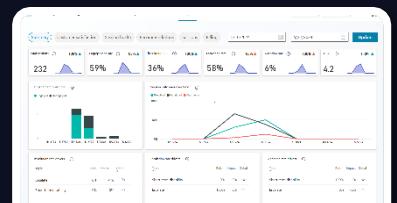
Create a copilot



Extend with Azure



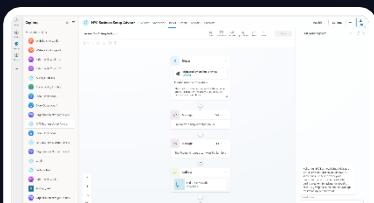
Chat over knowledge



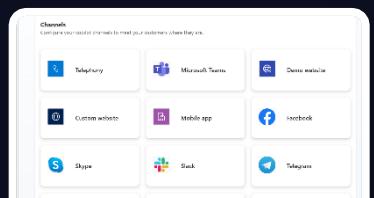
Monitor and Improve



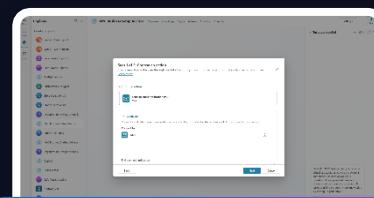
Copilot Studio  
Your copilot, your way



Add logic with topics



Multiple channels



Actions & Plugins

# Build the way you want

Users of all skill levels can create and test together

Preview

## Templates

The screenshot shows a list of pre-built templates under the heading "Start with a template". It includes options like "Approval Manager" (Streamline your approval process across multiple systems with summarized requests), "Job Craft" (Revolutionize your HR approach with AI constructed job descriptions and refined interview questions), and "Sustainability Insights" (Enables users to easily get insights and data about a company's sustainability goals and progress). Below this, there are sections for "Learning resources" with links to "Quick start: Create and deploy a copilot" and "Documentation", and "Support community" with a link to "Quick start: Use Generative AI in a copilot".

## Get started quickly

Choose from a diverse set of pre-built scenarios across popular industries and functions.

Preview

## Natural language

The screenshot shows a "Describe your copilot to create it" interface. It features a text input field with placeholder text "Use everyday words to describe what your copilot should do ...". Below the input field, a note says "This AI-powered feature is in preview. See terms". At the bottom, it shows "Modified by" and "Last published" information.

## Build conversationally

Build copilots by engaging in a conversational, natural, human-like experience.

## Visual canvas

The screenshot shows a graphical interface for building conversation logic. It includes a "Describe what the logic does" section, a "Conversation flow" diagram, and a "Conversation logic" panel on the right containing YAML code. The YAML code defines a conversation flow for "User" and "Bot" entities, including conditions like "kind: Condition" and "kind: Greet".

## Navigate a modern UX

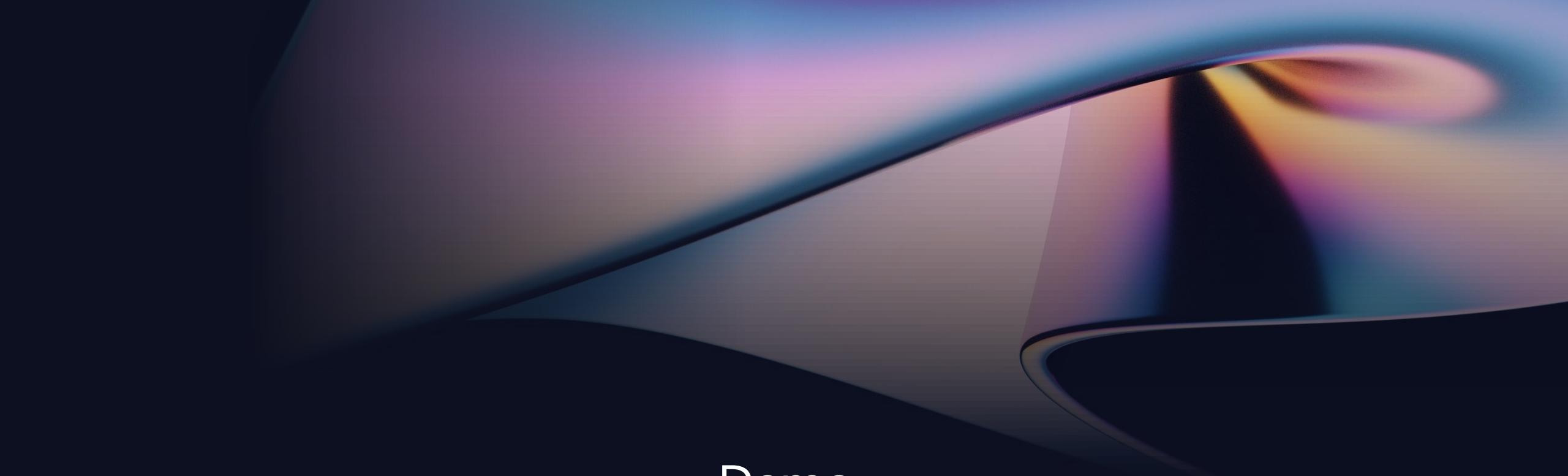
Design your conversation by following the low code graphical interface.

## Code

The screenshot shows a side-by-side view of a graphical interface and a YAML code editor. The graphical interface on the left shows a "Conversation logic" panel with a tree view of conversation steps. The YAML code editor on the right shows the corresponding YAML code for the conversation logic, such as "kind: Greeting" and "kind: Message".

## Switch to YAML

Share and re-use topic logic between developers and copilots in a side-by-side view.



Demo

Create a copilot from a template

Home - Microsoft Copilot Studio

https://copilotstudio.preview.microsoft.com/environments/825dbd88-6aa7-e719-a4ce-842df7deb603/home

Copilot Studio

Environment Community Demos

Home Create Copilots Library ...

# Describe your copilot to create it

Helpdesk Expense tracking HR and benefits

Use everyday words to describe what your copilot should do

This AI-powered feature above is currently in preview. [See terms](#) and [supplemental terms](#)

The screenshot shows the Microsoft Copilot Studio interface. At the top, there's a search bar and navigation links for 'Environment' and 'Community Demos'. On the left, a sidebar has icons for 'Home', 'Create', 'Copilots', 'Library', and three dots. The main area features a large 'Describe your copilot to create it' section with three buttons: 'Helpdesk', 'Expense tracking', and 'HR and benefits'. Below this is a text input field with placeholder text and a right-pointing arrow button. A note at the bottom says 'This AI-powered feature above is currently in preview. See terms and supplemental terms'. To the left of this section is a decorative graphic with colorful shapes and a stylized interface icon. Below this is a 'Recent' section with a table showing five entries. The columns are 'Name', 'Type', 'Last modified', 'Last published', and 'Owner'. The entries are: 'Microsoft Product Support' (Copilot, April Dunnam, 23 hours ago, Never, April Dunnam), 'EmployeePilot' (Copilot, # PowerVirtualAgentsProd, 11 days ago, 11 days ago, April Dunnam), 'Joke bot' (Copilot, # PowerVirtualAgentsProd, 3 months ago, Never, Daniel Laskewitz), and 'BKR203' (Copilot, # PowerVirtualAgentsProd, 2 months ago, Never, Daniel Laskewitz). The 'Joke bot' row has a cursor pointing to its 'Last modified' column. At the bottom, there's a 'Start with a template' section with four cards: 'Safe Travels', 'Store Operations', 'Sustainability Insights', and 'Team Navigator', each with a brief description and a small icon.

Name	Type	Last modified	Last published	Owner
Microsoft Product Support	Copilot	April Dunnam 23 hours ago	Never	April Dunnam
EmployeePilot	Copilot	# PowerVirtualAgentsProd 11 days ago	11 days ago	April Dunnam
Joke bot	Copilot	# PowerVirtualAgentsProd 3 months ago	Never	Daniel Laskewitz
BKR203	Copilot	# PowerVirtualAgentsProd 2 months ago	Never	Daniel Laskewitz

## Start with a template

Templates are currently a preview feature. See [supplemental terms](#)

See more

**Safe Travels**  
Provides answers to common travel questions and related health and safety guidelines

**Store Operations**  
Improve the efficiency of retail frontline workers by enabling easy access to store procedures and policies

**Sustainability Insights**  
Enables users to easily get insights and data about a company's sustainability goals and progress

**Team Navigator**  
Assists employees in finding colleagues and their hierarchy within the organization using Microsoft Teams

# Hands on Labs



Access the labs:  
[aka.ms/ai-tour/](https://aka.ms/ai-tour/)  
[workshop/copilotstudio](https://workshop.copilotstudio.com)

The image shows two screenshots of Microsoft Copilot Studio. The top screenshot displays the 'Describe your copilot to create it' interface, where users can input words to describe their copilot's capabilities. It also shows a list of recent copilots, including 'EmployeePilot', 'Joke bot', and 'BKR203'. Below this, there are sections for 'Start with a template' featuring 'Safe Travels', 'Store Operations', 'Sustainability Insights', and 'Team Navigator'. The bottom screenshot shows the 'Connect to Microsoft Power Platform' dialog box, which allows users to select a Power Platform environment and create a custom connector. It lists 'Power Platform environments' (e.g., 'testenvironment 1'), 'Power Platform Solutions' (e.g., 'Common Data Services Default Solution'), and 'Custom connectors' (with a '+' button). It also includes fields for 'OpenAPI specification' (with options for auto-generation or specifying a file path) and 'Select a public dev tunnel'.

## Lab 1

Building a copilot to chat over data and publishing to Teams

## Lab 2

Extend a copilot via a plugin with a custom connector built in Visual Studio



# Keep Learning



[aka.ms/copilotstudio-getstarted](https://aka.ms/copilotstudio-getstarted)

Extending M365  
Copilot and maximizing  
the potential of your  
Teams app with AI.



Copilot + Teams AI Library

A whole new way to work

A portrait of a middle-aged man with short, light-colored hair, wearing dark-rimmed glasses, a white collared shirt, and a dark suit jacket. He is smiling slightly and looking towards the camera. The background is dark.

“The **age of AI** is upon us. Modernizing applications is **mission-critical** to any company’s operations today.”

With AI you can  
increase revenue  
and reach more  
customers

on a platform with  
millions of users

**+ \$7T – 10T**

Estimated GDP growth  
from next-gen AI

**+ \$2T – 2.5T**

New addressable TAM for  
Microsoft & partners

**1.2 billion**

Active users across work,  
life and education

**300 million**

Microsoft Teams monthly  
active users

AI will increase  
global GDP

..and generate new  
partner  
opportunities



# Microsoft 365 Copilot



Foundation  
models

+



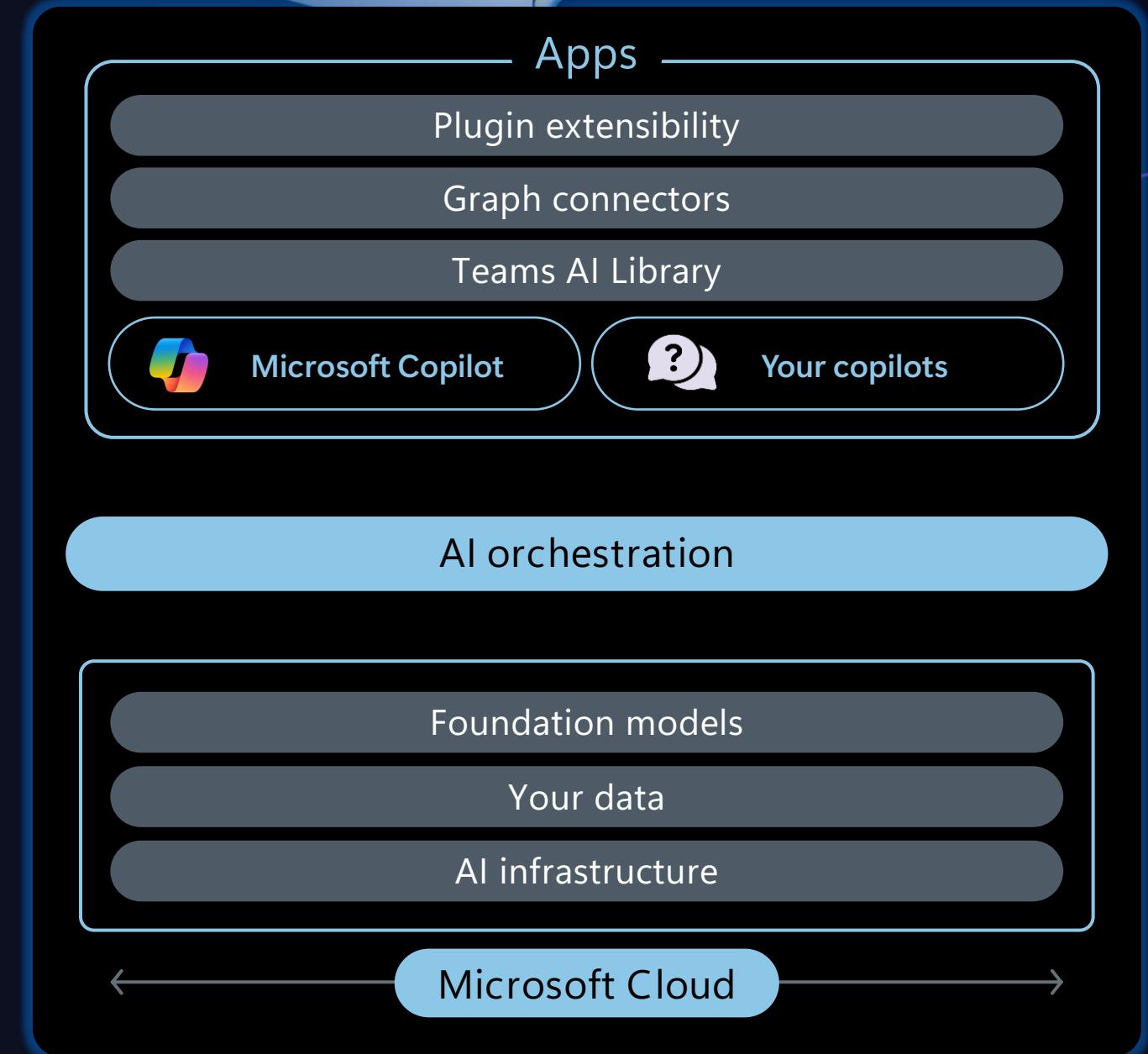
Microsoft Graph  
- Your Data -

+



Microsoft 365 &  
3<sup>rd</sup> party apps

# Copilot stack





A I S E R A



augeo



Canva



expedia group



FiscalNote



go1



KAYAK

Klarna.



Lucid



monday.com

Moveworks

# New and existing plugin developers



Noteable



OpenTable

ORACLE

Pieces



Polly



REDFIN

SAP SuccessFactors

servicenow

shop

skillsoft

Skyscanner

smartsheet

snowflake

Spotify

SPOTNANA

SurveyMonkey

TeamViewer

THOMSON REUTERS

Trello

Tripadvisor

Trip.com

twilio

WITIVIO

WOLFRAM

workhuman

wrike

zendesk

Zillow

Desk

# AI is changing the way users work and unlocking a new wave of productivity growth

## Unleash Creativity

Users can harness the power of AI so they never have to start with a blank page

## Unlock Productivity

AI can summarize actions for users and optimize their time

## Uplevel Skills

Helps users be better at what they're good at and master what they have yet to learn



**Microsoft 365 Copilot** is the next major step in the evolution of how people work with AI and how AI works with people

# Maximize efficiency of your apps with AI...

**App discoverability**

**Increase discoverability** of your app throughout Microsoft 365

**Return on investment**

**Unleash the value** of your investments with less effort from devs

**Product differentiation**

**Enable intelligent, differentiated product experiences** more quickly and efficiently

**Security and compliance**

**Inherit world-class security**, compliance, and privacy policies

**Cross-app integration**

**Surface apps in multiple contexts** with real-time access to data

# Unlock the full potential of your app with AI



## Copilot in Teams



### Plugins

Extend the Copilot experience, transforming how users interact with M365 data, apps and services



### Graph Connectors

Enable deep content retrieval and summarization via personalized, relevant results from Microsoft Graph connectors



## Teams



### Teams AI Library

Simplify the integration of large language models (LLMs) into Teams and build conversational experiences with ease

# Scenario to capability mapping

	Message extensions	Graph Connectors	Your Copilot
Read/write data to external systems	✓	Read only	✓
Search for and retrieve information from indexed data sets and 3 <sup>rd</sup> party clouds	✓	✓	✓
Perform actions on user's behalf, (e.g. create tasks, reminders, trigger actions)	✓		✓
Find, summarize and perform Q&A leveraging indexed or external data		✓	✓
Access & analyze with diverse datasets for rich data analysis & comprehensive insights		✓	
Conversational experiences in your Teams app			✓
Available across M365	M365 Copilot, Teams, Outlook	M365 Copilot, Workplace Search, Viva Topics, Context IQ, Feed	Teams + M365



## Which Microsoft 365 extensibility option for Copilot should you choose?

Start here!

Are you a Power Platform user & want to connect your data?

No

Do you want your data to be indexed?

No

Have you built Teams Message Extensions before?

Yes

Connect data in Microsoft Search, Context IQ, and Microsoft 365 app

Yes

Interact with real-time data

Yes

Congrats, you have the foundation of a plugin for Copilot!

No

Build a feature-rich solution using Bot Framework!

Create Power Platform connector to connect external data!



Power Platform connectors

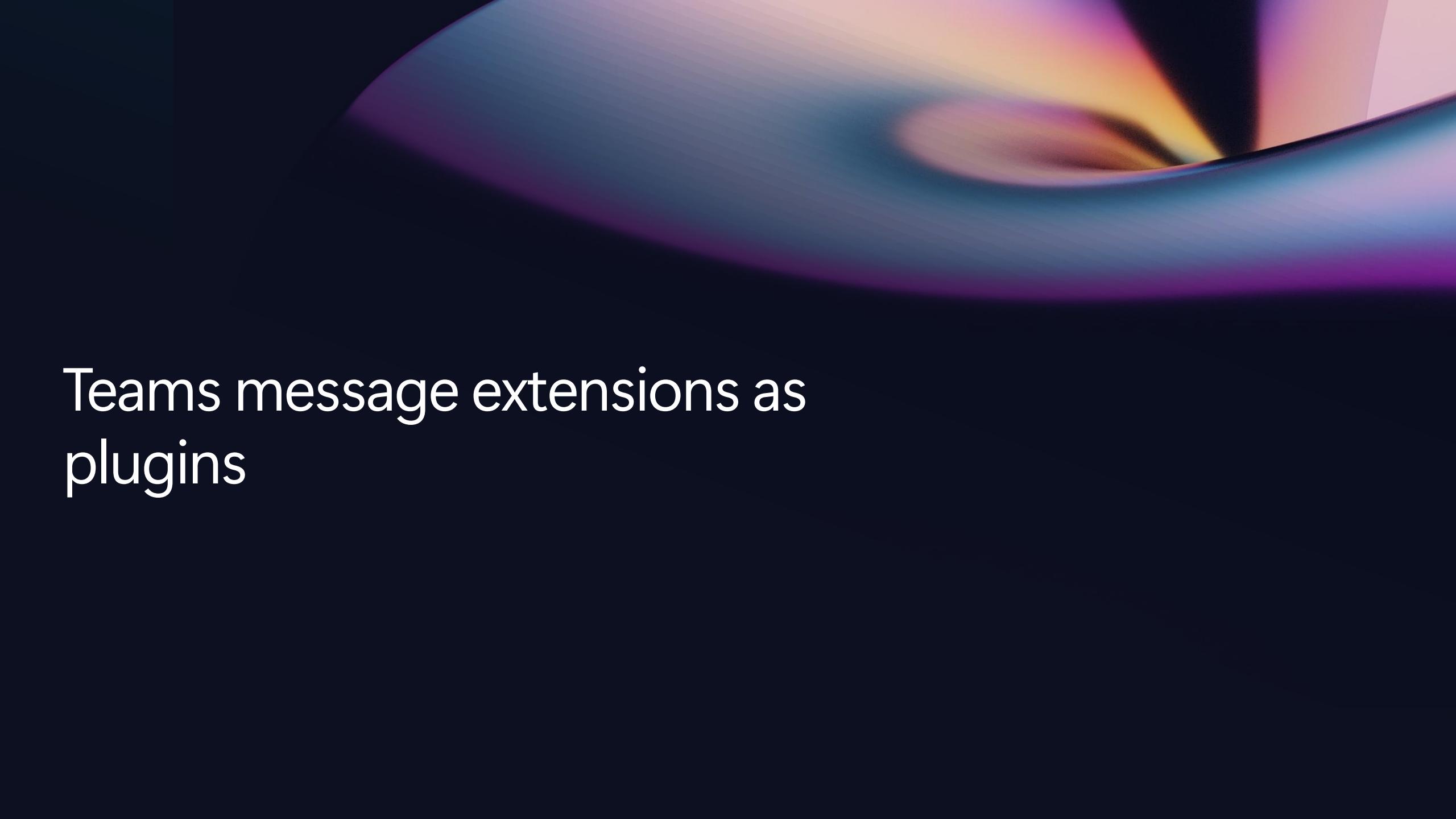
Create new Graph connectors using the API or SDK!



Microsoft Graph connectors



Message Extension



Teams message extensions as  
plugins

# Teams Message Extensions

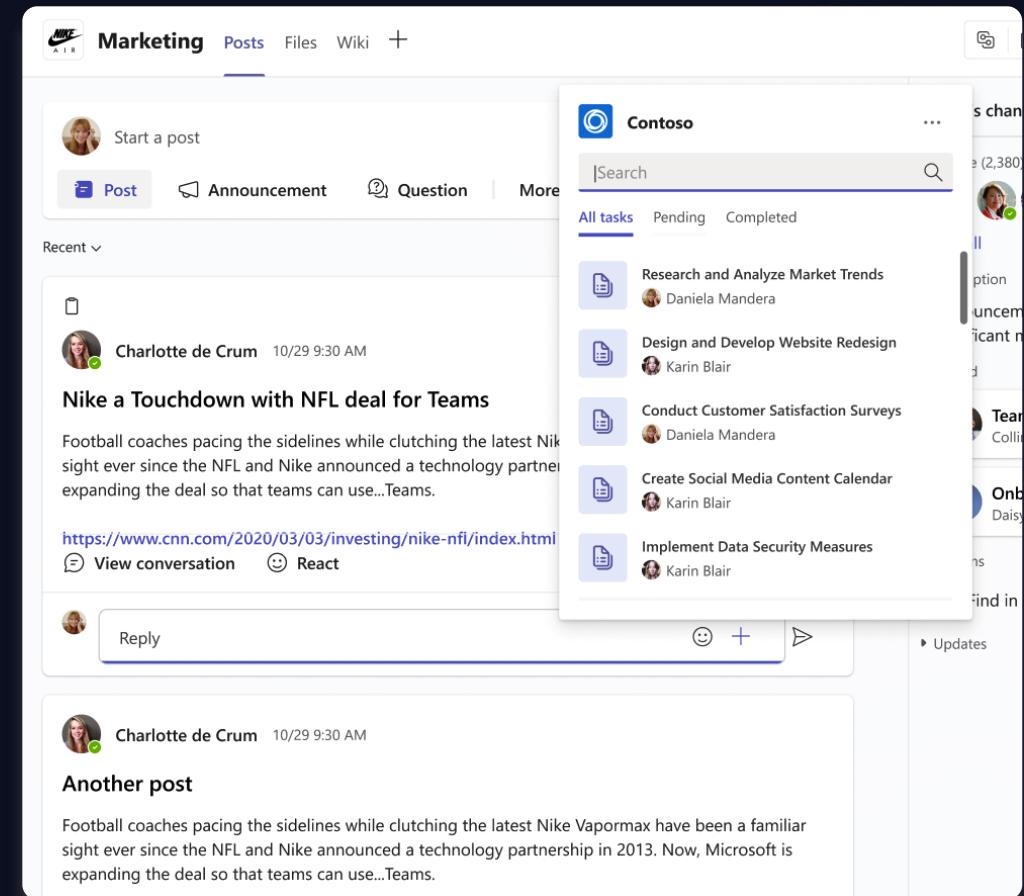
Message extensions search or perform actions in an external system (like your app) from Teams, and the web service sends back results as a richly formatted card.

Meet your users in the flow of conversation with message extensions in Copilot

 Access real-time information

 Retrieve knowledge-based resources

 Perform actions across apps



# Why Message Extensions?

Scenario	Example
You need an external system to perform an action and return the result to your conversation.	Reserve a resource and allow the channel to know the reserved time slot.
You need to search for something in an external system and share the results with the conversation.	Search for a work item in Azure DevOps and share it with the group as an Adaptive Card.
You want to complete a complex task involving multiple steps or large amount of information in an external system and share the results with a conversation.	Create a bug in your tracking system based on a Teams message, assign that bug to Bob, and send a card to the conversation thread with the bug's details.



## Daniela Mandera | Lead Engineer

Daniela wants a list of change management procedures for the website she's leading before pushing out a major release. Afterward, she plans to create a ticket for internal tracking with her engineers.

# Summarize distributed content in a meaningful way

The screenshot shows a Microsoft Copilot interface integrated into a Microsoft Teams chat window. The Teams sidebar on the left lists Activity, Chat, Teams, Calendar, Calls, Files, and Apps. The main area is a chat with several participants:

- Pinned messages:
  - Copilot: Create a ticket to track changes.. 9:22 AM
  - Cassandra Dunn: Ok, I'll send an update later 7:27 AM
  - Aadi Kapoor: You: Great work! 5:21 AM
  - Eric Ishida: Sure, I'll set something for next week t... 11:40 AM
- Recent messages:
  - Cortex Framework: Kayo: The review went really well! Can we... 4:41 PM
  - Will Little: I don't see that being an issue, Can you ta... 3:45 PM
  - Marie Beaudouin: Ohh, I see, yes let me fix that! 1:21 PM
  - Hillary Reyes: Haha! 1:07 PM
  - Charlotte and Babak: Charlotte: The client was pretty happy with... 11:48 AM
  - Reta Taylor: Ah, ok I understand now 11:40 AM
  - Joshua VanBuren: Thanks for reviewing 10:29 AM
  - Daichi Fukuda: You: Thank you 10:20 AM
  - Kadjji Bell: You: I like the idea, let's pitch it! 10:03 AM

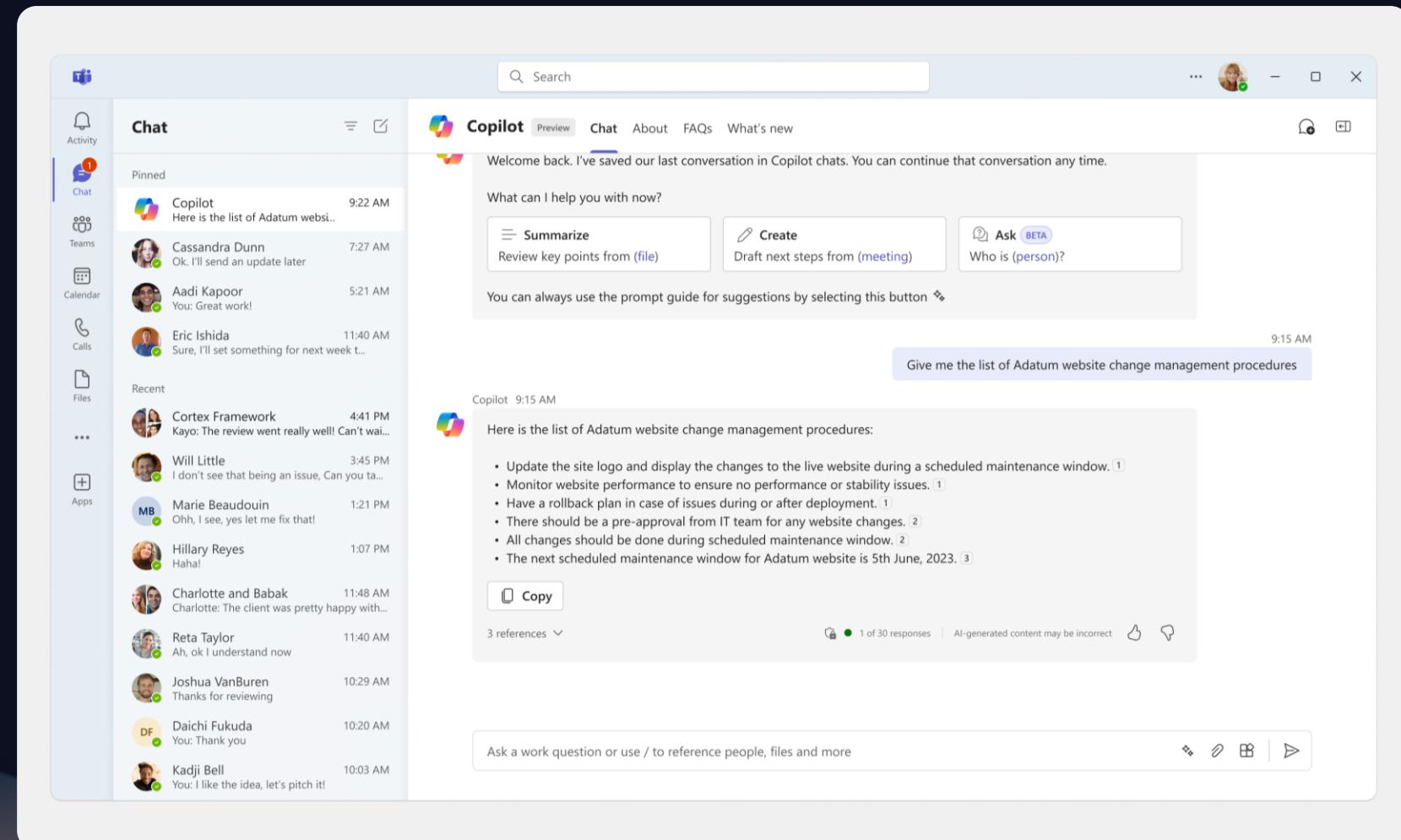
The Copilot interface at the top has tabs for Preview, Chat, About, FAQs, and What's new. It features three main buttons: Summarize (Review key points from (file)), Create (Draft next steps from (meeting)), and Ask (Who is (person)? BETA). A note says "You can always use the prompt guide for suggestions by selecting this button".

A message from Copilot at 9:15 AM asks for "Give me the list of Adatum website change management procedures". Copilot responds at 9:15 AM with a list of items:

- Update the site logo and display the changes to the live website during a scheduled maintenance window. 1
- Monitor website performance to ensure no performance or stability issues. 1
- Have a rollback plan in case of issues during or after deployment. 1
- There should be a pre-approval from IT team for any website changes. 2
- All changes should be done during scheduled maintenance window. 2
- The next scheduled maintenance window for Adatum website is 5th June, 2023. 3

At 9:20 AM, Copilot suggests creating a ticket: "Create a ticket to track changes outlined above, due by maintenance date". The bottom input field says "Ask a work question or use / to reference people, files and more".

# View citations and references with deep links to relevant sources.



# Create actionable work items based on insights and info.

The screenshot shows the Microsoft Copilot interface integrated into a Microsoft Teams chat window. On the left, the Teams sidebar is visible with sections for Activity, Chat (marked with 1 notification), Teams, Calendar, Calls, Files, and Apps. The main area is a chat window titled "Chat".

**Pinned:**

- Copilot 9:22 AM: Here is the list of Adatum webs...
- Cassandra Dunn 7:27 AM: Ok. I'll send an update later
- Aadi Kapoor 5:21 AM: You: Great work!
- Eric Ishida 11:40 AM: Sure, I'll set something for next week t...

**Recent:**

- Cortex Framework 4:41 PM: Kayo: The review went really well! Can't wai...
- Will Little 3:45 PM: I don't see that being an issue, Can you ta...
- Marie Beaudouin 1:21 PM: Ohh, I see, yes let me fix that!
- Hillary Reyes 1:07 PM: Haha!
- Charlotte and Babak 11:48 AM: Charlotte: The client was pretty happy with...
- Reta Taylor 11:40 AM: Ah, ok I understand now
- Joshua VanBuren 10:29 AM: Thanks for reviewing
- Daichi Fukuda 10:20 AM: You: Thank you
- Kadjie Bell 10:03 AM: You: I like the idea, let's pitch it!

**Copilot Response:**

9:15 AM: Give me the list of Adatum website change management procedures

9:15 AM: Here is the list of Adatum website change management procedures:

- Update the site logo and display the changes to the live website during a scheduled maintenance window. 1
- Monitor website performance to ensure no performance or stability issues. 1
- Have a rollback plan in case of issues during or after deployment. 1
- There should be a pre-approval from IT team for any website changes. 2
- All changes should be done during scheduled maintenance window. 2
- The next scheduled maintenance window for Adatum website is 5th June, 2023. 3

**Copy:** 3 references ^ 1 of 30 responses | AI-generated content may be incorrect

- 1 2023\_Adatum website change management\_v4
- 2 [IMP] New Adatum Change management procedures
- 3 [IT Comms] – Adatum website scheduled maintenance window

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

# Create actionable work items based on insights and info.

The screenshot shows a Microsoft Teams chat window with the Copilot tab selected. The sidebar on the left lists Activity, Chat (with 1 unread message), Teams, Calendar, Calls, Files, and Apps. The main area shows a conversation with Copilot and several team members (Cassandra Dunn, Aadi Kapoor, Eric Ishida, Cortex Framework, Will Little, Marie Beaudouin, Hillary Reyes, Charlotte and Babak, Reta Taylor, Joshua VanBuren, Daichi Fukuda, Kadjie Bell).

**Copilot:** OK, I'll look for 'Create a ticket tr... 9:22 AM

**Copilot:** Give me the list of Adatum website change management procedures 9:15 AM

**Copilot:** Here is the list of Adatum website change management procedures:

- Update the site logo and display the changes to the live website during a scheduled maintenance window. 1
- Monitor website performance to ensure no performance or stability issues. 1
- Have a rollback plan in case of issues during or after deployment. 1
- There should be a pre-approval from IT team for any website changes. 2
- All changes should be done during scheduled maintenance window. 2
- The next scheduled maintenance window for Adatum website is 5th June, 2023. 3

**Copilot:** Copy 3 references 1 of 30 responses | AI-generated content may be incorrect 9:20 AM

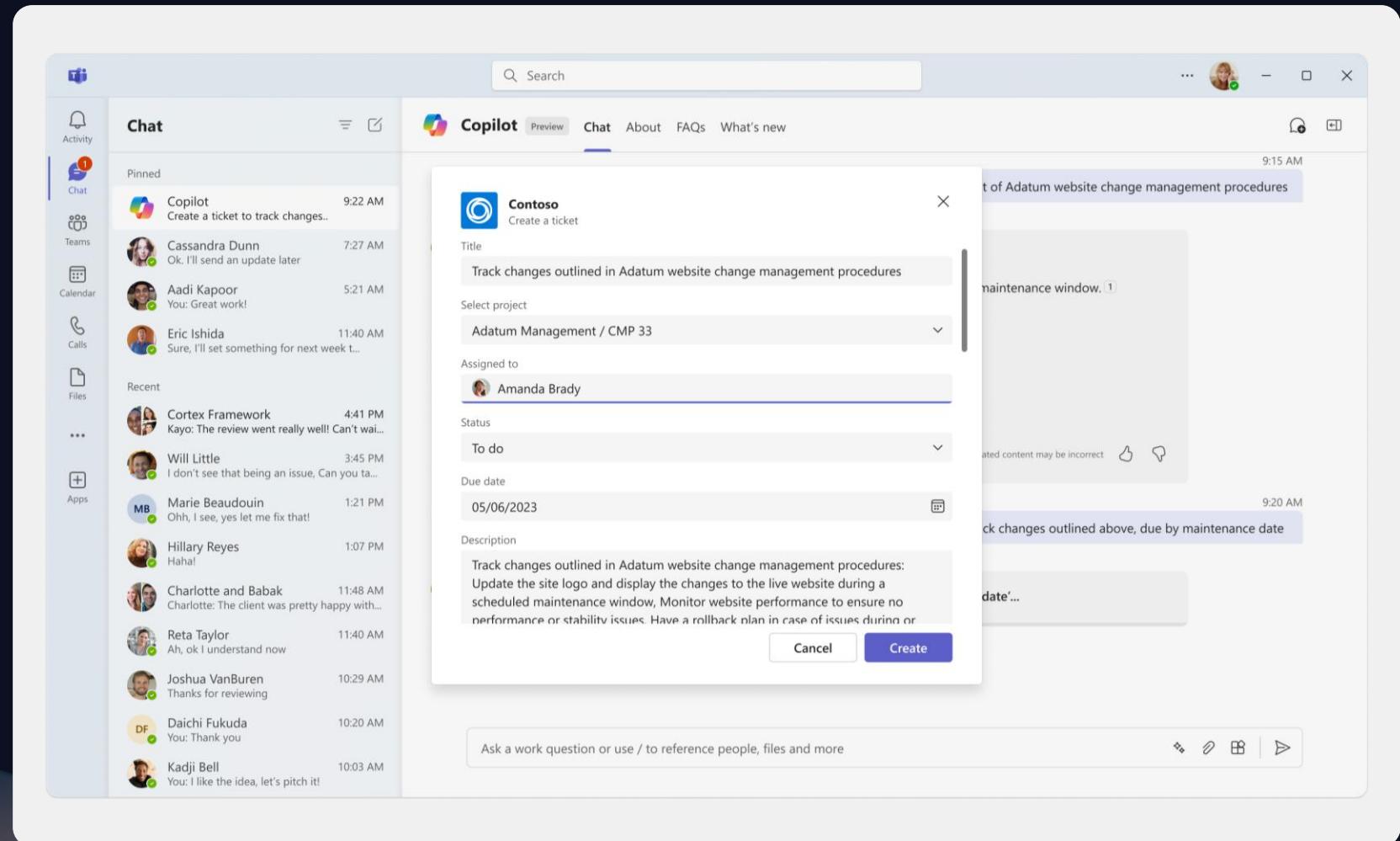
**Copilot:** Create a ticket to track changes outlined above, due by maintenance date

**Copilot:** OK, I'll look for 'Create a ticket to track changes outlined above, due by maintenance date'...

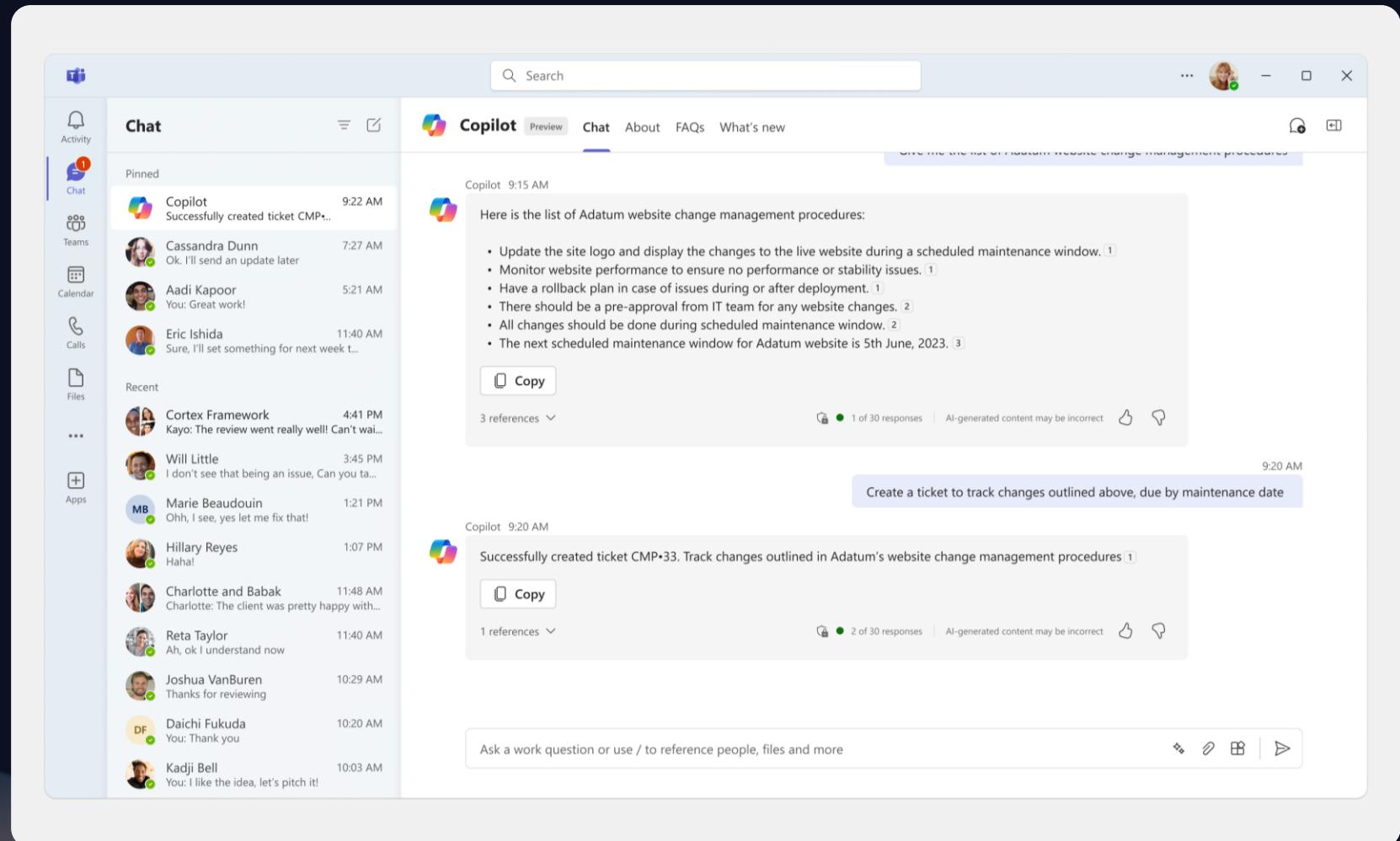
**Copilot:** Stop generating

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

# Use your existing Teams message extension to validate and create work items.



Return  
actionable  
adaptive cards  
for deep  
linking to  
relevant  
content,  
shareable  
broadly.



# Guidelines for Message extension plugin for Microsoft 365 Copilot

Criteria	Fulfillment
Manifest version	App manifest version must be 1.13 or later. <i>[Mandatory]</i>
Microsoft 365 Channel	For users to interact with your message extension from Outlook, you need to add Microsoft 365 channel to your bot. For more information, see <a href="#">Add Microsoft 365 channel</a> . <i>[Mandatory]</i>
Response Time	Response time must not exceed 9 seconds for 99 percent, 5 Seconds for 75 percent and 2 Seconds for 50 percent. <i>[Mandatory]</i>
Reliability	Apps must maintain 99.9% availability. For instance, if Microsoft 365 Chat calls a plugin 1000 times, it must provide a meaningful response 999 times. <i>[Mandatory]</i>
Zero Regressions	If you need to resubmit your app for validation, the existing message extension functionality that was working earlier mustn't break. This requirement is only applicable to ISV apps and not apps built for your organization. <i>[Mandatory]</i>
Single sign-on (SSO)	If applicable, update your Microsoft Entra ID app registration for SSO. <i>[Recommended]</i>
Content Security Policy	If applicable, modify your Content Security Policy headers. <i>[Recommended]</i>

# What makes a plug in high quality



## Support search

Anticipate and support the most common searches users will perform.



## Retrieve deep content

Search match with the surrounding paragraph. Provide an Adaptive Card response with additional information.



## Present actionable results

Include a way for the user to take action, such as a deep link to your website, or a modal dialog.



## Provide a preview

Guide your user through content previews.



# Best practices

## **Build for safety and responsible AI**

- Anti-Compete: Avoid using the name of any other plugin in both short and full descriptions.
- Responsible AI: Avoid using inappropriate or offensive keywords.
- Prompt injection: Ensure that text doesn't lead to prompt injections. Additionally, descriptions must not contain symbols or text that indicate they can be used as code for prompt injection. Avoid using phrases, functions, and codes that call an app recursively.

## **Support multi-parameter search queries**

## **Avoid generic descriptions of your plugin, its skills, and parameters**

- A generic plugin description prevents the appropriate plugin for the job from getting picked up and if this happens frequently the user might disable the plugin.
- When selected incorrectly, failures in plugin execution or response are likely outcomes. Copilot won't surface plugins that have high error rates, and user trust in the plugin could erode.



# Best practices

## **Don't assume Copilot can guess required inputs**

- Only in limited scenarios is Copilot able to guess an input to a user prompt

## **Validate operations Copilot can perform in terms of reasoning over the plugin response**

- While Copilot provides basic capabilities in reasoning over the output of a plugin response, results vary depending on the scenario

## **Provide visually rich responses to user queries**

- Respond to user input with structured, actionable, and visually rich Adaptive Cards

# Graph connectors



# Graph connectors

Graph connectors increase discoverability and engagement by deeply integrating your data into the Microsoft 365 Copilot experience



Make the most of your external data

The screenshot shows a Microsoft Copilot interface with a dark theme. At the top, it says "Cotoso 11:17 AM". Below that is a "Sales Analysis" card. The card header is "Sales Analysis". The main content states: "The sales analysis for July 2023 shows that there has been an overall increase in consumer spending, reflected in higher purchase volumes across various product categories." At the bottom of the card are three buttons: "View", "Share", and "Create report". To the right of the card is a larger, separate window titled "Sales Dashboard". This window displays several data points and charts. One chart shows "Sales Pipeline" with values: Actual: \$211,800, Average Value of Won Deals: \$69,500, and Total: \$139,000. Another chart shows "Monthly Goal" with a bar chart comparing Actual (\$139K) and Goal (\$100K). At the bottom of the dashboard window, it says "Sales Analysis Uploaded by Daniela Mandera".



Use Copilot as a research aid



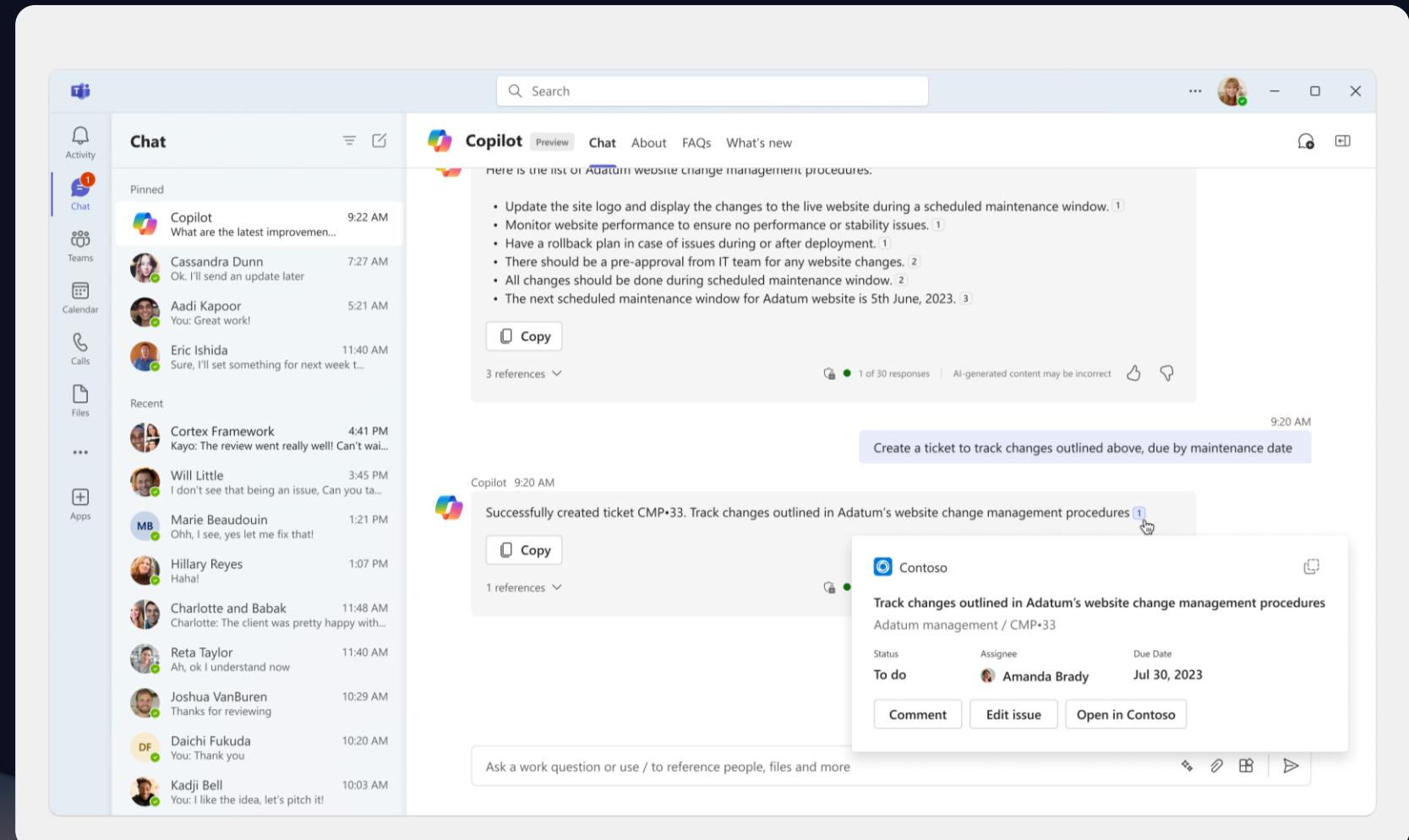
Perform search across apps



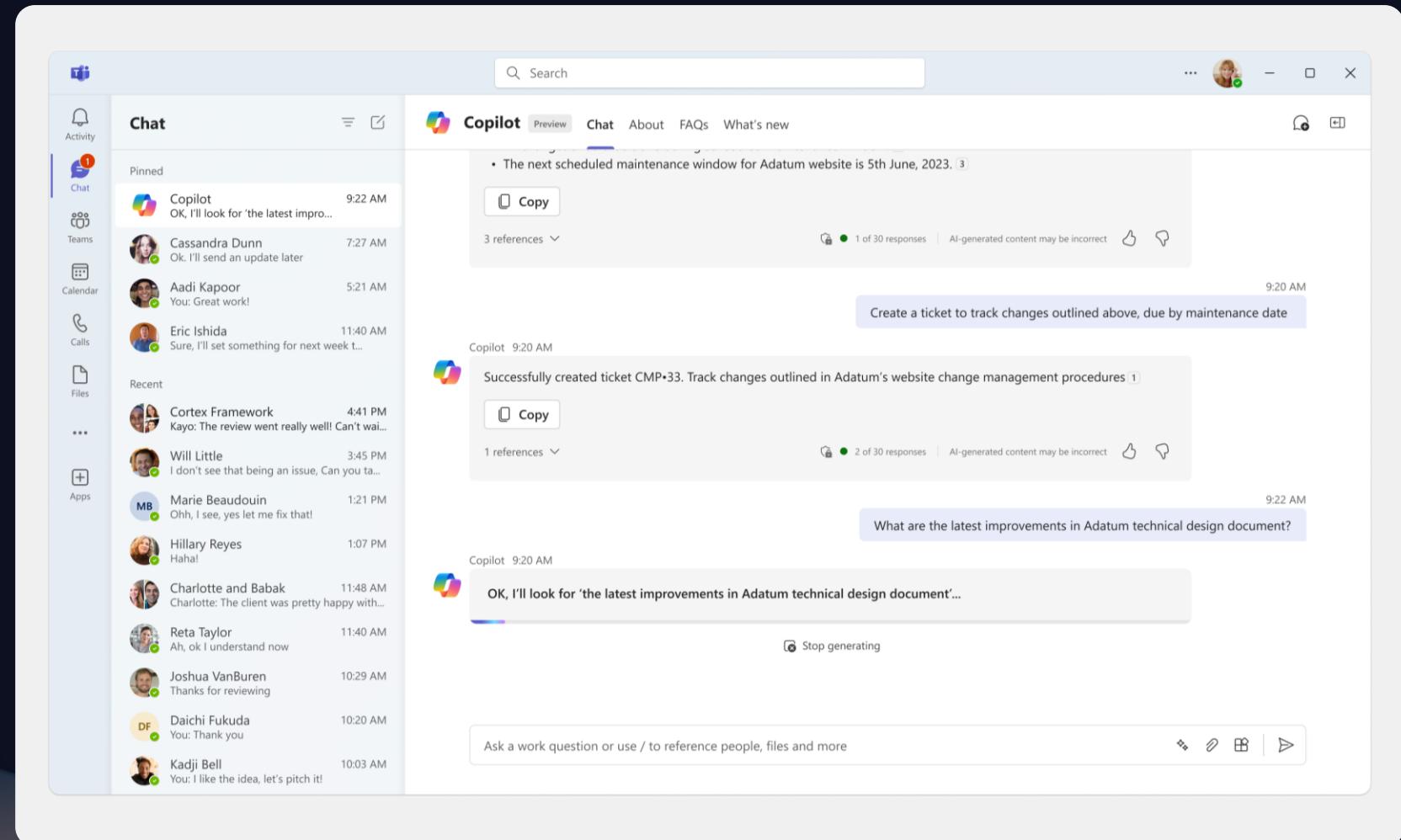
## Daniela Mandera | Lead Engineer

Daniela wants a consolidated update on the changes for the Adatum technical design document stored in Contoso, as well as from other asynchronous communications via chats and emails with her engineers.

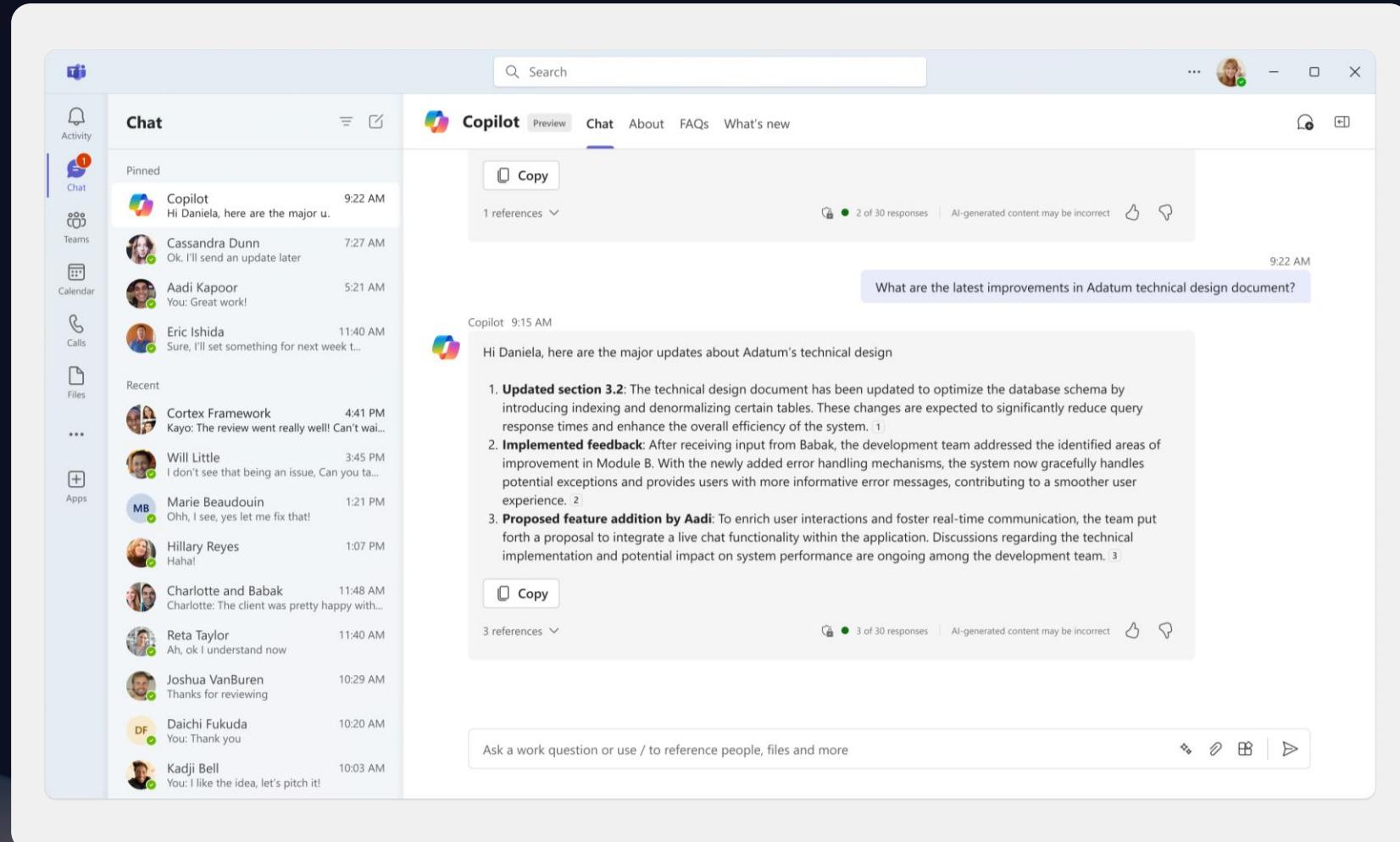
# Perform intuitive Q&A by bringing content from external services and M365 apps



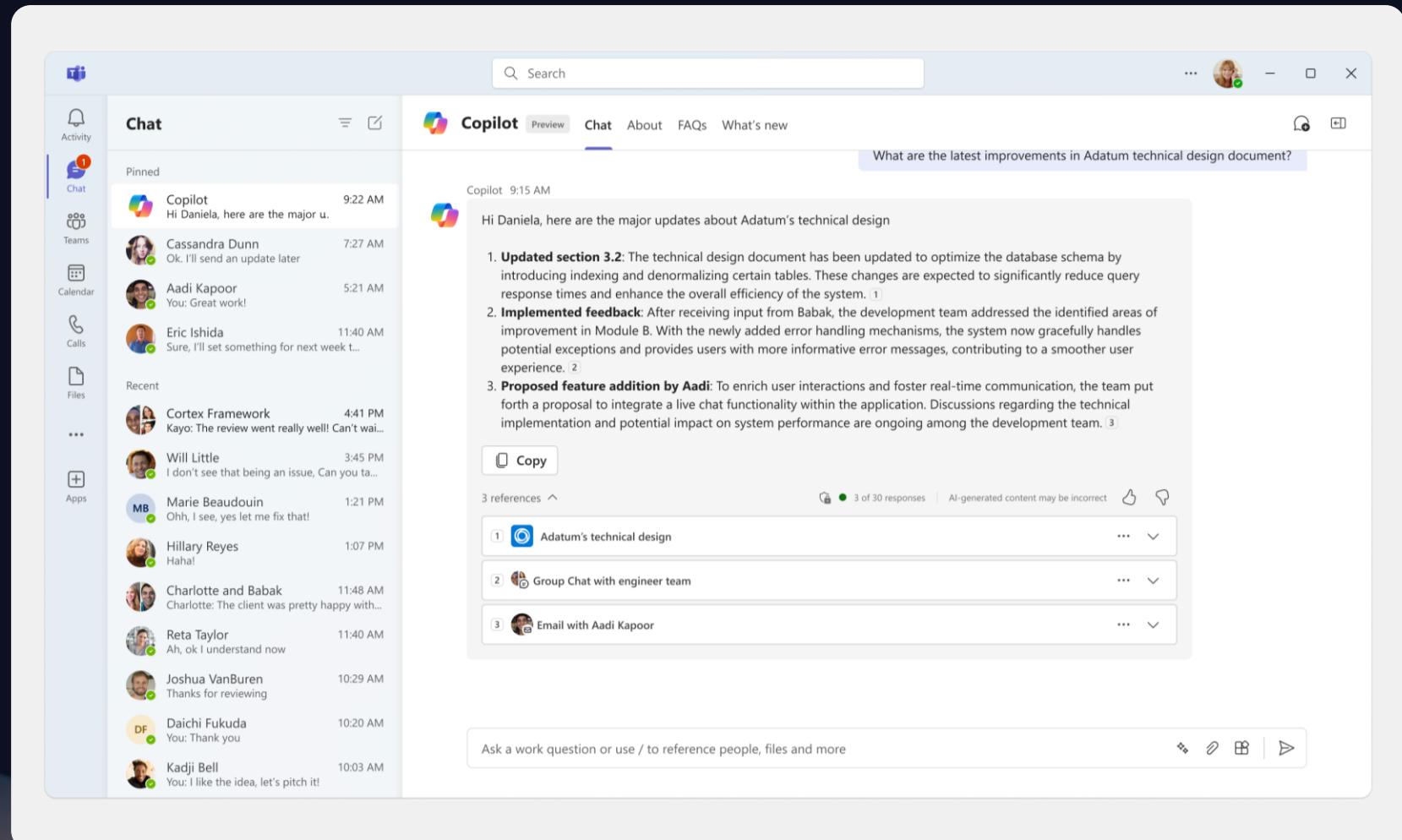
# Powered by Semantic Index, Copilot analyses your Graph data to map content relations



# Get personalized, context-aware and actionable responses from diverse datasets



# Access citations, enabling users to find summarized resources



# Copilot Handoff





# What is it?

- Copilot handoffs are plugin-provided deep links that carry over chat context, enabling users to seamlessly transition their chat with Microsoft 365 Copilot to your bot service
- You can enhance your Copilot message extension plugin to hand off a conversation to your custom engine copilot to handle scenarios where specialized knowledge or actions are required, such as complex IT support queries, detailed product inquiries, or interactive order management.
- Currently in public developer preview
- Samples available to test and start with: <https://github.com/OfficeDev/Microsoft-Teams-Samples/tree/main/samples/msgext-copilot-handoff/ts>



# Example

- A user looks for help on tech issues using Copilot and receives results from the enterprise dataset
- The user finds the available information insufficient and wants to continue the interaction with a Contoso bot plugin
- When the user selects the Contoso bot, a new chat starts and the conversation continues in the Contoso bot.
- This seamless switch from Copilot to the Contoso bot, without losing the conversation context is called a copilot handoff.

The screenshot shows a Microsoft 365 Chat window. On the left is a sidebar with icons for Home, Create, My Content, Feed, Apps, Copilot (which is highlighted), Outlook, Teams, Word, Excel, and PowerPoint. The main area shows a conversation with 'Copilot' on September 21, 2023. The user asks, "I'm having trouble with opening corp websites from my laptop, what should I do?". Copilot responds with troubleshooting steps: "Sorry you are having these issues. I found a few results which may help. I see you are using a 2019 Macbook Pro running the latest Sonoma 14.0 operating system. According to the information I found, If you are having trouble opening corp websites from your laptop, here are a few things you can try:

- Check your internet connection to make sure it is stable and strong.
- Restart your browser or try using a different browser.
- Clear your browser's cache and cookies.
- Restart your computer.
- Check if your firewall or antivirus software is blocking access to the websites.
- If the problem persists, you may want to contact your IT support team for further assistance.

Did this information solve your issue? To receive additional tech support you can start a chat with Contoso." Below this, there are 'Copy' and 'Chat with Contoso' buttons, a note about 2 references, and a lock icon. At the bottom, it says "Opened in Contoso" and has a text input field "Ask a work question or use / to reference people, files and more" with a character count of 84/2000.

# AI Library for Teams



# Teams AI Library

Create intelligent apps quickly and easily with prebuilt, reusable code snippets to deliver natural conversational interactions.



## Prebuilt templates



## Conversational experiences



## Guide conversations by user intent

The creative brief ready for the 'Contoso Orange Oil' campaign. Now, I would like you to create the draft marketing campaign materials based on the brief.

Contoso 11:17 AM

Absolutely! I'm here to assist you in creating the draft marketing campaign materials based on the 'Contoso Orange Oil' creative brief. I utilized the information and guidelines provided in the brief and generated the initial set of materials. Please check!

Copy Share

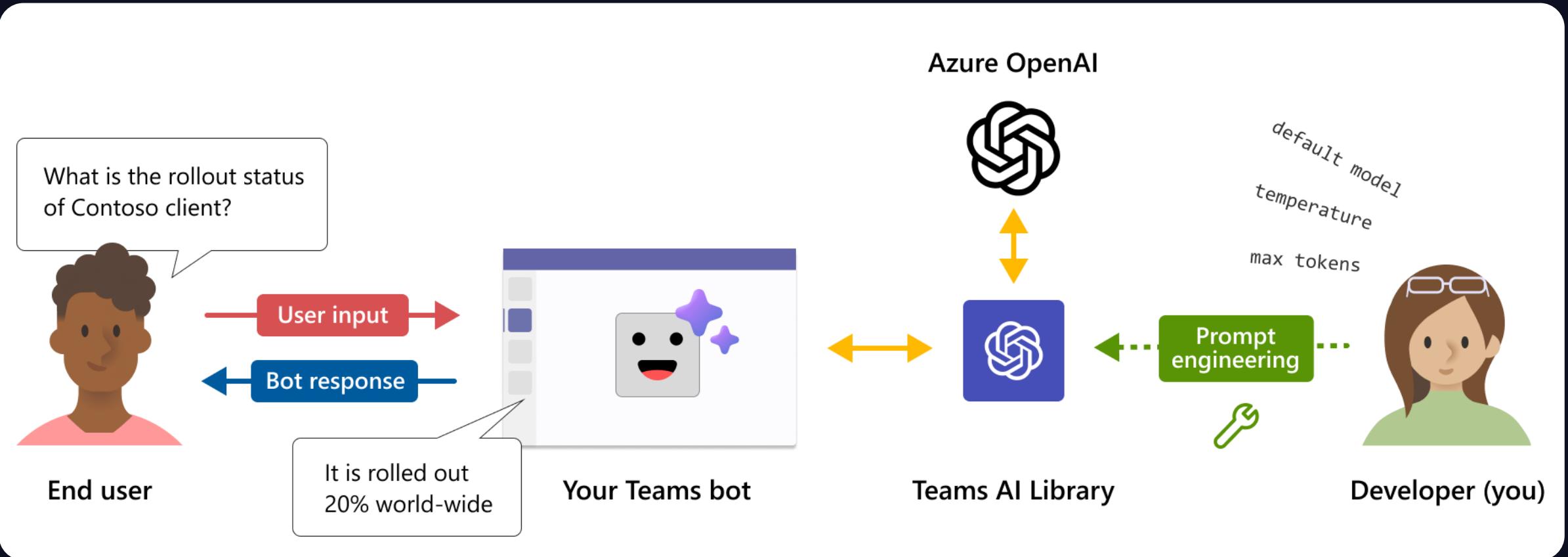
4 references ▾

AI-generated content may be incorrect.

1	Product shots (6)	...
2	Blog Post Copy	...
3	Landing Page	...
4	Instagram Ads	...

Ask a work question or make a request

# Teams AI Library





# What is it?

## Simple Teams-centric component scaffolding

- The Teams AI library simplifies the Teams app model to focus on the extension needed versus the protocol required.
- You can use prebuilt templates and add your business logic to this scaffold to add modules such as bots, message extensions, Adaptive Cards, or link unfurling.

## Natural language modeling

- The Teams AI library is built with GPT-powered language models, so that you don't need to spend time to write your conversational logic and identify user intents.
- Bots can run in-context and assist when the bot recognizes a user intent that maps to one of the bot actions.

## Conversational session history

- Teams AI library remembers context across messages and helps improve the bot performance by analyzing patterns in user behavior.

[Introduction to Teams AI Library - Teams | Microsoft Learn](#)

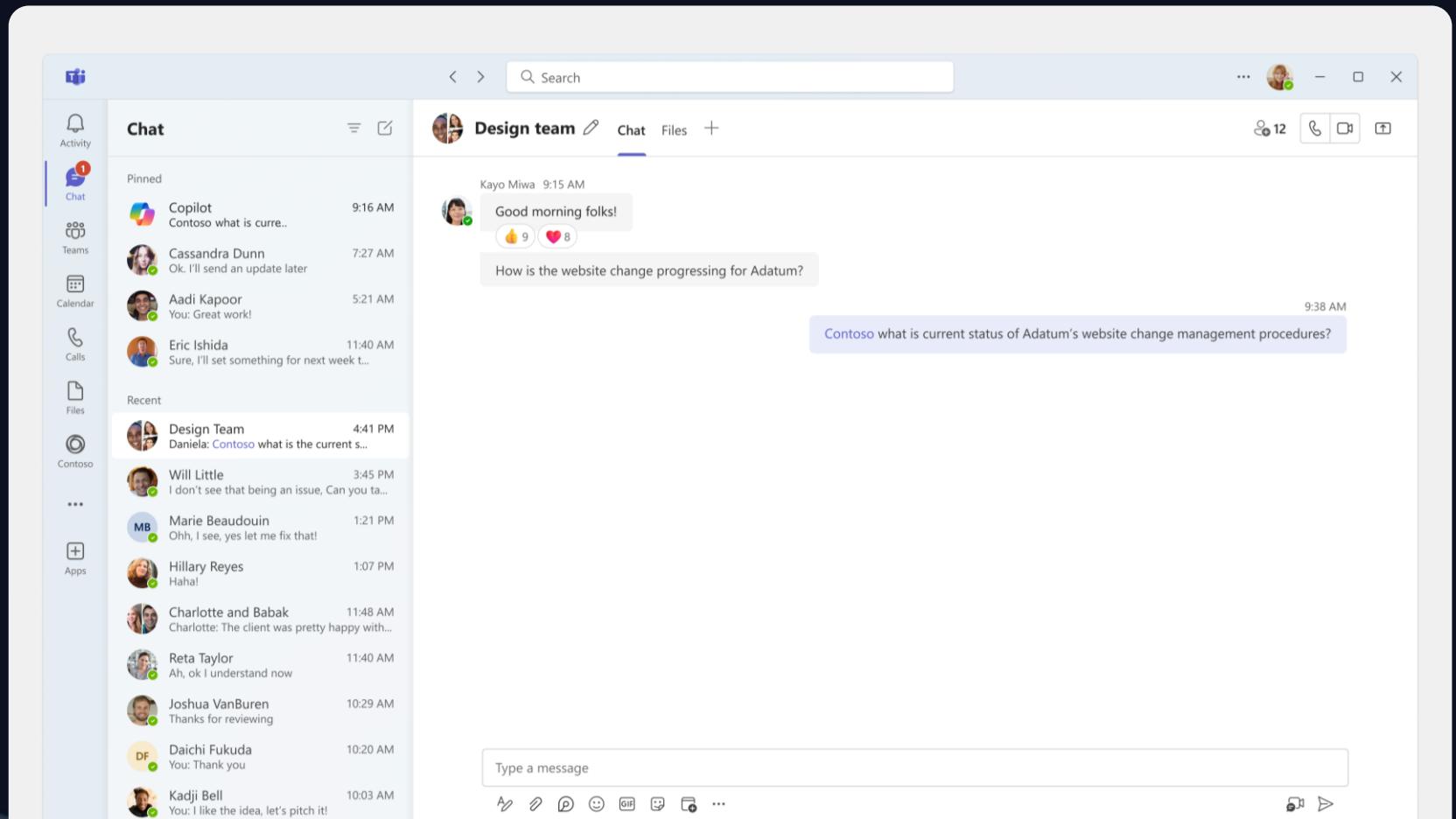
Samples: [teams-ai/js/samples at main · microsoft/teams-ai · GitHub](#)



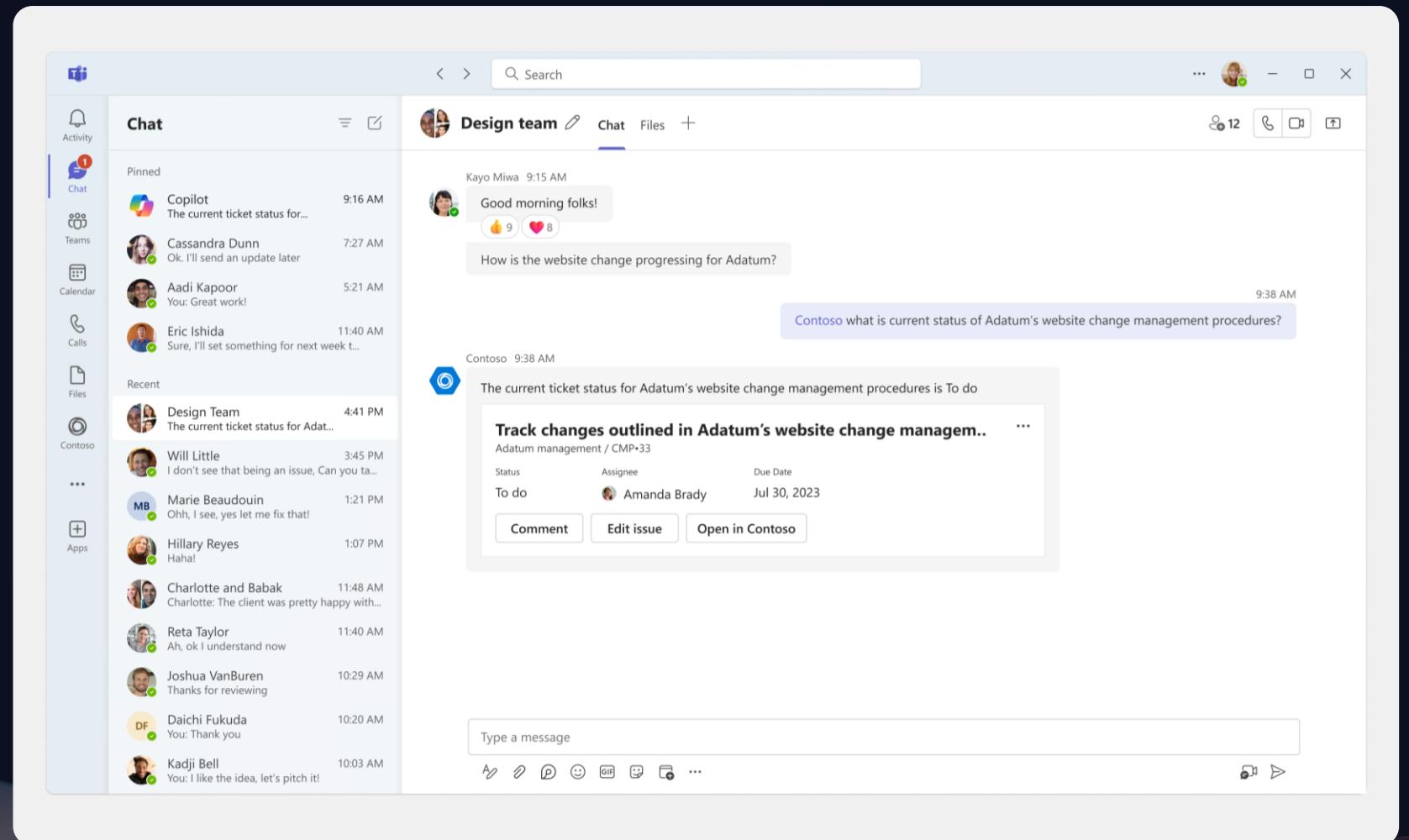
## Daniela Mandera | Lead Engineer

Daniela is a Team Lead who manages a team of 10 engineers. She uses Contoso, a task planner app, to create and manage the tasks for better visibility and collaboration within her team.

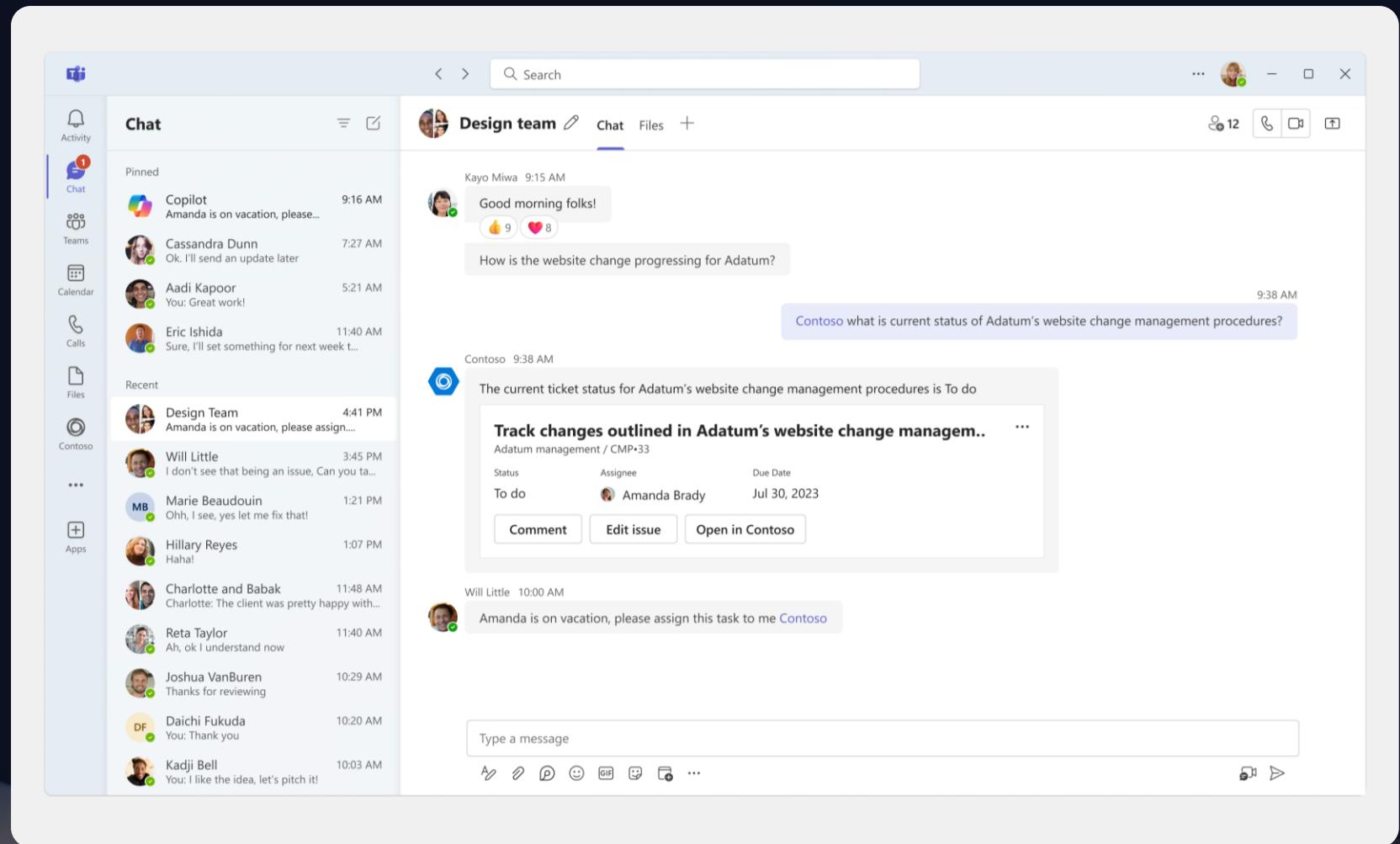
Your app will have natural language conversation capabilities without needing to rely on registered-only actions.



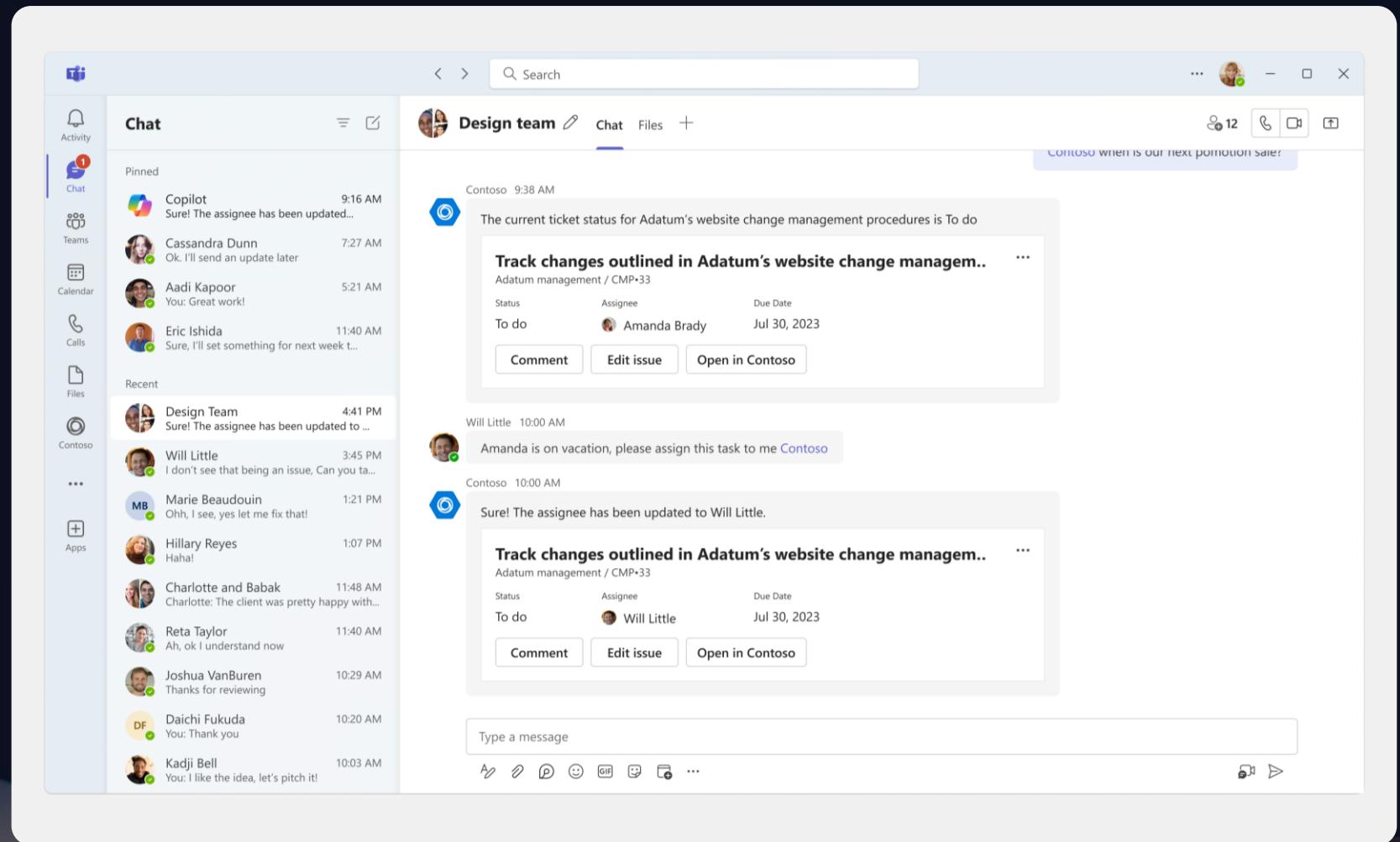
# Recognizes the user intent that maps to your bot actions



# Remembers context across messages and improves app performance

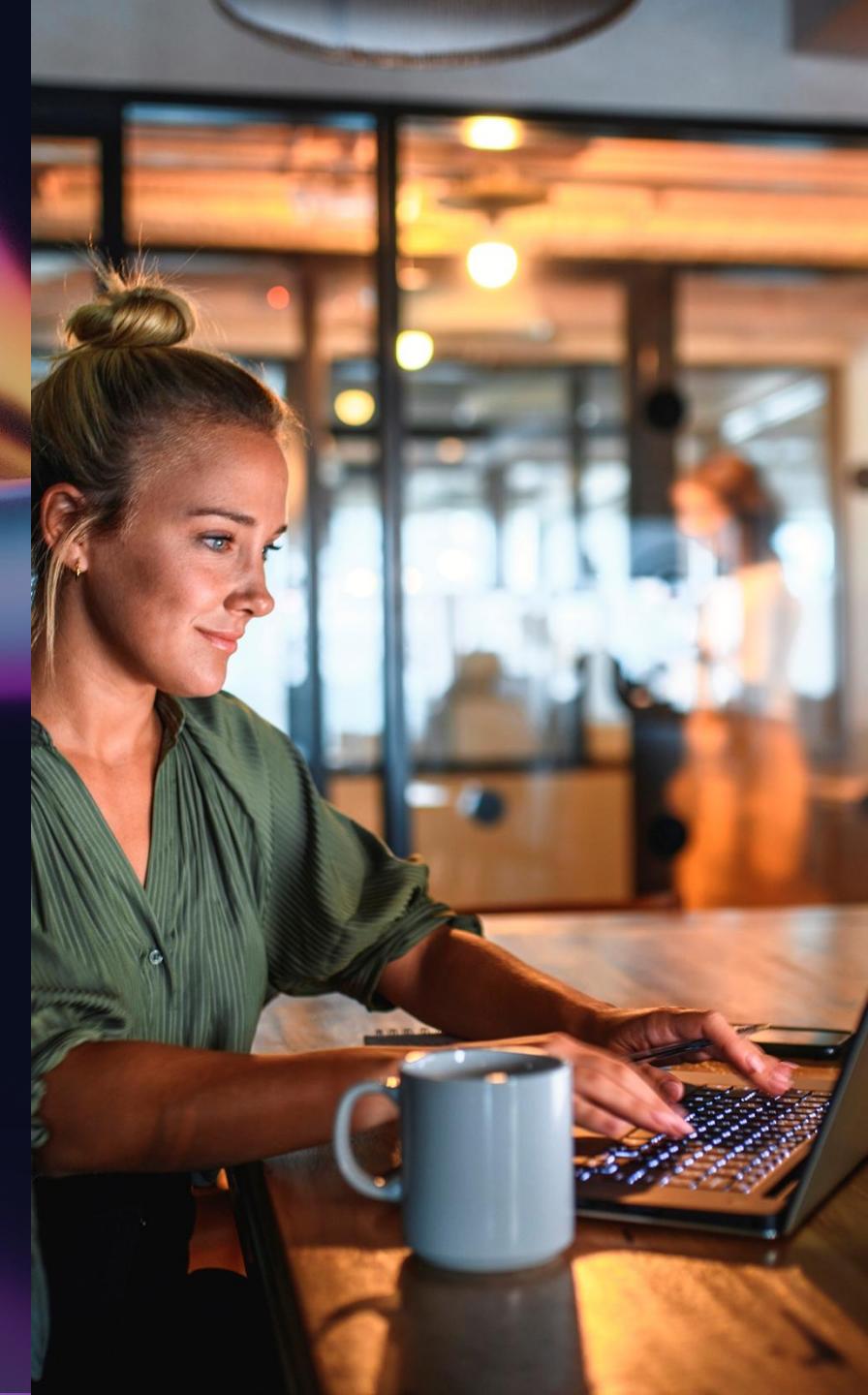


# Focus on your business logic; let Teams handle conversational bot complexities





Publish plugins for Microsoft  
365 Copilot to AppSource



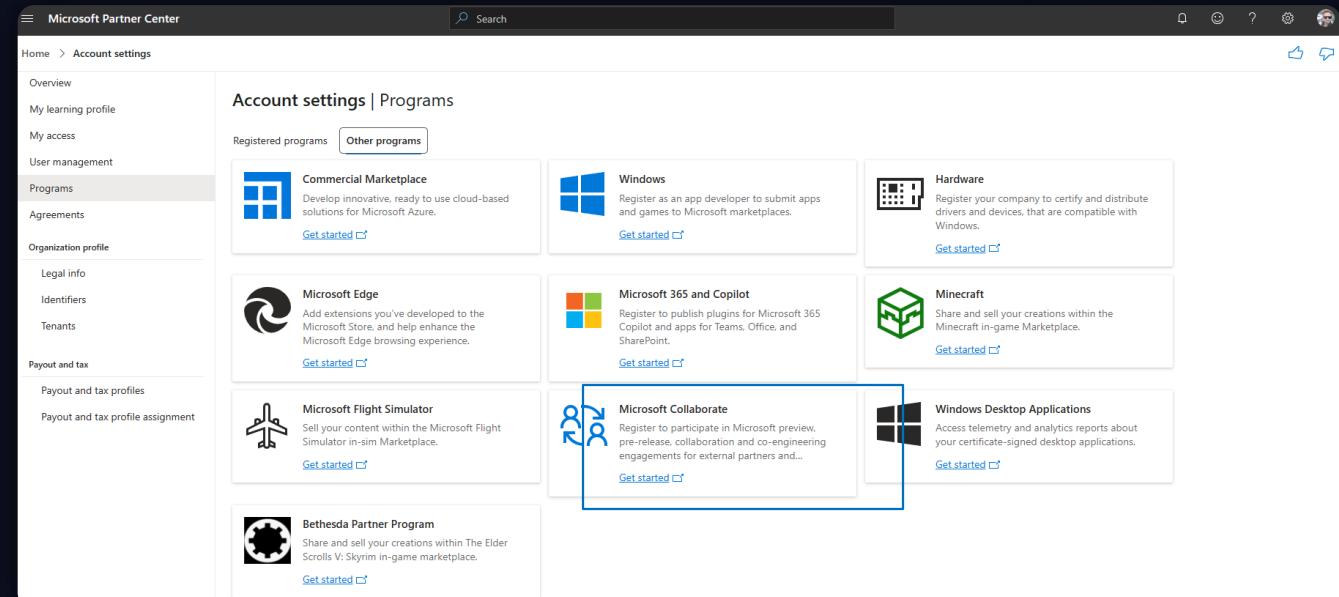
# Microsoft 365 and Copilot Program

As an independent software vendor, you can distribute your app through the **Microsoft 365 and Copilot** program of Microsoft Partner Center.

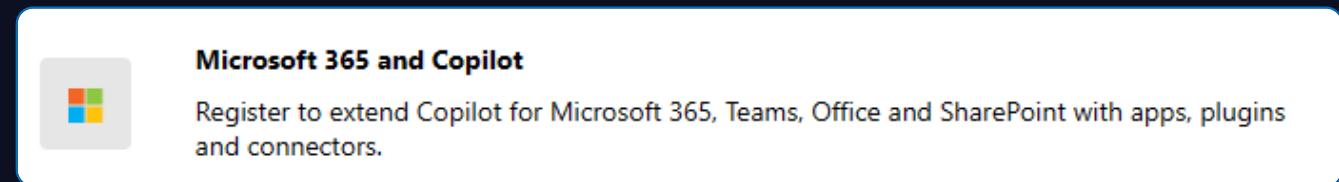
Submission of your app package to the program requires compliance with the following certification policies for acceptance to in-product stores:

-  Microsoft Commercial Marketplace certification policies:
  - [100 General](#)
  - [1140 Teams](#) (including [1140.9 Teams apps extensible as Microsoft Microsoft 365 Copilot plugins](#))

-  [Teams Store validation guidelines](#)
-  [Publisher verification](#)



The screenshot shows the Microsoft Partner Center interface under 'Account settings'. On the left, a sidebar lists 'Programs' as the selected category. The main area displays several program options with 'Get started' buttons: Commercial Marketplace, Windows, Hardware, Minecraft, Microsoft Edge, Microsoft Flight Simulator, Bethesda Partner Program, Microsoft Collaborate, and Microsoft 365 and Copilot. The 'Microsoft 365 and Copilot' section is highlighted with a blue border.



**Microsoft 365 and Copilot**  
Register to extend Copilot for Microsoft 365, Teams, Office and SharePoint with apps, plugins and connectors.

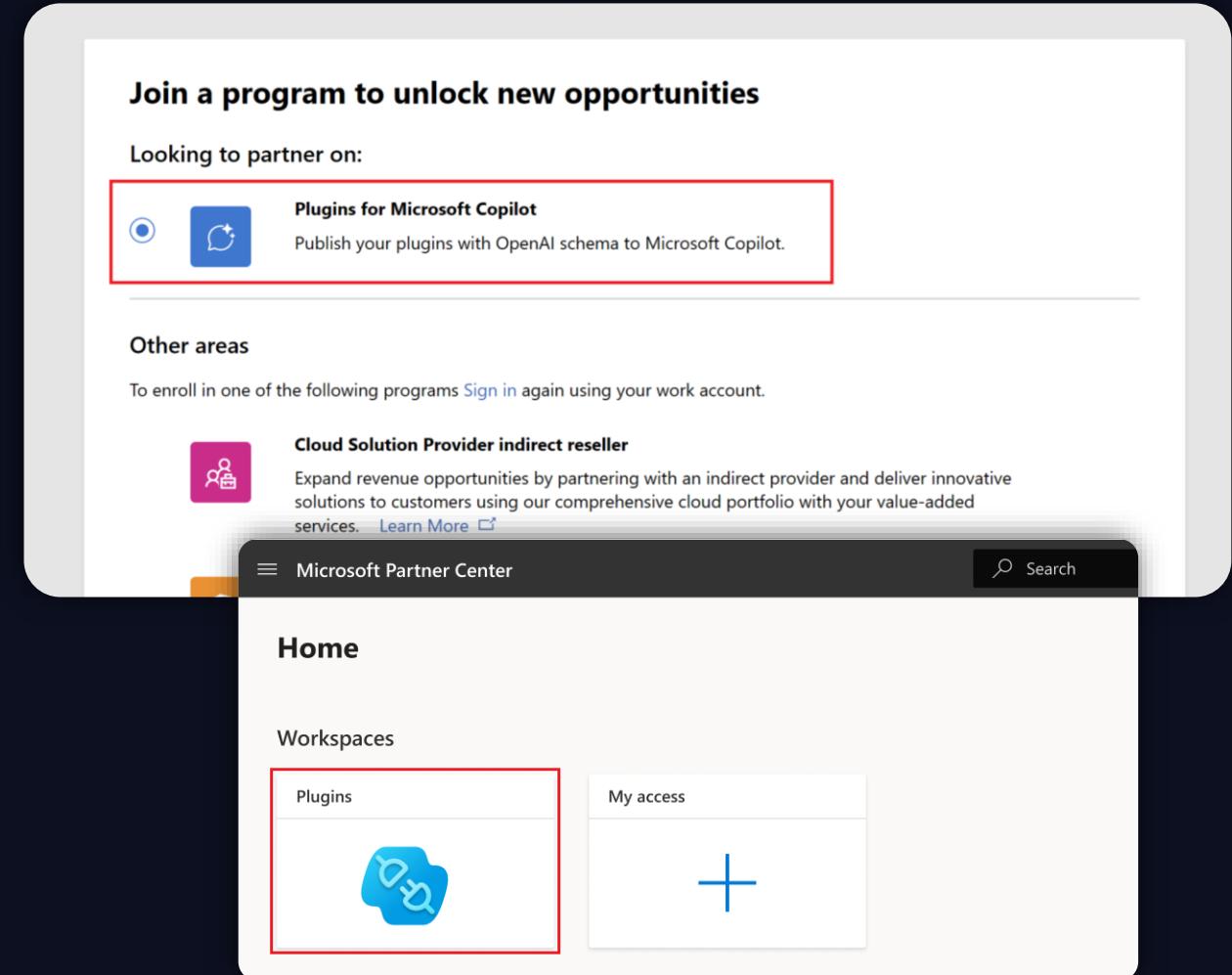
# Register for Plugins for Microsoft Copilot (Private Preview)

In the Welcome to Partner Center “Steps to program registration” page, click the “Sign in as organization button”, and then sign in using your work account the “Join a program to unlock new opportunities” page opens.

Confirm your account information details, read the Plugins for Microsoft Copilot program agreement, and then click the Accept and continue button.

Your account is submitted for verification, and the Plugins tile appears in your Partner Center dashboard.

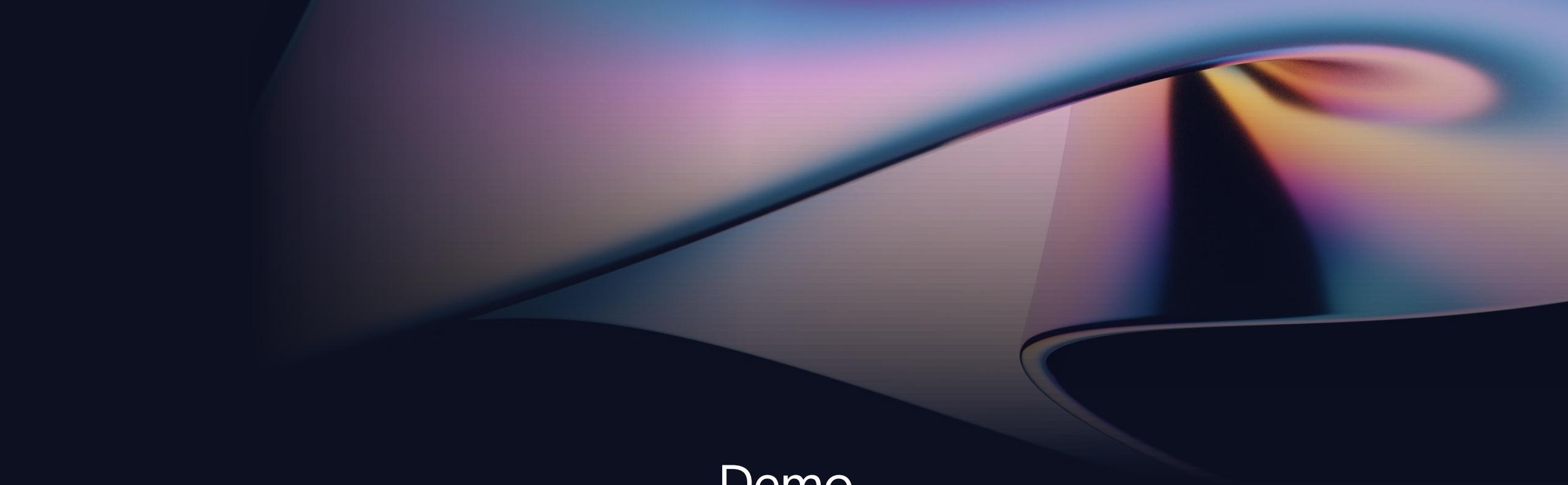
[Register as a developer for Plugins for Microsoft Copilot](#)



# Copilot extensibility scenario for Microsoft Commercial Marketplace

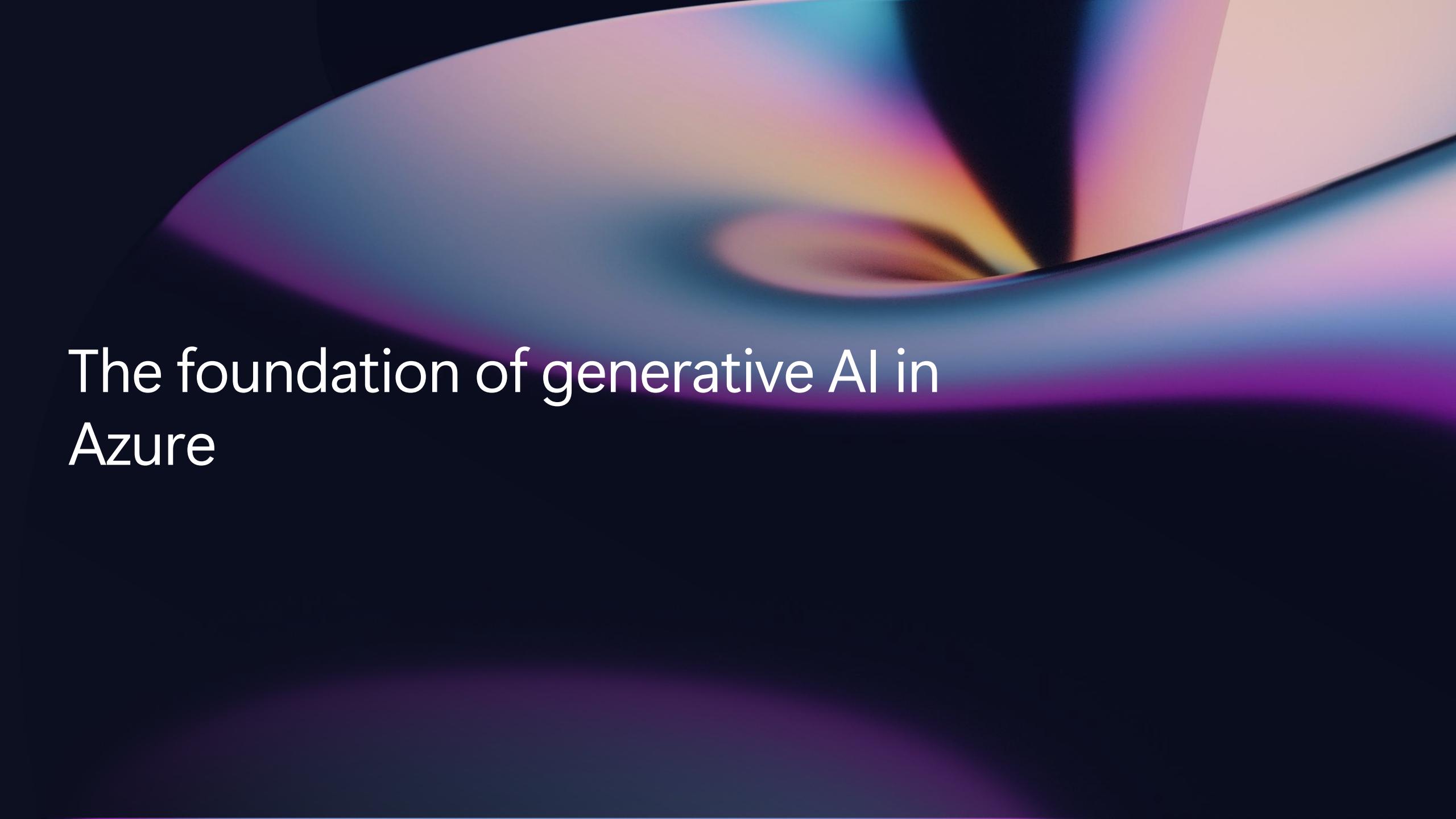
The following table summarizes the distribution support for Copilot extensibility scenarios, according to single tenant (line-of-business) or multi-tenant (independent software vendor, or *ISV*) channels.

Copilot extensibility type	Single tenant	Multi-tenant	Notes
<a href="#">Teams message extension apps as plugins</a>	✓	✓ *	*Store submission limited to verified publishers
<a href="#">Power Platform connectors as plugins</a>	✓	✗	
<a href="#">Microsoft Graph connectors</a>	✓	✗ *	*Standalone connectors not supported; can be distributed as Teams apps for verified publishers

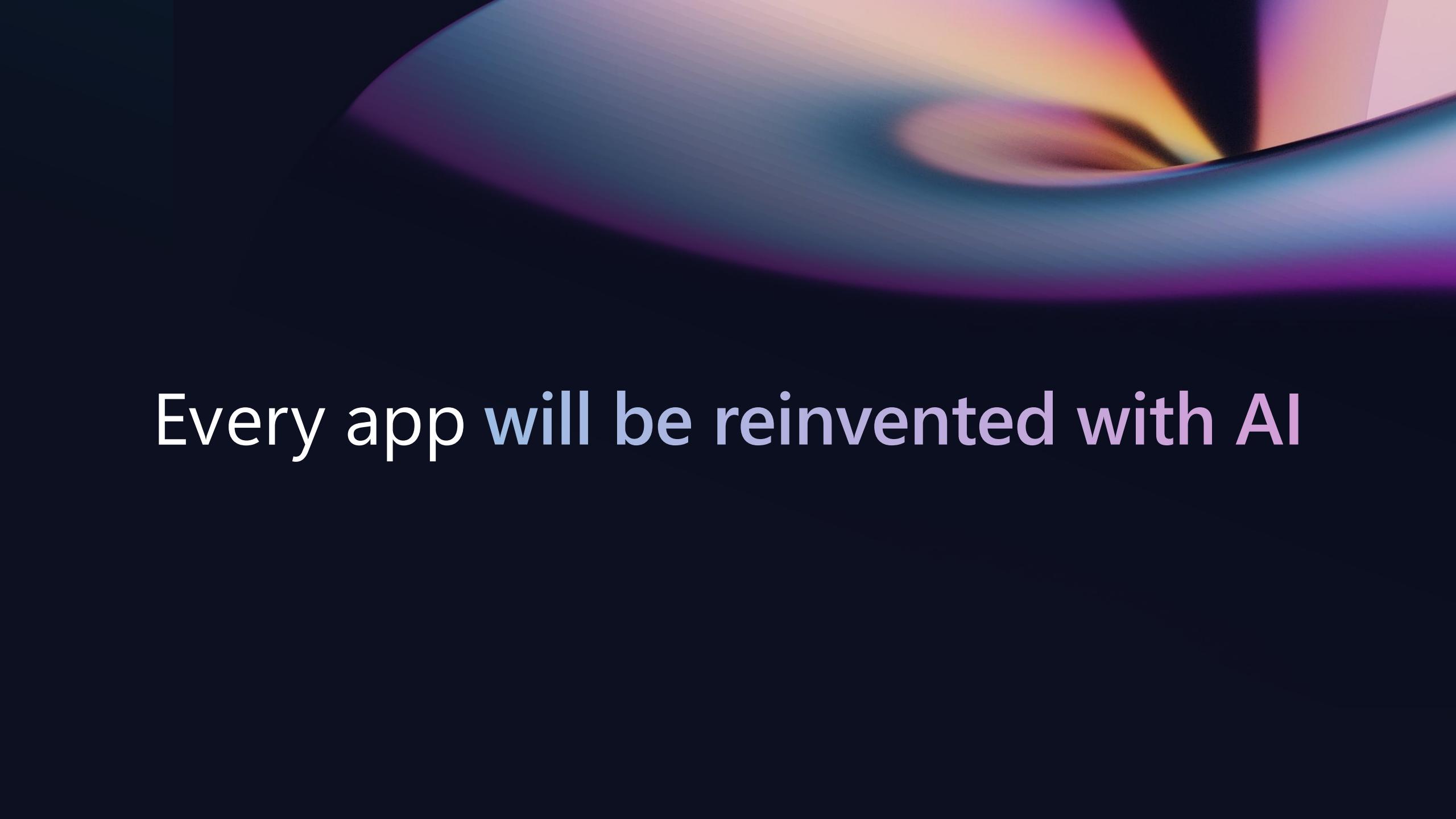


Demo

Build a bot-based message extension plugin for Microsoft  
365 Copilot



The foundation of generative AI in  
Azure



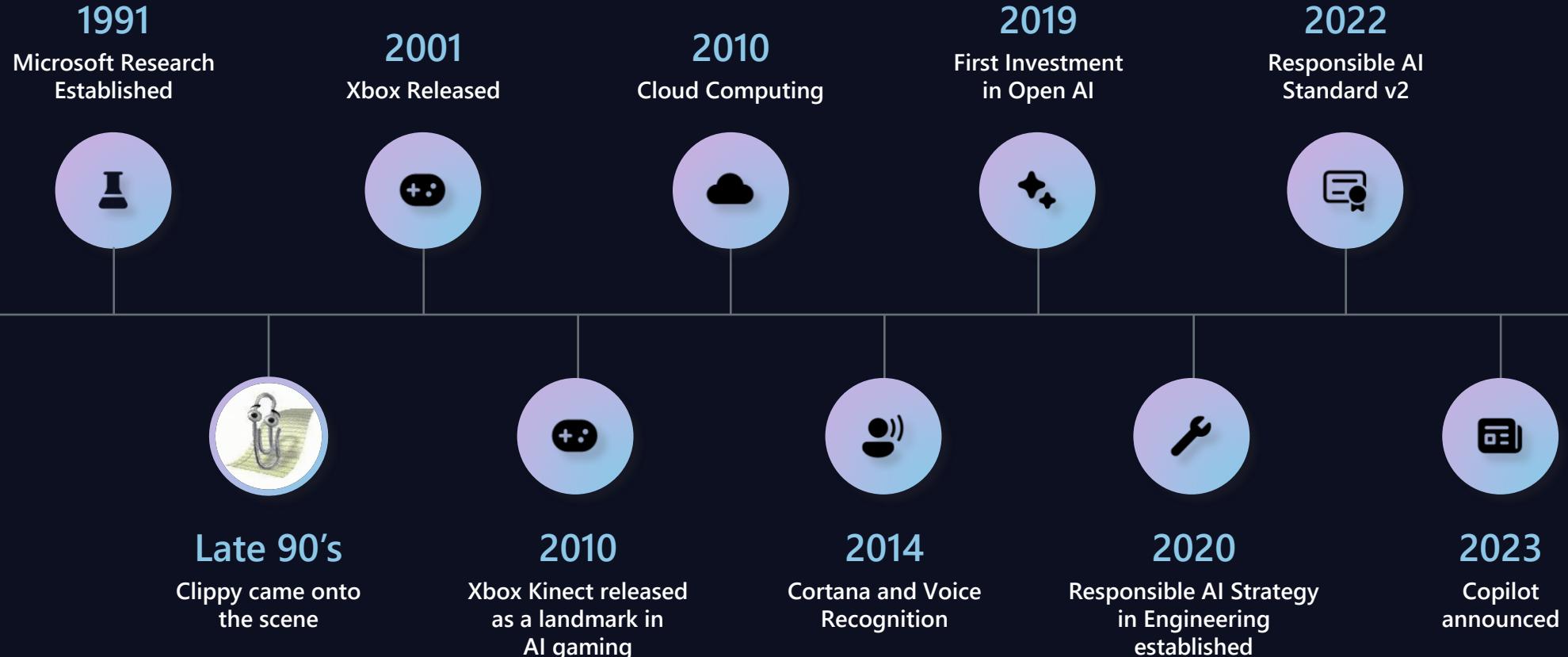
Every app will be reinvented with AI

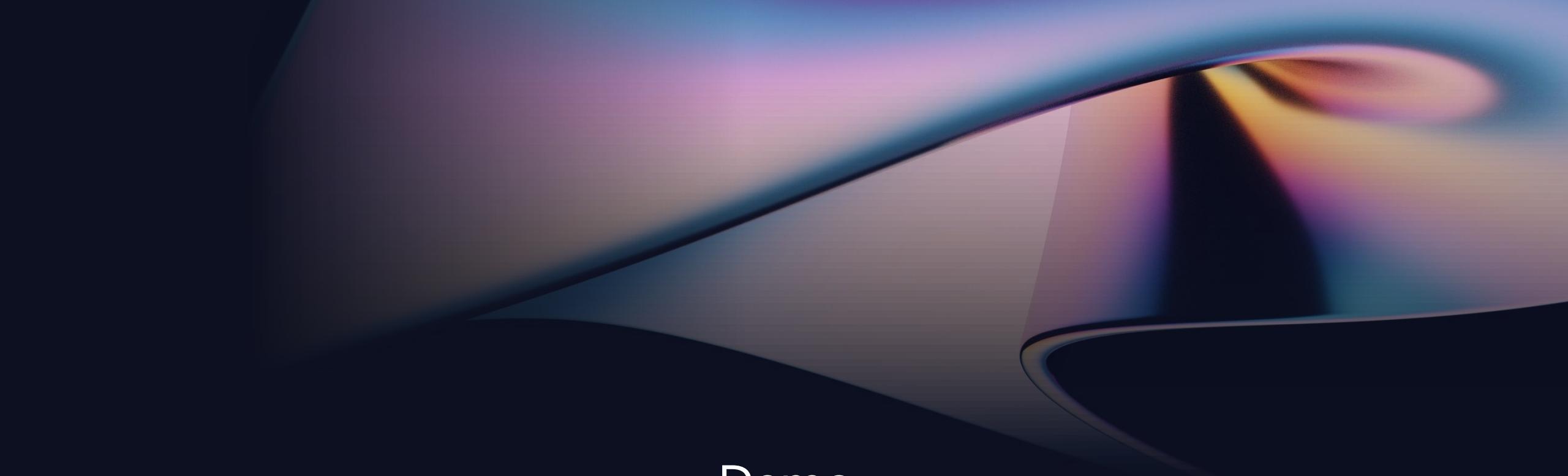
# Generative AI is in our lives

## Time to reach 100M users

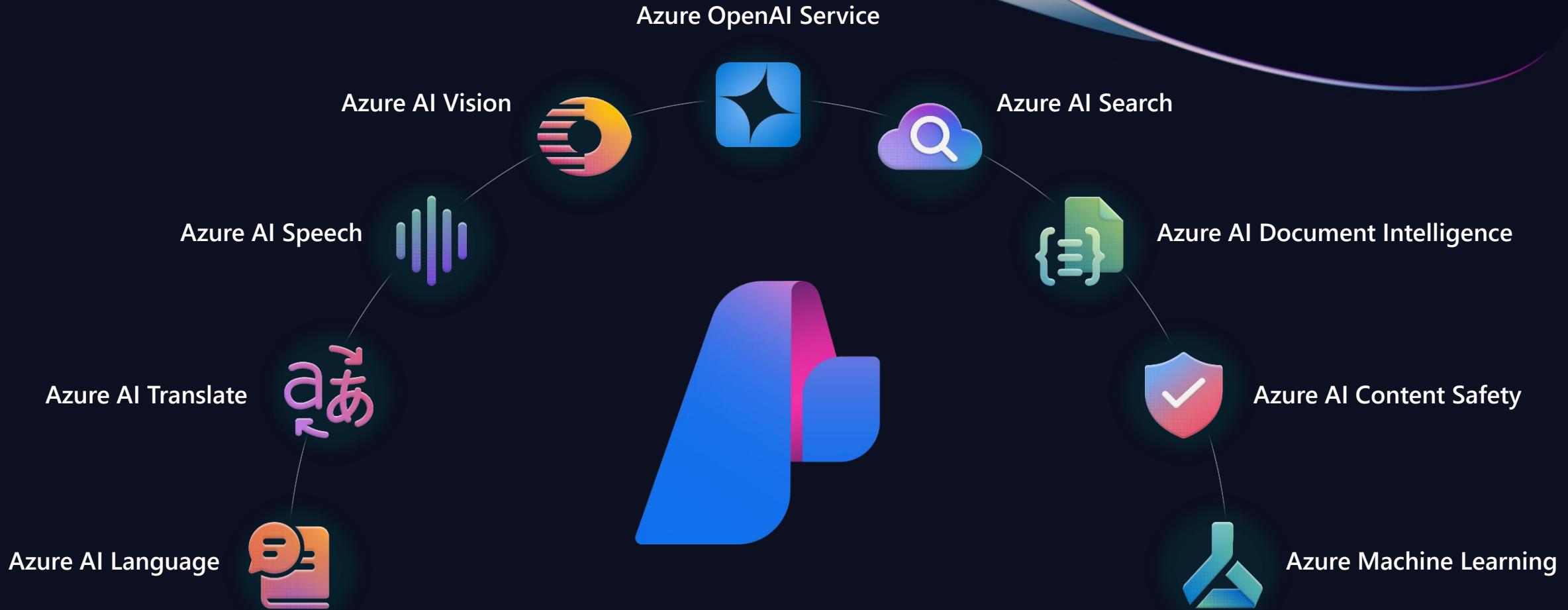


# Microsoft's AI Journey





Demo  
AI Capabilities today



# Microsoft Azure AI

Where innovators are creating the future

# Azure AI

## Best-in-class AI foundation models



### Azure AI Services

Pre-trained, turnkey solutions for intelligent applications



### Azure Machine Learning

Full-lifecycle tools for designing and managing AI models



### Responsible AI Tooling

Build and manage apps that are trustworthy by design



## Azure AI Foundry

A comprehensive platform to develop and deploy custom copilots

Generally available



# Azure AI Foundry

A comprehensive platform to develop and deploy custom copilots

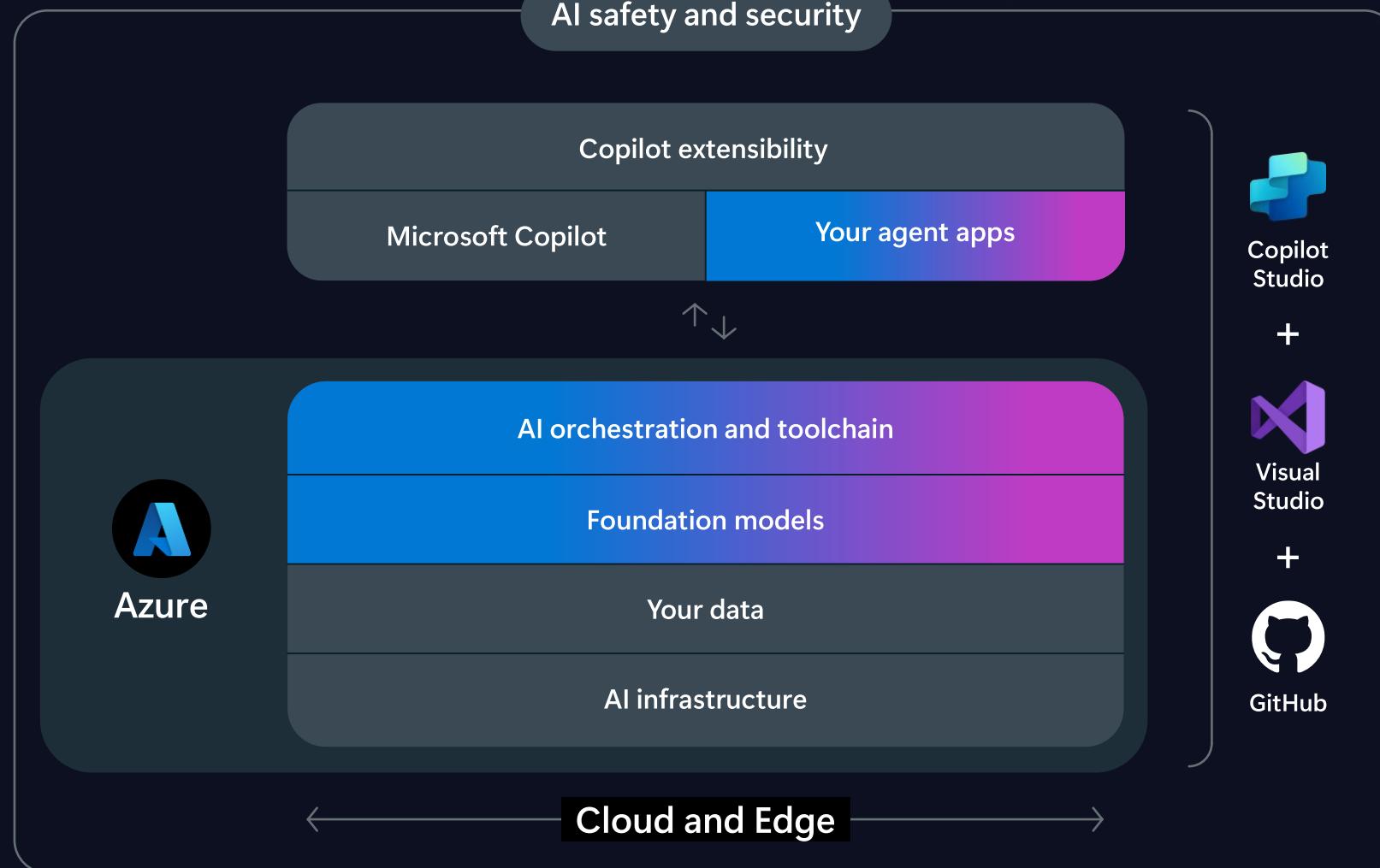
API and model  
choice

Complete AI  
toolchain

Responsible AI  
tools and practices

Enterprise-grade  
production at scale

# Copilot stack



# Use the option that fits your scenario the best



## Azure AI Foundry

Offers a wide range of **AI services and models** to build the entire AI development lifecycle

Fast and frictionless **prototyping for quick results**

Azure AI Foundry offers **state of the art evaluation, safety** and testing tools for your LLM application



## Copilot Studio

**1400+ connectors** available out-of-the-box + you can create your own connector

Channels like **Microsoft Teams, Facebook, and Slack** are easy to configure

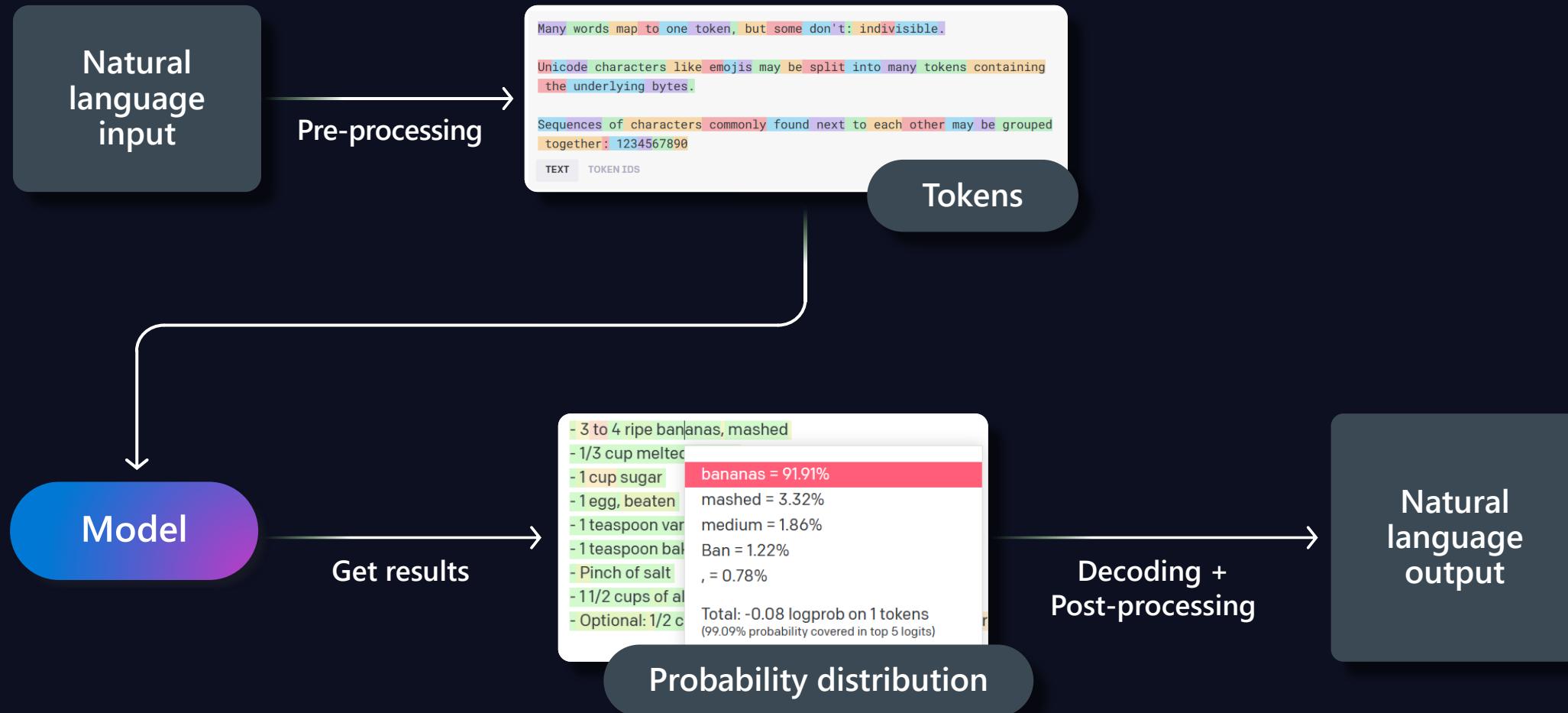
**Enterprise dialog management** and conversational orchestration



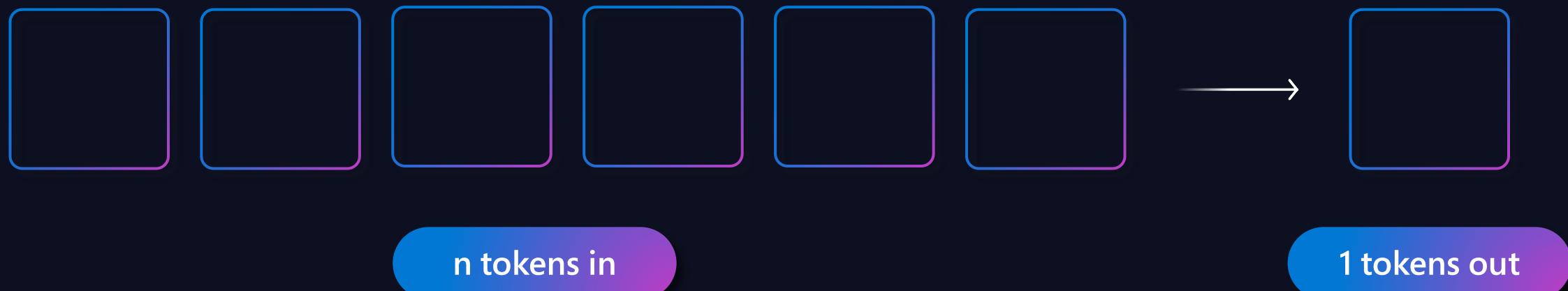
# How language models work

Predicting the next most  
likely token.

# How language models work



# How language models work



# How language models work

## Tokens

Tokens

11

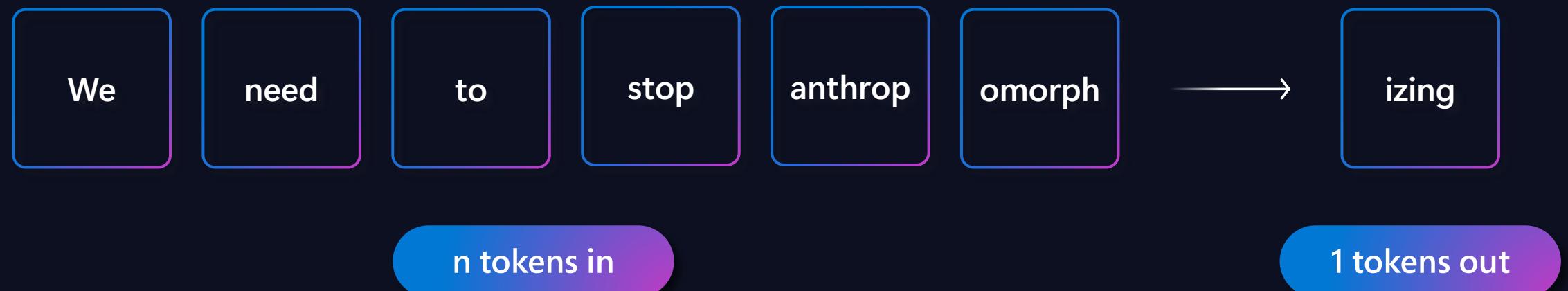
Characters

43

We need to stop anthropomorphizing ChatGPT.

[platform.openai.com/tokenizer](https://platform.openai.com/tokenizer)

# How language models generate text



# How language models generate text

in      out

We need to stop

We need to stop anthrop

We need to stop anthropomorph

We need to stop anthropomorphizing

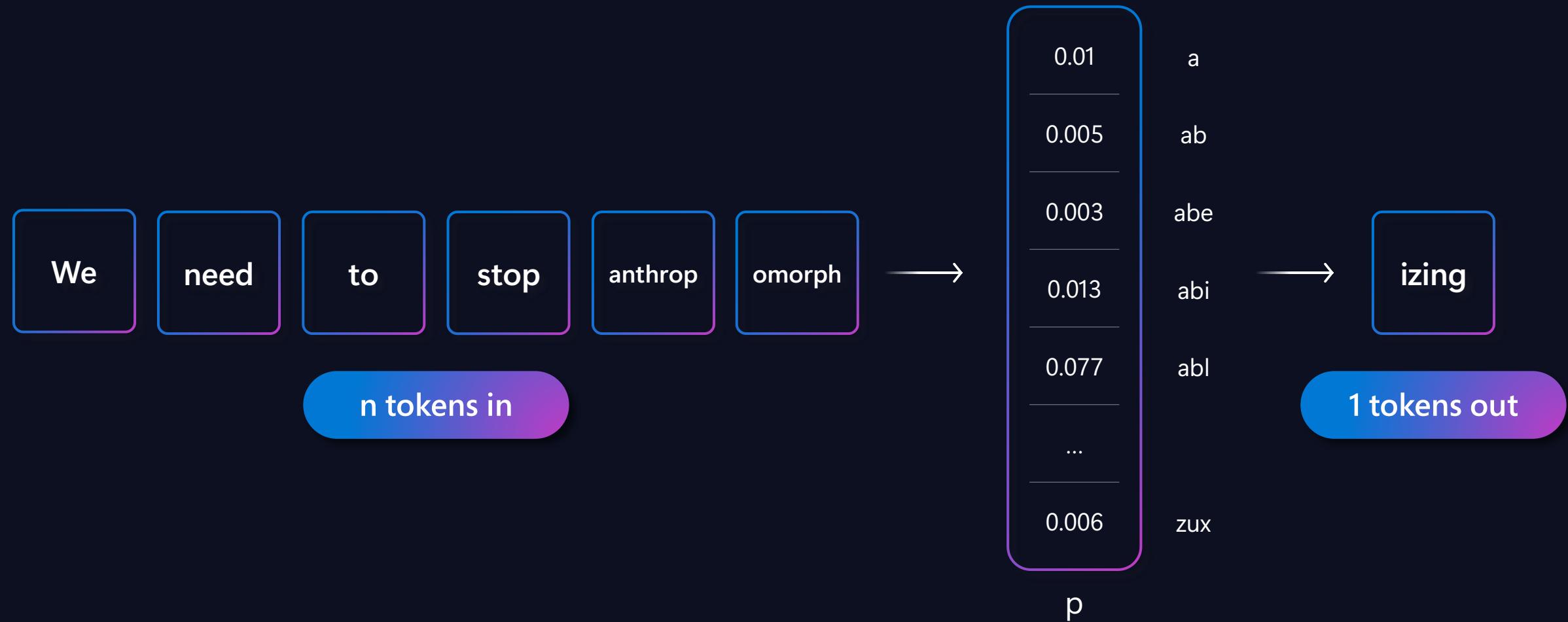
We need to stop anthropomorphizing Chat

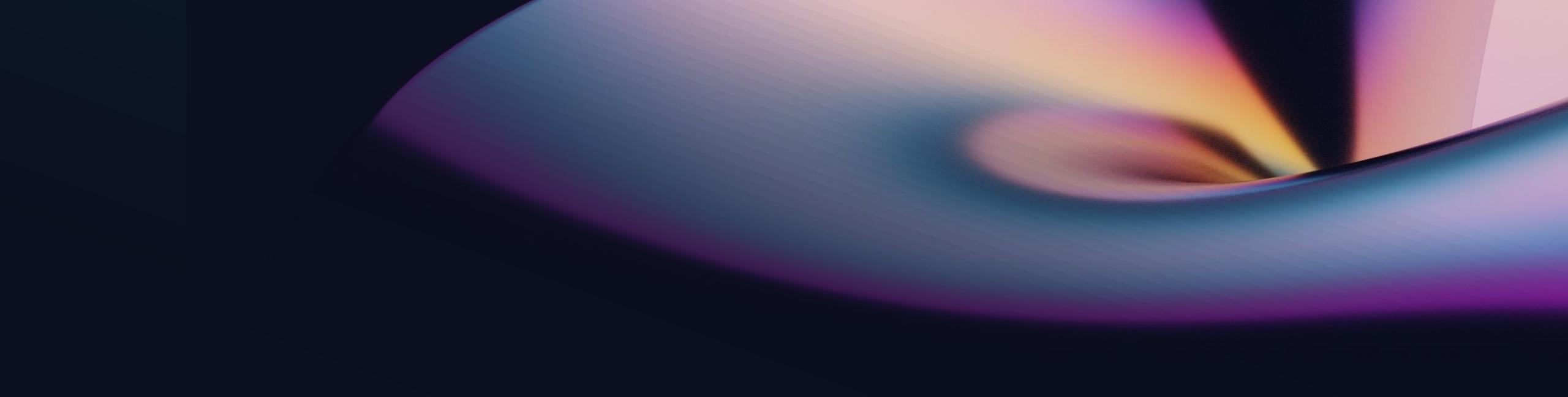
We need to stop anthropomorphizing ChatG

We need to stop anthropomorphizing ChatGPT

We need to stop anthropomorphizing ChatGPT.

# How language models generate text





The next most likely token

The only thing it does.



# Interacting with LLMs

Building applications using  
large language models.



**Prompt engineering** is a concept in Natural Language Processing (NLP) that involves embedding **descriptions** of **tasks** in input to prompt the model to output the desired results.

# Text to Text

User



What is the highest mountain in the world?

Assistant



The highest mountain in the world is Mount Everest. It is located in the Himalayas on the border between Nepal and the Tibet Autonomous Region of China.

The official height of Mount Everest is 8,848.86 meters (29,031.7 feet) above sea level, according to a 2020 revision by China and Nepal.

# Text to Image with DALLE-3

User



A close-up of a cute racoon walking through the forest, photorealistic texture and lighting

Assistant



# GPT-4o: Text & Image to Text

User



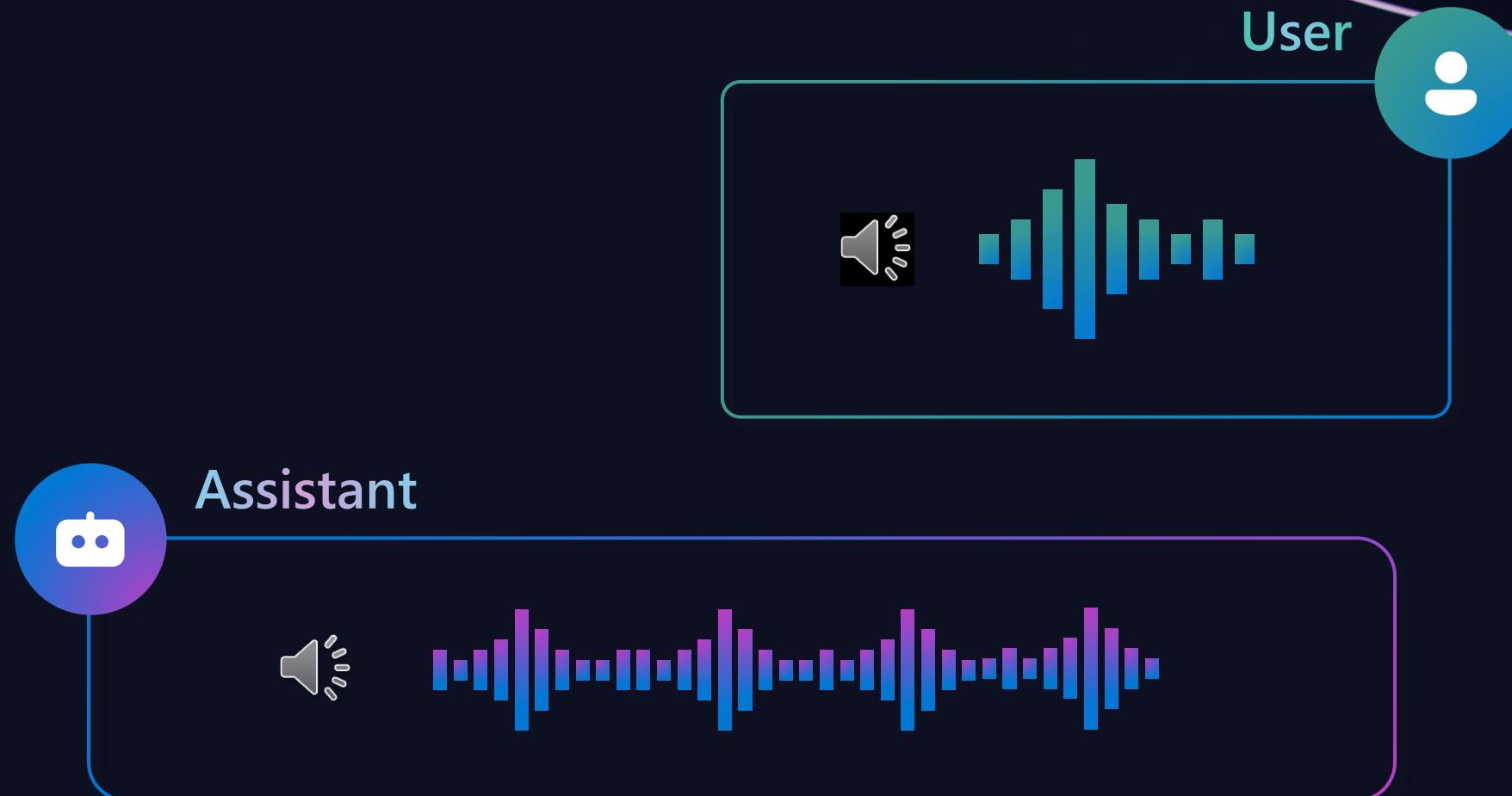
What is on this image?



Assistant

The image shows a cute raccoon in a forest setting. The raccoon is looking directly at the camera with large, expressive eyes. The forest in the background is lush and green, with sunlight filtering through the trees, creating a serene and enchanting atmosphere.

# GPT-4o-realtime: Speech to Speech



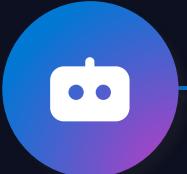
# System Message

Provide the model additional context  
to generate a response



User

What is your name?



Assistant

I don't have a name, but you can call me  
Assistant. How can I help you today?



## System message

You are a friendly  
assistant called Henk.

You always respond  
in a rhyme.

User

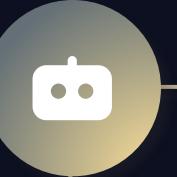


What is your name?



## Assistant

My name is Henk, nice to meet you,  
Here to help with what you need to do!



## System message

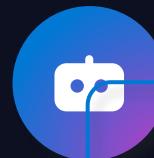
You are a friendly assistant called Henk.

You always respond in a rhyme.



User

What is your name?



## Assistant

My name is Henk, nice to meet you,  
Here to help with what you need to do!



User

A fun fact about a racoon



## Assistant

Their nimble hands are truly a sight,  
They'll eat what they find, both day and night!

# Recommended System Message framework

## Define the model's profile, capabilities, and limitations for your scenario

Define the specific task(s)

Define how the model should complete the tasks,

Define the scope and limitations of the  
Define the posture and tone

## Define the model's output format

Define the language and syntax of the output format

Define any styling or formatting

## Provide example(s) to demonstrate the intended behavior of the model

Describe difficult use cases where the prompt is ambiguous or complicated

Show chain-of-thought reasoning to better inform the model

## Define additional behavioral and safety guardrails

Define the specific task(s)

Define how the model should complete the tasks,

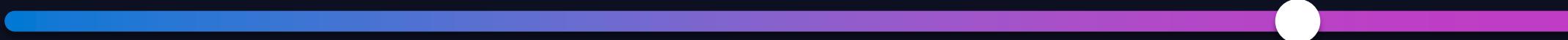
Define the scope and limitations of the  
Define the posture and tone

# Model parameters

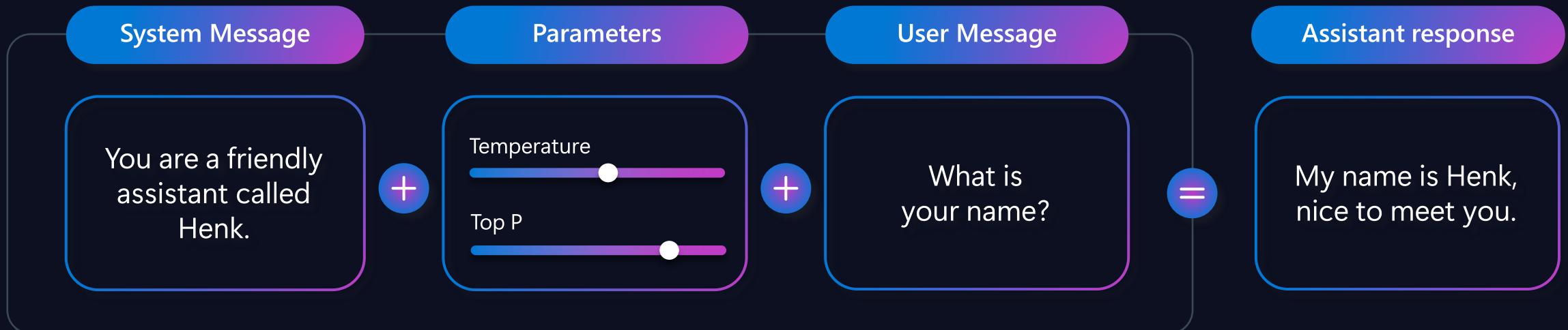
Temperature



Top P



# Interacting with LLMs





Which model to use?

Easily find various types of models

# Azure AI model breadth

Offering a wide collection of frontier and open models

## Azure OpenAI Service



GPT-4o  
GPT-4-Turbo with Vision, GPT-4, GPT-3.5  
Embeddings  
DALL-E  
Whisper, Text to speech

## Phi models



Phi-3-mini  
Phi-3-small  
Phi-3-medium  
Phi-3-vision

## Meta



Llama-2-70b/70b-chat  
Llama-2-13b/13b-chat  
Llama-2-7b/7b-chat  
Llama-3  
CodeLlama

## Mistral AI



Mistral Large  
Mistral 7B  
Mixtral 8x7B –  
Mixture of Experts

## Cohere



Cohere R+  
Cohere R  
Embed v3-Multilingual  
Embed v3-English

## Hugging Face



Falcon/TII  
Stable Diffusion/Stability AI  
Dolly/Databricks  
CLIP/OpenAI

## Databricks



Databricks/dbrx-base  
Databricks/dbrx-instruct

## NVIDIA



Nemotron-3-8B-4k  
Nemotron-3-8B-Chat-SFT/RLHF/  
SteerLM  
Nemotron-3-8B-QA

## Snowflake



Snowflake/arctic-base  
Snowflake/arctic-instruct

Model catalog - Azure AI Foundry

https://ai.azure.com/explore/models?wsid=/subscriptions/4e42df61-f5e6-4a7a-ade9-714785cfef28/resourceGroups/rg-aycabas-brk440/providers/Microsoft.MachineLearningServices/workspaces/aycabas-brk440&tid=93d9f3a5-1a1b-4f0a-8fd2-51c487cf1af5

# Find the right model to build your custom AI solution

## What's new?

tsuzumi is now available! [Check out models](#)

Announcing BRIA 3.2 Fast [Check out models](#)

News from Cohere! [Check out models](#) [Read blog](#)

New SLM from Mistral [Check out models](#) [Read blog](#)

Meta Llama 3.2 models are here! [Check out models](#) [Read blog](#)

## New model benchmarks available now in model catalog

Model benchmarks are integrated into model catalog for easier navigation. Compare benchmarks across models and datasets available in the industry to assess which one meets your business scenario.

[Compare with benchmarks](#) [How model benchmarks are scored](#)

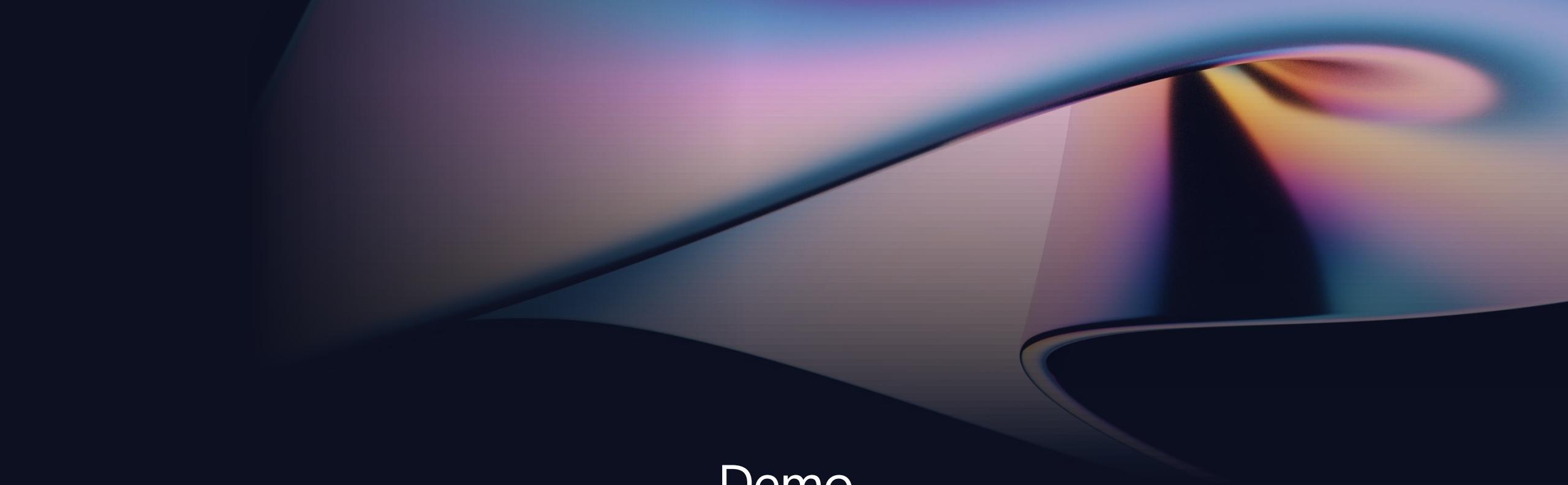
Collections Industry Deployment options Inference tasks Fine-tuning tasks Licenses

Compare models Models 1812

Search

gpt-4-realtime-preview Audio generation	gpt-4 Chat completion	gpt-35-turbo Chat completion	o1-preview Chat completion	o1-mini Chat completion	gpt-4o-mini Chat completion
gpt-4o Chat completion	gpt-4-32k Chat completion	gpt-35-turbo-instruct Chat completion	gpt-35-turbo-16k Chat completion	dall-e-3 Text to image	dall-e-2 Text to image
whisper Speech recognition	tts-hd Text to speech	tts Text to speech	text-embedding-3-small Embeddings	text-embedding-3-large Embeddings	Phi-3.5-mini-instruct Chat completion
Phi-3-small-8k-instruct Chat completion	Phi-3-mini-4k-instruct Chat completion	Phi-3-mini-128k-instruct Chat completion	Phi-3-medium-4k-instruct Chat completion	Phi-3-medium-128k-instruct... Chat completion	Phi-3.5-MoE-instruct Chat completion

Management center



Demo  
Interact with LLMs



What is next?  
Autonomous agents

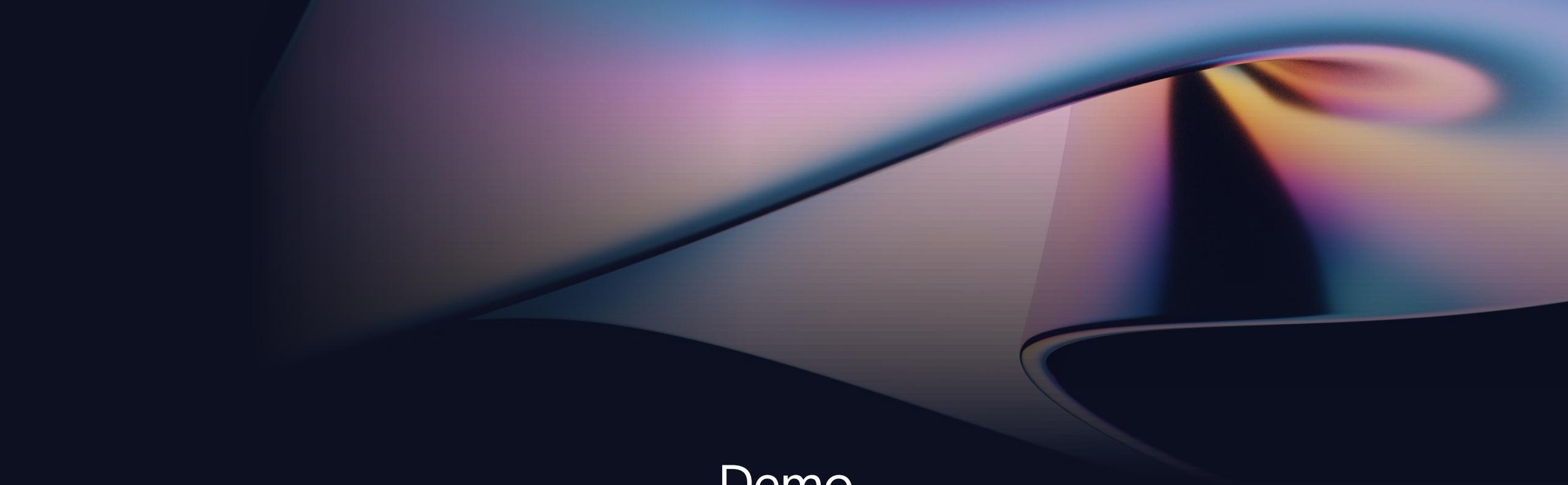
# Agent

An agent in LLM-based applications is an autonomous software entity leveraging large language models to perform specific tasks through natural language interaction.

Independent

Goal-focused

Interactive

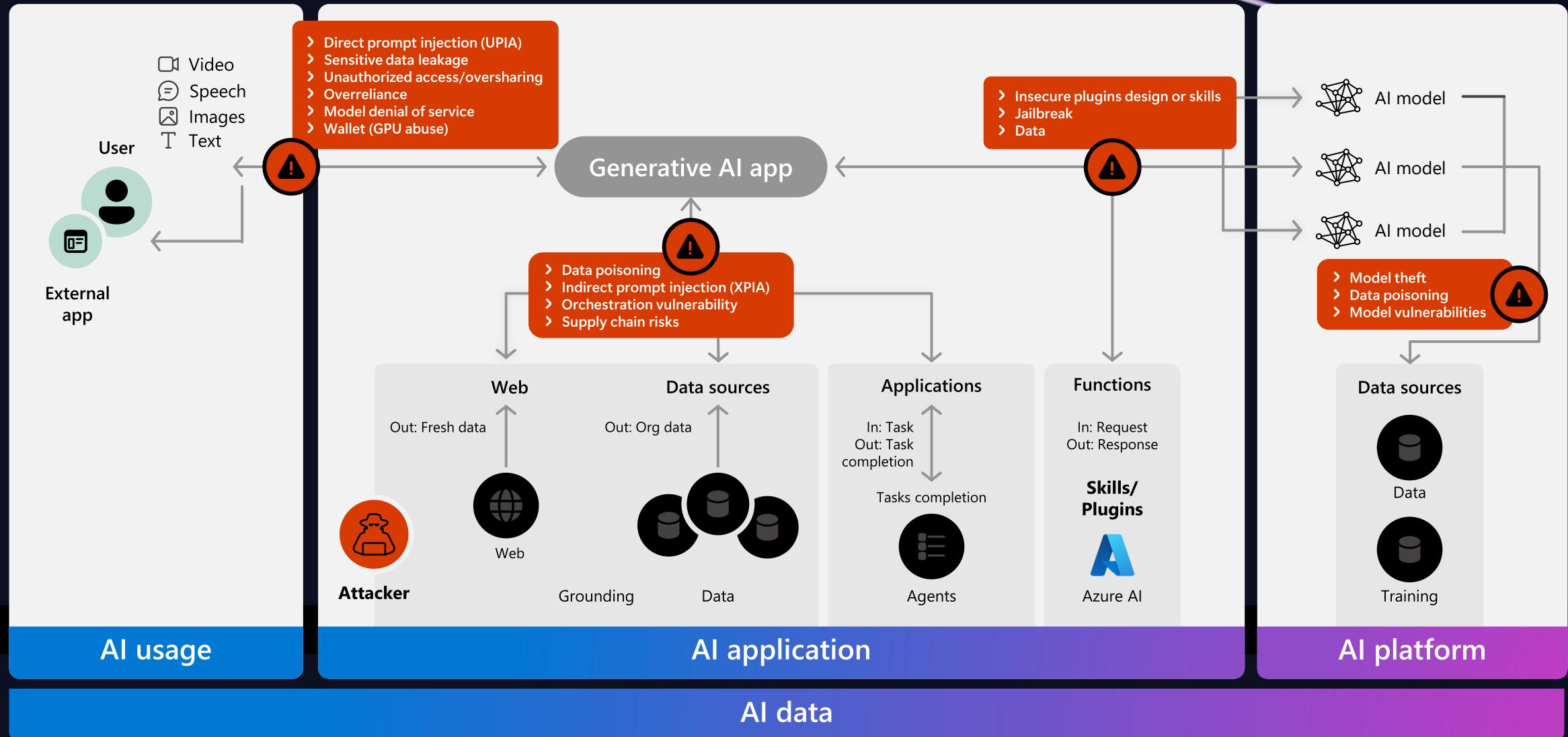


# Demo Assistant API

# Securing AI applications on Azure



# Generative AI threat landscape



## The cybersecurity bell curve

Basic security hygiene still protects against 98% of attacks<sup>1</sup>



### Enable multifactor authentication

Make it harder for bad actors to utilize stolen or phished credentials by enabling multifactor authentication. Always authenticate and authorize based on all available data points, including user identity, location, device health, service or workload, data classification, and anomalies.

### Apply least privilege access

Prevent attackers from spreading across the network by applying least privilege access principles, which limits user access with just-in-time and just-enough-access (JIT/JEA), risk-based adaptive policies, and data protection to help secure both data and productivity.

### Keep up to date

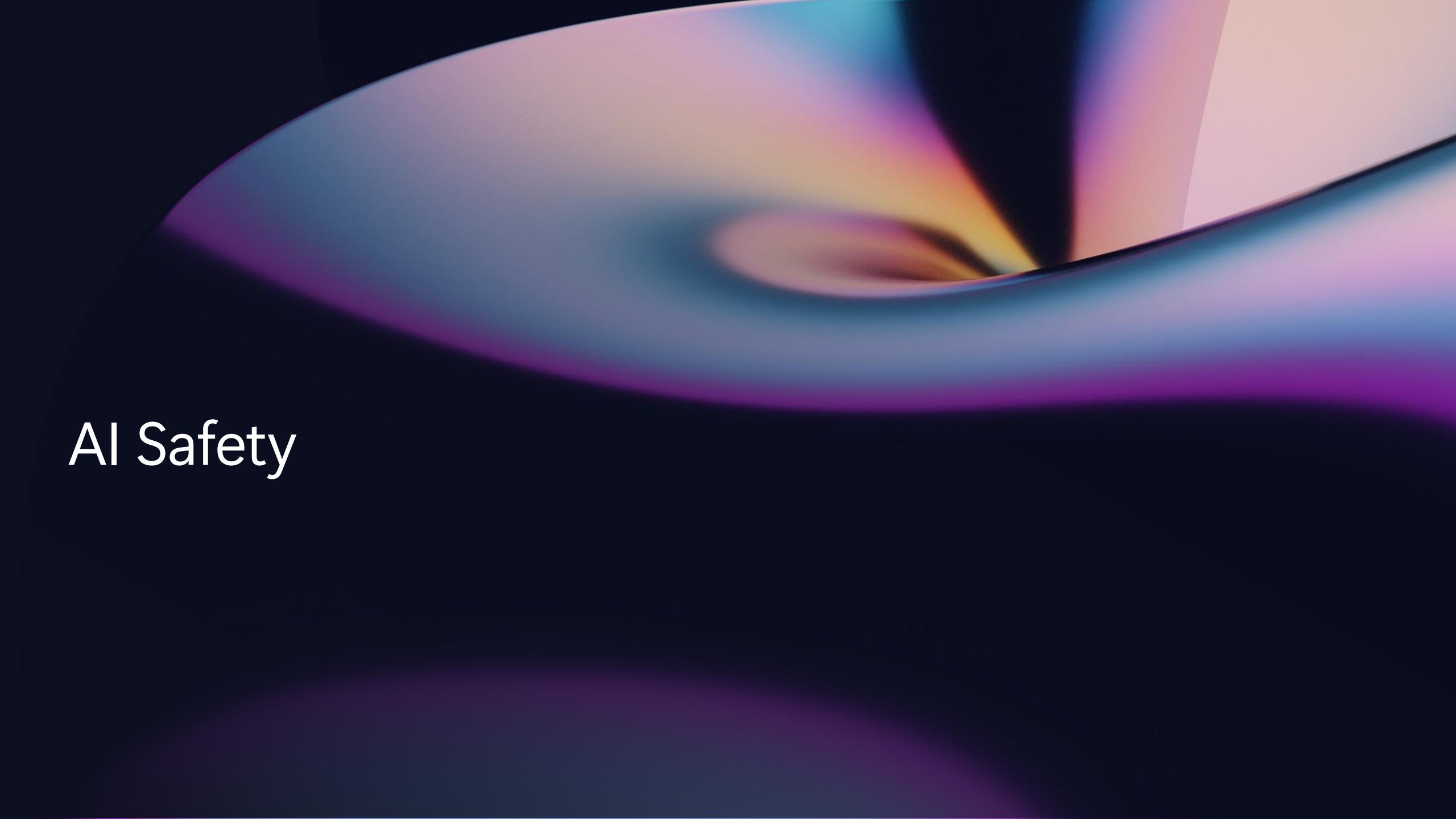
Mitigate the risk of software vulnerabilities by ensuring your organization's devices, infrastructure, and applications are kept up to date and correctly configured. Endpoint management solutions allow policies to be pushed to machines for correct configuration and ensure systems are running the latest versions.

### Utilize antimalware

Stop malware attacks from executing by installing and enabling antimalware solutions on endpoints and devices. Utilize cloud-connected antimalware services for the most current and accurate detection capabilities.

### Protect data

Know where your sensitive data is stored and who has access. Implement information protection best practices such as applying sensitivity labels and data loss prevention policies. If a breach does occur, it's critical that security teams know where the most sensitive data is stored and accessed.



AI Safety

# Microsoft's Responsible AI Principles



## Fairness

AI systems should treat all people fairly.



## Reliability and safety

AI systems should perform reliably and safely.



## Privacy and security

AI systems should be secure and respect privacy.



## Inclusiveness

AI systems should empower everyone and engage people.



## Transparency

AI systems should be understandable.



## Accountability

People should be accountable for AI systems.

# Microsoft's Responsible AI Principles



## Fairness

AI systems should treat all people fairly.



## Reliability and safety

AI systems should perform reliably and safely.



## Privacy and security

AI systems should be secure and respect privacy.



## Inclusiveness

AI systems should empower everyone and engage people.



## Transparency

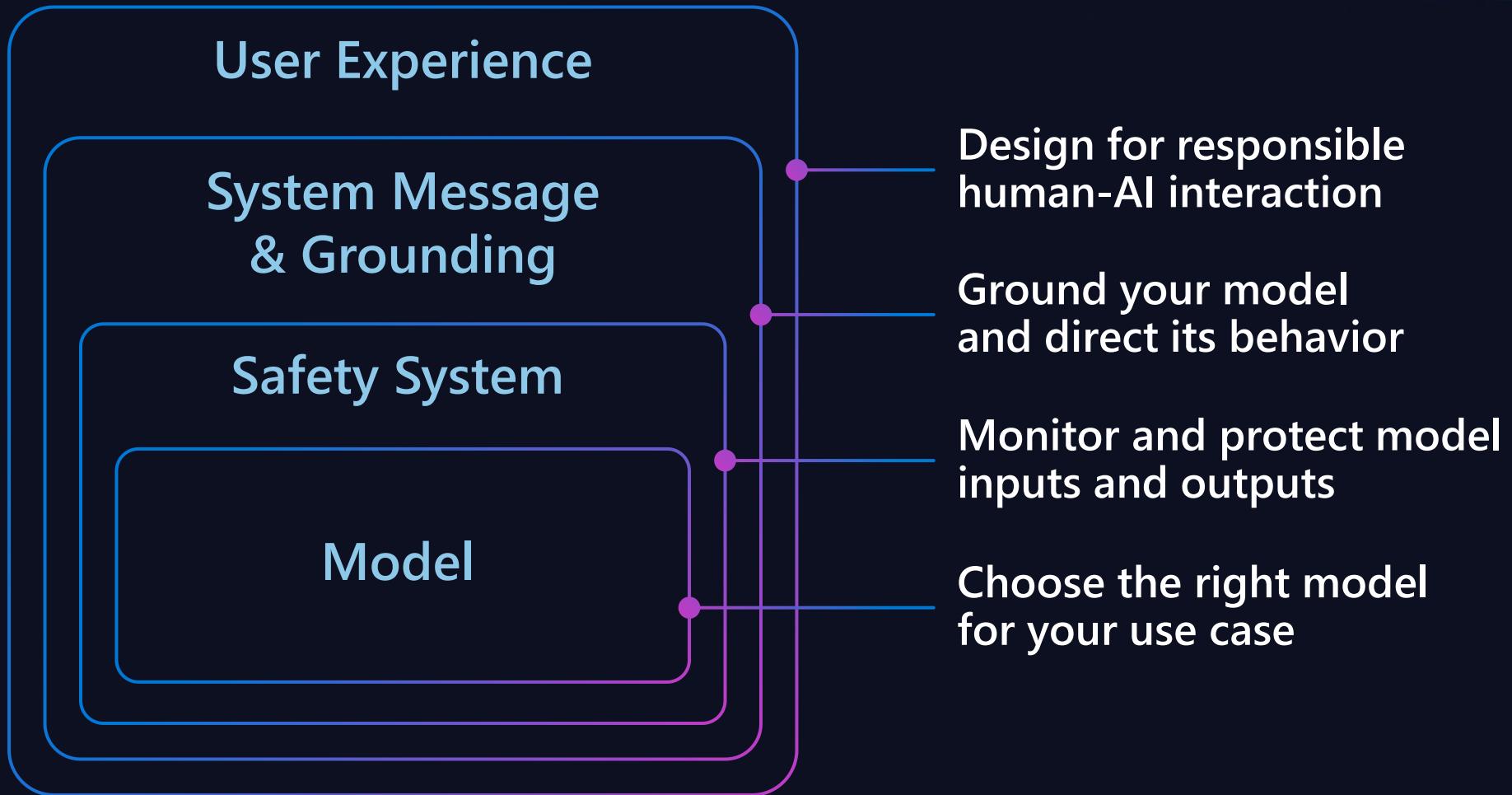
AI systems should be understandable.



## Accountability

People should be accountable for AI systems.

# Risk mitigation layers



# Content filters

Set input filter

Content will be annotated by category and blocked according to the threshold you set. For the violence, hate, sexual, and self-harm categories, adjust the slider to content of high, medium, and/or low severity.

What are these categories?

Category	Media	Action	Threshold
Violence	Text Image	Annotate and block	Medium Allow Low / Block Medium and High
Hate	Text Image	Annotate and block	Medium Allow Low / Block Medium and High
Sexual	Text Image	Annotate and block	Medium Allow Low / Block Medium and High
Self-harm	Text Image	Annotate and block	Medium Allow Low / Block Medium and High
Prompt shields for jailbreak attacks ⓘ	Text	Annotate and block	Jailbreak attacks will be blocked
Prompt shields for indirect attacks ⓘ	Text	Annotate only	Content will be annotated but not blocked



## Presenting the new Azure AI Studio (Preview)

Build, evaluate, and deploy your AI solutions from end to end.

[Explore Azure AI Studio](#)

Content Safety Studio

### Get started with Content Safety Studio

#### Run moderation tests

Explore, try out, and view sample code for different types of content.



##### Moderate text content

Run moderation tests on text contents. Assess the test results with detected severities. Experiment with different threshold levels.

[Try it out](#)

##### Moderate image content

Run moderation tests on image contents. Assess the test results with detected severities. Experiment with different threshold levels.

[Try it out](#)

##### Moderate multimodal content

Run moderation tests on image and text combined contents. Assess the test results with detected severities.

[Private preview - sign up.](#)

### Explore safety solutions for Gen-AI



Try out the latest capability for AI.



##### Groundedness detection

Region not supported

Groundedness detection detects ungroundedness generated by the large language models (LLMs).



##### Prompt Shields

Prompt Shields provides a unified API that addresses the following types of attacks: Jailbreak attacks and Indirect attacks.



##### Protected material detection

Use protected material detection to detect and protect third-party text material in LLM output.



##### Safety metaprompt

Use the framework of metaprompt that helps you potentially mitigate different types of harm.

# Content safety filters

Category	Media	Action	Threshold
Violence	<input type="checkbox"/> Text <input type="checkbox"/> Image	Annotate and block <span>▼</span>	<p>Low</p>  <p>Block Low, Medium and High</p>
Hate	<input type="checkbox"/> Text <input type="checkbox"/> Image	Annotate and block <span>▼</span>	<p>Medium</p>  <p>Allow Low / Block Medium and High</p>
Sexual	<input type="checkbox"/> Text <input type="checkbox"/> Image	Annotate and block <span>▼</span>	<p>Medium</p>  <p>Allow Low / Block Medium and High</p>
Self-harm	<input type="checkbox"/> Text <input type="checkbox"/> Image	Annotate and block <span>▼</span>	<p>High</p>  <p>Allow Low and Medium / Block High</p>

# Content safety in APIs

HTTP GET:

```
https://myservice.openai.azure.com/openai/deployments/chatgpt/chat/completions?api-version=2024-02-15-preview
```



```
{"error": {  
    "message": "The response was filtered due to the prompt triggering Azure OpenAI's content management policy.",  
    "code": "content_filter",  
    "status": 400,  
    "innererror": {  
        "code": "ResponsibleAIPolicyViolation",  
        "content_filter_result": {  
            "hate": {  
                "filtered": false,  
                "severity": "safe"  
            },  
            "self_harm": {  
                "filtered": false,  
                "severity": "safe"  
            },  
            "sexual": {  
                "filtered": false,  
                "severity": "safe"  
            },  
            "violence": {  
                "filtered": true,  
                "severity": "medium"  
            }  
        }  
    }  
}
```

Headers:

```
Content-Type: application/json  
Authorization: Bearer 123abc
```

Body:

```
{"messages": [{  
    "role":  
    "system",  
    "content":  
    "How do I make explosive fireworks?"  
}]  
}
```

# HiddenLayer

## Model scanning for Azure AI Foundry Model catalog

Azure AI Foundry / Model catalog / Llama-3.3-70B-Instruct

← Llama-3.3-70B-Instruct

▷ Deploy

Details   Benchmarks   Code samples   License

The Meta Llama 3.3 multilingual large language model (LLM) is a pretrained and instruction tuned generative model in 70B (text in/text out). The Llama 3.3 instruction tuned text only model is optimized for multilingual dialogue use cases and outperform many of the available open-source closed chat models on common industry benchmarks.

**Built with Llama**

**Model Architecture:** Llama 3.3 is an auto-regressive language model that uses an optimized transformer architecture. The tuned version was trained using supervised fine-tuning (SFT) and reinforcement learning with human feedback (RLHF) to align with human preferences for helpfulness and safety.

Training Data	Params	Input modalities	Output modalities	Context length	GQA	Token count	Koala	
Llama 3.3 (text only)	A new mix of publicly available online data.	70B	Multilingual Text	Multilingual Text and code	128k	Yes	15T+*	2.2B

\*Token counts refer to pretraining data only. All model versions use Grouped-Query Attention (GQA) for improved inference scalability.

 HIDDEN<sup>LAYER</sup>

Verified by HiddenLayer Model Scanner

HiddenLayer Model Scanner did not detect any vulnerabilities, embedded code or integrity issues with the model artifacts.

[Read More](#)

## Find the right model to build your custom AI solution

[? Help](#)

What's new?

[Collections](#)[Industry](#)[Deployment options](#)[Inference tasks](#)[Fine-tuning tasks](#)[Licenses](#)[Compare models](#)

Search

Models 1820



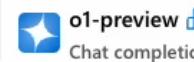
Chat completion



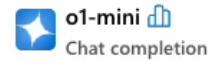
Chat completion



Chat completion



Chat completion



Chat completion



Audio generation



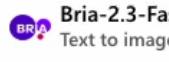
Chat completion



Chat completion



Chat completion



Text to image



Chat completion



Embeddings



Embeddings



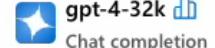
Chat completion



Chat completion



Chat completion



Chat completion



Chat completion



Chat completion



Chat completion



Chat completion



Chat completion



Chat completion



Chat completion

# Keyless auth to Azure AI with Microsoft Entra

Get the slides:

[aka.ms/aitour/sec/mx](https://aka.ms/aitour/sec/mx)



# Goal: Move from keys to tokens

API keys can be easily leaked

API keys can be passed around  
a company (unintentionally)

API keys can be painful to rotate

Tokens are short-lived

No key vault necessary!

Role-based access can provide fine-grained  
access to services

```
https://myopenai.openai.azure.com/openai/deployments/mychat/chat/completions?api-version=2024-02-15-preview
```

Content-Type: application/json

api-key: YOUR\_API\_KEY



```
https://myopenai.openai.azure.com/openai/deployments/mychat/chat/completions?api-version=2024-02-15-preview
```

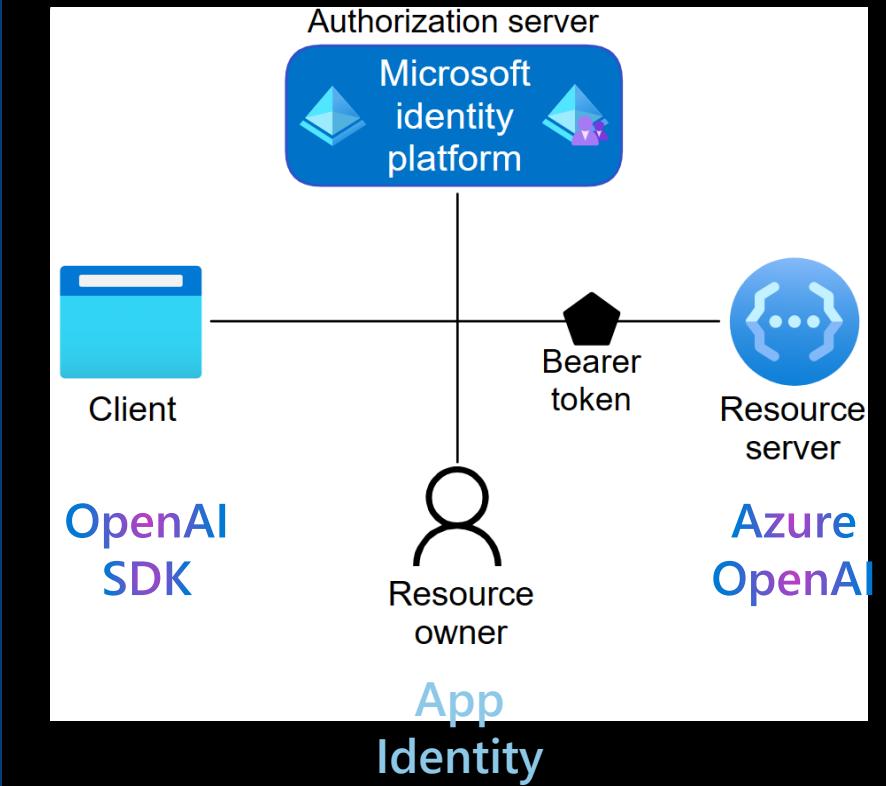
Content-Type: application/json

Authorization: Bearer YOUR\_API\_TOKEN

# Use Microsoft Entra for keyless auth to Azure services

1. Create the Azure OpenAI service
2. Create the Azure Container App
3. Create an identity for the App to use
4. Give your App identity permissions to use the OpenAI service
5. Use an Azure Identity SDK to generate tokens for the OpenAI SDK

Example project:  
[aka.ms/keyless-azure-containerapps](https://aka.ms/keyless-azure-containerapps)



# Accessing Azure services with managed identity

Option 1



Azure  
Container App



System  
identity



Azure  
OpenAI

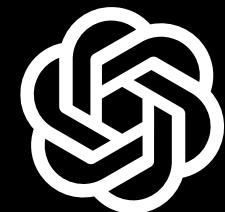
Option 2



Azure  
Container App



User-assigned  
identity



Azure  
OpenAI

# Configuring role-based access to Azure OpenAI

Give role-based access control  
to users or applications

Use managed identities for  
deployed apps

Use built-in roles with  
desired permissions

```
// Cognitive Services OpenAI User
roleDefinitionId = '5e0bd9bd-7b93-4f28-af87-19fc36ad61bd'

resource role 'Microsoft.Authorization/roleAssignments' = {
    name: guid(subscription().id, resourceGroup().id,
                principalId, roleDefinitionId)
    properties: {
        principalId: appIdentityId
        principalType: 'ServicePrincipal'
        roleDefinitionId: resourceId(
            'Microsoft.Authorization/roleDefinitions',
            roleDefinitionId)
    }
}
```

Bicep

# Connecting to Azure OpenAI with app credential

Use the Azure Identity SDK to get a credential

Pass a credential or token provider to the OpenAI SDK

Token refresh is taken care of for you!

.NET

```
OpenAIclient client = new(  
    new Uri(GetEnvironmentVariable("OPENAI_ENDPOINT")),  
    new ManagedIdentityCredential());
```

Python

```
azure_credential = ManagedIdentityCredential()  
token_provider = get_bearer_token_provider(  
    azure_credential,  
    "https://cognitiveservices.azure.com/.default")  
  
client = AzureOpenAI(  
    azure_endpoint=os.getenv("OPENAI_ENDPOINT"),  
    azure_ad_token_provider=token_provider  
)
```

# Adding user authentication

Get the slides:

[aka.ms/aitour/sec/mx](https://aka.ms/aitour/sec/mx)



# Goal: Require authentication for an AI app

**Code:** [aka.ms/ragchat/acl](https://aka.ms/ragchat/acl)

**Code:** [aka.ms/azai/auth-builtin](https://aka.ms/azai/auth-builtin)

**Demo:** [aka.ms/azai/auth-builtin/demo](https://aka.ms/azai/auth-builtin/demo)

# Auth: Authorization and Authentication

Ensures the right user gets access to the right resource

## Authorization



**Validates users have permission to complete the attempted action**

OAuth2

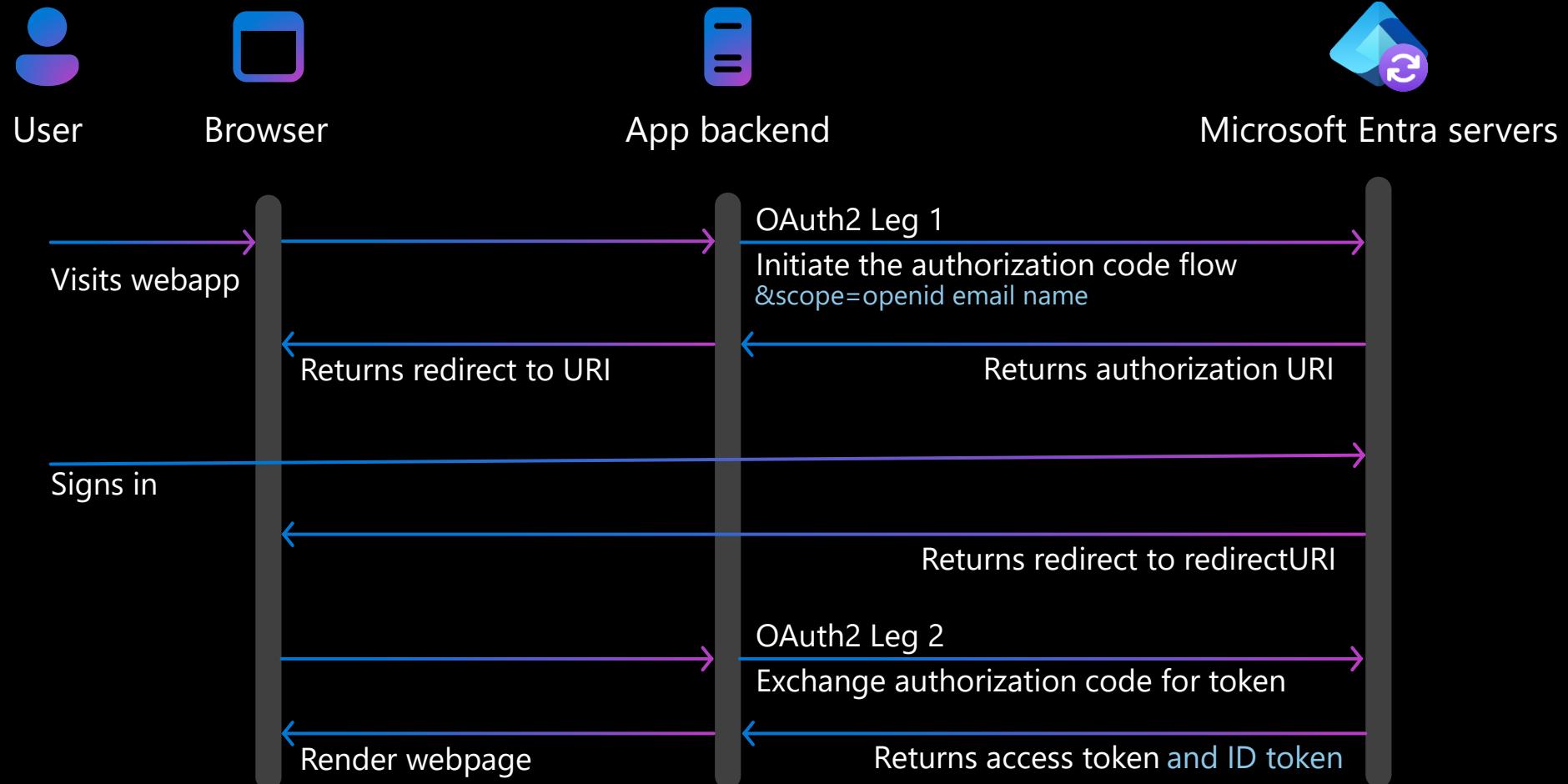
## Authentication



**Confirms users are who they say they are**

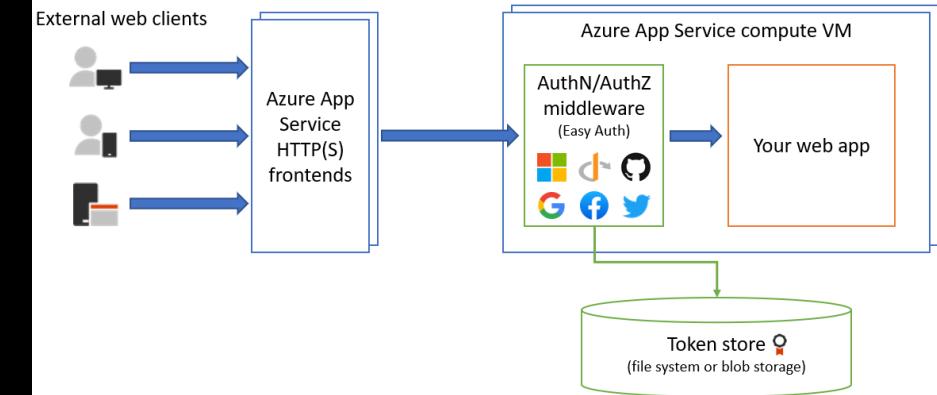
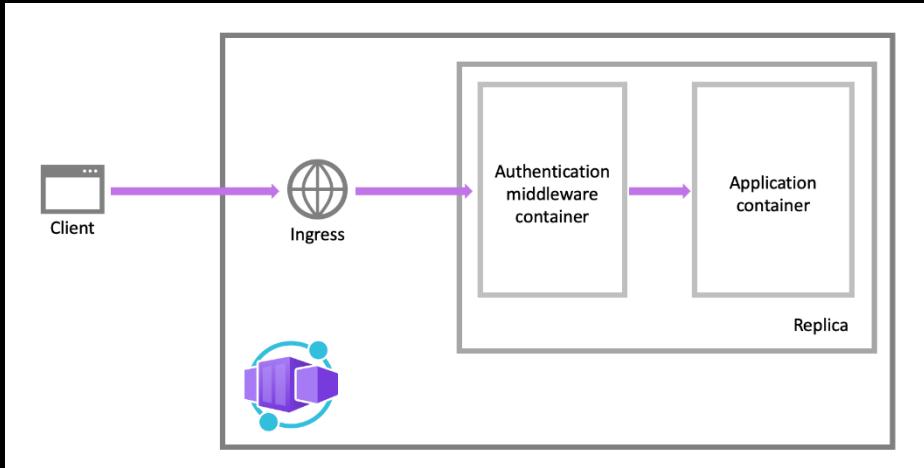
OIDC

# OAuth2 authentication flow with OIDC



# Implementing the authentication flow

## Option 1: Built-in auth on Azure App Service or Container Apps



## Option 2: MSAL for auth on any host (including local)

Use MSAL packages to orchestrate OIDC flow using app registration

📺 Video: User Auth with MSAL [aka.ms/msal-sdk-stream](https://aka.ms/msal-sdk-stream)

# Registering with the Microsoft identity platform

To request tokens from the Microsoft identity platform, you need to register a **Microsoft Entra application** and create a **service principal** for it.



Microsoft Entra  
Application Object



Microsoft Graph  
Service Principal



Microsoft  
identity platform

# Creating an Entra application

Entra applications can be created with the **Portal**, **Graph SDKs**, **Powershell**, **Azure CLI**, or **Bicep**.

The screenshot shows the Azure portal interface for managing an application. The left sidebar has a navigation menu with items like Overview, Quickstart, Integration assistant, Diagnose and solve problems, Manage (with sub-options like Branding & properties, Authentication, Certificates & secrets, Token configuration, API permissions, and Expose an API), and a search bar. The 'Authentication' option under 'Manage' is currently selected and highlighted with a grey background. The main content area is titled 'Azure Search OpenAI Chat Client App 95828 | Authentication'. It contains sections for 'Implicit grant and hybrid flows' (describing token issuance for SPAs) and 'Supported account types' (with two radio button options: 'Accounts in this organizational directory only (Contoso only - Single tenant)' which is selected, and 'Accounts in any organizational directory (Any Microsoft Entra ID tenant - Multitenant)'). There are also sections for 'Access tokens (used for implicit flows)' and 'ID tokens (used for implicit and hybrid flows)', with the 'ID tokens' checkbox being checked.

Home > Azure Search OpenAI Chat Client App 95828

## Azure Search OpenAI Chat Client App 95828 | Authentication

Search Got feedback? ⚡ ...

- Overview
- Quickstart
- Integration assistant
- Diagnose and solve problems
- Manage
  - Branding & properties
  - Authentication**
  - Certificates & secrets
  - Token configuration
  - API permissions
  - Expose an API

Implicit grant and hybrid flows

Request a token directly from the authorization endpoint. If the application has a single-page architecture (SPA) and doesn't use the authorization code flow, or if it invokes a web API via JavaScript, select both access tokens and ID tokens. For ASP.NET Core web apps and other web apps that use hybrid authentication, select only ID tokens. [Learn more about tokens](#).

Select the tokens you would like to be issued by the authorization endpoint:

Access tokens (used for implicit flows)

ID tokens (used for implicit and hybrid flows)

Supported account types

Who can use this application or access this API?

Accounts in this organizational directory only (Contoso only - Single tenant)

Accounts in any organizational directory (Any Microsoft Entra ID tenant - Multitenant)

# Configuring built-in authentication

Built-in authentication can be configured with the **Portal** or **Bicep**.

The screenshot shows the 'Authentication' section of the Azure App Service configuration interface for a web application named 'authapp-iiflhjqlwy5-web'. The left sidebar lists various settings like Deployment slots, Performance, and Identity provider. The 'Authentication' option is selected and highlighted.

**Authentication settings** [Edit](#)

Requiring authentication ensures that requests to your app include information about the caller, but your app may still need to make additional authorization decisions to control access. If unauthenticated requests are allowed, any client can call the app and your code will need to handle both authentication and authorization. [Learn more](#)

App Service authentication	Enabled
Restrict access	Require authentication
Unauthenticated requests	Return HTTP 302 Found (Redirect to identity provider)
Redirect to	Microsoft
Token store	Enabled

**Identity provider**

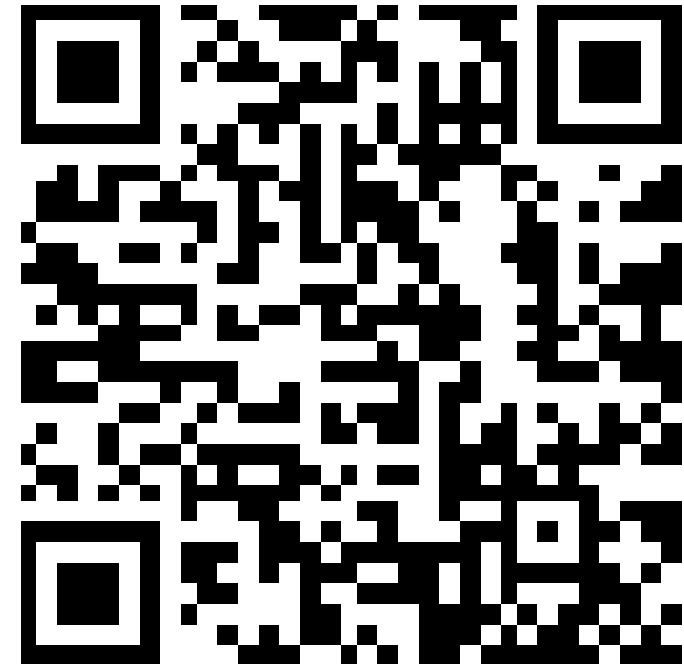
+ Add provider

Identity provider	App (client) ID	Learn more
Microsoft ( <a href="#">Simple Flask Server Client App</a> )	2495d1ef-5190-4f51-9102-10989b7ff78e	<a href="#">Quickstart</a>

# Network security for AI apps

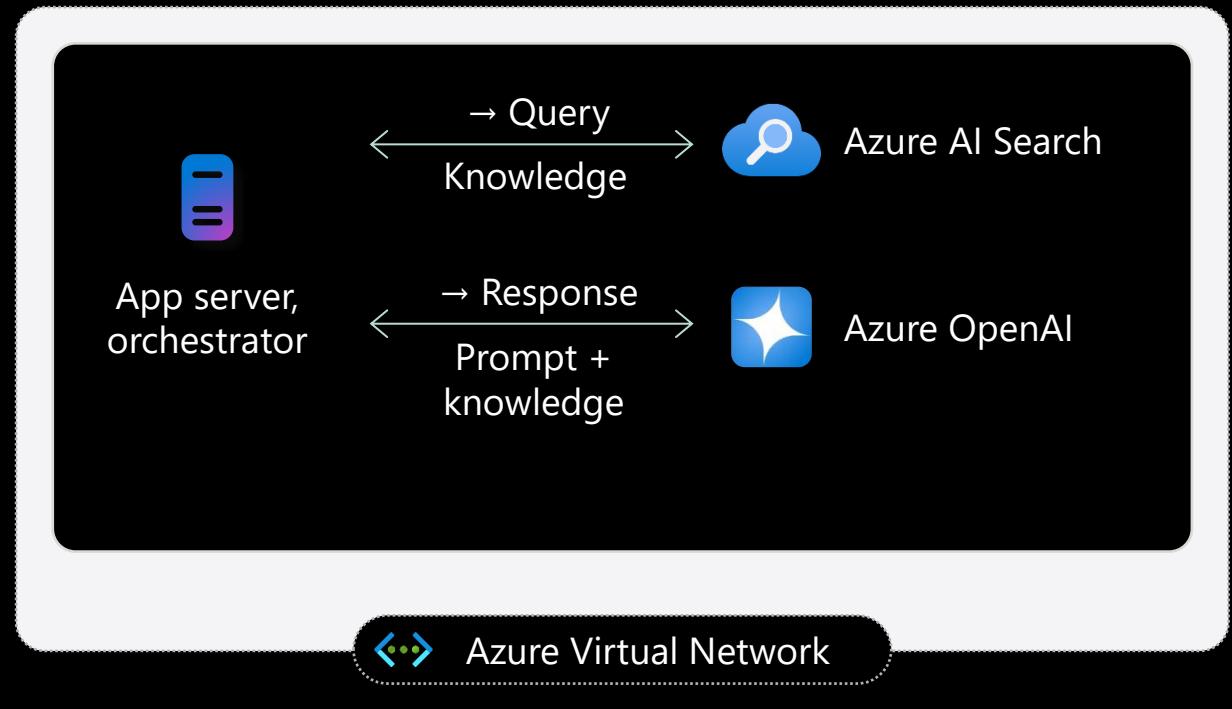
Get the slides:

[aka.ms/aitour/sec/mx](https://aka.ms/aitour/sec/mx)

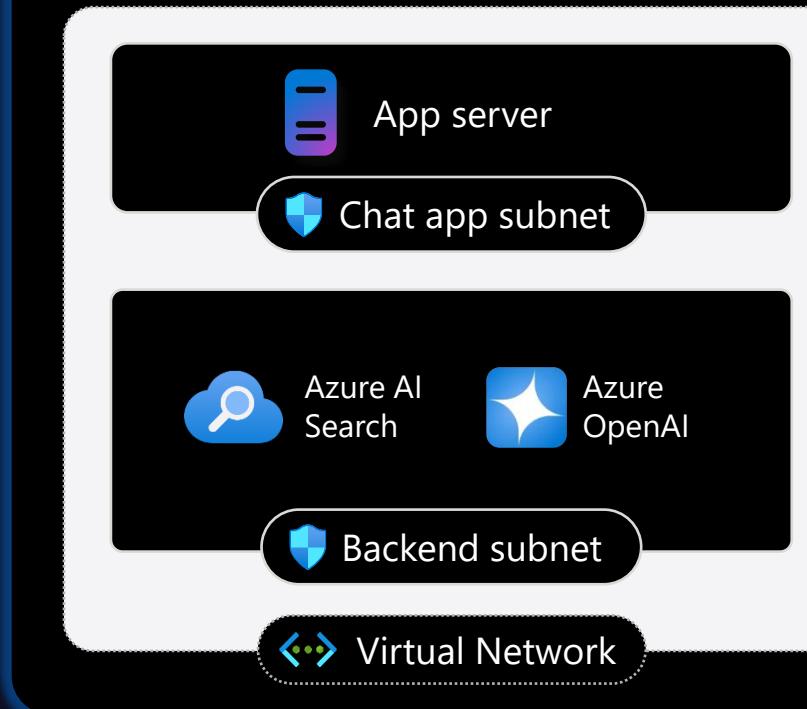


# Securely networked architecture (internal facing app)

Move all resources into a virtual network:



Use subnets for further isolation:



Deploy a RAG chat inside a VNet [aka.ms/ragchat/private](https://aka.ms/ragchat/private)

# VNet configuration in Bicep

Creates a subnet for:

1. App Service app
2. Backend services

Different rules can be applied to each subnet.

See full Bicep in:

[aka.ms/ragchat](https://aka.ms/ragchat)

infra/network-isolation.bicep

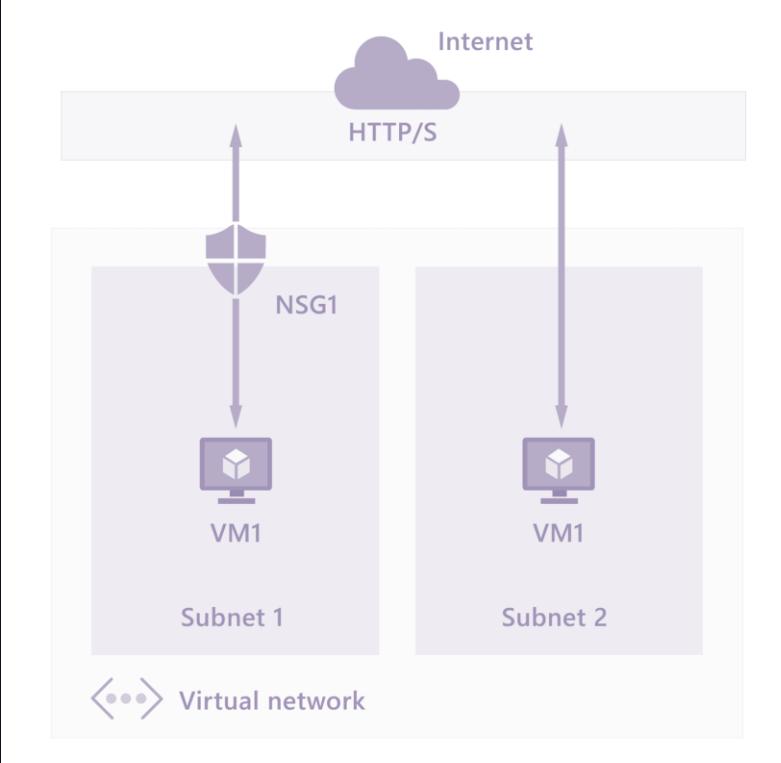
```
module vnet './core/networking/vnet.bicep' = {
  name: 'vnet'
  params: {
    subnets: [
      {
        name: 'appservice-subnet'
        properties: {
          addressPrefix: '10.0.3.0/24'
          privateEndpointNetworkPolicies: 'Enabled'
          privateLinkServiceNetworkPolicies: 'Enabled'
          delegations: [
            {
              id: appServicePlan.id
              name: appServicePlan.name
              properties: {
                serviceName: 'Microsoft.Web/serverFarms'
              }
            }
          ]
        }
      }
      {
        name: 'backend-subnet'
        properties: {
          addressPrefix: '10.0.1.0/24'
          privateEndpointNetworkPolicies: 'Enabled'
          privateLinkServiceNetworkPolicies: 'Enabled'
        }
      }
    ...
  }
}
```

# Azure Network Security Groups (NSG)

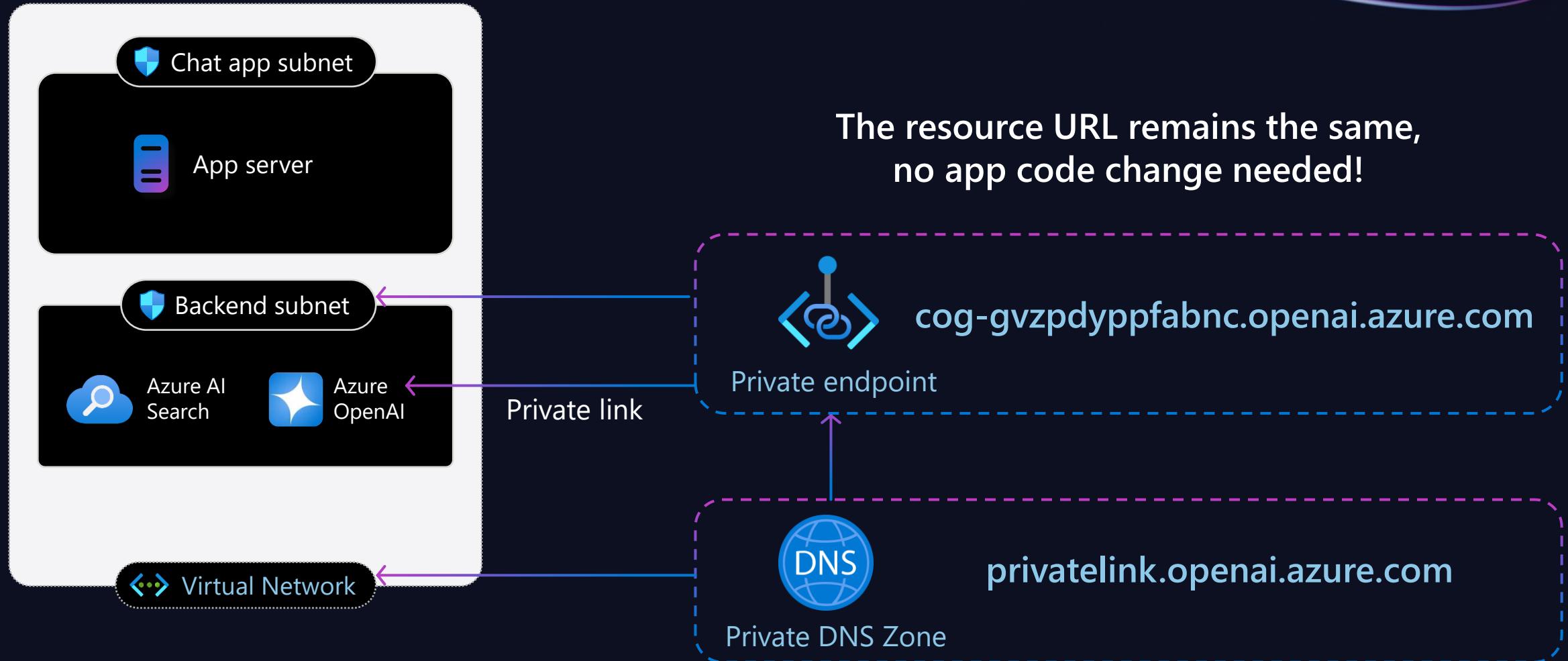
Azure network security groups can automatically allow or deny traffic

Contains security rules

NSG security rules are evaluated by priority using five information points



# Private endpoints and DNS zones



# Private endpoints in Bicep

Create private DNS zones  
and endpoints for:

- Azure Blob Storage
- Azure OpenAI
- Azure AI Search
- Azure App Service

The endpoint for the service remains  
the same! *No changes to backend  
code are needed.*

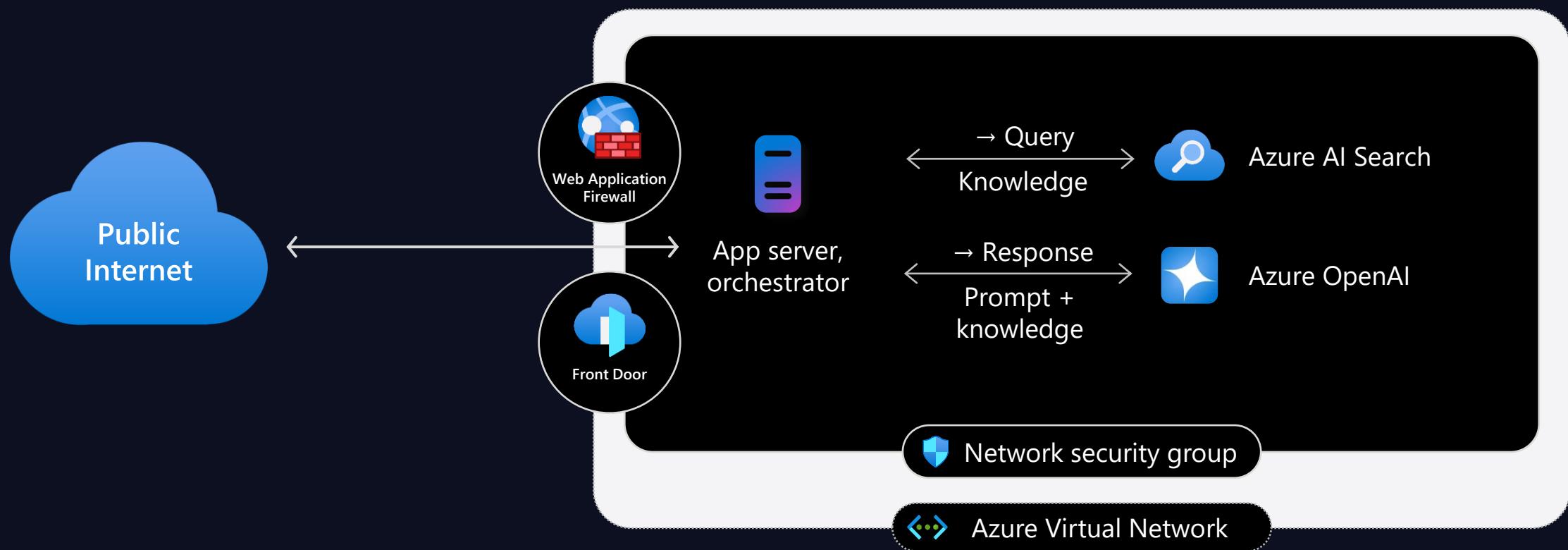
See full Bicep in: [aka.ms/ragchat](https://aka.ms/ragchat)  
`infra/network-isolation.bicep`

```
module dnsZones 'private-dns-zone.bicep' =
[for privateEndpointConnection in privateEndpointConnections:
{
  name: '${privateEndpointConnection.groupId}-dnszone'
  params: {
    dnsZoneName: privateEndpointConnection.dnsZoneName
    tags: tags
    virtualNetworkName: vnetName
  }]
}

module privateEndpoints 'private-endpoint.bicep' =
[for privateEndpointInfo in flatten(privateEndpointInfo):
{
  name: '${privateEndpointInfo.name}-privateendpoint'
  params: {
    location: location
    name: '${privateEndpointInfo.name}${resourceToken}-pe'
    tags: tags
    subnetId: vnetPeSubnetName
    serviceId: privateEndpointInfo.resourceId
    groupIds: [ privateEndpointInfo.groupId ]
    dnsZoneId:
      dnsZones[privateEndpointInfo.dnsIdx].outputs.id
  }
  dependsOn: [ dnsZones ]
}]
```

# Securely networked architecture (public app)

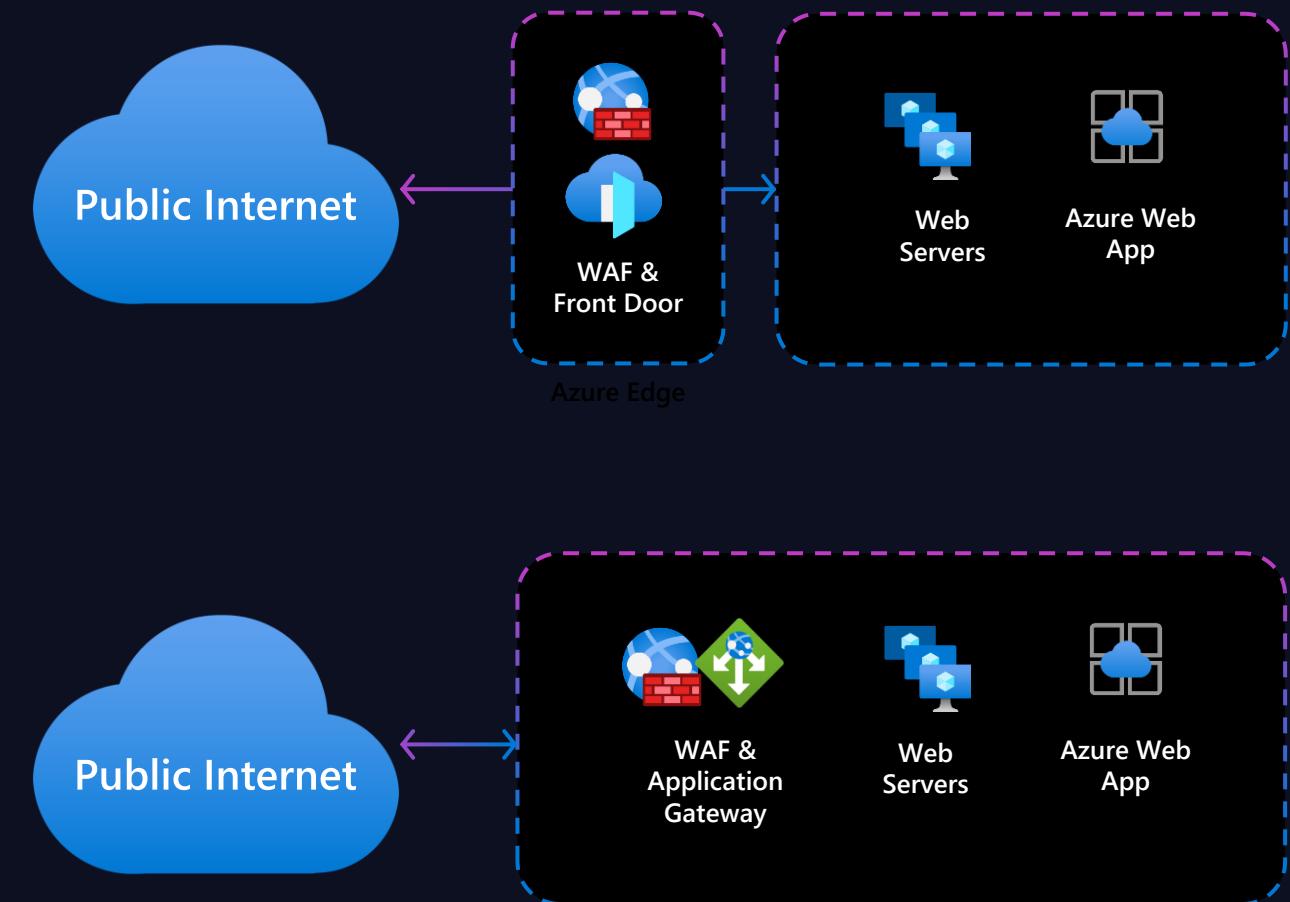
Protect public-facing applications with  
Azure Web Application Firewall plus Front Door:



\*Front Door can be replaced with Application Gateway for a regionally distributed app

# Azure Web Application Firewall (WAF): Front Door or Application Gateway?

- 1 Scalable, highly available, Low latency service provided at network edge
- 2 Easy setup with managed ruleset (OWASP TOP 10) and custom rules
- 3 Bot protection using threat intelligence-based filtering (preview)
- 4 Global insights
- 5 Built-in DDoS protection
- 6 Azure Front Door provides built-in CDN capabilities
- 7 Cost efficient: Pay as you go



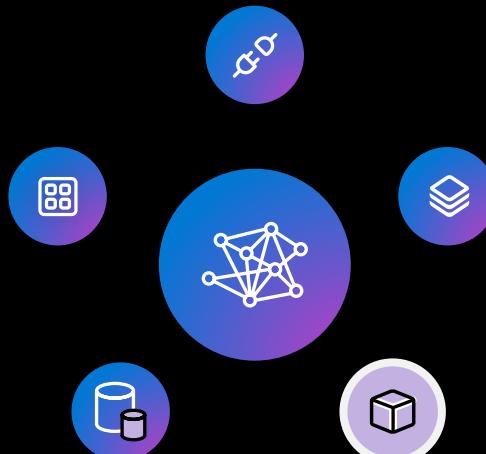


Continuous security for AI

# Protect AI apps from code to runtime

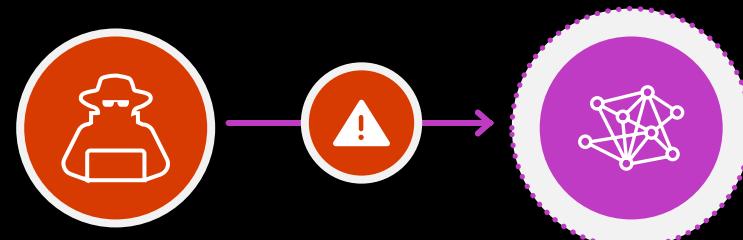
Start secure

AI security posture management (AI-SPM)



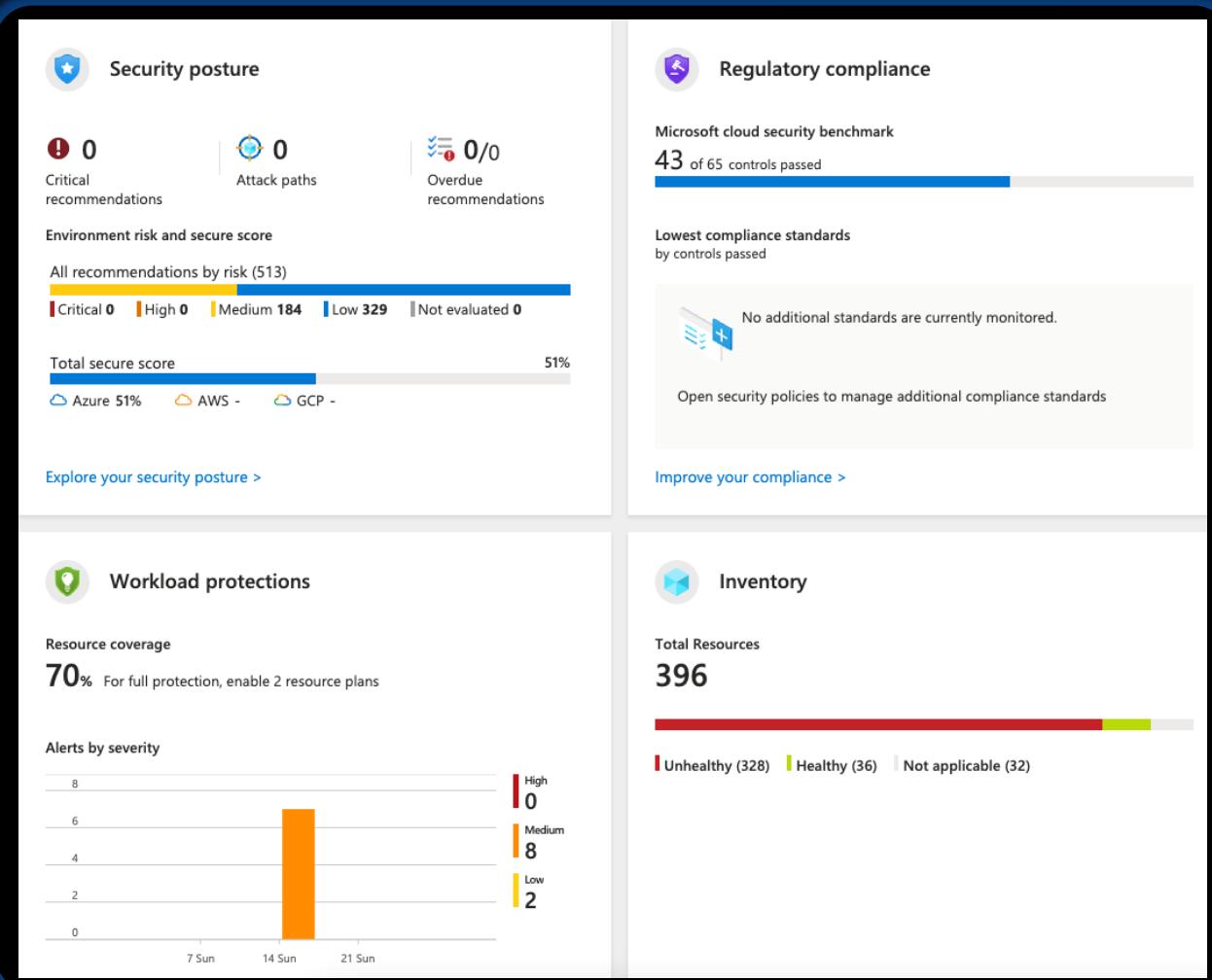
Stay secure

Threat protection for AI workloads



Microsoft Defender for Cloud

# Defender for Cloud



## Security alerts:

Detects DDOS, suspicious logins, etc.

## Security posture:

Audits Azure resources and their settings

## Workload protections:

Scans for known vulnerabilities in SQL, container images, etc.

## Data security:

Scans stored data for PII and sensitive data

## Regulatory compliance:

Ensure compliance with benchmarks.

[aka.ms/enable-defender](http://aka.ms/enable-defender)

# DfC recommendations: RAG without VNet

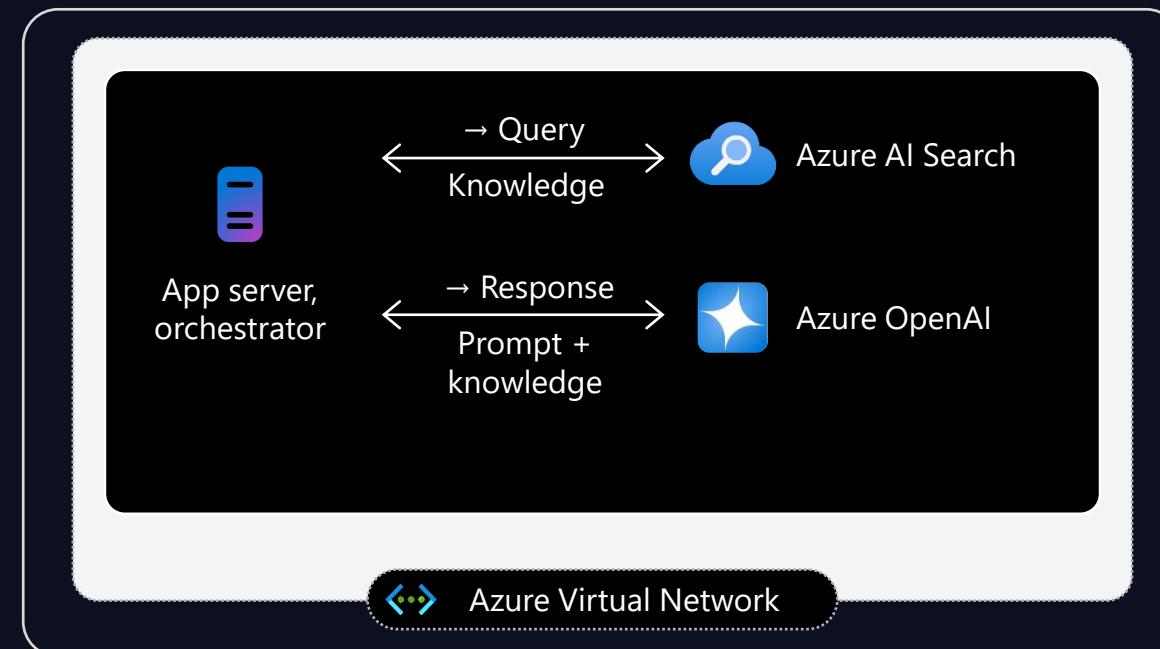
10 recommendations for azure-search-openai-demo, non-private deployment:

Title	Affected resource	Risk level ⓘ
✖ Storage accounts should restrict network access using virtual network rules	stj25rgqsibtmlo	Low
✖ Storage account should use a private link connection	stj25rgqsibtmlo	Low
✖ Diagnostic logs in App Service should be enabled	app-backend-j25rgqsibtmlo	Low
✖ Azure AI Services resources should use Azure Private Link	cog-j25rgqsibtmlo-b2	Low
✖ Azure AI Services resources should use Azure Private Link	cog-j25rgqsibtmlo	Low
✖ Azure AI Services resources should use Azure Private Link	cog-fr-j25rgqsibtmlo	Low
✖ Azure AI Services resources should restrict network access	cog-fr-j25rgqsibtmlo	Low
✖ Azure AI Services resources should restrict network access	cog-j25rgqsibtmlo-b2	Low
✖ Azure AI Services resources should restrict network access	gptkb-j25rgqsibtmlo	Low
✖ Azure AI Services resources should restrict network access	cog-j25rgqsibtmlo	Low

# DfC recommendations: RAG with VNet

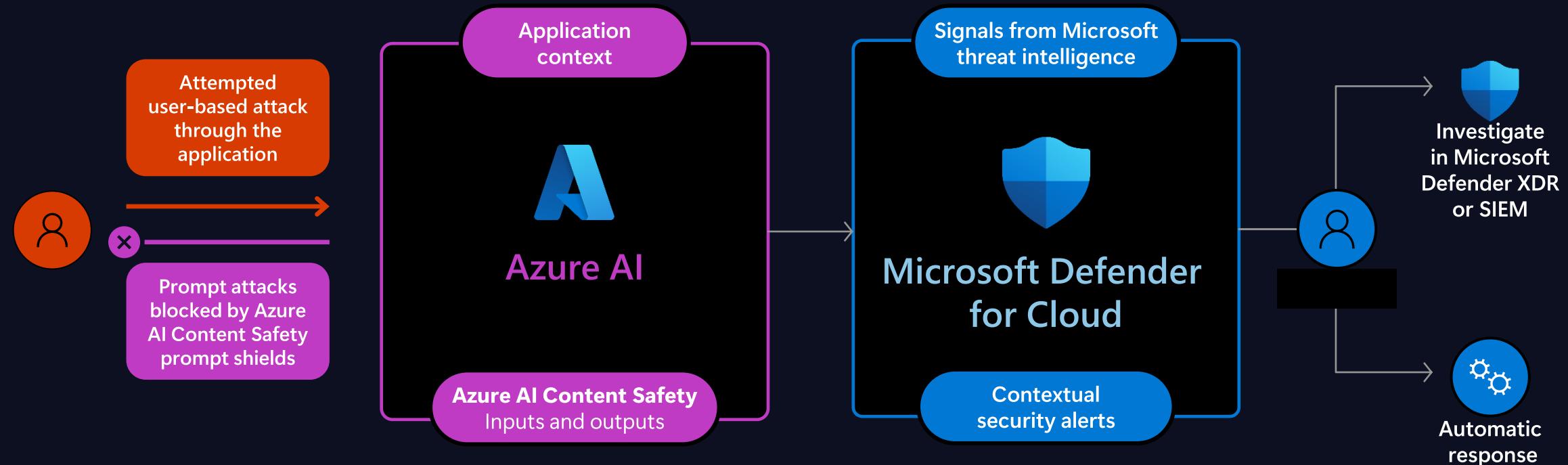
2 recommendations for azure-search-openai-demo, private deployment:

Title	Affected resource	Risk level ⓘ
💡 Virtual networks should be protected by Azure Firewall	◀▶ vnet-xm5ap2cgji52q	Low
💡 Diagnostic logs in App Service should be enabled	🌐 app-backend-xm5ap2cgji52q	Low



# Threat protection for AI workloads

Microsoft Defender for Cloud + Azure AI Content Safety



[learn.microsoft.com/azure/defender-for-cloud/ai-onboarding](https://learn.microsoft.com/azure/defender-for-cloud/ai-onboarding)

Key: Security teams Developers

# GitHub actions for security recommendations

Use **ps-rule** action on your Bicep to auto-scan for security issues

[github.com/microsoft/ps-rule](https://github.com/microsoft/ps-rule)

Blog post:

Securing Azure deployments  
with PSRule  
[aka.ms/blog-psrule](https://aka.ms/blog-psrule)

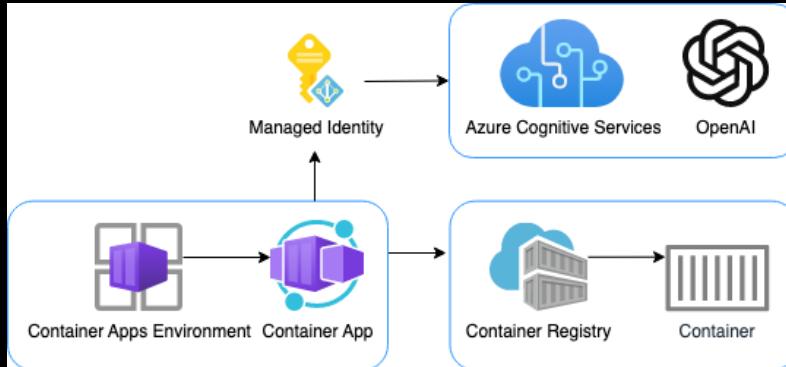
```
- name: Run PSRule analysis
uses: microsoft/ps-rule@v2.9.0
with:
  modules: PSRule.Rules.Azure
  baseline: Azure.Pillar.Security
  inputPath: infra/*.test.bicep
  outputFormat: Sarif
  outputPath: reports/ps-rule-results.sarif
  summary: true
  continue-on-error: true
  env:
    PSRULE_CONFIGURATION_AZURE_BICEP_FILE_EXPANSION:
      'true'
    PSRULE_CONFIGURATION_AZURE_BICEP_FILE_EXPANSION_TIMEOUT
      : '30'
- name: Upload results to security tab
uses: github/codeql-action/upload-sarif@v3
with:
  sarif_file: reports/ps-rule-results.sarif
```

# GitHub actions for security recommendations: Results

<input type="checkbox"/>  <b>Use secure parameters for any parameter that contains sensitive information.</b>	 Error	main
#54 opened last month • Detected by PSRule in infra/main.test.bicep:0		
<input type="checkbox"/>  <b>Virtual network (VNET) subnets should have Network Security Groups (NSGs) assigned.</b>	 Error	1 main
#53 opened last month • Detected by PSRule in infra/main.test.bicep:14641		
<input type="checkbox"/>  <b>Use secure parameters for any parameter that contains sensitive information.</b>	 Error	main
#52 opened last month • Detected by PSRule in infra/main.test.bicep:0		
<input type="checkbox"/>  <b>Use secure parameters for any parameter that contains sensitive information.</b>	 Error	main
#46 opened last month • Detected by PSRule in infra/main.test.bicep:0		

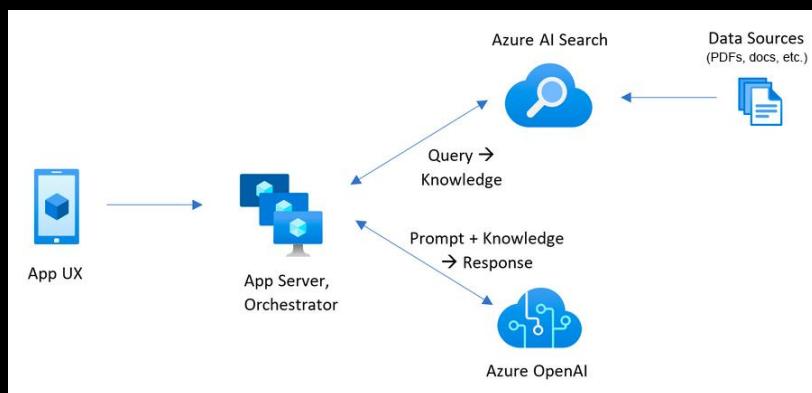
[github.com/Azure-Samples/azure-search-openai-demo/actions/runs/9378324878](https://github.com/Azure-Samples/azure-search-openai-demo/actions/runs/9378324878)

# Get started with our samples



[aka.ms/azai/chat](https://aka.ms/azai/chat)

Azure OpenAI + Container Apps + Keyless



[aka.ms/ragchat](https://aka.ms/ragchat)

Azure OpenAI + AI Search  
+ Entra + MSAL + App Service Built-in Auth  
+ VNet + Private Endpoints

[aka.ms/azai/auth-builtin](https://aka.ms/azai/auth-builtin)

Azure OpenAI + Container Apps + Built-in Auth  
+ Entra

# Learn more about securing your AI application

Microsoft Entra developer center - [aka.ms/dev/ms-entra](https://aka.ms/dev/ms-entra)

Get started with Defender for Cloud - [aka.ms/enable-defender](https://aka.ms/enable-defender)

Python Risk Identification Tool for generative AI – [aka.ms/pyrit](https://aka.ms/pyrit)

Azure Well Architected Framework – [aka.ms/wellarchitectedframework](https://aka.ms/wellarchitectedframework)

Azure AI Content Safety – [aka.ms/aicontentsafety](https://aka.ms/aicontentsafety)

# Workshop: Build your first Agent with Azure AI Agent Service





General availability

# Azure AI Agent Service



Public Preview

# Azure AI Agent Service

**Securely build, deploy, and scale AI agents with ease**

Rapid development  
and automation

Extensive data  
connections

Flexible model  
selection

Enterprise-grade  
security

[ai.azure.com](https://ai.azure.com)

# Using the AI Agent Service



## Agent

Large Language model with defined instructions and tools



## Tool

Services and functions that extend the agent's ability



## Threads

Manages and truncate messages during an agent-user conversation to fit the model's context.



## Run

Activation of an agent to perform tasks based on Thread contents and configured Tools

# AI Agent Service in Action

- Step 1: Create an Agent
- Step 2: Create a Thread
- Step 3: Run the Agent
- Step 5: Check the Run status
- Step 6: Display the Agent's Response

**Agent:**  
Contoso Sales Agent

**Instructions:**  
You are an advanced sales analysis agent for Contoso, specializing in assisting users with sales data inquiries

**Model** 

**Your data (optional):**  
 Azure AI Search  
 Files (local or Azure Blob)

**Tools (optional):**  
File Search  
Code Interpreter  
Function Calling  
Bing Search  
Microsoft SharePoint  
Microsoft Fabric  
Azure Logic Apps  
Azure Functions  
OpenAPI 3.0 specified tools

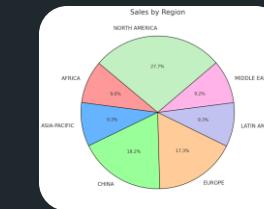
**Thread:**  
Sales analysis

**User's message**  
Tell me the total sales by region

**Agent's message**  
Here is the sales:  
Europe: \$15478.00  
America: \$78792.00

**User's message**  
Show as a pie chart

**Agent's message**



**Run 1**

- 1 Function Calling Tool  
Query SQLite DB
- 2 Create message

**Run 2**

- 1 Code Interpreter Tool  
Create a pie chart
- 2 Create message

# Wrap up



Thank you for attending this session

Template:

[github.com/Azure-Samples/agent-openai-python-prompty](https://github.com/Azure-Samples/agent-openai-python-prompty)

Prompty:

[prompty.ai](https://prompty.ai)

AI Studio:

[Azure AI Studio](https://azure.ai/studio)

# Copilot hub & community



**Copilot hub on [adoption.microsoft.com/copilot](https://adoption.microsoft.com/copilot)**  
Enablement and usage guidance for Microsoft Copilot



Ask questions and get answers in our community [aka.ms/M365CopilotCommunity](https://aka.ms/M365CopilotCommunity)

**Copilot for Microsoft 365**

Microsoft Copilot for Microsoft 365 combines the power of large language models (LLMs) with your organization's data – all in the flow of work – to turn your words into one of the most powerful productivity tools on the planet.

It works alongside popular Microsoft 365 apps such as Word, Excel, PowerPoint, Outlook, Teams, and more. Copilot for Microsoft 365 provides real-time intelligent assistance, enabling users to enhance their creativity, productivity, and skills.

**Explore the Copilot Success Kit**  
Use our Copilot Success Kit to accelerate your AI journey.  
[View the kit >](#)

**Learn how Copilot works**  
Get an inside look at how large language models (LLMs) work when you use them with your data in Microsoft 365.  
[Learn now >](#)

**Join the Copilot community**  
The Microsoft 365 Copilot community is your hub for the official blog, latest news, and discussions.  
[Join now >](#)

**Copilot for Microsoft 365**

Welcome to the Copilot for Microsoft 365 community. Your hub for the latest news, live events, and discussions on Copilot for Microsoft 365.

For help & learning (how-to articles and training resources), please visit [Microsoft 365 Copilot Adoption hub](#).

Members 9,629 | Spaces 4 | Discussions 746 | Blog Articles 30



## Copilot for Microsoft 365 Success Kit



# Start your AI journey today

## General info

[aka.ms/copilot\\_extensibility](https://aka.ms/copilot_extensibility)

## Plugins

[aka.ms/Copilot-Plugins](https://aka.ms/Copilot-Plugins)

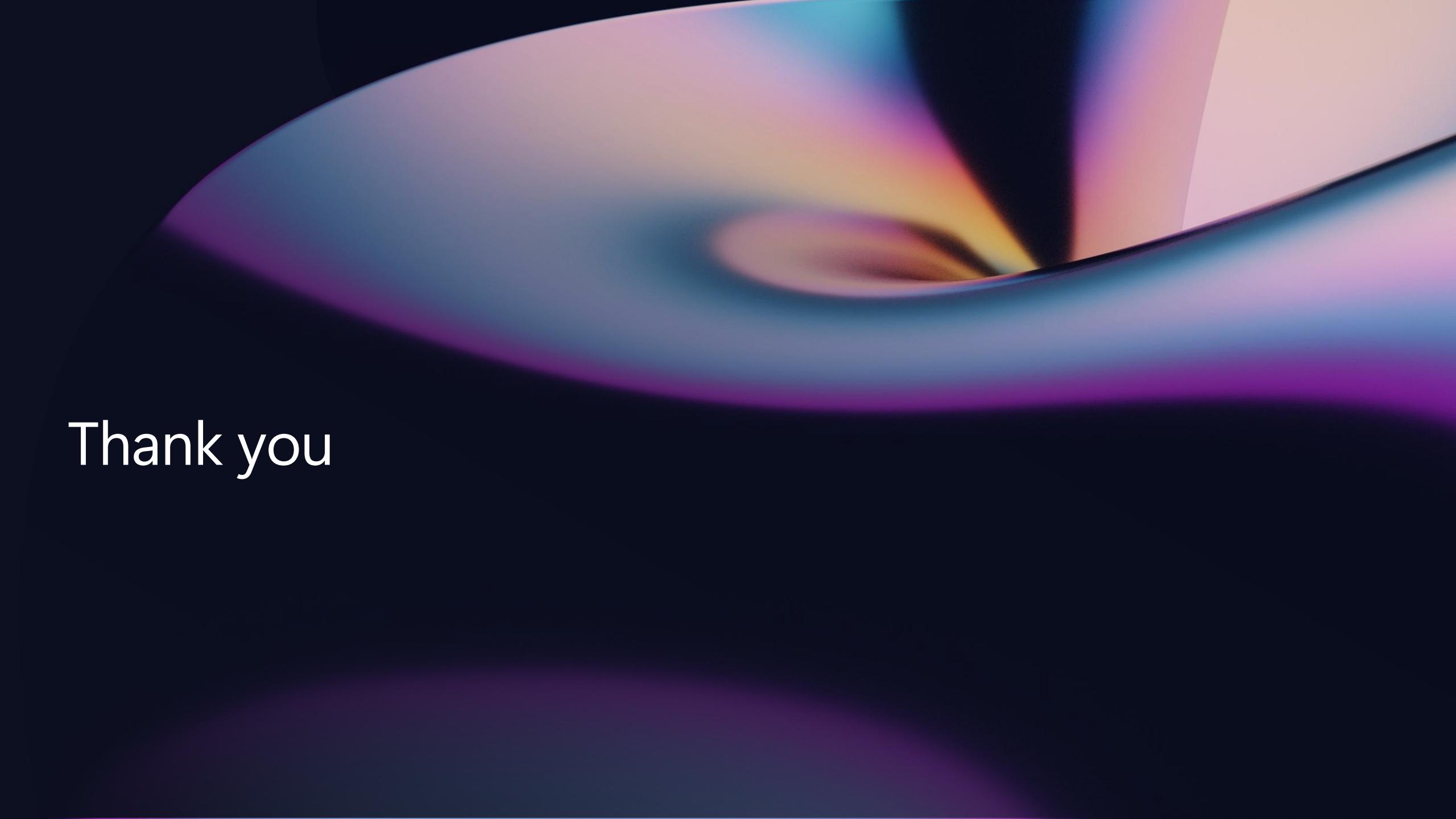
## Graph connectors

[aka.ms/GraphConnectorsAPI](https://aka.ms/GraphConnectorsAPI)

## Teams AI Library

 Tutorial and docs | [aka.ms/teams-ai-library](https://aka.ms/teams-ai-library)

 Library and NPM | [github.com/microsoft/teams-ai](https://github.com/microsoft/teams-ai)

The background of the slide features a dynamic, abstract design. It consists of several concentric, curved bands of light that radiate from a central point. The colors transition through a spectrum, including shades of blue, purple, pink, orange, and yellow. The overall effect is reminiscent of a black hole's event horizon or a nebula's glowing edges. The lighting is dramatic, with bright highlights on the outer curves and deep shadows in the inner regions.

Thank you