

AGENTS AT OUR SERVICE

Copilot Agents



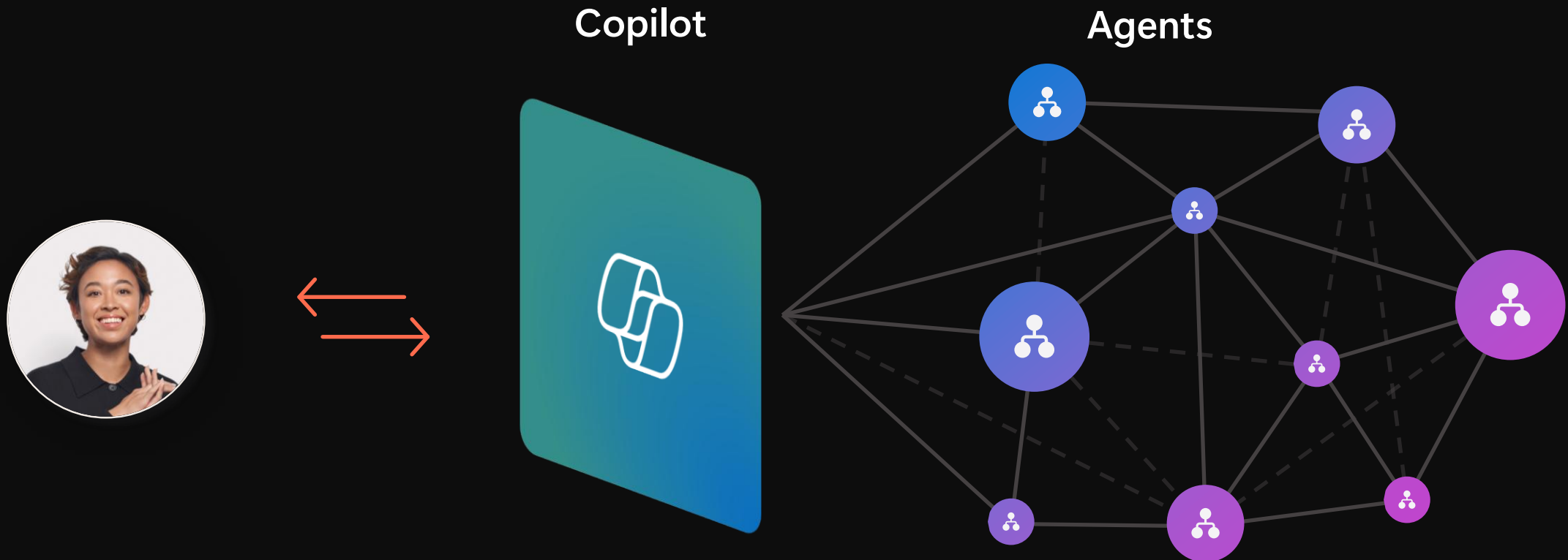
Agenda

- What are agents?
 - Copilot Studio
 - Agent builder
- Management + licensing
- Power Platform governance model



Copilot is the UI for AI

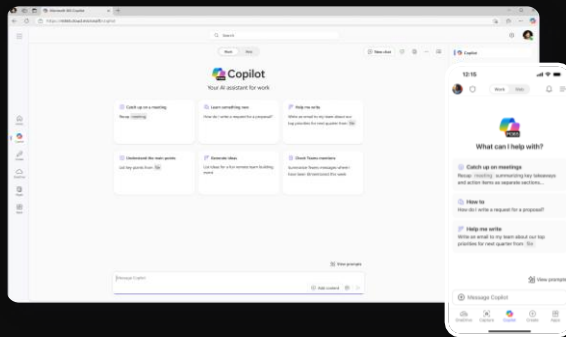
Our ambition is to empower every employee with a copilot and transform every business process with agents



Microsoft 365 Copilot Chat

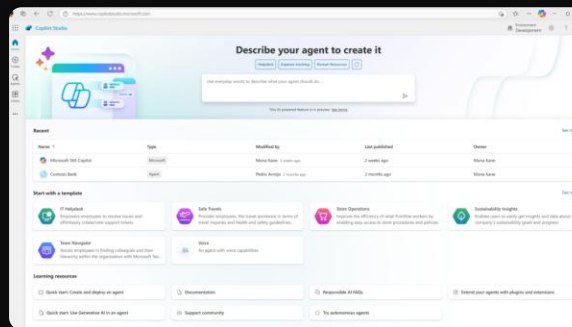


Bringing AI to everyone through a simple UI with chat and agents and solid ROI since you only pay for what you use.



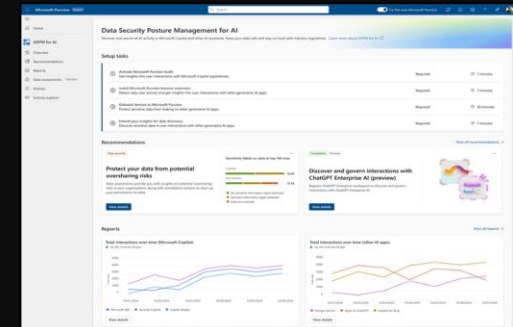
Chat

Free, secure AI chat –
powered by the latest GPT models and
web grounded



Agents

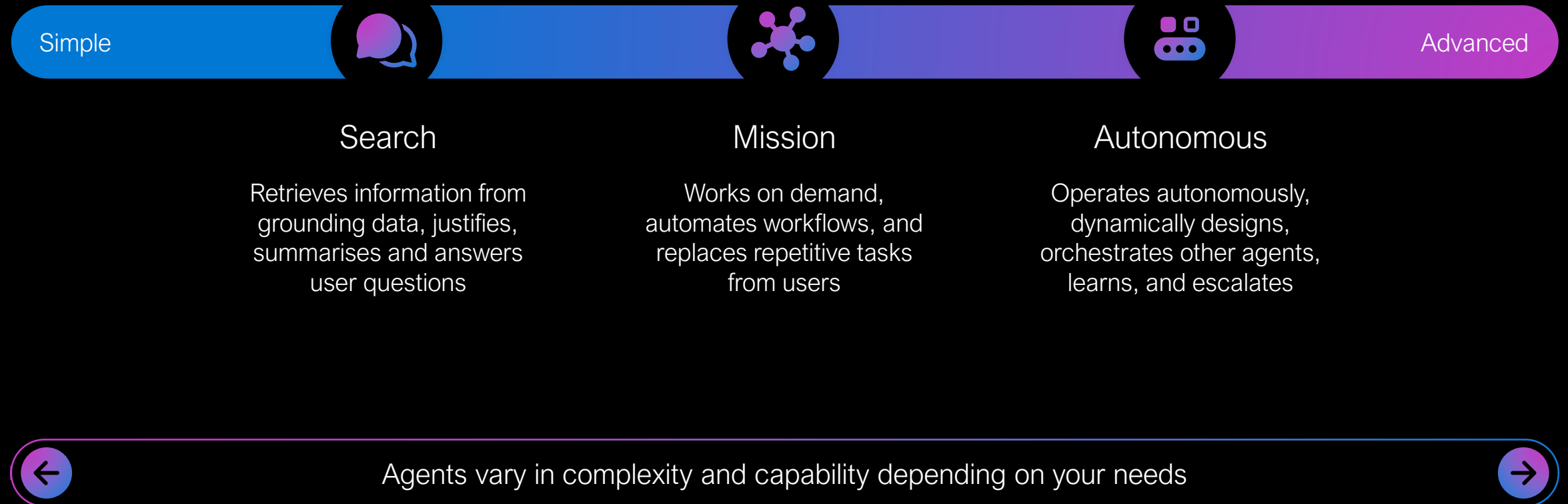
Integrated into the chat experience and
paid for on a consumption basis



IT Controls

Enterprise Data Protection
and agent management

Scale of Copilot agents



Scale of Copilot agents

IT Helpdesk Agent

How do I connect to a corporate network?



Device Update Agent

Request a new laptop and send approvals through the IT service tool.



Lead Generator Agent

The agent has identified and researched 15 new leads for you to check.



Simple



Advanced

Project Status Agent

What is the status of phase 2 in project X and the remaining budget?



Budget Management Agent

Review open purchase orders and start financial planning.



Customer Support Agent

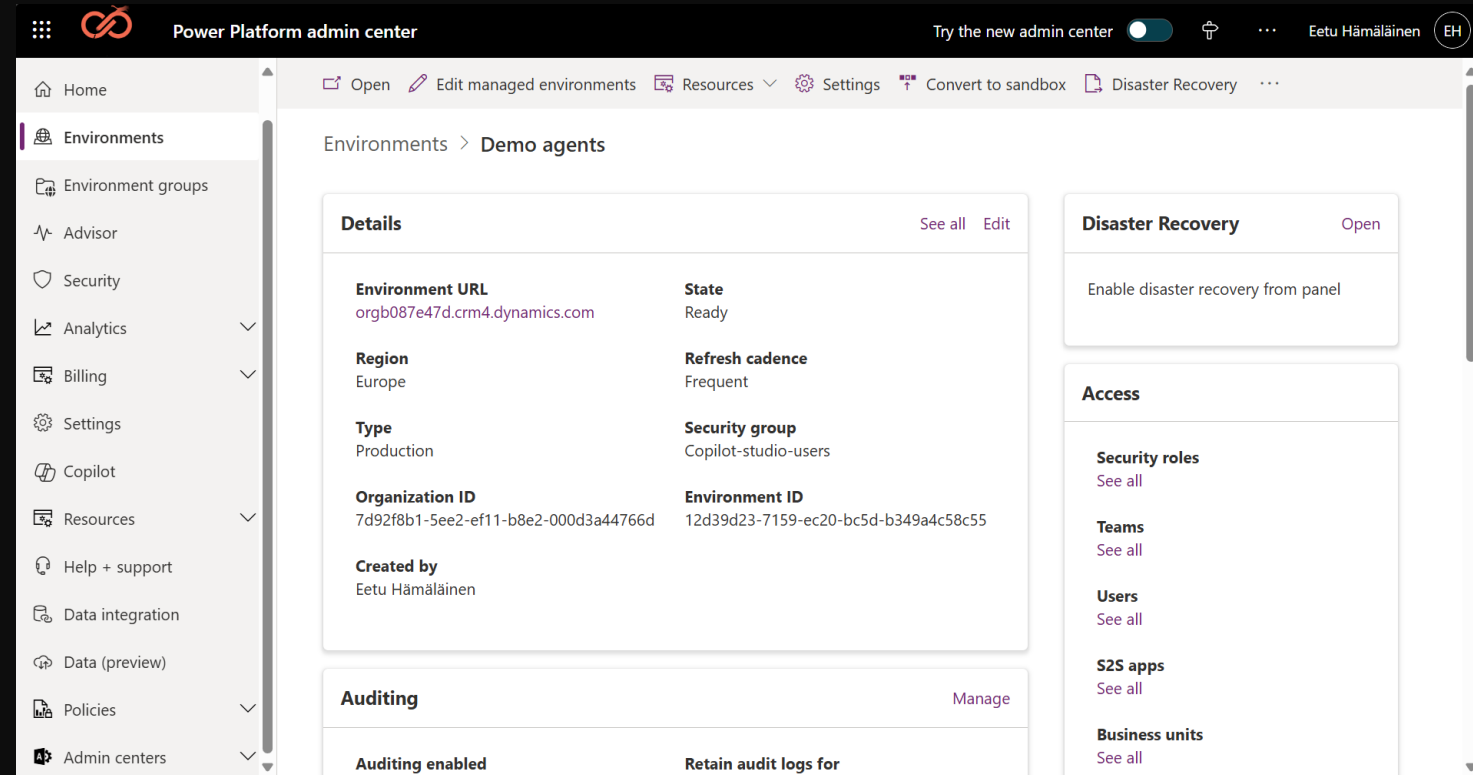
The customer support agent has identified new support issues and categorized them for the following agents to resolve.



Copilot Studio platform

- Copilot Studio uses the Power Platform in the background, which is used to manage Copilot agents

It is also recommended to go through the Power Platform governance models if/when Copilot Studio is deployed more widely or a Copilot Studio license is acquired.



Microsoft 365 Copilot



Grounded in your work data, M365 Copilot delivers added value through Copilot in M365 Apps and unlimited usage of chat and many types of agents

Copilot Chat

Free, secure AI chat



Chat

Work scope

Copilot in M365 apps

Teams, Outlook, Word, Excel, PowerPoint. etc.

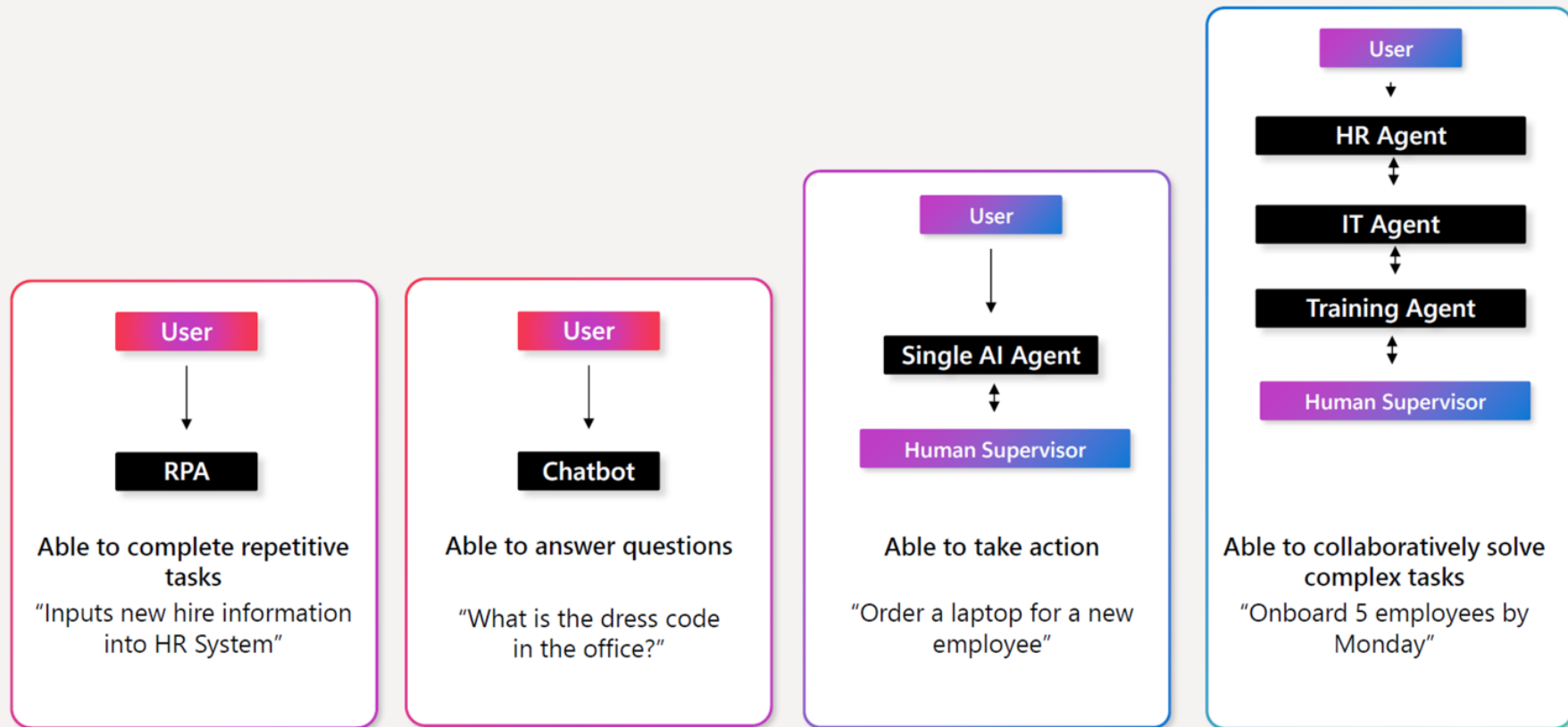
Agents

Copilot Control System

Copilot Analytics

There is still a place for automation – It doesn't always make sense to make an agent

RPA and Agents



What is conversational AI?

Conversational AI refers to a system that understands, processes and produces human language – in text or speech – in a natural way. Most of today's solutions are based on large language models (LLMs).

WHY IT MATTERS



User Experience

The chat interface is
More intuitive than menus
navigation.



Scalability

One agent handles
tens or hundreds
simultaneous conversations.



Efficiency

LLM-based agent
Adapts to user inputs
without rule scripts.



Expandability

The agent can use
databases and APIs
business workflows.

Large Language Models (LLMs) – What to Understand

LLMs are neural networks trained on massive amounts of text. They learn the statistical patterns of language and generate consistent sentences, answers, and ideas.



Training data

Terabytes of text:
websites, books,
articles.



Tokenization

The text is broken down
into tokens.
The model predicts one
token at a time.



Context Window

Limit how much
fits on the model at once.
The oldest tokens will be
eliminated.



Prompt

The more specific the
prompt,
the more targeted and
a more meaningful
answer.



Fine-tuning

Zero shot = model
as-is. Fine-tuning
adapt it to your own data.

PRO TIP

An LLM is like a "superintelligent autocomplete": it doesn't understand meaning like a human, but it predicts the next word or phrase very well.

Retrieval-Augmented Generation (RAG)

An LLM that relies solely on training data can hallucinate or become obsolete. RAG provides a model to retrieve up-to-date information before forming an answer.

1

User Survey

The user asks, for example.
"What are the most recent
Q3 figures?"

2

Search (retriever)

The system searches for
Relevant points
SharePoint, information
or wiki.

3

Augmentation

The requested points are
attached
part of the LLM
prompt.

4

Generation

LLM answers the question
searched, up-to-date
context.

WHAT THIS ENABLES

With RAG, the agent can take advantage of the company's wikis, APIs and FAQ databases – the answers are not limited to the static parameters of the model, but are updated with the documentation.

Conversational vs. autonomous agents

In the context of Copilot Studio, "agent" can refer to several different forms of AI assistants. It is useful to draw a line between the two.

TALKING AGENTS

- Focus on two-way dialogue.
- Maintain context for multiple rounds of discussion.
- Orchestrate with predefined themes and triggers.
- Ideal for customer support, FAQ content, guided interactions, and scheduling.
- Always waiting for the user's next input.

AUTONOMOUS AGENTS

- Acting on behalf of the user, not just chatting.
- Use the inference loop: plan → act → observe → redesign.
- Connect to tools and APIs (Power Automate, Dataverse, calendar).
- Handle multi-step processes independently once triggered.
- Require a tighter management model and strict access limits.

Conversational and autonomous agents – examples



Conversational agent

A Teams chatbot that answers questions about HR policy.

A Copilot Studio bot on a SharePoint page that guides the user through the form.



Autonomous agent

An agent who prepares an itinerary, books flights, and sends confirmations.

The "Meeting Summarizer" associated with the Teams call transcribes it and writes the summary in OneNote.

KEY DIFFERENCE

Conversational agent

Waits for user feedback and stays in the dialog. The user decides what happens next.

Autonomous agent

Proactively plans and executes a series of steps with a wider range of tools.

Building Block 1 of 4: Knowledge

Information is the data and context that the agent uses to respond accurately. It consists of two parts: custom instructions and context, and data sources.



Custom help and context

You write a brief description of the agent's intent and tone, for example: "You are an IT support person. You help employees troubleshoot software issues and escalate urgent tickets."

The agent remembers previous shifts in the conversation – if the user first says "my printer is offline", the context is preserved for follow-up questions.



Data sources (grounding data)

You connect the agent to SharePoint libraries, documentation sites, wikis, or databases.

The agent retrieves the relevant extracts from these sources, in which case the answer is based on the organization's own practices.

The agent can be forced to answer only for these sources, so that it does not guess or hallucinate.

EXAMPLE

The "Policy Assistant" agent connects to the SharePoint site in HR. When a user asks about a leave policy, the agent retrieves the exact text from the HR policy document instead of relying on a generic AI response.

Building Block 2 of 4: Tools (Actions)

The tools determine what the agent can do in addition to the conversation. Each action is a task that the agent performs programmatically.



Communication

Send an e-mail or
A Teams message.



Calendar

Create or update
calendar event.



Records

Add or edit a row
SharePoint list, or
in a Dataverse table.



Workflows and APIs

Calls Power Automate
workflow or REST
API.

HOW THE FEATURES WORK

- 1) Define feeds and outputs – for example, "Send email" needs a recipient, a subject line, and the content of the message.
- 2) Combine actions into workflows, as a user's request often requires many steps.
- 3) Connect to external systems: Copilot Studio integrates with Power Platform and any HTTP-based endpoint.

Tools in action: "Expense Helper" agent

An example of how to chain multiple actions into a single workflow that handles the user's request from start to finish.

1

Listen to the request

The agent recognizes request "Send expenses".

2

Collect the data

The agent takes the user expense information from the form.

3

Save data

"Add to SharePoint list" function saves the data.

4

Notify the approver

"Send email" function starts automatically.

NOTE

If the flow needs to update the CRM or call the internal API, a custom action is created for it. The agent also generates an LLM summary of the retrieved data before sending the message.

Building Block 3 of 4: Topics

The topics define the conversation triggers and entry points. Each topic corresponds to one functionality or category of questions.



Triggers

The subject can be "Send an IT ticket", "Check Holiday Balance" or "Create Sales Report".
Generative Orchestration interprets the user's intent.



Subject descriptions

Every topic is written about a clear description of what the topic is covers. AI uses description to decide when a topic is activated – even if the wording wouldn't quite match.



Mapping to Operations

Each topic is related to one or more for more than one function, or information retrieval phase. Agent guides the discussion by defining in your order.

EXAMPLE

The user says, "I need help setting up a new laptop." The AI targets this to the topic "Submit an IT ticket", asks for the device model and user information, and sends the ticket to the helpdesk system.

Building Block 4 of 4: Instructions

Prompts or "system messages" guide the tone, style, and boundaries of the LLM. They influence how the agent reacts in each situation.



Role and personality

You tell the AI who it is:
"You are in Contoso Retail
customer service representative."
This will determine the tone –
friendly, concise,
formal or casual.



Instructions for answering

"Always summarize policy information
as list items."
"If you don't know the answer, say
that you don't have that knowledge."
"Never include
confidential information."



Memory and context

You can instruct the agent to:
How many conversations
It remembers the rounds.
"Remember this user's
Details of requests
to a maximum of three
until the question."

EXAMPLE – "BENEFITS ADVISOR"

"Always use the most up-to-date HR handbook when responding. If you are asked about enrollment deadlines, please provide the exact dates of the policy. Keep answers under 150 words."

How the four building blocks work together

As you gather information, tools, topics, and guidance, Copilot Studio's AI orchestrator creates an agent that:

1. **Listens to the relevant topic (guiding the descriptions of the topic).**
2. **Apply instructions to set the mood, decide when to ask follow-up questions, and enforce the rules.**
3. **Leverage data sources to base their responses on your organization's data.**
4. **Invokes tools (actions) as needed to perform tasks—sending messages, updating records, or calling an API.**

Behind the scenes, the orchestrator uses generative design: it decides which steps to take and in what order to fulfill the user's request. If an action fails (for example, an email can't be sent), the agent follows your exception handling instructions (ask a clarifying question or report an error). Because the LLM adapts to the conversation context, the agent can retain its memory for several rounds and incorporate new information as the conversation progresses.

Visual workflow example:

1) User: "Show my vacation balance." → 2) Topic is identified: "Check vacation balance" → 3) Instructions: friendly and concise tone → 4) Information: search in HR's SharePoint list (vacation balance = 12 days) → 5) Action: reply to the user in Teams: "Your vacation balance is 12 days."

Done!

Four essential building blocks for any agent in Copilot Studio:

1. Knowledge – Where the agent searches for factual information and maintains conversation memory.
2. Tools – Tasks that an agent can perform to make things happen automatically.
3. Topics - How an agent identifies user intent and decides which flow to run.
4. Guidelines – The rules, tone, and boundaries that guide each answer.

Differences between products

● Included ▲ Included — Metered

		Microsoft 365 Copilot Chat	Microsoft 365 Copilot
Chat	Copilot Chat – Web grounded (powered by GPT 4o)	●	●
	Copilot Chat – Work grounded (work data in your tenant's Microsoft Graph and 3rd party data via Graph connectors)		●
	Copilot Pages	●	●
	File upload ¹	●	●
	Code Interpreter ¹	●	●
	Image generation ¹	●	●
Agents ²	Create agents using Copilot Studio ³ , including SharePoint agents	●	●
	Discover and pin agents	●	●
	Use agents grounded on Web data	●	●
	Use agents grounded in work data (work data in your tenant's Microsoft Graph and 3rd party data via Graph connectors)	▲	●
	Use agents that act independently using autonomous actions	▲	▲
Personal assistant	Copilot reasons over personal work data (e.g., Outlook, OneDrive, meeting transcripts)		●
	Copilot in Teams (Copilot in Meetings and Meeting Recap, insights from screen-shared content coming soon)		●
	Copilot in Outlook (Prioritize my inbox, schedule focus time and 1:1 meetings, draft agendas, summarize message threads)		●
	Copilot in Word (Suggestions for structure, flow, and tone, draft and summarize documents)		●
	Copilot in Excel (Python, getting started experience, create formulas and visualizations using natural language)		●
	Copilot in PowerPoint (Narrative builder, presentation translation, generate slides or images aligned to company branding)		●
	Copilot Actions		In preview
	Pre-built M365 agents (Interpreter, Facilitator, Project Manager, Employee Self-Service)		
Copilot Control System	Enterprise Data Protection (EDP)	●	●
	IT management controls	●	●
	Agent management	●	●
	SharePoint Advanced Management		●
	Copilot Analytics to measure usage and adoption ⁴		●
	Pre-built reports and advanced analytics to measure ROI		●

1. Limits apply. 2. Applies to employee-facing agents only. 3. Learn more about the full capabilities of Copilot Studio: aka.ms/CopilotStudioCapabilities 4. Basic reporting in Microsoft Admin Center available for Copilot Chat.

Agents in Copilot

Agents operate on a secure and reliable platform



Data security

Take advantage of classification label inheritance and DLP policies

Smart grounding respects your rights and security specifications

Comprehensive visibility into user, data, and agent risks



Access and cost management

Managed Agent Availability and Access

Control who can create and distribute agents

Track and manage agent costs and operational insights



Measurement and reporting

Track usage telemetry and license usage

Track user productivity improvements and compare impacts across different groups

Analyze the impact of Copilot and agents on business outcomes

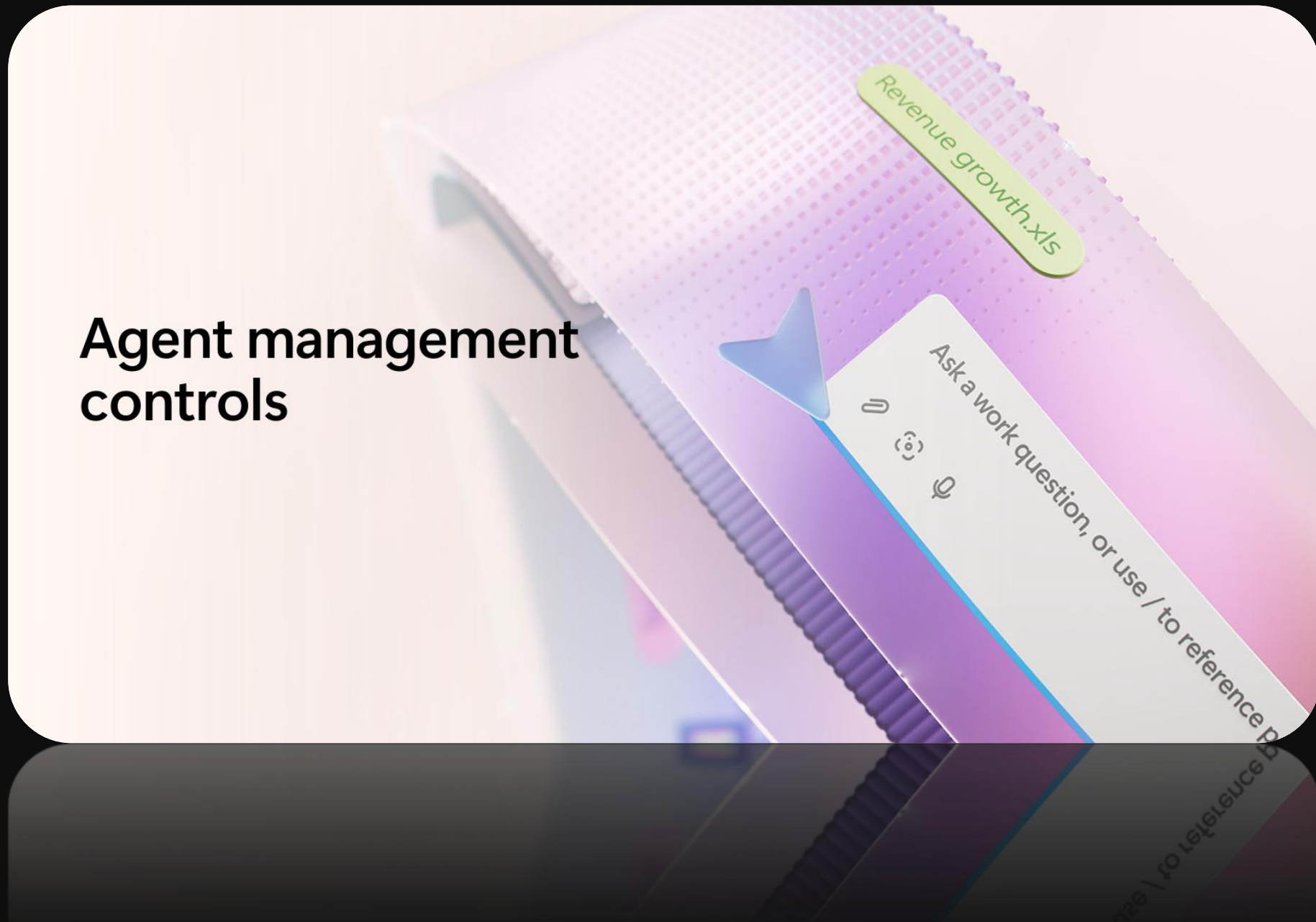
Agent interactions remain within Microsoft 365 and Azure service boundaries, and Microsoft 365 security, governance, compliance, and privacy policies apply

Different tools for creating agents



* Declarative = prompts processed by Microsoft 365 Copilot; Custom-engine = prompts handled by a custom AI engine (e.g., orchestration and foundational models)

Agent management controls



Agent access and cost control

*Tenant-wide distribution & access,
including 3P agents*

Controls for user and maker created agents in the tenant

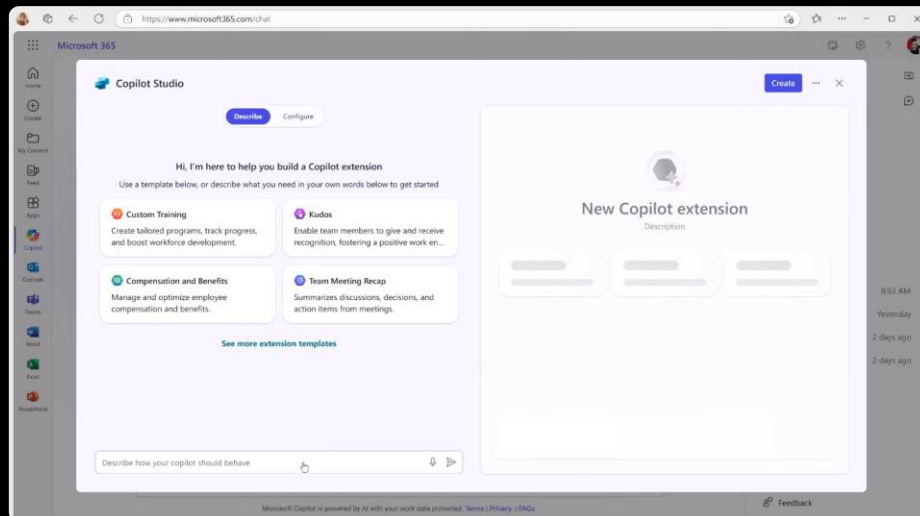
	IT managed	Agent builder	Copilot Studio	SharePoint
Creation		Microsoft 365 Admin Center Assign M365 Copilot license Power Platform Admin Center <u>Configure pay-as-you-go plan or prepaid message capacity</u>	Microsoft 365 Admin Center <u>Assign Copilot Studio license</u> Power Platform Admin Center <u>Control access to Copilot Studio based on Security Groups</u>	Microsoft 365 Admin Center Assign M365 Copilot license Microsoft 365 Admin Center Configure pay-as-you-go plan or prepaid message capacity
Use	Microsoft 365 Admin Center Pin Copilot Chat Control availability of agents* -enable or disable agents, deploy or remove individual agents	Microsoft 365 Admin Center See IT managed options	Microsoft 365 Admin Center See IT managed options	SharePoint Online <u>Use file permissions on the agent file to control who can access</u>
Sharing		Power Platform Admin Center <u>Use "Manage sharing" to limit how broadly agents can be shared</u>	Power Platform Admin Center <u>Use "Manage sharing" to limit how broadly agents can be shared</u>	SharePoint Advanced Management <u>Restricted access control</u>
Costs	Azure Portal <u>Control and track costs</u>	Power Platform Admin Center Manage and track costs	Power Platform Admin Center Manage and track costs	Azure Portal <u>Control and track costs</u>

* Applies to Agent builder and Copilot Studio

Copilot Studio

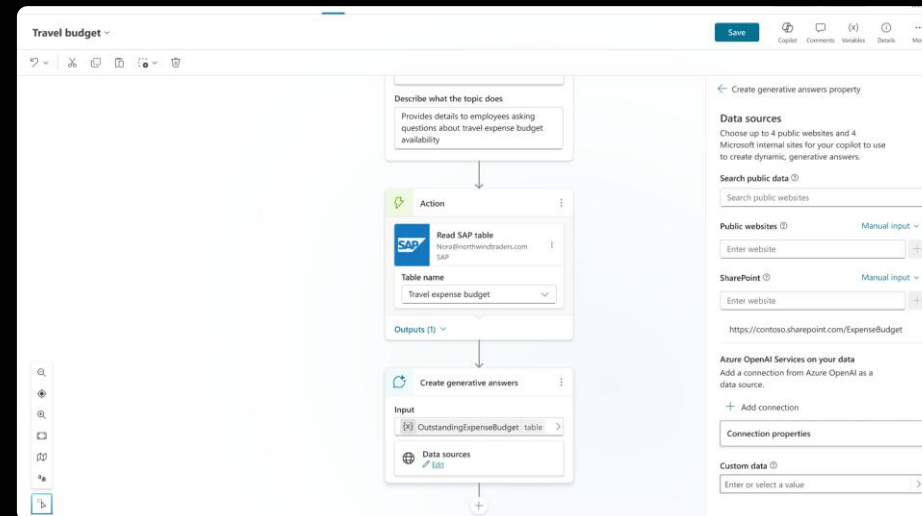
- Copilot Studio is an environment where you can create agents that extend Microsoft 365 Copilot or work independently

For end users



Copilot Studio agent builder
Microsoft 365 Copilot Chat & SharePoint

For IT and developers



Copilot Studio platform

A good Copilot agent plan starts with a clear understanding of what problem or need the agent is addressing, who it is intended for, and how it will produce value.

Here are step-by-step instructions for you to plan:

1. Definition of the purpose of use

- **What is the role of an agent?** (e.g. user support, information retrieval, process automation)
- **Who is it aimed at?** (e.g. end users, experts, IT team)
- **What problem does it solve?**
- **What benefits are expected from the agent?** (e.g. time savings, better customer experience)

2. Use cases and scenarios

- List the concrete use cases:
e.g. "The user asks how to share the file through Intune", "The agent helps to create a Power BI report"
- Define what the agent should know how to do in each case.
- Think about which channels the agent works in: Teams, Outlook, SharePoint, websites?

3. Knowledge base and integrations

- **Where does the agent get their information** from? (e.g. SharePoint, intranet, databases, documentation)
- **Are integrations needed?** (e.g. Microsoft Graph, Azure, Intune, Power Platform)
- **Is there a need to use external APIs or data warehouses?**

4. Agent's capabilities and limitations

- Define what the agent can do:
 - Answer questions
 - Perform tasks (e.g. create a file, send an email)
 - Suggest solutions
- Limit what it **does not** do (e.g. does not provide legal advice, does not make decisions on behalf of the user)

5. User experience and interaction

- How does the agent communicate? (e.g. friendly, knowledgeable, neutral)
- How does it react to unclear questions?
- Do you need visual elements such as charts or tables?

6. Data security and responsibility

- How do you ensure that the agent does not reveal sensitive information?
- Does the agent only have access to certain data or user groups?
- How do I verify a user's identity and permissions?

7. Metrics and continuous development

- How do you measure success? (e.g. utilization rate, user satisfaction, number of resolved requests)
- How to collect feedback and develop the agent?
- Is there a plan for ongoing maintenance and updating of content?

8. Documentation and communication

- Create clear documentation of the agent's operations, limitations, and usage patterns.
- Communicate to the organization what the agent does and how to use it.

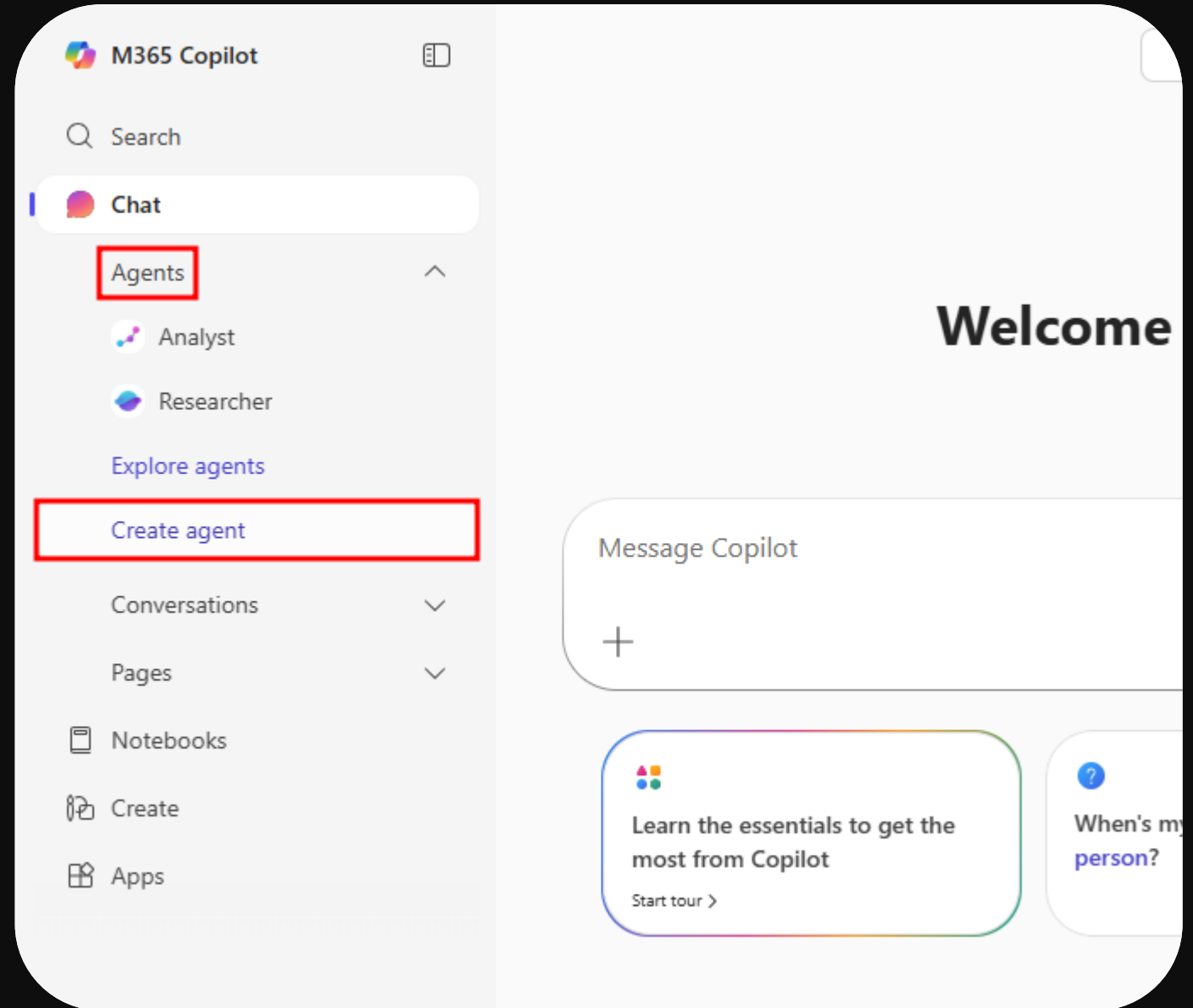
Creating a culture

- **Creating a culture**
 - Encourage business units to develop their own apps
 - Ensure that the governance model prevents risks
- **Internal community**
 - Create a Power Platform user group
 - Foster collaboration and knowledge sharing
- **Communication**
 - Document Usage Instructions
 - Release Guidelines
 - Reporting instructions



Create an agent

Agents use AI to make Copilot Chat more personal and intelligent for your day-to-day work. Agents automate repetitive tasks and processes – think of them like Copilot apps. Copilot Chat comes with a set of agent templates that you can use to get started, or you can create your own agents for your own needs.



Create an agent

When you select Create an agent, a window opens that resembles the Copilot Studio natural language agent builder. The Describe window is the home page for defining and building a new agent in Copilot Chat. These are the following options available for building an agent in Copilot Chat via the Description screen:

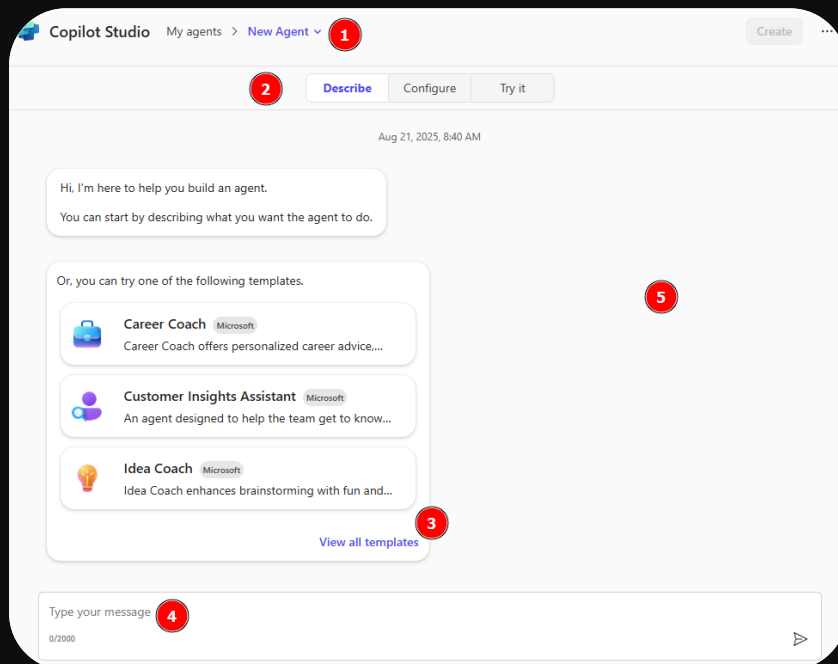
1.Currently Selected Agent – This area displays the title of the modified agent, and once selected, you can navigate to the other agents you want to edit.

2.Describe or Define – This switch allows you to choose whether you want to edit the agent in natural language on the Description tab or manually configure the agent details on the Configure tab.

3.Templates – Every time a new agent is created, you will be offered templates as an option to configure the agent. Templates are pre-configured agents, such as Career Coach, Idea Coach, and Learning Coach. Select View All Templates to see all available templates, you can also access the templates directly without any settings through the Agent Store in Copilot Chat.

4.Chat Box – The chat box at the bottom of the Describe window is where you enter text to configure the agent's settings. Think of this area as a conversation with an agent in the form of instructions. If you need ideas, checking the Config window for available agent settings can be helpful to understand what you can edit in your agent.

5.Test Panel – This panel displays a test screen of the settings that are currently being sent to the selected agent.



Create an agent



Note

Users who don't have a Microsoft 365 Copilot license are restricted only website URLs as data sources.

Select Configure to access the classic agent building experience, allowing you to edit agent settings directly. The following options are available on the Configuration screen when a user doesn't have a Microsoft 365 Copilot license:

1.Template – A drop-down menu for quick implementation of templates in agent building.

2.Details – This menu allows you to change the agent's profile picture, name, and user-facing description of the agent's purpose.

3.Instructions – Instructions for the agent when responding to users. Think of this as a list of rules that the agent should follow before responding to the user. If there is difficulty with ideas, choosing a template fills this section with predefined information that can spark creativity or provide a faster agent-building experience.

4.Knowledge – Add data sources to base your agent's responses on relevant information.

Copilot Studio My agents > New Agent

Describe Configure Try it

Template: None

Details

Name

New Agent

Description

Describe your agent

Instructions

Describe what this agent should do, define its tone, and outline any rules or guidelines it must follow

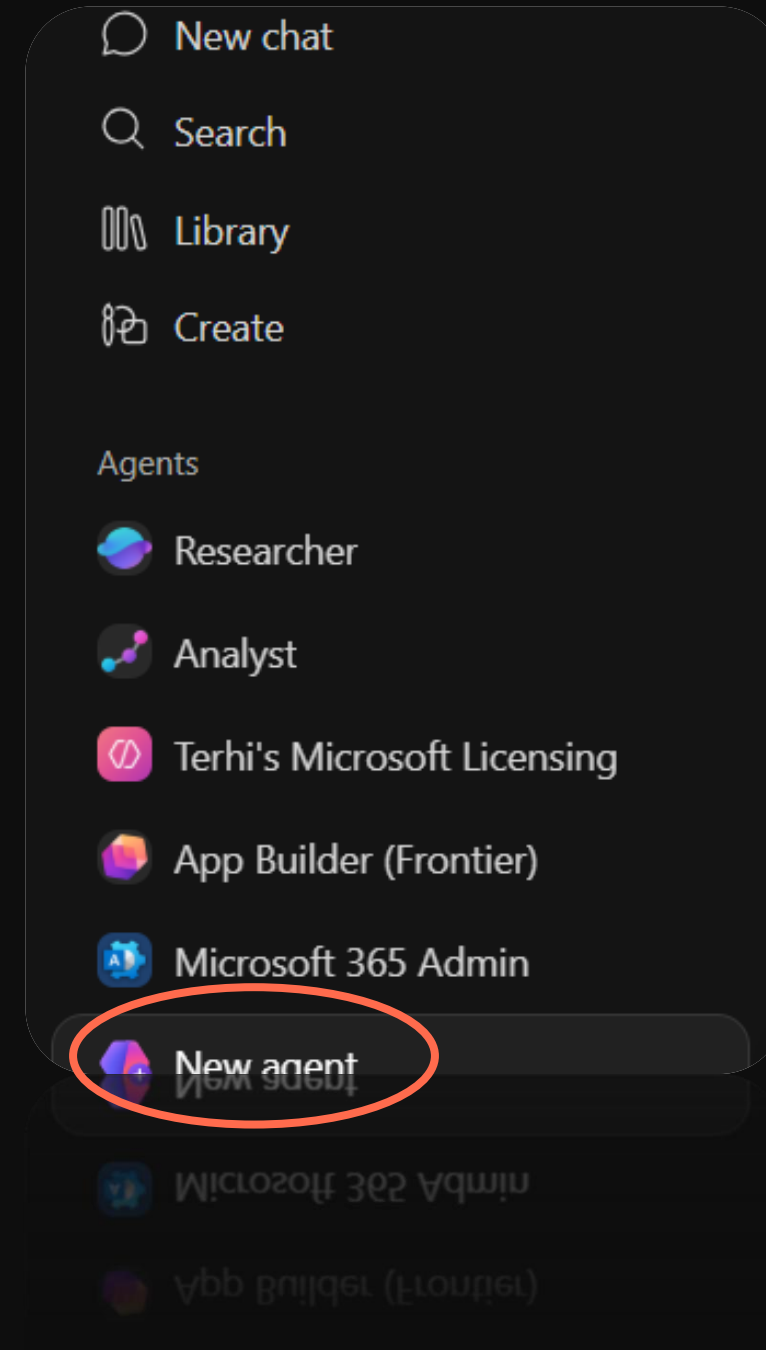
Knowledge

Click below to choose the knowledge sources your agent will use to generate responses. You can enter URLs, upload files, and use Microsoft SharePoint, Microsoft Teams, and Microsoft Outlook emails. [Learn more](#)

Search by name, enter a URL, or drop a file

Prioritize the knowledge sources you added for agent knowledge-based queries. [Learn more](#)

Agent Builder



Top 10 Questions

Q: What agent capabilities does Copilot Chat offer?

A: Copilot Chat users can create, discover, and access agents.

An admin must set up a Copilot Studio subscription before using agents that are billed based on consumption.

Agents based on instructions, public websites, or uploaded files are available to all users at no additional cost.

Top 10 Questions

Q: What agent-building capabilities do Copilot Chat users have?

A: Copilot Chat users can build agents **using Copilot Studio, Agent Builder, and SharePoint** if their IT admin has allowed access to the Microsoft 365 admin center.

Top 10 Questions

Q: Are agents enabled by default?

A: Agents that access data from SharePoint or Graph Connectors are billed on a consumption-based basis.

Consumption-based agents **aren't turned on by default.**

Admins must enable a Copilot Studio subscription before using these agents.

These agents are managed through Copilot and Power Platform settings.

- Agents based only on **instructions, public websites, or uploaded files** are available to all users **at no additional cost**. These agents **don't have access to the tenant's work data**.
- The visibility of agents in Copilot Chat depends on your organization's previous store/app store management settings (Teams and Microsoft 365 Apps).
Based on these settings, some free agents may be available by default.

Top 10 Questions

Q: Which agents are billed on a consumption basis in Copilot Chat? Are some agents available at no additional cost?

A: Agents who consume data from SharePoint or Graph Connectors are billed on a consumption basis. Agents based on **instructions, public websites, or downloaded files** are available **at no additional cost**.

Top 10 Questions

Q: What controls are available to manage agents? Can I control who creates and uses agents?

A: There are controls available for admins to manage tenant-level grounding settings.

More information:

Manage Copilot agents in Integrated Apps – Microsoft 365 admin (Microsoft Learn)

<https://learn.microsoft.com/en-us/microsoft-365/admin/manage/manage-copilot-agents-integrated-apps>

Top 10 Questions

Q: Does it cost the same to use agents regardless of whether they are used in Copilot Chat or other channels?

A: Yes.

If a user doesn't have a Microsoft 365 Copilot license, using agents consumes the same number of messages per message packet—or costs the same amount per message—regardless of whether the agent is used in Microsoft 365 Copilot Chat or in a Copilot Studio environment.
If the user has a Microsoft 365 Copilot license, there is no additional cost.

Thank you

Towards an agent world!