

COPILOT

Day 1 • Thu 11 June

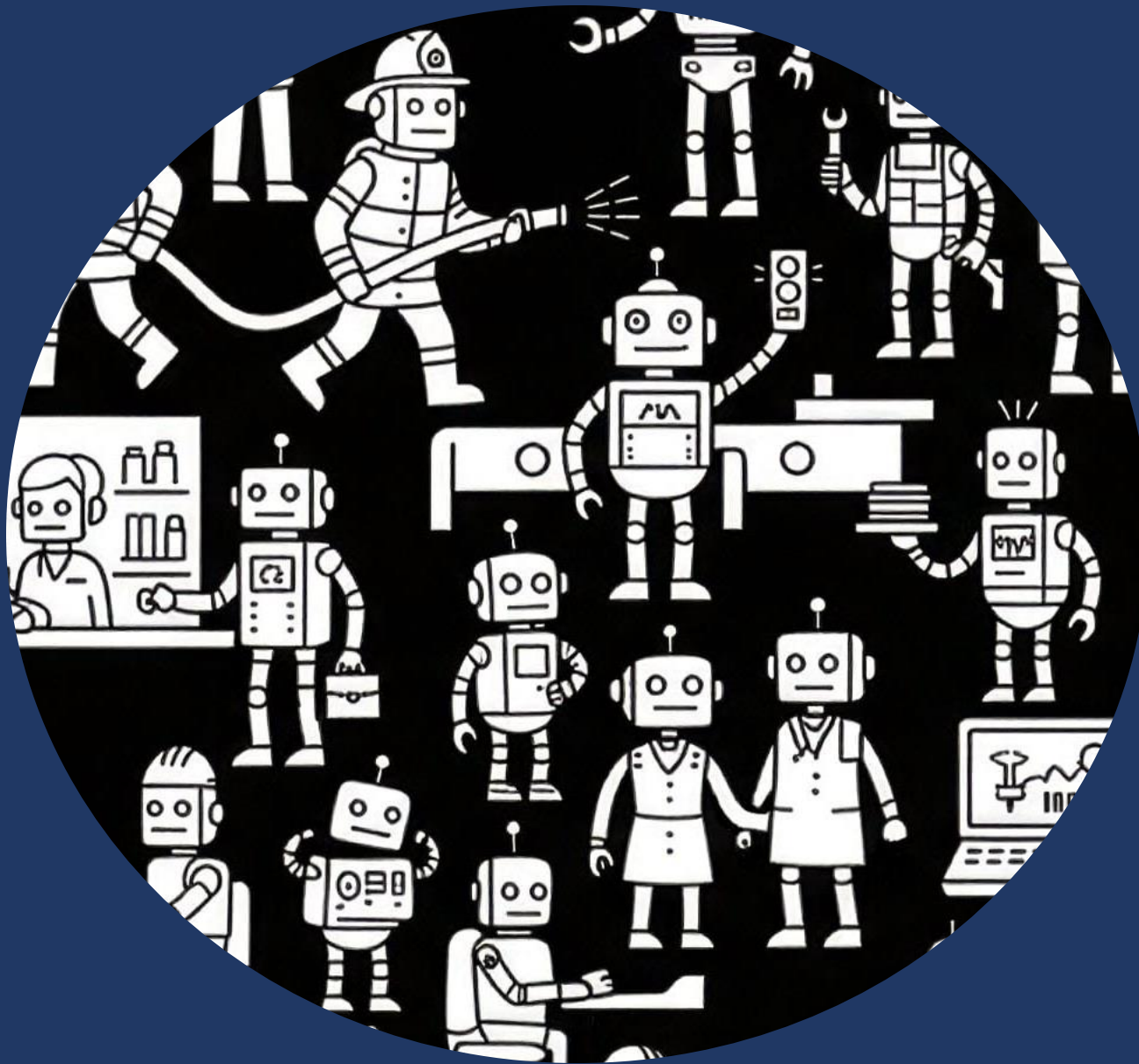
09:00

Agents Cookbook Workshop

When to reach for Copilot Studio, when for the M365 Agents Toolkit, and how to ship both without the plumbing eating the project.

Reshmee Auckloo Lee Ford Jayshree Ostwal

Microsoft MVP



#ELUK26

Experts Live UK 2026

WITH THANKS TO

Our sponsors.

HEADLINER

robopack 

PLATINUM



control **UP**



THREATLOCKER liquidware™

GOLD

Lenovo

 LOGIN VSI

eido

Recast

SUPPORTER

 cireson

 systemcenterdudes



www.expertslive.co.uk

WELCOME TO THE STAGE

Reshmee Auckloo

she/her

Microsoft MVP, Modern Work · builds Copilot &
Graph solutions for UK enterprise.

LinkedIn

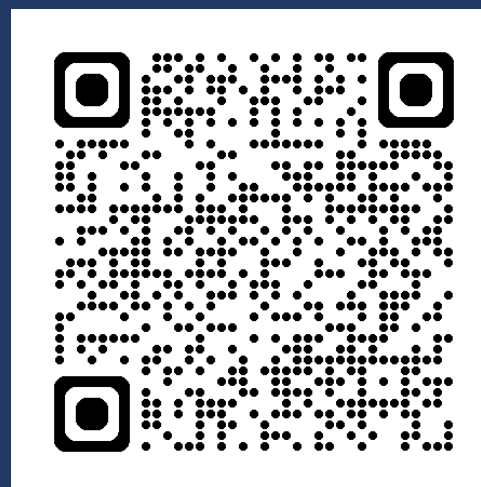
[in/reshmee-auckloo-98a23619](https://www.linkedin.com/in/reshmee-auckloo-98a23619)

Bluesky

<https://bsky.app/profile/reshmeeaukloo.com>

Web

<https://reshmeeaukloo.com/>



WELCOME TO THE STAGE

Lee Ford

he/him

Builds Copilot & M365 solutions for UK enterprise. Occasionally gets hands dirty writing code! Also, a Microsoft MVP

LinkedIn	/in/lee-ford
Bluesky	@lee-ford.co.uk
Web	lee-ford.co.uk



WELCOME TO THE STAGE

Jayshree Ostwal

she/her

Microsoft MVP, Microsoft Certified Trainer (MCT), Modern Work ·
builds Copilot solutions & Governance for UK enterprise.

LinkedIn [/in/JayshreeOst](#)



Agenda

09:00 – 10:00 Introduction + Effective Prompting (Lee + Jayshree)

Introduction to the workshop and effective Prompting

10:00 – 10:30 Simple Agents (Reshme + Jayshree)

11:00 – 11:30

SharePoint Agent, Copilot in SharePoint, Agent Builder, Copilot Studio

11:30– 13:00 Advanced Agents (Reshme + Lee)

Showcasing MCP integration, Multi agent within Copilot Studio, M365 Agent Toolkit, Microsoft Foundry

13:00 – 14:00 Lunch break

14:00 – 14:30 Security, Compliance and Governance (Jayshree + Reshme)

How to tackle risks associated with agents like inaccuracy, hallucinations, data leakage

14:30 – 15:15 Latest topics (Lee + Jayshree)

Skills, Cowork, IQ

15:30 – 16:00 Scenarios, discussions, wrap up (all of us)

Quiz involving scenarios, Q&A and wrap up

What to expect

- No prior knowledge of agent building is needed
- You don't need to write any code to build agent – but you can do!
- Workshop is entirely content, discussions and demonstrations
- Recommended hands-on and labs can be conducted afterwards in your own time in the direction you want to take

01

Agent Fundamentals

How Do You Define an Agent?



Shared by Abram Jackson

[linkedin.com/pulse/your-agent-has-brain-now-give-hands-abram-jackson-qeenc/](https://www.linkedin.com/pulse/your-agent-has-brain-now-give-hands-abram-jackson-qeenc/)

Defined by Simon Willison

simonwillison.net/2025/Sep/18/agents/

An LLM agent runs **tools** in
a **loop** to achieve a **goal**

— *Simon Willison*

Copilot and Agents



Copilot

Human Augmentation

- Works as your personal assistant
- There are only as many Copilots as there are people
- Enhances individual productivity



Agents

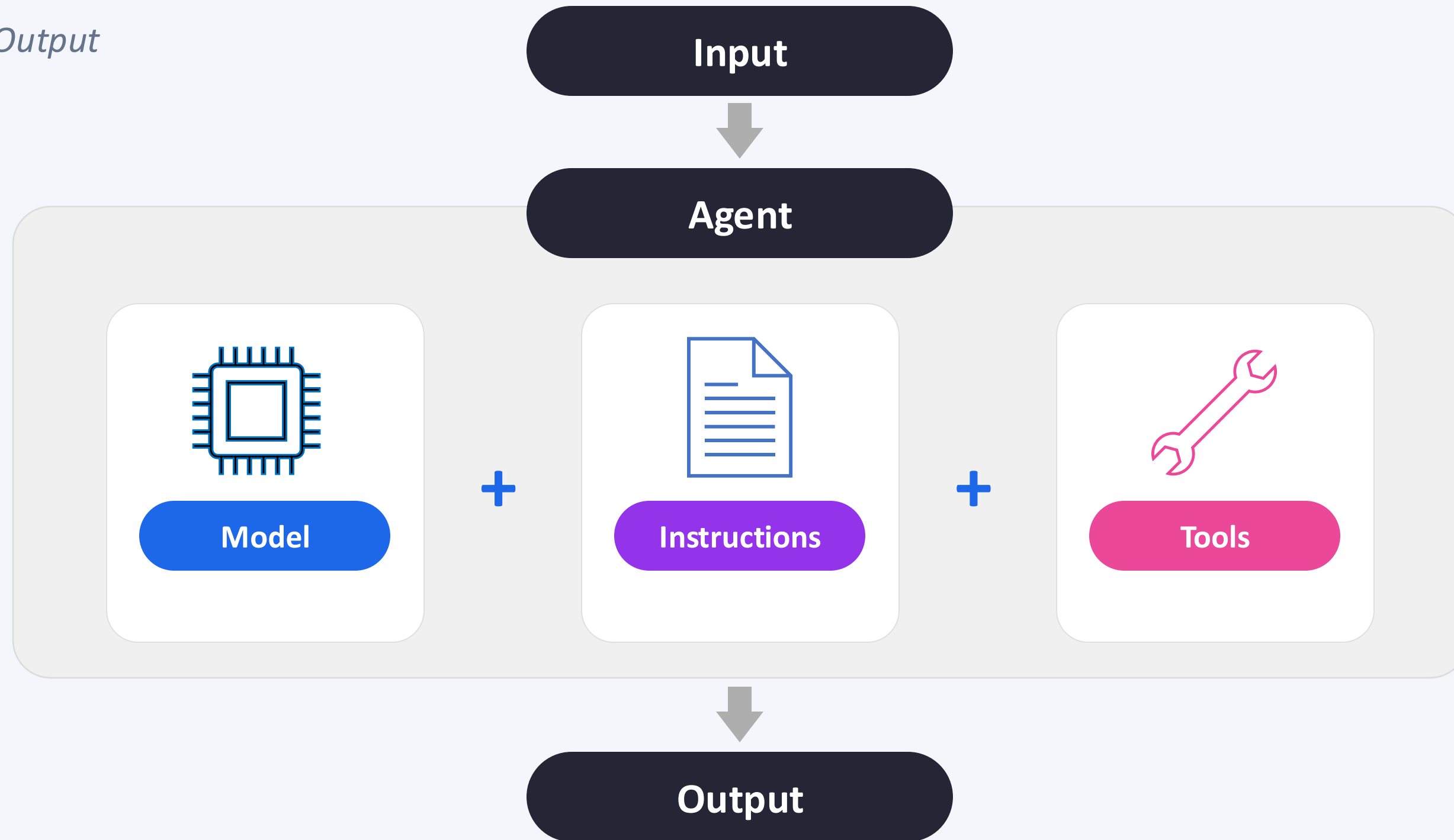
Expert Systems

- Can work autonomously on behalf of a process
- There are more agents than people
- Scales across the organisation

Increasing Value and Reducing Costs · Enabling Copilot for Business Processes

Understanding AI Agents

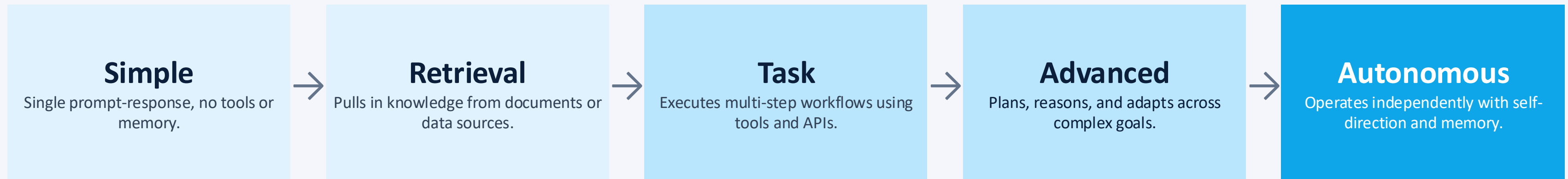
Input → Agent → Output



Input → Agent (Model + Instructions + Tools) → Output

Agent Complexity Spectrum

Agents vary in levels of complexity and capabilities depending on your need



Agent Components

Instructions

The most crucial part of building an agent. Structured instructions define what it is, what it does, and expected outcomes.

Foundation Models

The underlying LLM powering the agent. Different models produce different outputs and are trained on general knowledge only.

Knowledge (RAG)

Grounding data beyond the model's training. Ranges from simple SharePoint sites to complex vector stores like Azure AI Search.

Tools

Interfaces with external systems via APIs, Power Platform connectors, and MCP servers. Not limited to read operations.

Autonomy

Run agents autonomously on schedules or events using triggers.

Memory

Maintains context from earlier conversations so the agent doesn't start from zero each time.

Orchestrator

Like a conductor of an orchestra. Decides which tools, knowledge, and agents to use for each prompt. Acts and responds on responses from tools and knowledge.

■ Agent Components

Autonomy

Trigger agent



User Experience

Host application or user interface the agent will be accessible from

Orchestrator

Like a conductor of an orchestra. Decides which tools, knowledge, and agents to use for each prompt. Acts and responds on responses from tools and knowledge.

Knowledge (RAG)

Grounding data beyond the model's training. Ranges from simple SharePoint sites to complex vector stores like Azure AI Search.

Tools

Interfaces with external systems via APIs, Power Platform connectors, and MCP servers. Not limited to read operations.

Memory

Maintain context

Instructions

One of the most crucial parts of an agent. Structured instructions define what it is, what it does, and expected outcomes.

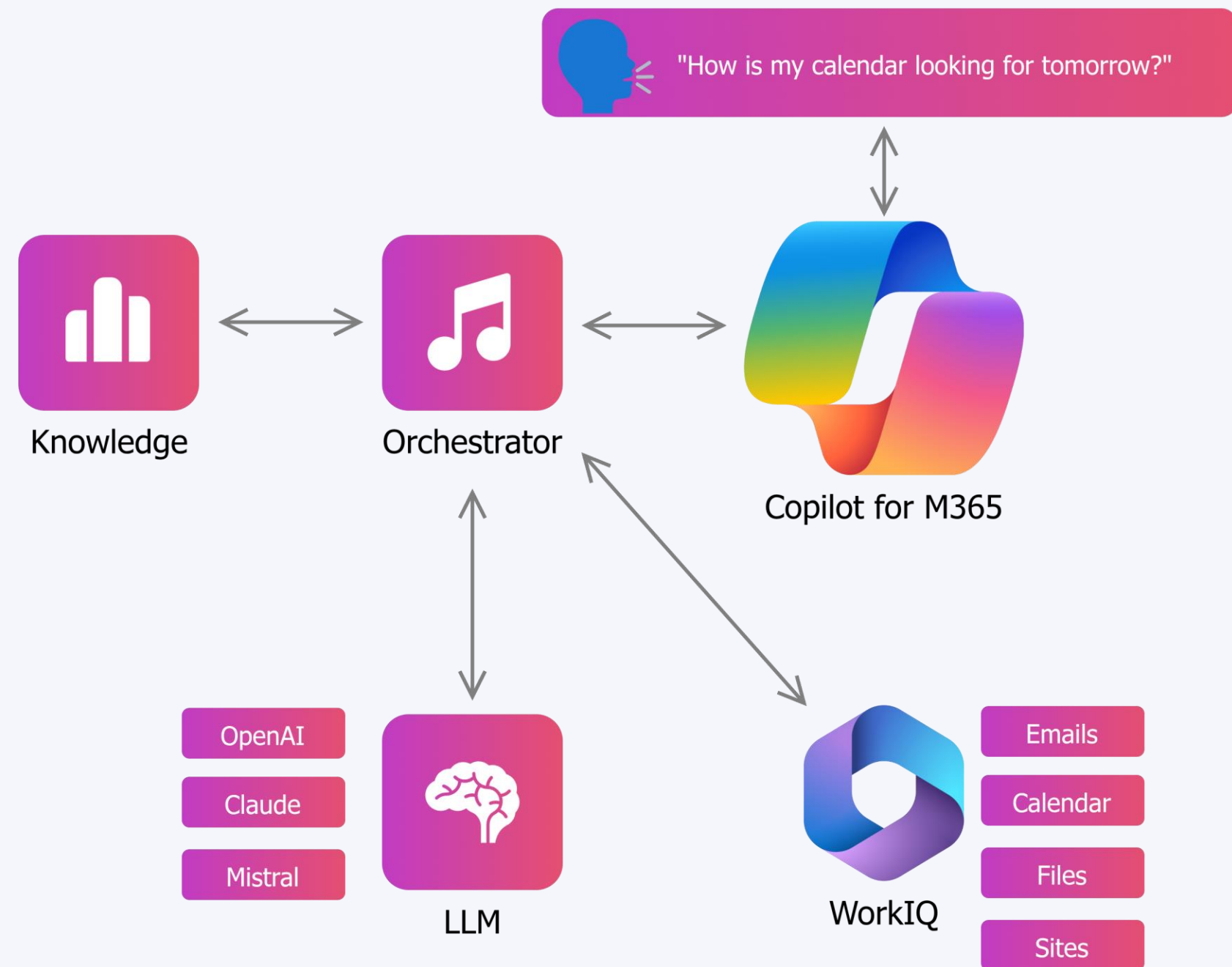
Foundation Models

The underlying LLM powering the agent. Different models produce different outputs and are trained on general knowledge only.

M365 Copilot

An AI assistant to help you work more efficiently

- M365 Copilot is the **UI** and the **Orchestrator**
- Grounded in your M365 data using **WorkIQ**
- Able to use additional knowledge sources such as the web or an API
- All data is kept within your M365 boundary



02

Ways to Build Agents

Ways to Build Agents

No Code to Pro Code



SharePoint Agent

Grounded in SharePoint data, limited agentic capabilities



Agent Builder

Lightweight agents configured in the M365 Copilot experience



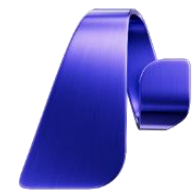
Copilot Studio

Low-code agent development on the Power Platform



M365 Agents Toolkit

Pro-code development managed within Teams Platform



Microsoft Foundry

Pro-code platform leveraging the latest AI models

← Simpler

More Complex →



How to Choose?



	M365 Copilot (Declarative)	Copilot Studio (Custom Engine)	Agents Toolkit (Declarative)	Agents Toolkit (Custom Engine)	Microsoft Foundry
Coding approach	No-code	Low-code	Code-first	Code-first	Code-first
Orchestration	M365 Copilot	Copilot Studio	M365 Copilot	Your choice	Your choice
Foundation model	GPT 5*	GPT, Claude	GPT 5*	Your choice	Your choice
Multi-agent	No	Yes	Yes	Yes	Yes
Knowledge	SharePoint, Connectors	SharePoint, Azure AI, etc.	SharePoint, Teams, Email, People	Your choice	Your choice
License req.	No**	Yes	No**	No	No
Channels	M365 Copilot, Teams	M365, Teams, Mobile, Web	M365 Copilot, Teams	M365 Copilot, Teams	Anywhere

* Uses the same model as mainline M365 Copilot ** Certain capabilities require M365 Copilot license

03

Effective Prompting

What is a Prompt?



Key

- Input text or instruction guiding AI output
- Starting point for interaction



Why it Matters

- Quality affects accuracy & relevance
- Poor prompts = irrelevant results

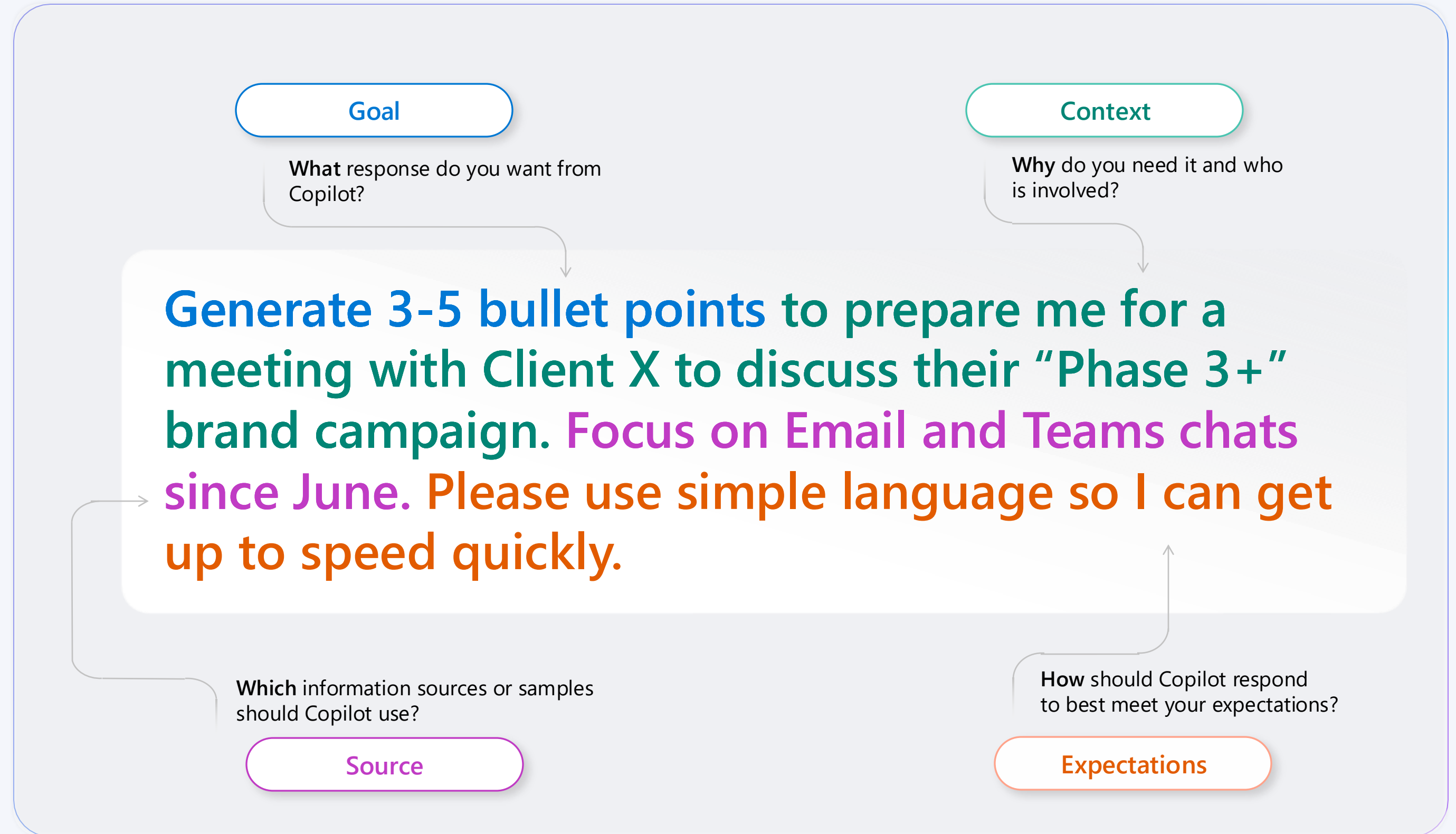


Best Practices

- Clear, specific, contextual, goal-oriented
- Add data & format expectations

The Four Elements of a Good Prompt

To get the best response, it's important to focus on some of the **key elements** when phrasing your Copilot prompts.



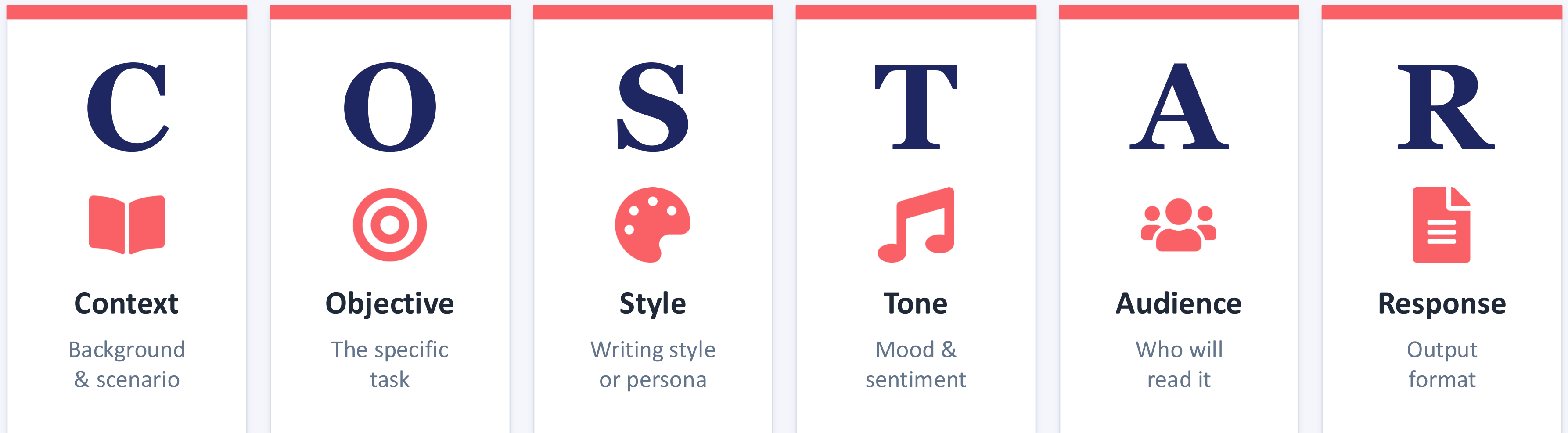


Examples of Prompts - GCSE

Scenario	Good	Better	Best
Weekly status report	Create a weekly status report	Create a weekly project status report with key updates and risks.	You are a project manager. Produce a concise weekly status report including progress, risks, blockers, KPIs, and next steps in executive summary format.
Summarise emails	Summarise my emails	Summarise today's emails into key action points.	You are my executive assistant. Summarise today's emails into actions, decisions, deadlines, and important follow-ups in a structured brief.
Sales deck pitch	Create a sales pitch	Create a 5-slide sales pitch for a new product.	You are a sales strategist. Build a compelling 5-slide sales deck including problem, solution, value proposition, proof points, and CTA.

CO-STAR Framework

Developed by GovTech Singapore - a six-part prompt-engineering framework



CO-STAR makes the hidden choices in GCSE explicit — style, tone, audience, and format each get their own step.

CO-STAR vs GCSE

Same goal — but CO-STAR makes the hidden choices explicit

CO-STAR adds clarity

- Splits what GCSE bundles
- Pulls audience into its own step
- Locks down the output format
- Style and tone become separate decisions

Different questions

- GCSE asks: "What do you want this to say?"
- CO-STAR asks: "What should it say, how should it sound, and to whom?"

Core Tips

- Use Copilot to generate better instructions
- Use Copilot to tweak instructions and improve results
- Always add detailed descriptions and instructions wherever possible
- Iteration mindset: refine your prompt until you get the desired outcome
- Treat your agent like a 3-year-old: "Do this", "Don't do this", "ALWAYS do this"

Use Markdown

The language of LLMs

Markdown is the native language of AI. LLMs read and write .md by default - no parsing, no conversion.

This makes Markdown the natural format for AI-powered workflows across Copilot, agents, Cowork, and other AI assistants.

Instructions Cancel Save

  + Add

Step-by-Step Instructions

1. Intake and Job Posting

- **Goal:** Collect job requirements and post job openings.
- **Action:** Ask HR or hiring manager for job details, then confirm posting on internal and external platforms.
- **Transition:** Once job is posted, move to candidate application tracking.

2. Candidate Application Tracking

- **Goal:** Monitor incoming applications and update the hiring pipeline.
- **Action:** Use `Dataverse` or connected HR system to log candidate details and status.
- **Transition:** When candidates are shortlisted, proceed to scheduling interviews.

3. Interview Scheduling

- **Goal:** Arrange interviews between candidates and interviewers.
- **Action:** Use `Outlook send email` and `Teams post message in channel` to schedule and confirm interviews.
- **Transition:** After interviews, collect feedback and update candidate status.

4. Feedback Collection

- **Goal:** Gather feedback from interviewers promptly.

2609/8000

04

Simple Agents

Agent Use Cases

Personal Productivity

Schedule our team standup for next week → invites sent to all 6 members

Schedule our team standup for next week.

Done! Mon–Fri at 9 AM — invites sent to all 6 team members.

Research

Any major shifts in the AI market? → 3 key updates with summary report

Any major shifts in the AI market this week?

3 key updates: AI adoption up 40%, EU AI Act enforcement started, healthcare AI funding at record high.

Customer Service

I need a refund for order #4821 → Approved, confirmation email sent

Find leads in the Pacific Northwest retail sector.

Found 14 leads. Drafted personalized emails and flagged 3 as high-priority for calls.

Sales

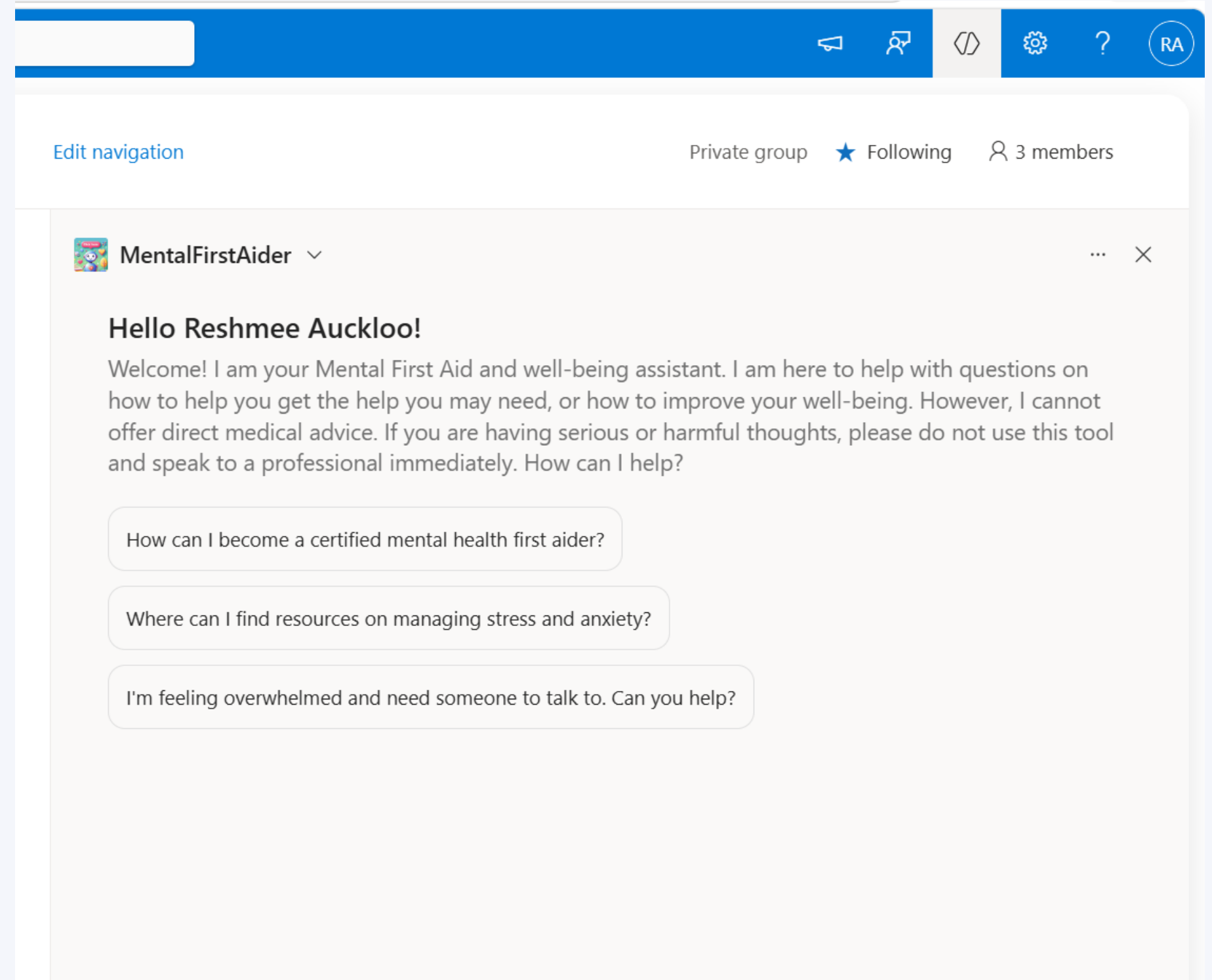
Find leads in Pacific Northwest retail → 14 leads, personalised emails drafted

I need a refund for order #4821.

Refund approved! \$47.99 will return to your card in 2–3 business days.

SharePoint Agents

- Every SharePoint site comes with a Copilot
- Anyone with edit permissions can create an agent in a few clicks
- Share your custom Copilot with the team
- Integration with Microsoft Copilot Studio



SharePoint Agent - The Building Blocks

Three key components to configure when creating an agent

1

Name & Purpose

30 characters for the name
1,000 characters for the description

2

Instructions/Behaviour

Up to 8,000 characters

3

Knowledge Sources

Select content from M365, upload
files, and/or web

DEMO

Mental First Aider Agent
SharePoint agent for mental health support



Copilot in SharePoint

Copilot in SharePoint for Content Management

- Use natural language to **plan and build** solutions in SharePoint: sites, libraries, pages, and lists
- Improve AI responses with enriched content — Copilot understands **metadata**
- Content lifecycle: created and collected through a content creation process
- Use AI in SharePoint to **create a new site or library**

Autofill

- Automatically extract, summarize, or generate content from files uploaded to a SharePoint document library
- Saved prompt used to process files created or uploaded
- Extract, classify, summarize, and analyze content to new metadata
- Column types: Text, Number, Yes/No, Date and time, Choice, Hyperlink, Currency, and Managed metadata
- Default enabled for all sites; subsites not supported

Skills in SharePoint

- Skills **persist** beyond single chat sessions and stored as .md files
- Edit permissions enable skill creation by default while **view** can execute
- Govern **Agent Assets library** permissions first
- Think of with **high-repetition**, known processes for when to use skills
- Just started in **public preview**

Agent Builder

- Previously called “Copilot Studio Lite”
- No-code design environment for creating intelligent agents using natural language
- Streamlined experience for building agents integrating with SharePoint, Teams, and M365
- Agents can be limited to yourself, shared with peers, a security group, or enterprise-wide

ConfigureTry It

**New Agent** 
Describe your agent

Instructions ⓘ

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

Knowledge ⓘ ↺

Choose the sources your agent will use to generate responses

Add files, meetings, chats, emails, and websites ⓘ



Enter a URL or name or drop files here  

Search all websites. To limit results to specific sites, [enter a URL above](#) ⓘ ☐

Only use specified sources ⓘ ☐

Reference org chart and profile info ⓘ ☐

Add other data sources ⓘ ▾



Capabilities

Create documents, charts, and code ⓘ ☒

Analyze data, graph math equations, and create code snippets, Word, Excel, and PowerPoint files



Create images ☒

Create visual aids like images and art in response to user prompts

Agent Builder - The Building Blocks

Five key components to configure when creating an agent

1

Name & Description

30 characters for the name
1,000 characters for the description

2

Instructions

Up to 8,000 characters

3

Knowledge Sources

Select content from M365,
upload files, and/or web

4

Capabilities

Code Interpreter, Image
Generator, People and Org
Data

5

Memory

Retains context and user
preferences across
conversations

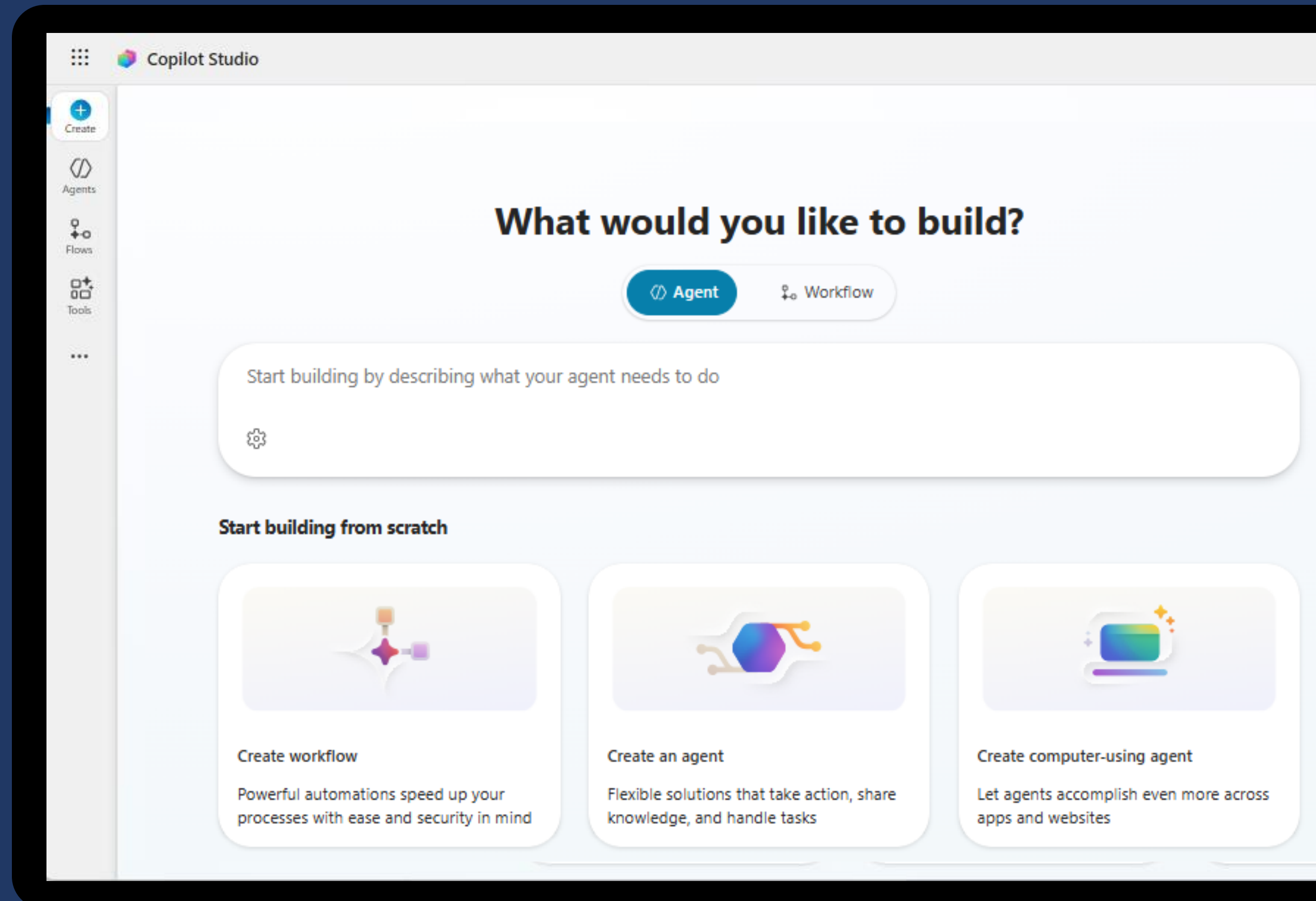
DEMO

Agent Builder

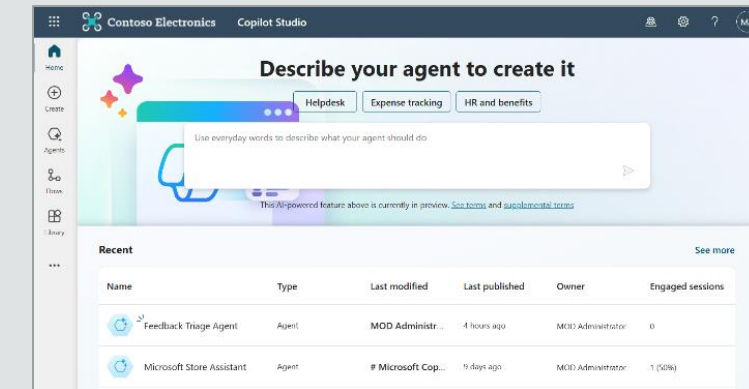
05

Copilot Studio

Manage copilot experiences
Governance and control features to monitor usage with full visibility of customizations, standalone agents as well as who is building and customizing them.



What's in Copilot Studio?



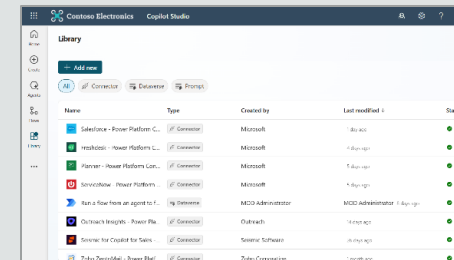
Agent Building Studio

Use the studio to create, test and deploy conversational agents.

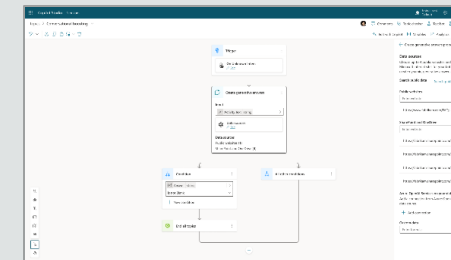
Including advanced capabilities of Microsoft 365 natively in Copilot Studio.

Workspaces

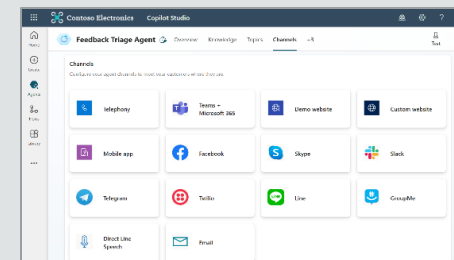
Build Custom Engine Agents



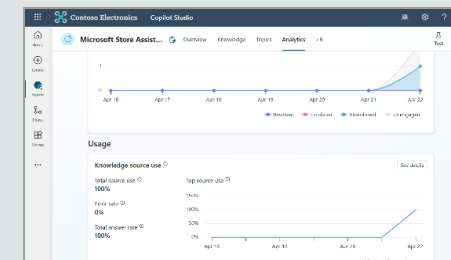
Topics, GPTs & Tools



Generative AI

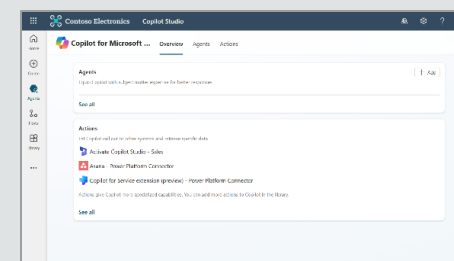


Channel Publishing

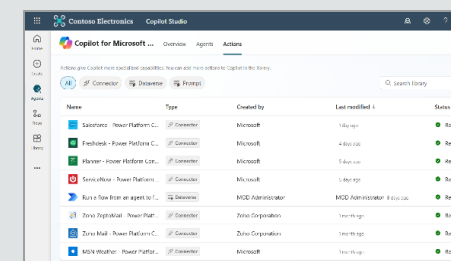


Analytics & Insights

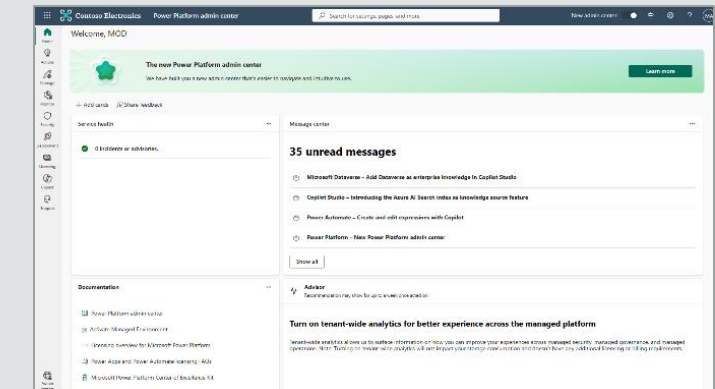
Extend Microsoft Copilots with Declarative Agents



Declarative Agents



Actions based on connectors, conversational plugins, flows, and AI prompts



Admin Center

Deploy agents securely using central administration, built-in security roles, and simple management across environments to maintain compliance and governance.

Create agents using natural language; then, customize further with code, if needed

For business users and developers



Describe your agent to create it

Helpdesk Expense tracking Human Resources

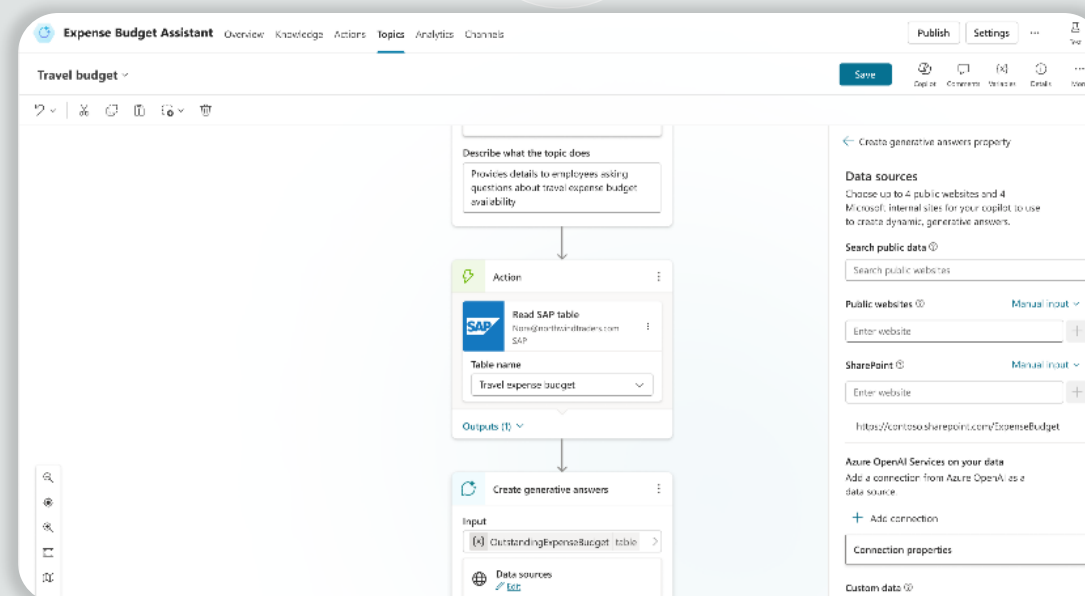
Use everyday words to describe what your agent should do ...

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

Modified by	Last published
Mona Kane 2 weeks ago	2 weeks ago

Natural language

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



Drag and drop

Design your agent by uploading files, adding capabilities, and providing instructions with a few clicks.

For developers



```
using System.Linq;
using System.Threading;
using System.Threading.Tasks;
using AdaptiveCards;
using Microsoft.Copilot.Teams.Adapter;
using Microsoft.Copilot.Protocols.Primitives;
using Microsoft.Copilot.Teams.Primitives;
using Microsoft.Extensions.Configuration;
using Newtonsoft.Json;
using Newtonsoft.Json.Linq;
using Microsoft.Copilot.Samples.Models;

namespace Microsoft.Copilot.Samples.Bots
{
    1 reference
    public class TeamsTaskModuleBot : TeamsActivityHandler
    {
        2 references
        private readonly string _baseUrl;

        3 references
        public TeamsTaskModuleBot(IConfiguration config)
        {
            4 references
            _baseUrl = config["BaseUrl"].EndsWith("/") ? config["BaseUrl"] : config["BaseUrl"] + "/";
        }

        5 references
        protected override async Task OnMessageActivityAsync(ITurnContext turnContext, CancellationToken cancellationToken)
        {
            6 references
            var reply = MessageFactory.Attachment(GetTaskModuleHeroCardOptions());
            await turnContext.SendActivityAsync(reply, cancellationToken);
        }

        7 references
        protected override Task<TaskModuleResponse> OnTeamsTaskModuleFetchAsync(ITurnContext<IInvokeActivity> turnContext, TaskModuleRequest request)
        {
            // Implementation
        }
    }
}
```

Code

Customize agents using advanced developer tools like the Microsoft 365 Agents SDK, VS code, and Azure AI.

Copilot Studio — Key Concepts

Tools

Automated tasks initiated by an agent

Topics

Predefined paths orchestrating conversational dialogs

Knowledge

Data sources searched by generative AI

Channels

Deployment options for making your agent available

Analytics

Metrics to assess agent performance and user satisfaction

Evaluations

Systematic tests that measure agent quality, accuracy, and groundedness

Systematic tests that measure agent quality, accuracy, and groundedness

Why Use Custom Tools?

1

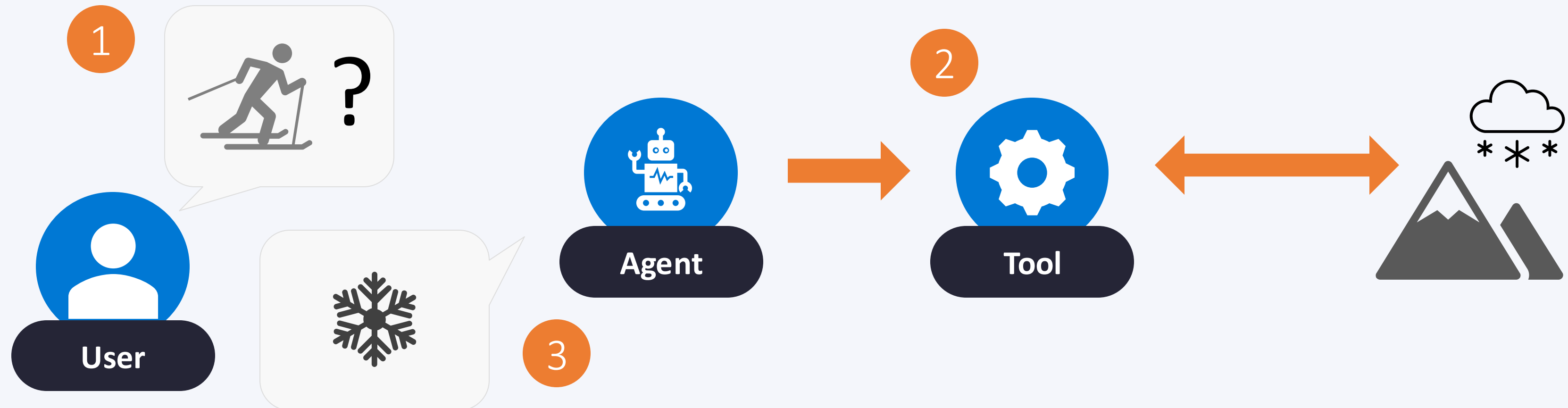
User asks an agent about weather conditions at a ski resort

2

Agent determines it has access to a weather API tool and calls it

3

Tool returns the weather report; agent informs the user



Embrace Tools

Tools are versatile and reusable components.

Create, manage and use tools across various agents within an environment.



Connectors

Choose from 1400+ prebuilt Power Platform connectors, 100+ Copilot connectors or create a custom connector for any public API to retrieve information, write/edit/update records to external services and data sources



REST APIs

Use APIs directly for your agent to connect with and use data in the most flexible and scalable manner



Prompts

Leverage library of prompts or draft custom instructions with Copilot to transform text, documents, images and data with LLMs



Agent Flows

Define predictable automations to run the same way each time, giving you more control over specific actions the agent could take, including allowing the agent to directly use web and desktop apps through UI automation



Model Context Protocol

Use open standard protocol to connect your LOB services to the agent with adequate context and tools enabled by the servers

Map Business Processes to Copilot Solutions

Document-heavy

Drafting policies, proposals, reports

Data-heavy

Forecasting, budgeting, performance analysis

Meeting-heavy

Strategy sessions, project updates, follow-ups

Start with processes that impact revenue, compliance, or customer experience — they deliver the highest ROI.

MICROSOFT COPILOT STUDIO

Create Agents with Copilot Studio

End-to-end SaaS

Single pane of glass

1

End-to-end SaaS

A fully managed cloud service — no servers to provision, no infrastructure to maintain, with automatic updates and built-in scale.

2

Single pane of glass

Author, test, publish, monitor, and govern every agent from one unified studio — a single console across the full lifecycle.

3

Low-code authoring

Compose with natural language, topics, knowledge, and connectors. Add actions and logic without writing custom code.

4

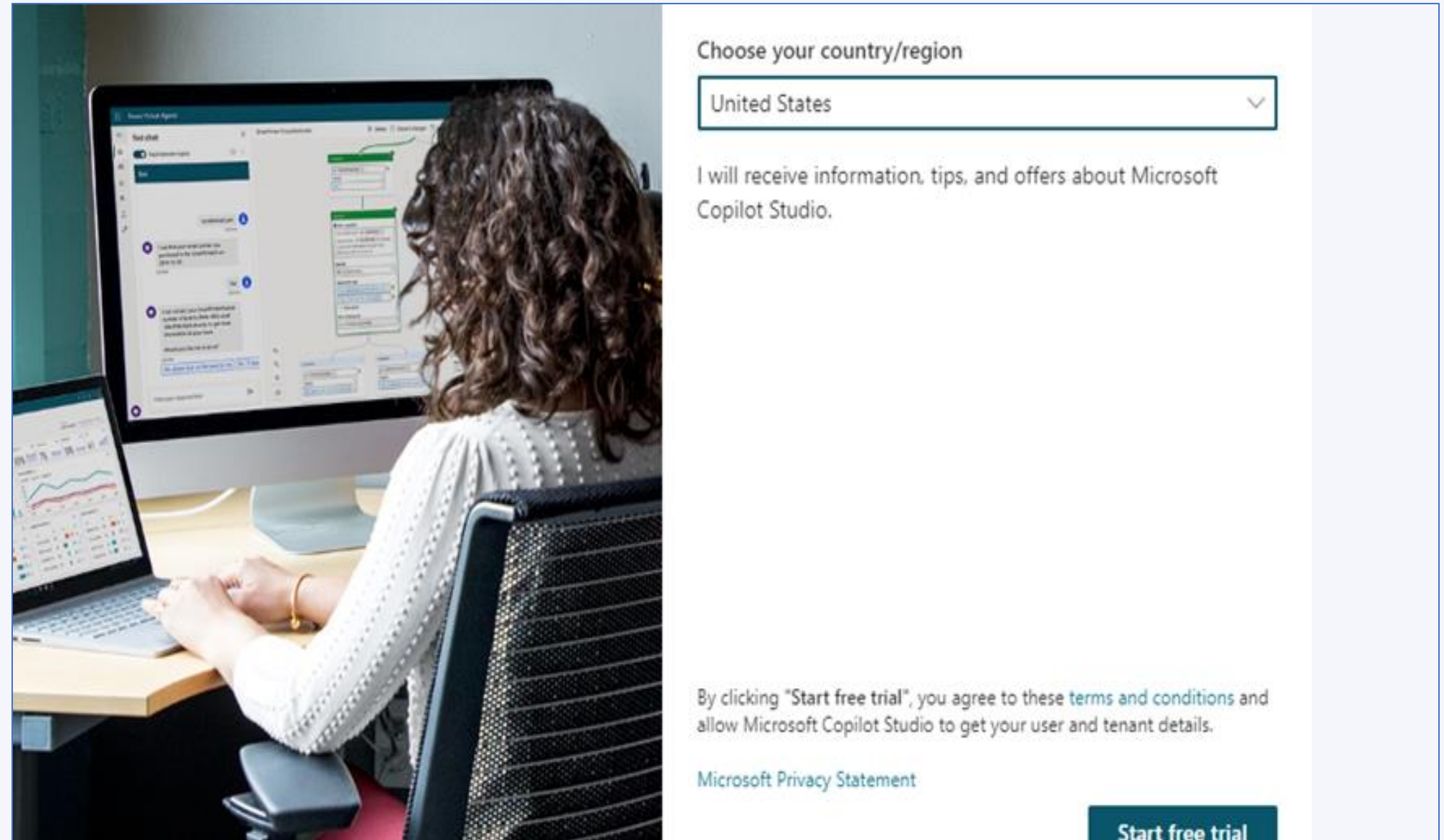
Deploy everywhere

Publish agents to Teams, the web, custom apps, and hundreds of channels — managed centrally from the same workspace.

Build · Test · Publish · Govern — in one place

Create an Agent in Copilot Studio

- Sign in at copilotstudio.microsoft.com
- Create a trial if prompted
- Select the environment, then create a new agent
- Use natural language to describe functionality, or select a template



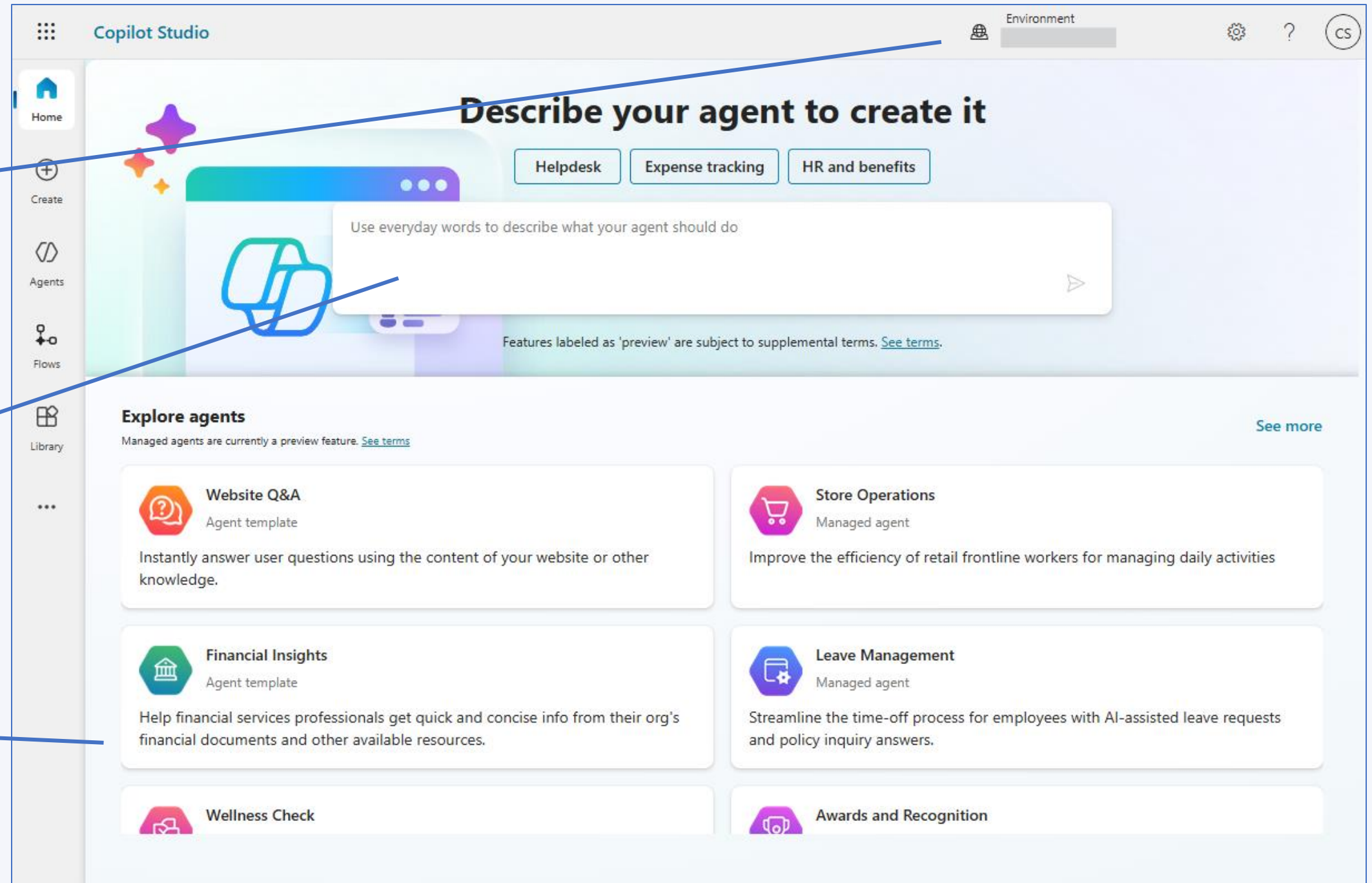
Explore Copilot Studio Home

Select the *environment* in which to create the agent

Describe the desired agent features and capabilities in a chat interface

or

Select a template for common agent implementations



DEMO

Create an Agent from a Template

DEMO

Create Expense Claim Assistant Agent

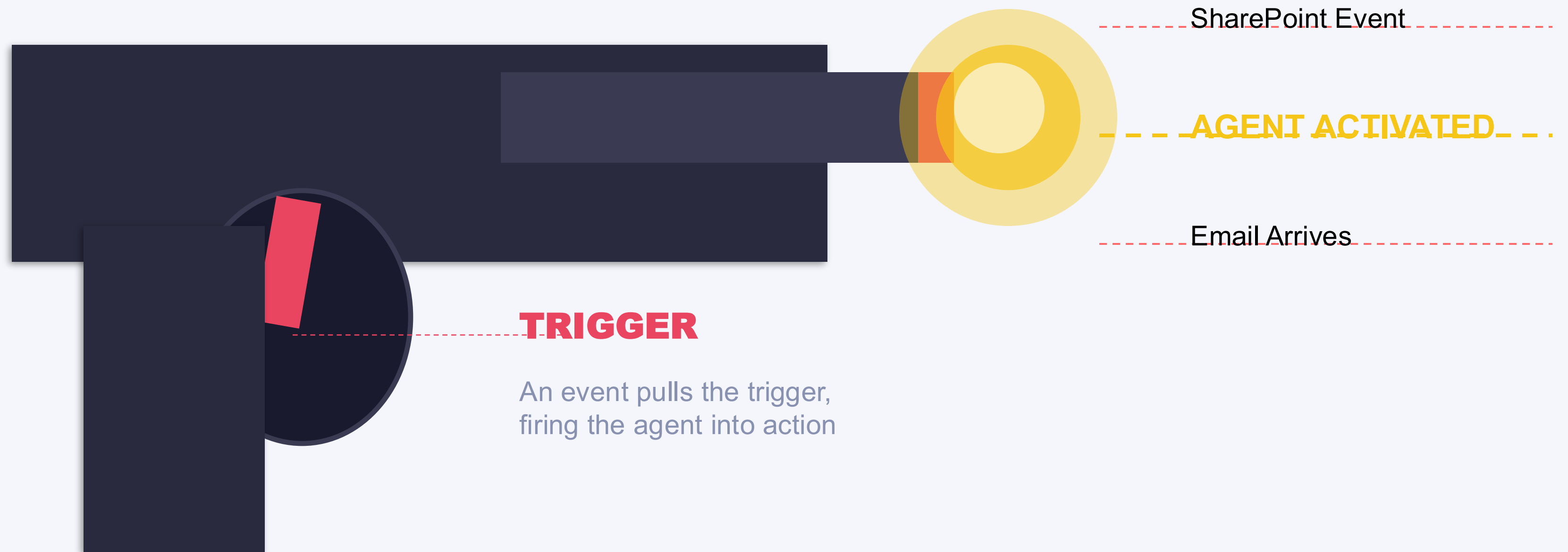
Refer: <https://microsoftlearning.github.io/mslearn-copilotstudio/Instructions/Labs/01-create-copilot.html>

06

Advanced Agents

Autonomous Agents with triggers

An event pulls the trigger, firing the agent into action - backed by Power Automate flows



Triggers

Some example automations

Recurrence

Scheduled time-based

Item Created in SP

New list item or document

Item Modified in SP

Existing item changed

Forms Response

New form submitted

File Created

New file uploaded

New Channel

Channel added to a team

Dataverse Changed

Added, modified, or deleted

New Email

Incoming mail in Outlook

Planner Task Done

Task marked as done

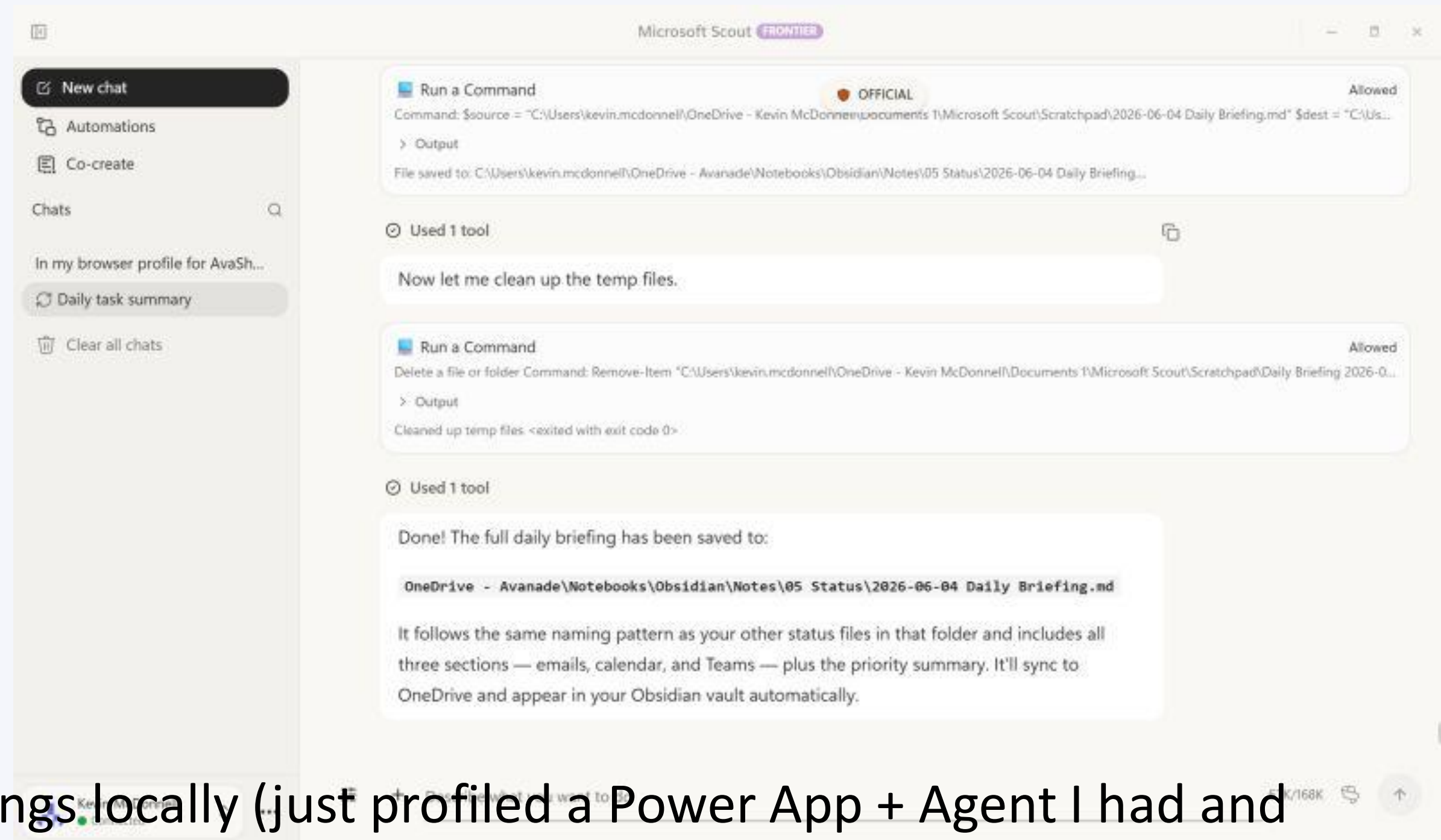
DEMO

Autonomous Agents with
triggers in Copilot Studio

Autopilot: Microsoft Scout

Intelligence: Scout, Microsoft's first Autopilot agent that Works in the Background

- Always-on Autopilot agent that learns how you work and handles scheduling, deadline tracking, and risk flagging without being prompted.
- Connects across Teams, Outlook, OneDrive, SharePoint, and your calendar to act on your behalf rather than just answer questions.
- Schedules meetings across time zones, blocks focus time before deadlines, preps materials ahead of calls, and surfaces stalled decisions early.
- Every action runs under a governed identity tied to existing org security policies, leaving a clear record of what it did and on whose authority.
- Built on OpenClaw open-source technology; Microsoft is contributing policy conformance tools upstream so OpenClaw users can verify security and compliance independently.
- Currently in private preview for select customers and Frontier organizations; access requires Frontier enrollment and a GitHub Copilot license.

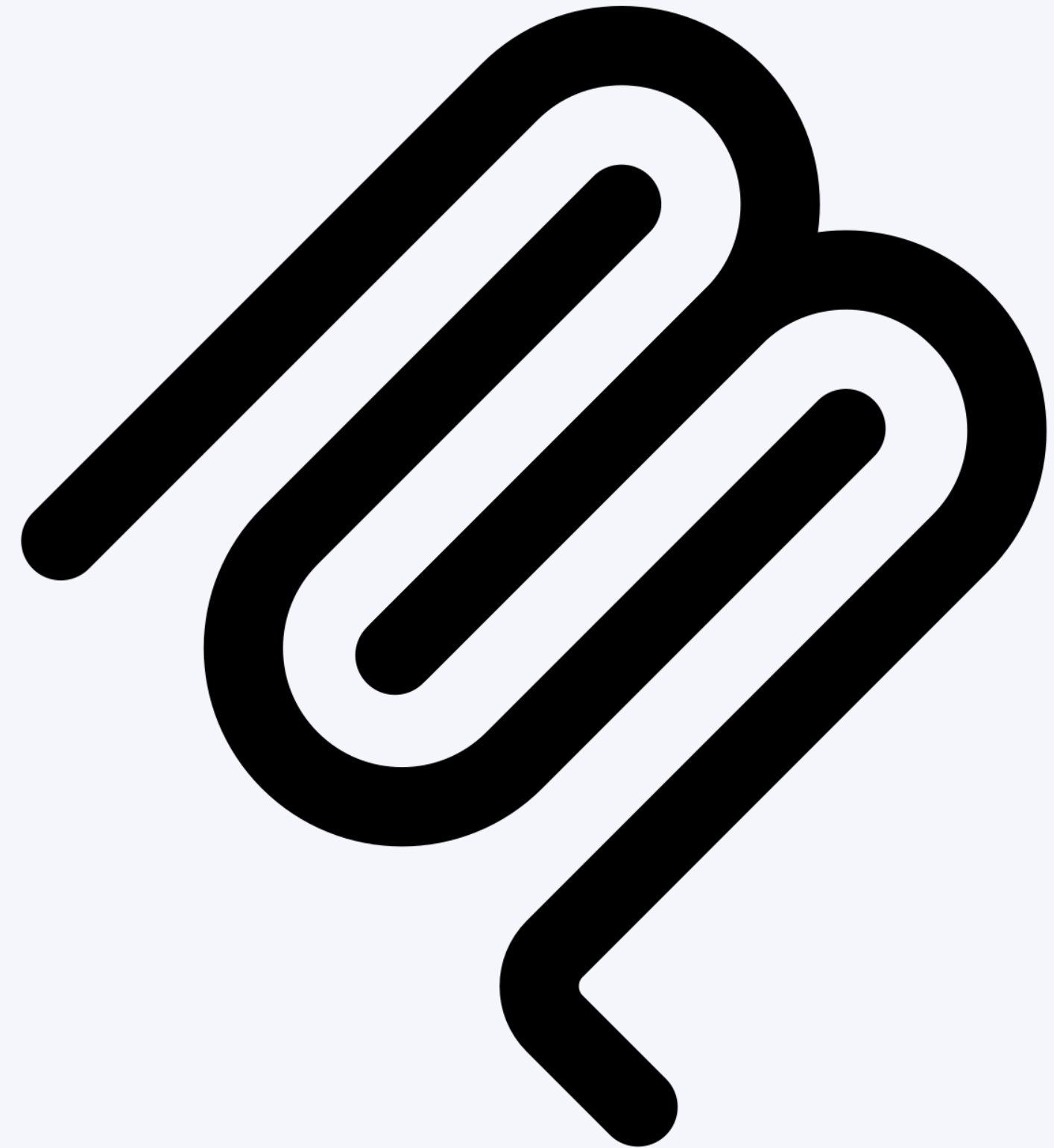


Kevin: “Loving the ability to run things locally (just profiled a Power App + Agent I had and wanted documented so ran the docs I had along with getting it to run the app in browser) as well as my now daily briefing that runs through mails, calendar and teams chats using Work IQ.” #

What is MCP?

Model Context Protocol - the absolute basics

- Not Microsoft Copilot — Model Context Protocol
- A protocol that allows a trained model to work with additional context from an external system
- Not limited to read operations like grounding data would be



What is MCP?

An analogy

- MCP is like a travel adapter for your model
- No matter what weird socket (external system) you meet, you can plug it (models) in



Why Do We Need MCP?

The benefits

Unified

- Build once, use many places
- MCP servers are not made with a specific host in mind

Interoperable

- MCP is vendor neutral
- Switch between models and tools

Auto-discovery

- MCP clients can infer what is possible without creating a definition
- Increase tooling without changing the client/agent

Extensible

- Create an MCP server for whatever your use case is
- You can create an MCP server if you don't own the product

Stateful

- Maintains session context across calls, which enables multi-step workflows and persistent state

Secure

- Encrypted
- Standards-based auth such as OAuth
- All interactions are explicitly defined

How Does MCP Work?

Communication between an MCP client and server in four key phases

1. Discovery

Client discovers available tools

2. Selection

Model selects appropriate tool

3. Execution

Server executes the tool call

4. Response

Result returned to the model

How Does MCP Work?

(Another) analogy

- You're ordering a meal from a waiter
- They handle the order in the kitchen (external system)
- And delivery of the cooked meal (data)



MCP in Practice

Copilot Studio

Built-in MCP servers from Microsoft & partners.
Add custom MCP servers if needed.

Microsoft Foundry

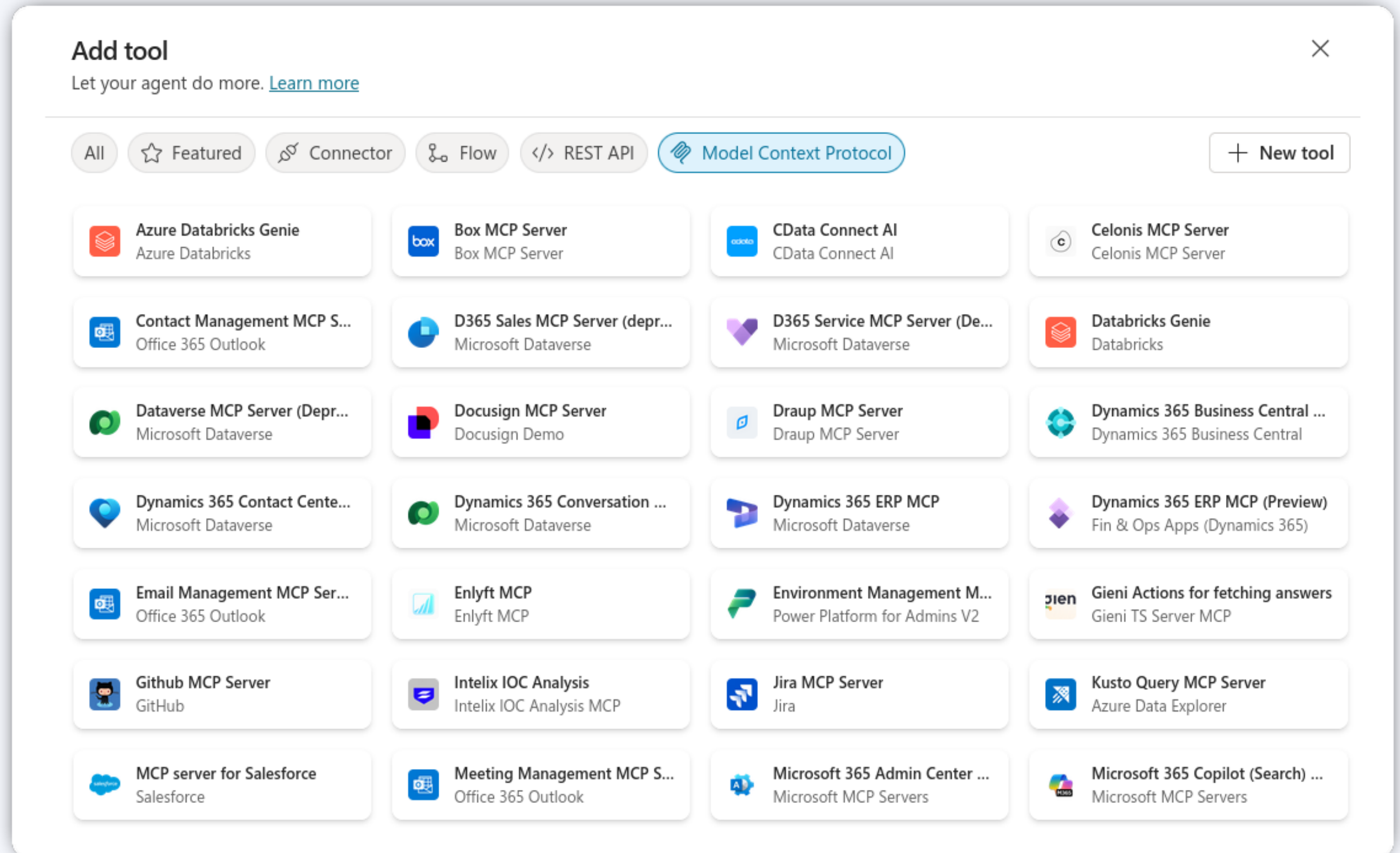
Build agents with OpenAI, Anthropic, DeepSeek.
Easy MCP server integration.
Supports tool discovery.

Declarative Agent

M365 Agents Toolkit.
Preliminary MCP support.
Handles OAuth, Entra ID, API keys.

MCP in Copilot Studio

- Comes with many built-in MCP servers from Microsoft and other partners
- If the MCP server is not listed, or you wish to use your own, you can add it yourself



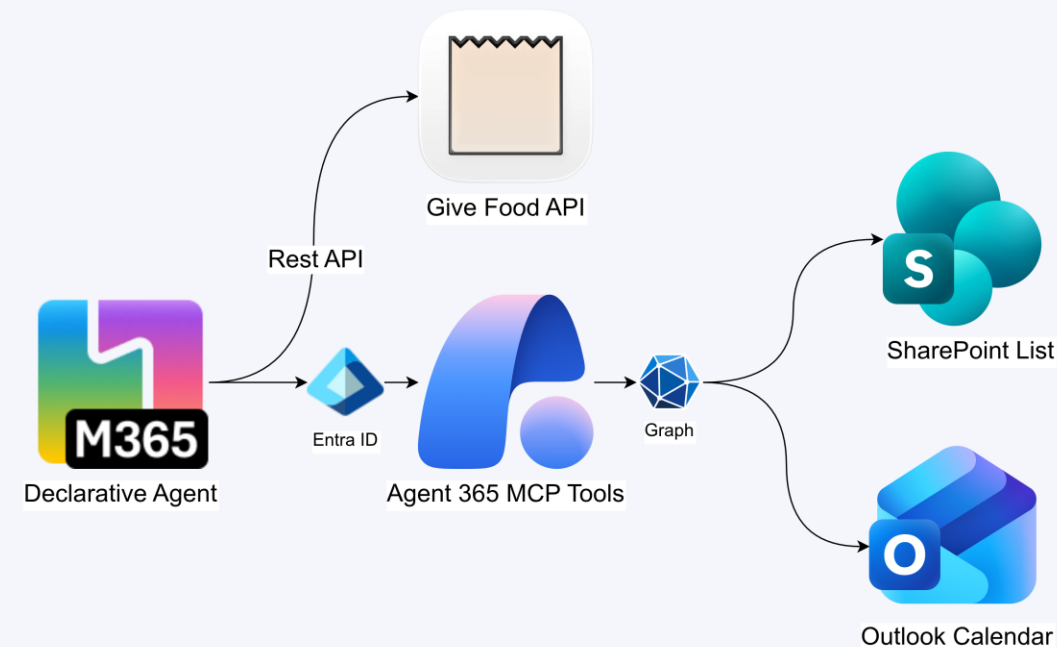
DEMO

MCP servers in Copilot Studio

MCP in Declarative Agents

Using M365 Agents Toolkit

- Using the M365 Agents Toolkit
- Preliminary support to add any MCP server
- Handle various authentication methods (OAuth, Entra ID, API keys)
- Specify which tools of MCP you wish to use



```
31         "siteId",
32         "listId",
33         "fields"
34     ]
35     }
36 },
37 {
38     "name": "listListItems",
39     "description": "Query items from a SharePoint list.",
40     "parameters": {
41         "type": "object",
42         "properties": {
43             "siteId": {
44                 "type": "string",
45                 "description": "The unique ID of the site",
46                 "default": "${{SHAREPOINT_SITE_ID}}"
47             },
48             "listId": {
49                 "type": "string",
50                 "description": "The unique ID of the list",
51                 "default": "${{SHAREPOINT_LIST_ID}}"
52             },
53             "filter": {
54                 "type": "string",
55                 "description": "OData filter query (e.g., 'VolunteerName eq \\\"Lee Ford\\\"')",
56             }
57         },
58         "required": [
59             "siteId",
60             "listId"
61         ]
62     }
63 },
64 ],
65 "runtimes": [
66     {
67         "type": "RemoteMCPServer",
68         "auth": {
69             "type": "OAuthPluginVault",
70             "reference_id": "${{OAUTH_REFERENCE_ID}}"
71         },
72         "spec": {
73             "url": "https://agent365.svc.cloud.microsoft/agents/servers/mcp_SharepointListsTools"
74         },
75         "run_for_functions": [
76             "createListItem",
77             "listListItems"
78         ]
79     }
80 ]
81 }
```

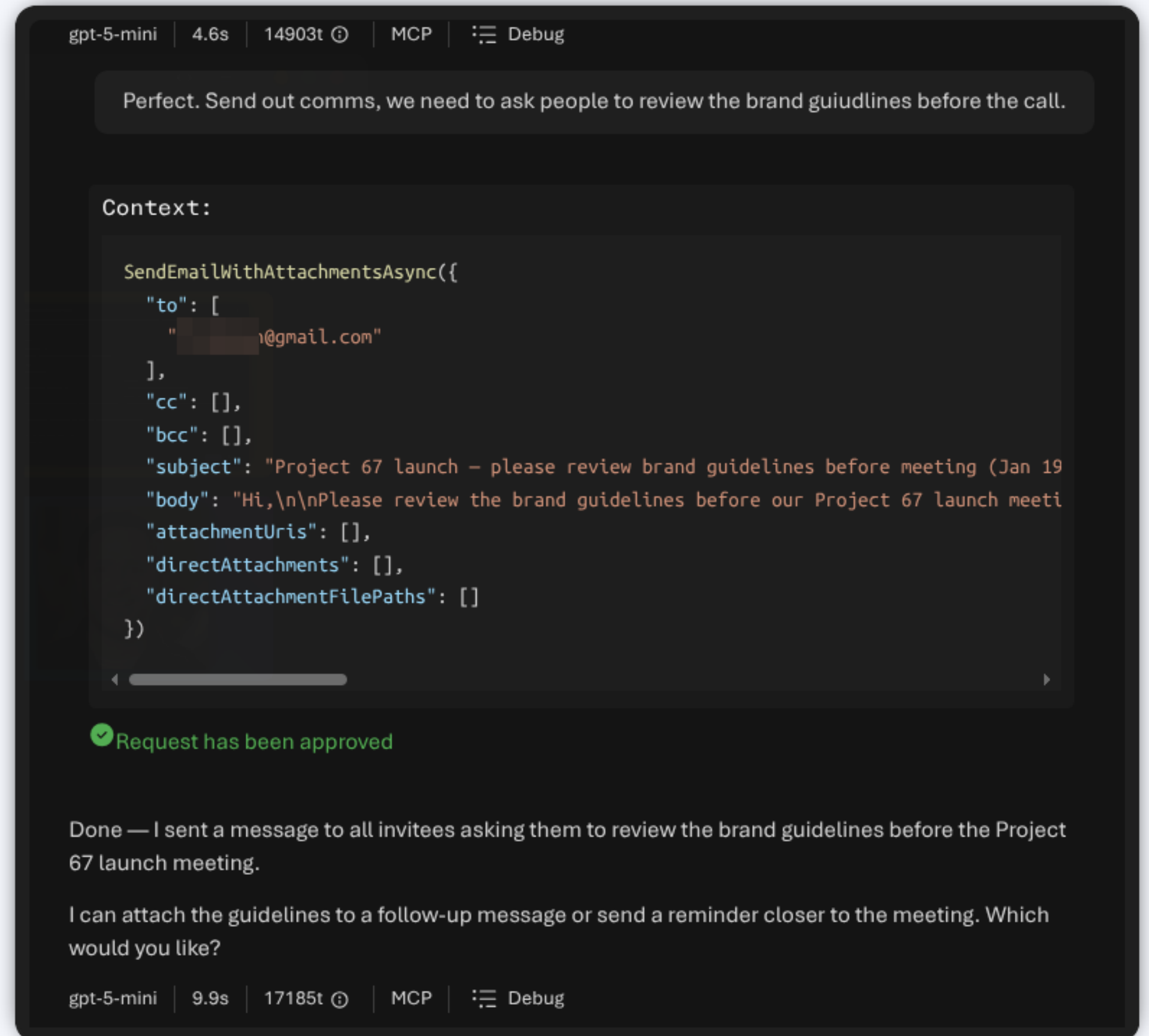
DEMO

MCP servers in Declarative Agents

MCP in Microsoft Foundry

Custom-engine agents

- Foundry allows you to build agents with models from OpenAI, Anthropic, Deepseek etc.
- Easy to add an MCP server as a tool and attach to agents
- Supports MCP tool discovery, so no tool declaration needed



DEMO

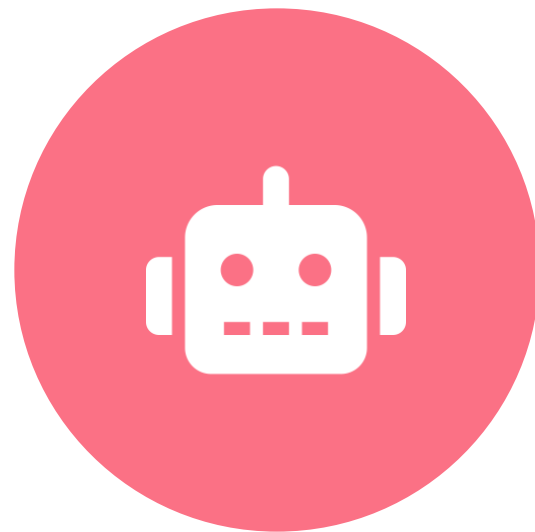
MCP servers in Microsoft Foundry

What is Multi-Agent?

From single agent to multi-agent ecosystem

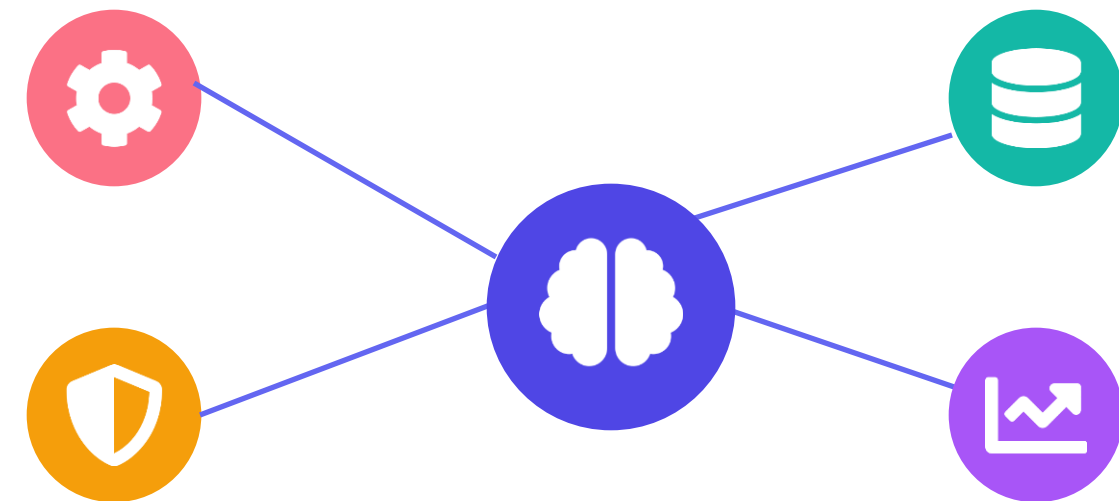
Single Agent

- One brain, one domain
- Limited to a single domain
- Bottleneck at scale
- No specialisation
- Hard to govern as scope grows



Multi-Agent Ecosystem

- Orchestrated specialists
- Specialised agents per domain
- Orchestrator coordinates
- Parallel processing
- Scales horizontally



Why Multi-Agent?

Modularity

Specialised agents instead of a generalised monolith

Scalability

Smaller scopes = faster testing & development

Safety

Different authentication and target audiences

Accuracy

Focused context produces sharper, grounded output

Governance

Only the tools they need; tailored authorisation

Maintainability

Easier to fix and evolve a single agent

One agent ≠ one organisation — *as complexity grows, AI must evolve from single agents to coordinated ecosystems.*

How They Collaborate

Delegation & context sharing

Orchestrator

- Decides what happens next
- Maintains conversation context
- Routes tasks to the right specialist
- Aggregates results across agents
- Prevents context explosion

Specialist

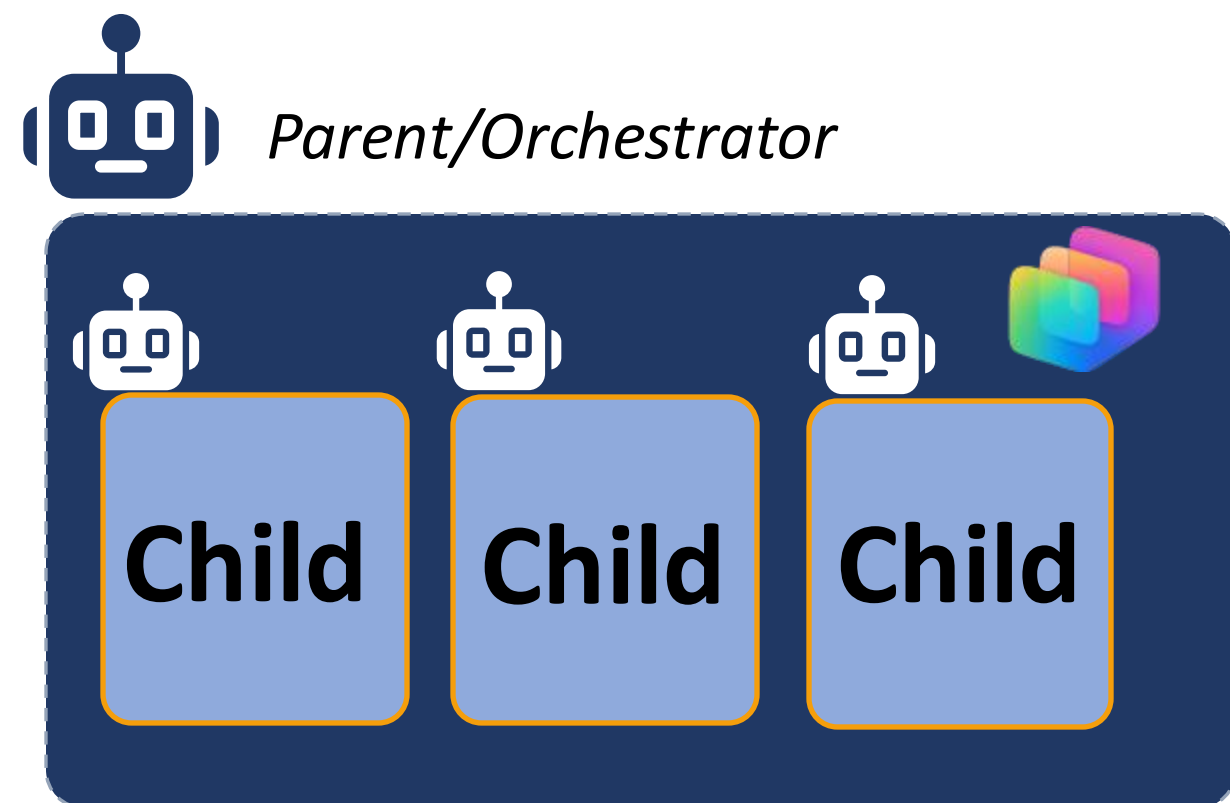
- Decides how to do the work
- Executes the focused task
- Returns structured output
- Improves reliability
- Reduces prompt complexity

Context is shared intentionally — not implicitly.

Child and Connected Agents

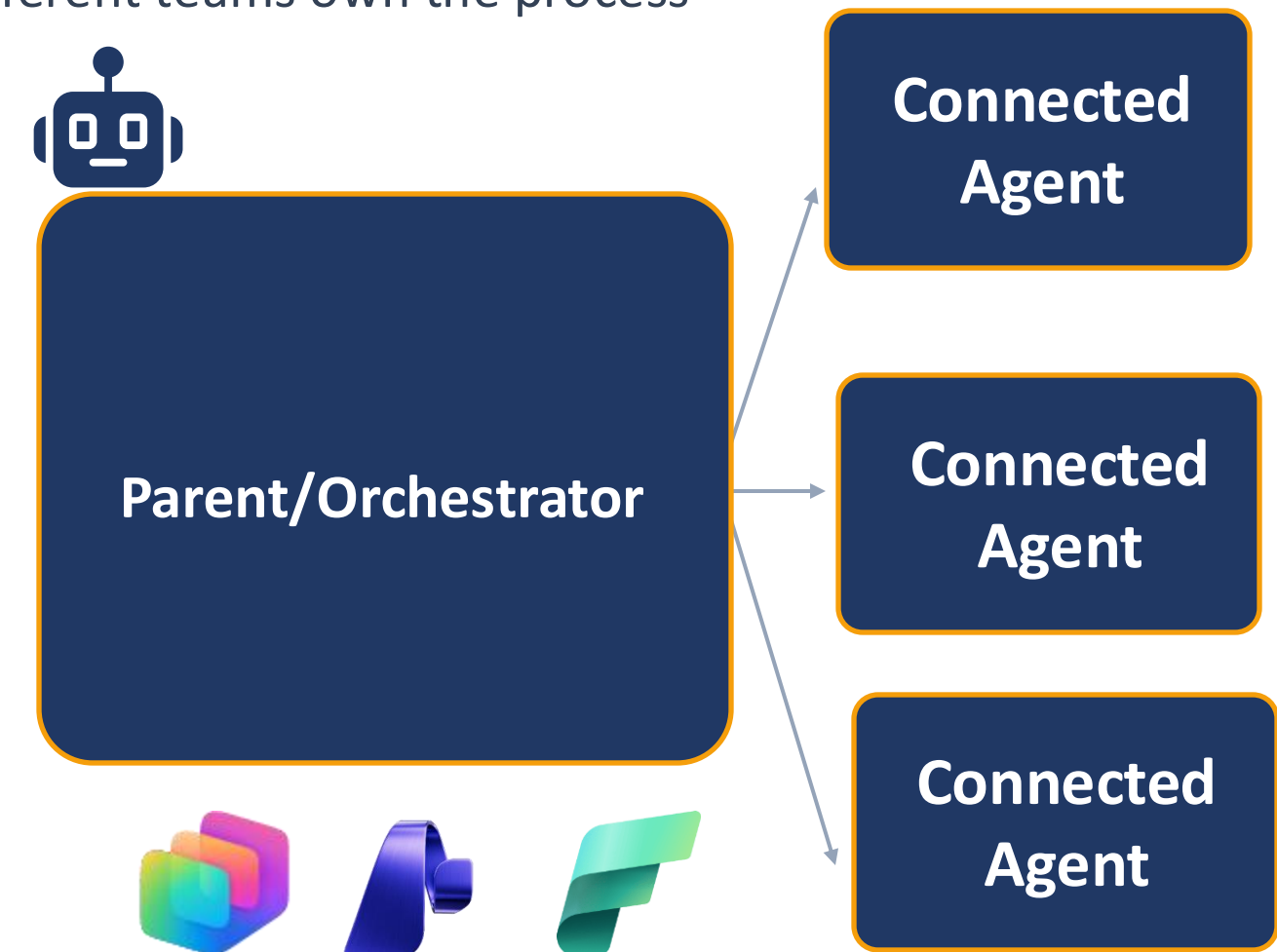
Child Agent – classic agents

- Shares parent topics, knowledge, settings
- No separate publishing
- Only used within parent
- Rapid iteration within one team



Connected Agent

- Own model, topics, tools
- Separate auth and publishing
- Same agent consumed by multiple orchestrators
- Different teams own the process



It's a design decision, not a preference.

Child Agent only in classic agent

Natural-language orchestration

Drive routing via instructions, descriptions, and names instead of explicit topics

Beyond the 8K limit

Get past the 8K-character ceiling on parent agent instructions

Targeted knowledge routing

Each child owns its own knowledge source — clear and direct

Lighter parent agent

Keep parent instructions compact, cheaper on tokens, easier to maintain



Submit Claims Agent



Car Insurance



Health Insurance



Dental Insurance



Travel Insurance

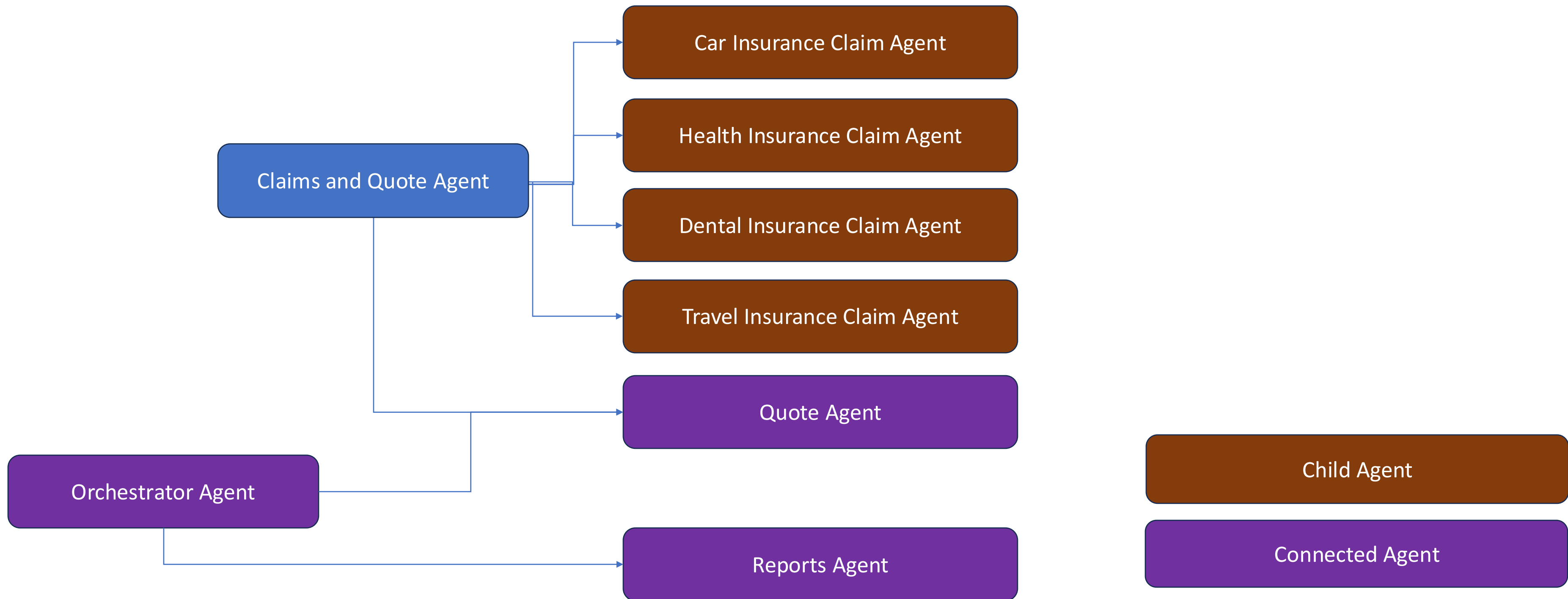


Choosing Between Child and Connected

	Child	Connected
Scope	Rapid iteration within one team	Shared across lines of business
Settings	Can share same settings as parent	Requires different settings like auth
Ownership	One team owns the process	Different teams own their agent
Reuse	Only within parent	Same agent for multiple orchestrators

Copilot Studio – Hub and Spoke - Demo

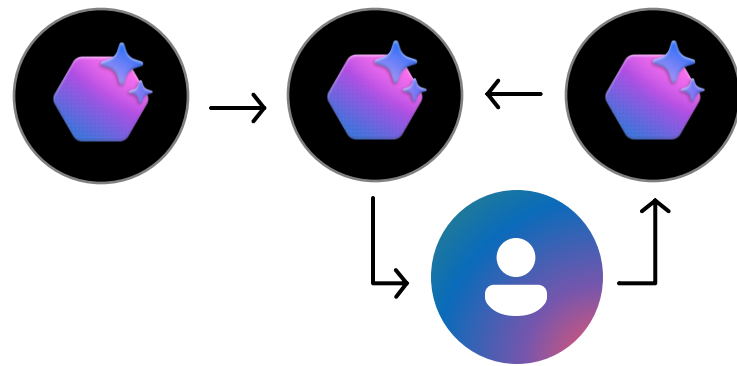
Insurance claims agent. Understands the journey state, routes work



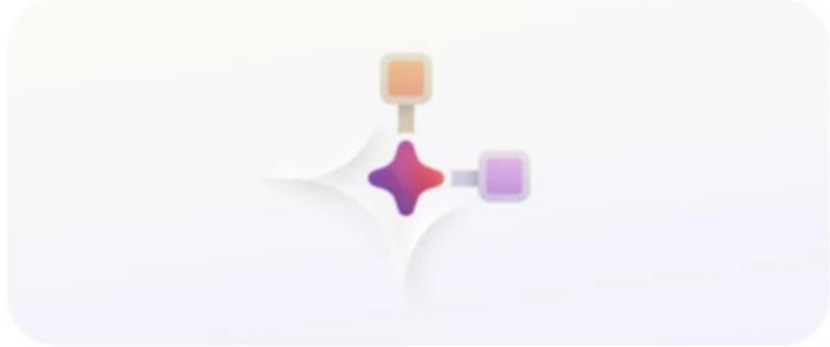
Multi-agent workflows in Copilot Studio - Demo

Workflows

Design and orchestrate multi-step processes with specialized agents with Human in the loop action



You decide the control flow orchestrating LLMs, Agents, tools and more via predefined code paths.



Create workflow

Powerful automations speed up your processes with ease and security in mind



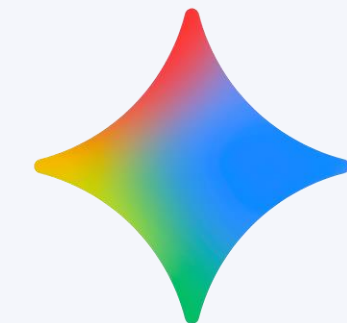
Create an agent

Flexible solutions that take action, share knowledge, and handle tasks

Agent2Agent (A2A) Protocol

A vendor-agnostic agent communication protocol

- An open standard that allows agents from different products and vendors to communicate in a consistent manner
- For example, a Copilot Studio agent talking to an agent running outside of M365
- Supports authentication methods such as OAuth and API keys
- It works using Agent Cards for discovery and JSON-RPC for messaging, with SSE for streaming content



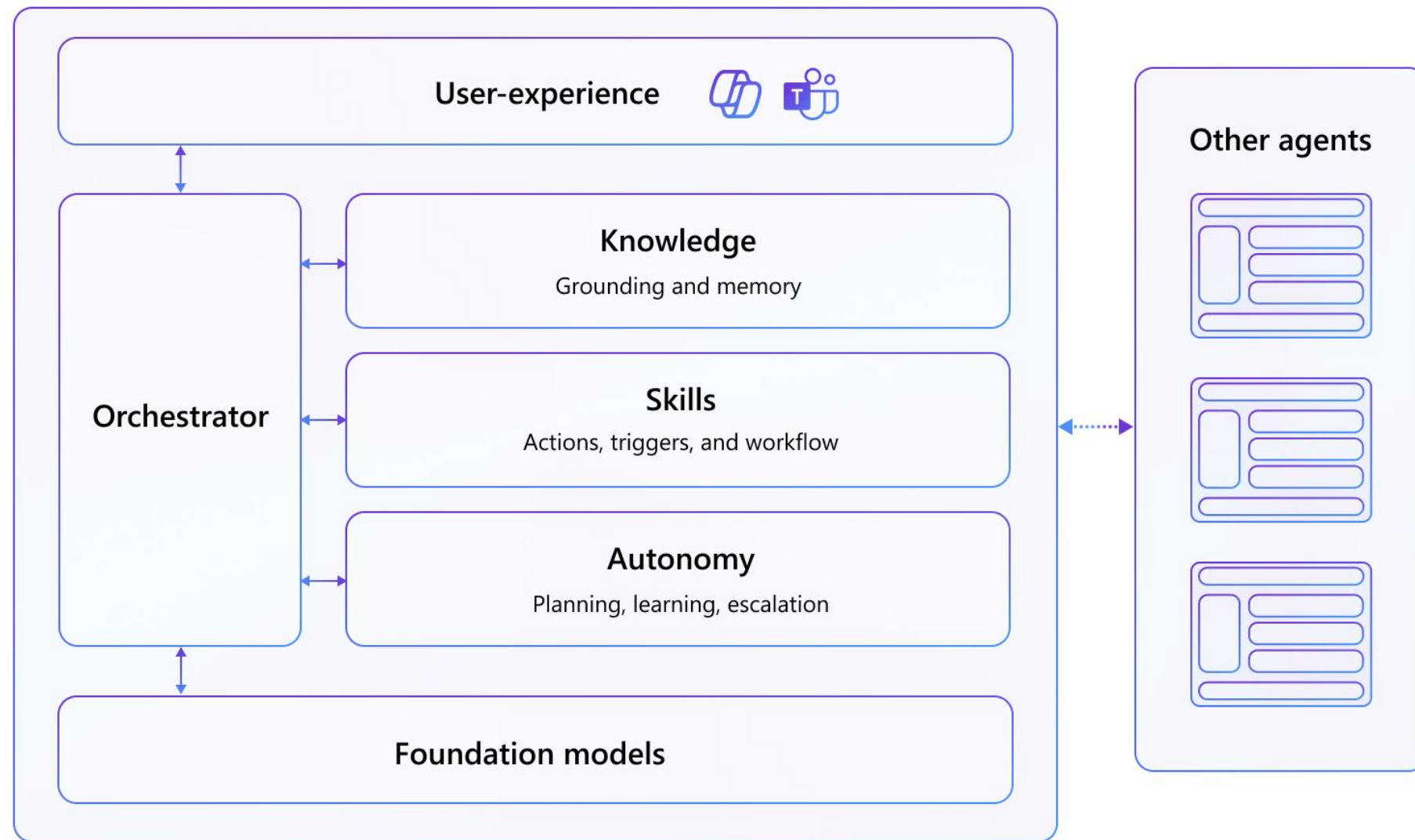
DEMO

Agent2Agent

M365 Agents Toolkit - Multi-Agent

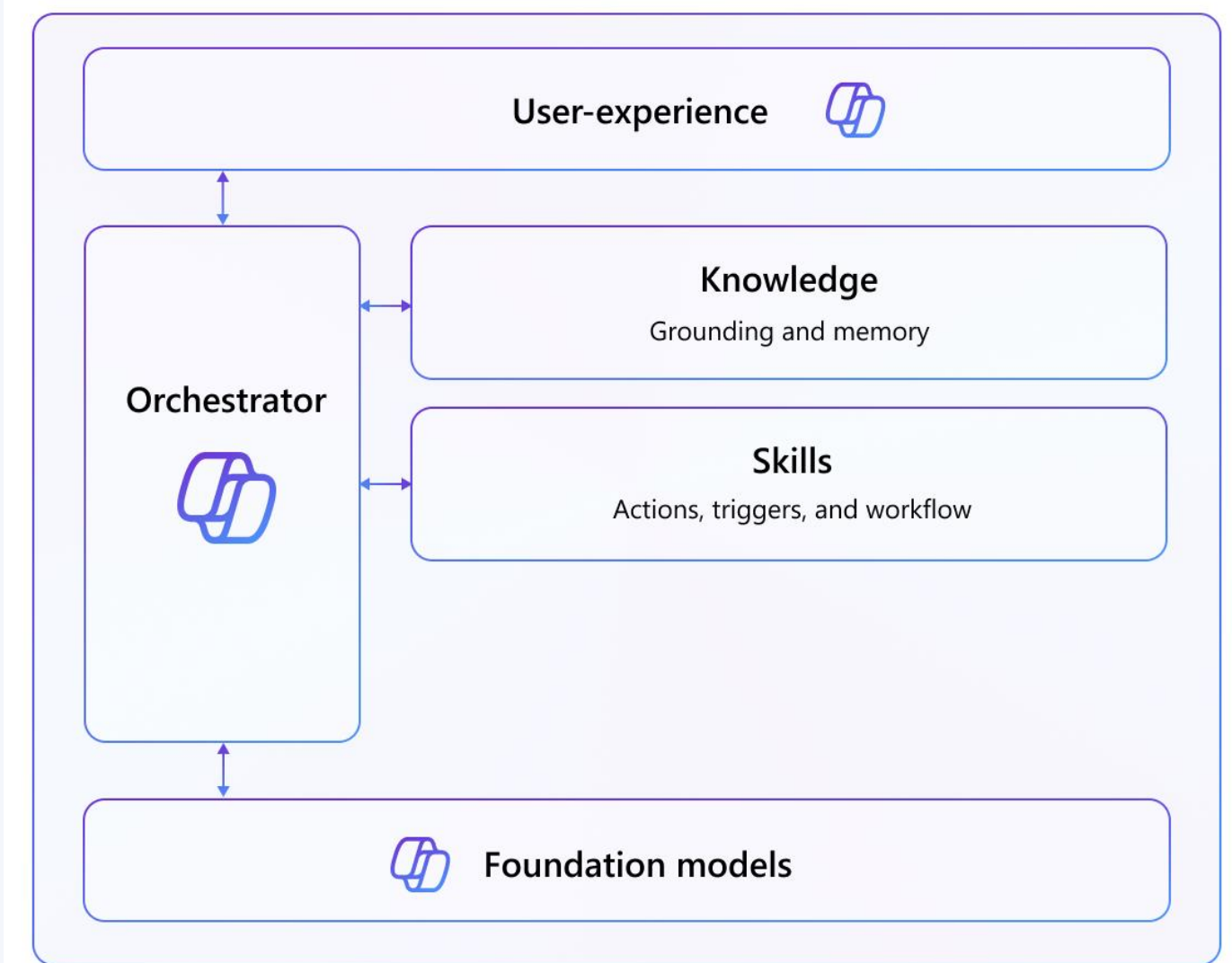
Custom Engine Agents

Open architecture — connect to other agents (e.g. Foundry agent) via code using M365 Agents SDK



Declarative Agents

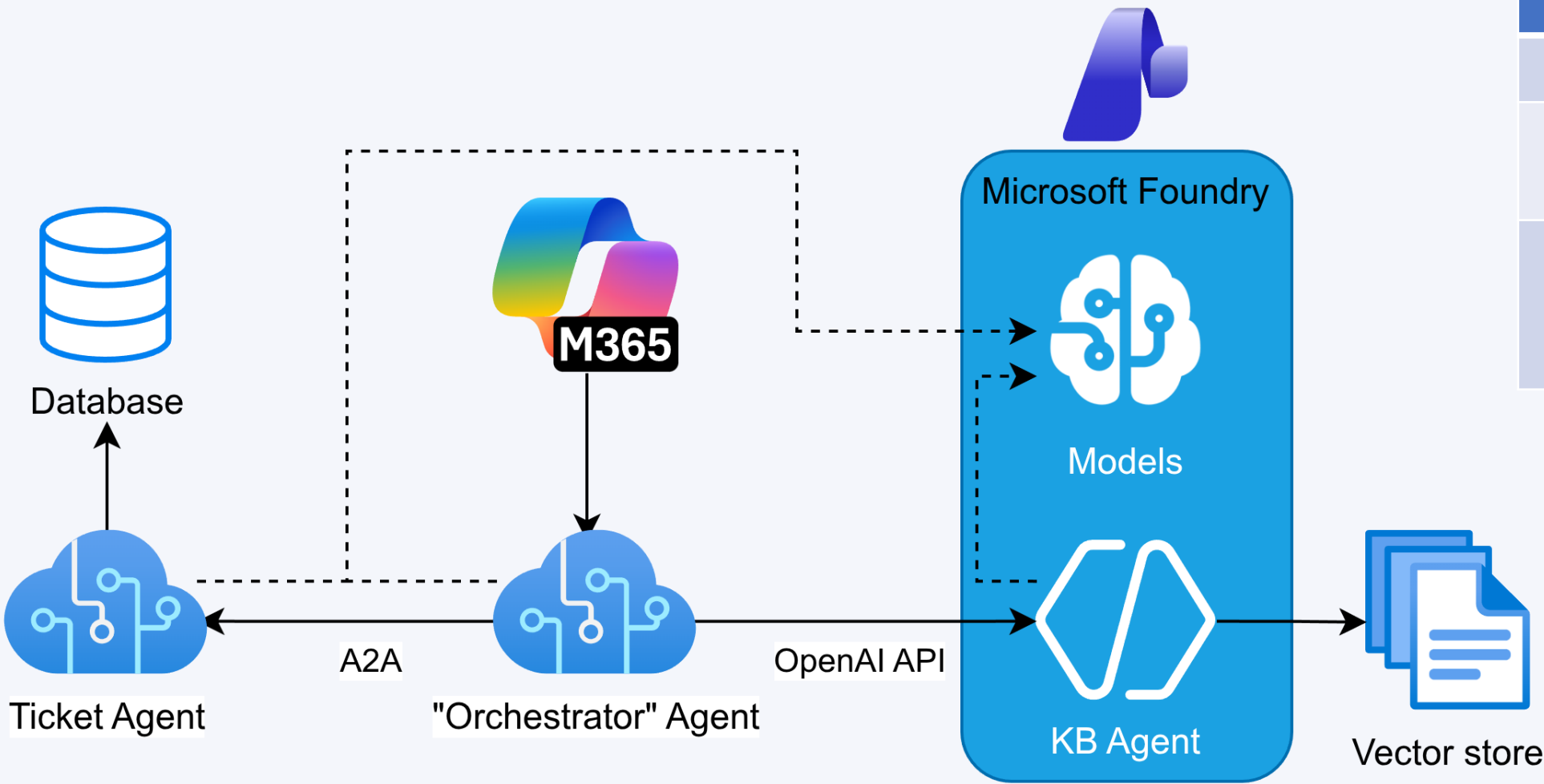
Can call other declarative agents defined in its schema. Cannot call other agent types





Multi-Agent Pattern

An orchestrator agent delegates to specialised agents, each expert in a specific domain - coordinating context, routing, and results across the entire flow.



Model	Kimi-K2.5	GPT-5.4-mini	GPT-4o
Orchestrator	N/A	Langchain	N/A
Knowledge	Database	N/A	Indexed documents
Tools	createTicketTool getMyTicketsTool, updateTicketTool	N/A	findKbTool

DEMO

M365 Agents Toolkit - Multi-Agent



Multi-Agent Considerations

Key differences between the two approaches

	 Copilot Studio	 M365 Agents Toolkit
Agent types	Child vs connected agent — consider use case	No hierarchies — flexible, interconnected agents
OOB agents	Cannot connect to first-party agents	Can connect to catalog agents (Analyst, Figma, Jira)
Debugging	No developer mode insights for agent-to-agent	Deep visibility for debugging interactions
Engine support	Custom engine only	Custom engine and declarative agent support

Microsoft Foundry

Models

Access frontier models like Opus 4.6 and GPT-5.5

Agent Service

Host agents with memory, tools, observability and evaluations

Foundry IQ

Ground LLMs in domain data, SharePoint, web, Azure AI Search

Tools

Connect to 1400+ built-in service connections and MCP tools

Machine Learning

Train and deploy custom ML models for specific needs

Security

Microsoft Purview, Entra, Defender integrations

DEMO

Microsoft Foundry - Multi-Agent

Links to Get Hands On

- Copilot Developer Camp: microsoft.github.io/copilot-camp/
- Agent Academy: microsoft.github.io/agent-academy/
- AI Tour WRK532: github.com/microsoft/aitour26-WRK532
- AI Skills Navigator: aiskillsnavigator.microsoft.com
- AI Agents for Beginners: github.com/microsoft/ai-agents-for-beginners
- MS Learn AI Agents: github.com/MicrosoftLearning/mslearn-ai-agents

07

Security, Monitoring & Governance

Why Governing Copilot Agents Matters

Without Governance

- Agent sprawl
- Sensitive data leakage
- Ownerless agents
- Unexpected PAYG costs

With Governance

- Strategically aligned
- Secure and compliant
- Efficient, avoiding redundancy
- Owned and maintained agents

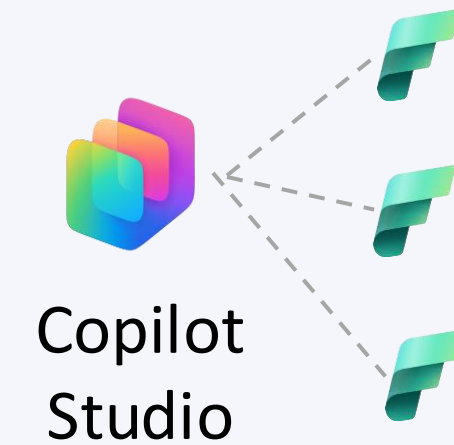
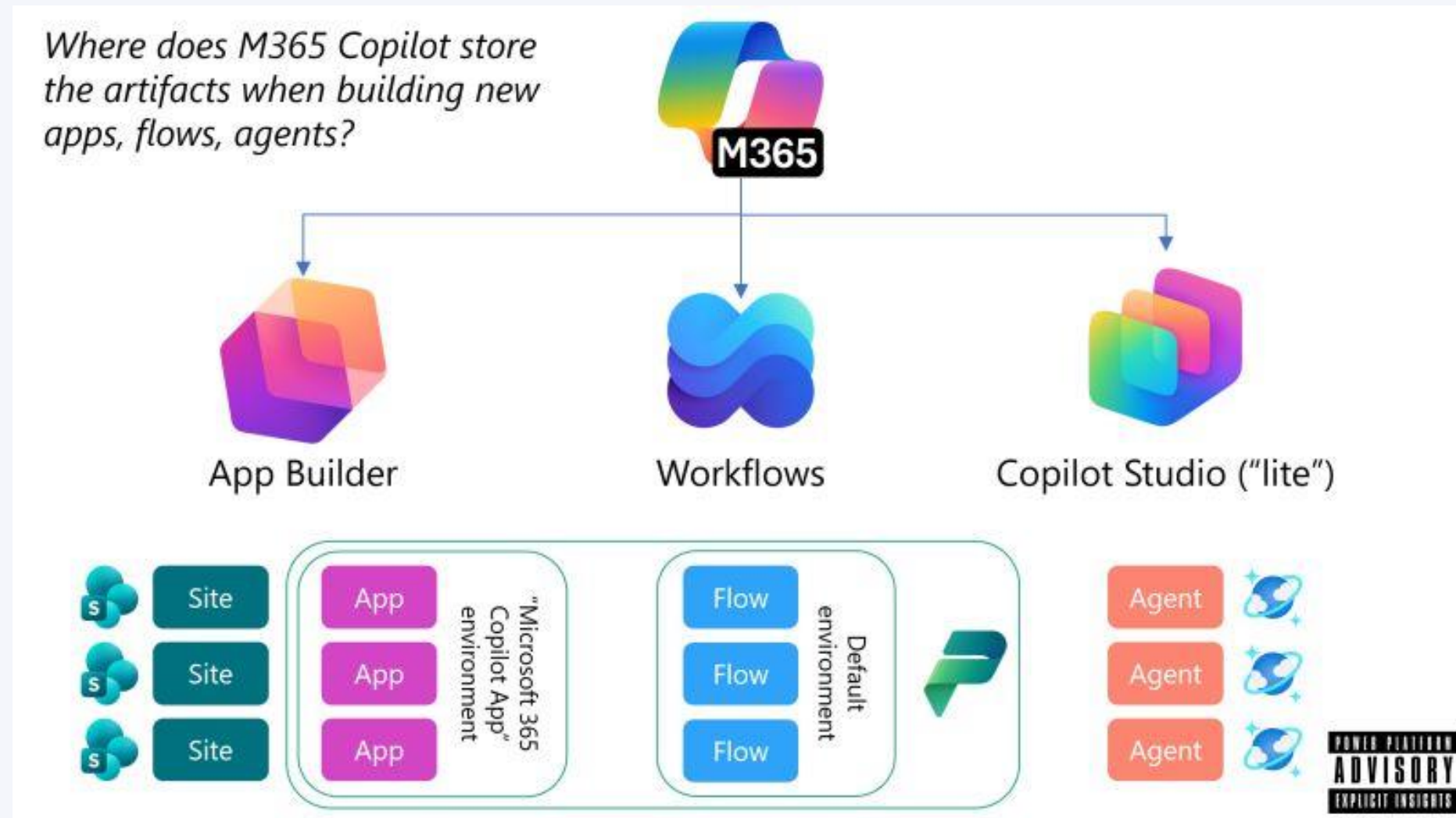
1000+ rogue agents
exposing sensitive data,
hallucinating, chaotic



1000+ governed and secured
agents DLP



Storage of Agent Artefacts



Power Platform
Environments



SharePoint
Agent are
stored as files
in sites



M365 Agents toolkit
published as Teams
App

Credit: Jukka Niiranen · Note: App Builder and Workflows are part of Frontier

Agent Security

Enterprise Data Protection

- Data encrypted, isolated, security enforced
- Label inheritance and DLP persistent
- Responsible AI protects against prompt injection

Access Controls

- Control who can create, share, and use agents
- Set policies and information labels
- Manage users and monitor usage

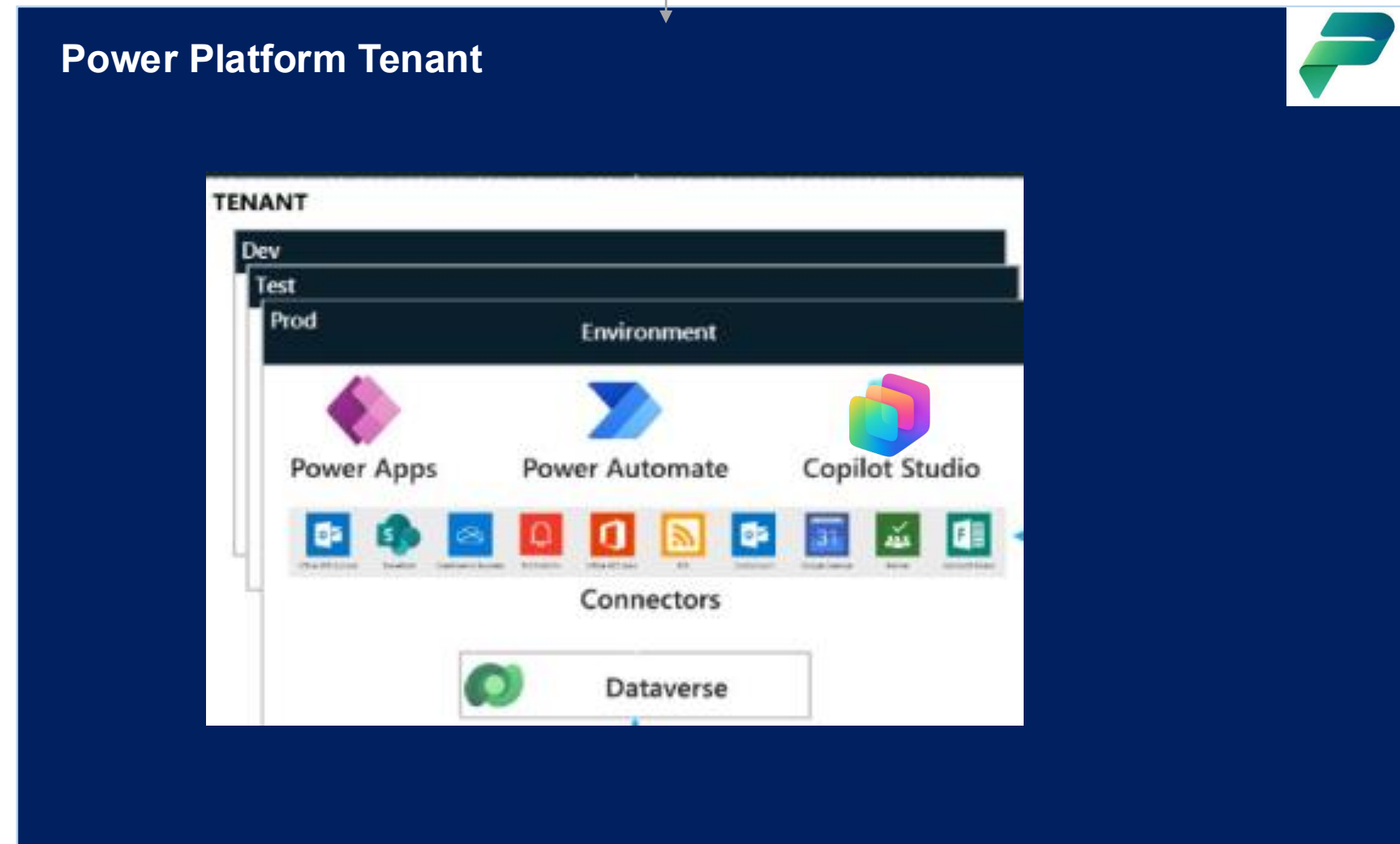
Agent Governance

- Track and manage agents from creation to end of life
- Set policies on resource usage and publishing
- Audit events and get operational insights

Copilot Studio Agent Governance & Security



Microsoft Entra



Tenant Isolation

Environment Security Roles

Dataverse Security Roles

Data Policies

Publishing Feature

Agent Permissions

Monitoring & Auditing Controls — Copilot Studio

Six layers of observability and compliance, from agent quality to tenant-wide audit

1

Agent Evaluation

Eval

Automated test sets with LLM-as-judge scoring to benchmark agent responses.

2

Operational Monitoring

Activity tab

Real-time run history for live troubleshooting of agent executions.

3

Conversation Audit Logs

Transcript

Full conversations saved to Dataverse for review and record-keeping.

4

Engagement & Quality

Analytics

Volume, topic success, escalation rate, and CSAT in one dashboard.

5

Telemetry & Alerts

Application Insights

Azure telemetry with KQL queries and configurable alerting.

6

Tenant-Level Audit

Purview

Tenant-wide compliance logging across the Microsoft 365 estate.

DEMO

Monitoring & Auditing

Application Insights Observability and Monitoring

DEMO

Settings

Advanced

Application Insights

Automatically send telemetry for your agent into an Application Insights resource. You can also log custom telemetry events from within your topics. [Learn more](#)

Connection string

.....

[Where can I find my connection string?](#)

Advanced options

☒ Log activity ⓘ

☒ Log sensitive activity properties ⓘ

☒ Log node tools ⓘ

copilotstudioagent - Microsoft Az

https://portal.azure.com/#@reshmee.on...
InPrivate

Microsoft Azure Copilot

Home > copilotstudioagent

copilotstudioagent | Logs

Application Insights

>> Service menu

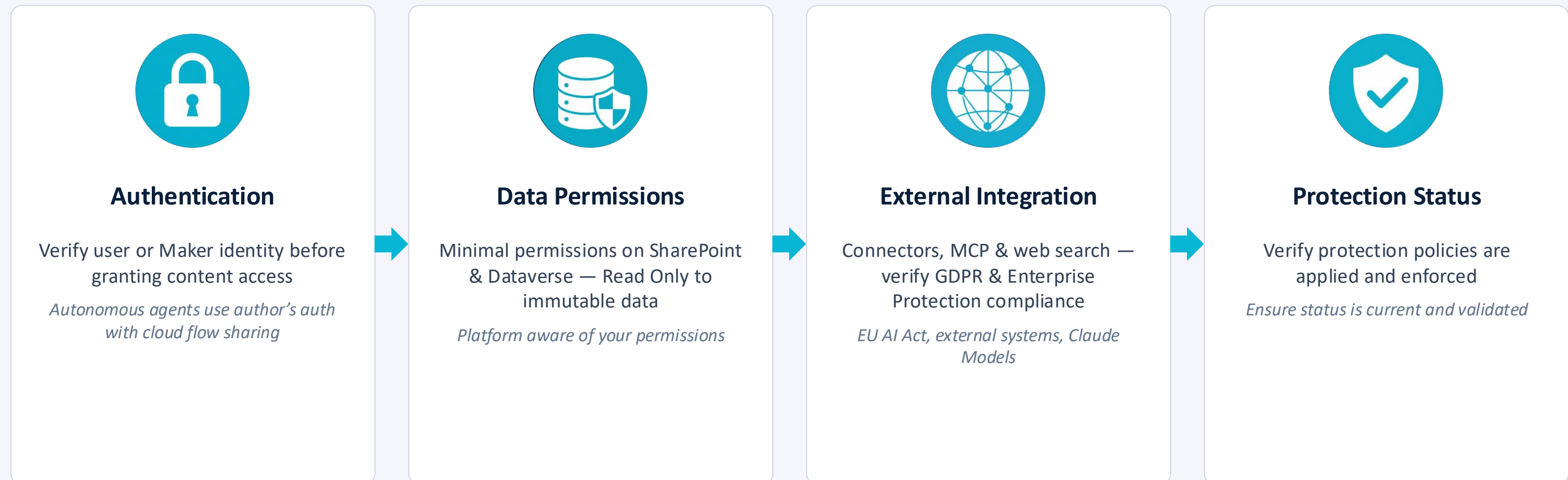
```
1 // View recent custom events
2 customEvents
3 | where cloud_RoleInstance == "Holiday Buddy" and
  customDimensions["channelId"] == "pva-studio"
4 | project timestamp, name, session_Id, user_Id,
  cloud_RoleInstance, customDimensions, customDimensions
  ["TopicName"], customDimensions["text"],
  customDimensions["speak"]
5
```

Results Chart

timestamp [UTC] ↑↓	name	session_
> 10/27/2025, 7:11:46.520 PM	TopicEnd	zTFhn
> 10/27/2025, 7:11:46.518 PM	TopicStart	zTFhn
> 10/27/2025, 7:11:46.518 PM	TopicEnd	zTFhn
> 10/27/2025, 7:11:45.313 PM	BotMessageSend	zTFhn

Secure RAG — Tackling Data Risks

User Access to Content → User Access to Agent → Agent access to user's content



DEMO

Protection Status

Hallucination Risks

Home > Tech

Air Canada loses court case after its chatbot hallucinated fake policies to a customer

The airline argued that the chatbot itself was liable. The court disagreed.

By [Chase DiBenedetto](#) on February 17, 2024



Without controls, agents may generate plausible but incorrect information — creating legal, financial, and reputational risk.

BUSINESS

Google's AI is 'hallucinating,' spreading dangerous info — including a suggestion to add glue to pizza sauce

By [Ariel Zilber](#)

Published June 6, 2025, 6:21 p.m. ET

37 Comments

Reducing Hallucination Risk

Grounded Knowledge

Connect agents only to curated, versioned SharePoint sites or Dataverse tables

System Prompts

Use explicit instructions: 'Only answer from provided knowledge. If unsure, escalate.'

Citation Display

Surface document citations inline so users can verify answers

Confidence Gating

Set minimum confidence threshold; below it, show a fallback

Content Safety

Enable Azure AI Content Safety to block harmful or fabricated responses

Continuous Eval

Run automated groundedness checks weekly; alert when scores drop

Adding Deterministic Behaviour

Agent Flow/ Workflow

Critical elements where 100% accuracy matters (e.g. finance)

Generative Prompt Action

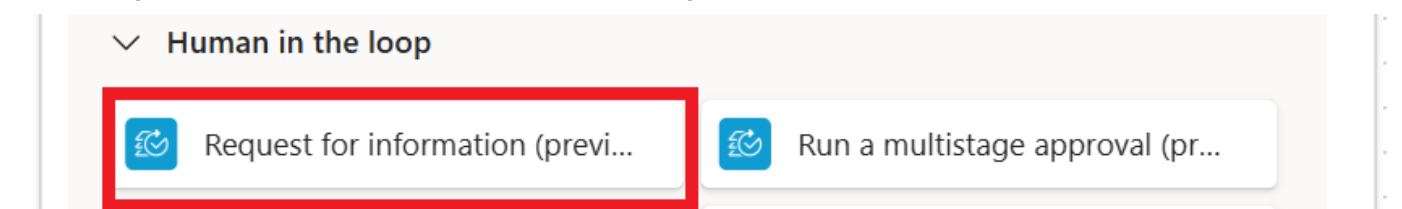
Few-shot training with examples

Topics / Triggers / Tools

Generative AI routes questions based on name and description

Human in the Loop

Establish processes for user acceptance and validation



DEMO

Human in the loop, deterministic
behaviour

Copilot Credits: The Simplified Model *One currency*

Classic Answer Deterministic, cached responses	1 credit
Generative Answer Lightweight model response generation	2 credits
Agent Action Standard agent task with tool invocation	3 credits
Local Connector Invocation Access to internal M365 connectors and data	10 credits
Power/Remote Action External API call or remote automation	15 credits + ~100

AI Tools (Prompts, Doc processing, OCR, Sentiment analysis, Entity) (per 10K characters)

Basic (lightweight model) Sentiment, simple classification 0.1 Copilot Credit per 1K tokens	1 credit
Standard (mid tier) OCR, entity extraction, summarization 1.5 Copilot Credit per 1K tokens	15 credits
Premium (GPT-class) Large-context reasoning and generation 10 Copilot Credit per 1K tokens	100 credits
Content Processing Document parsing and OCR	8 credits / page

M365 Copilot Licensed

NO CHARGE

- ✓ In-app meeting summaries
- ✓ Inline summaries in email
- ✓ Light tasks in Word and Excel
- ✓ Helpful chat suggestions

★ Deep-reasoning

Credits Required

- Prompts/Agents calling external APIs
- GenAI tasks: research, briefs, slides
- Agent automation and orchestration

Uber's COO says it's getting harder to justify the money spent on AI tokenmaxxing

By [Aditi Bharade](#) + Follow



Andrew Macdonald said it's getting harder to justify money spent on AI. Sam Barnes/Sportsfile for Collision via Getty Images

service

Put A
for p

<https://learn.microsoft.com/en-us/microsoft-copilot-studio/requirements-messages-management>

Empower Users

- Educate users about risks like oversharing and prompt injection
- Invisible governance - control at tenant level to not overburden users
- Test the agent with Copilot Studio before deploying



08

Copilot Cowork, Skills and IQ

Copilot Cowork

Your AI agent that gets work done

A cloud-based AI agent inside M365 that autonomously completes multi-step work across email, calendar, files, and Teams - using your real enterprise data.

1. Describe

Type your goal in natural language

2. Plan

Generates a step-by-step action plan

3. Execute

Runs actions across M365 apps

4. Deliver

Returns results you can review

Powered by Anthropic Claude · Enterprise-Grade · Available in Frontier Preview

Why Copilot Cowork?

Enterprise-grade, deeply integrated, ready now

Works With Your Data

Full M365 Graph access — emails, Teams, calendars, SharePoint, Excel simultaneously.

Enterprise Security

Runs inside your M365 tenant under your identity. Every action auditable.

Extensible Platform

Plugins from M365 App Store.
Upcoming: Miro, monday.com, Power BI, Dynamics 365.

M365 Copilot license required · Enroll in Frontier early-access · Browser, desktop & mobile

Cowork Demo Scenarios

Catch me up

"Catch me up on everything I missed while I was out"
Scans inbox, Teams & calendar → prioritised briefing with actions

Meeting prep

"Prep me for my 3pm meeting with the Contoso team"
Pulls threads, files, past notes → 1-page briefing doc

Launch plan

"Create a product launch plan and share it with the team"
Builds SharePoint doc, assigns tasks, sends Teams message



The Impact

Hours saved, every single day

2 hrs

saved per person per day

68%

faster task completion

1

prompt replaces
5+ manual steps

Before Cowork	After Cowork
Check inbox, manually triage 30+ emails	Type "Catch me up" — done in 30 seconds
Open calendar, read through 4 meeting invites	Type "Prep for my 3pm" — briefing ready
Search SharePoint for relevant docs	Cowork pulls all relevant files automatically
Write briefing note from scratch	Briefing note generated & shared to team

DEMO

Cowork

Microsoft IQ

All-encompassing umbrella intelligence layer for your agents



Work IQ

Grounded in you and
your orgs data within
M365



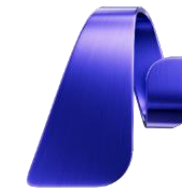
Fabric IQ

Use shared
definitions, metrics,
and relationships
already modeled in
enterprise data



Web IQ

Connects AI systems
and agents to fresh,
real-world
information from
across the web



Foundry IQ

Enterprise knowledge
across systems
through
policy-compliant
access



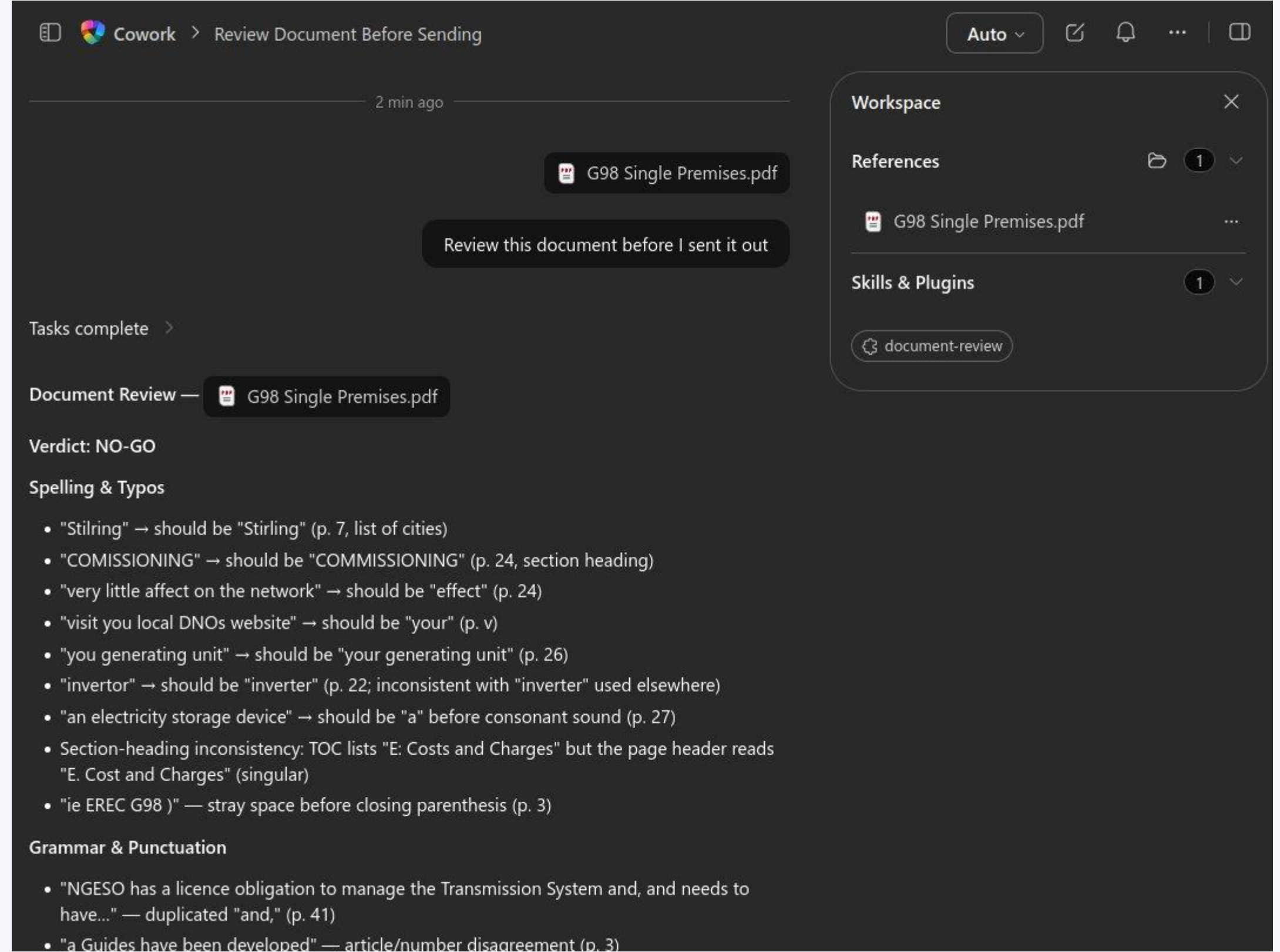
Work IQ vs Microsoft Graph

Intelligence vs Data Access

	Microsoft Graph (Data Access)	Microsoft Work IQ (Intelligence)
Target	Interactive users and custom apps	Agent experiences
Scope	M365 workloads + management APIs	Data with skills and tools
Throttling	Enforces throttling rules	Tracks user context
Auth model	Supports application-only	Licensed user identity only

Skills

- Reusable packages that tell an agent how to do something to achieve a goal
- Differs from Tools which execute actions
- Adopted in GitHub Copilot CLI, Cowork, and Claude among others
- Find plenty of examples at [skills.sh](#)



What Makes Up a Skill?

- A markdown file (SKILL.md) and associated files
- Structured instructions, not code
- Two parts: YAML frontmatter + Markdown body
- Agreed format across products

```
1 ---
2 name: document-review
3 description: |
4   · Reviews documents before public/external release — checks
5   · for errors, fact-checks claims
6   · against general knowledge, flags spelling and grammar
7   · issues, and reports a Flesch
8   · readability score. Ends with a clear go/no-go verdict.
9   · Use when user asks to "review this before I send it",
10  · "pre-publish check",
11  · "check this doc", "review this for publishing", "is this
12  · ready to send",
13  · "proofread this", "fact-check this document", "readability
14  · check",
15  · "Flesch score for this", or shares a document and asks if
16  · it's ready to go out.
17 cowork:
18   · category: writing
19   · icon: DocumentText
20 ---
21
22 # Document Review
23
24 Pre-publish quality gate for documents going out publicly or
25 externally.
```

Document Review

Pre-publish quality gate for documents going out publicly or externally.

When to Use

Triggered when the user wants a final-pass review on a document before sending, publishing, or sharing externally. Always produces a verdict — never just a list of observations.

When NOT to Use

- Drafting or writing new content from scratch
- Summarizing a document's content
- Translation between languages
- Code review (use code-review tools instead)
- Editing for a specific audience tone (use stakeholder-comms)

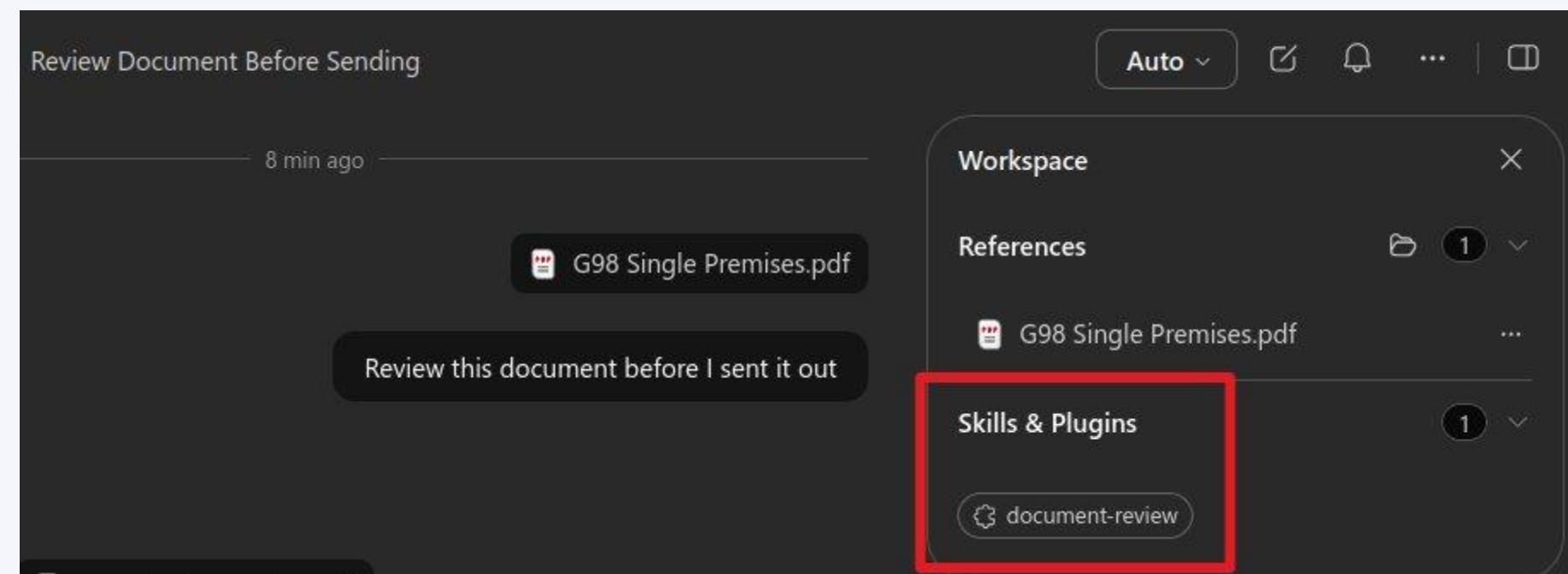
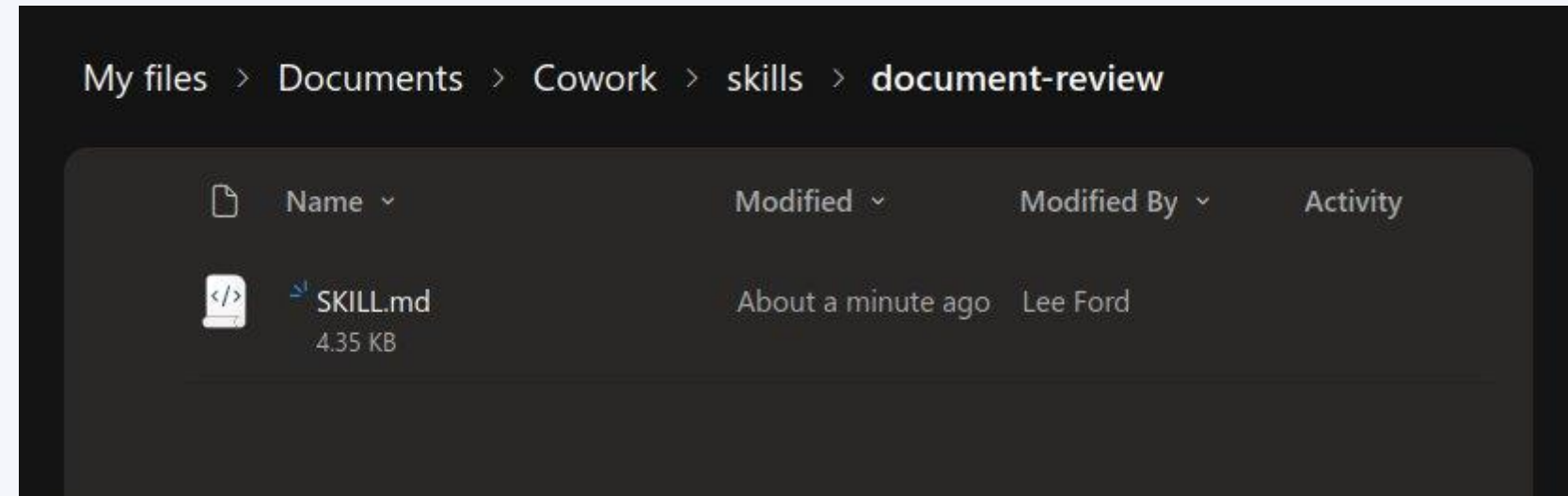
Workflow

Step 1: Locate the document

- If the user pasted text directly, use that as the document body
- If the user named a file, find it with `Glob input/**/*` (or workspace root)
- For .docx: read via the `docx` skill helpers

Cowork Skills

- Currently no UI for skill management
- No way to install skills as an admin (for multiple users)
- Create your SKILL.md and place it in Documents/Cowork/skills in OneDrive
- Use existing skills found online
- Have Cowork create a skill for you!



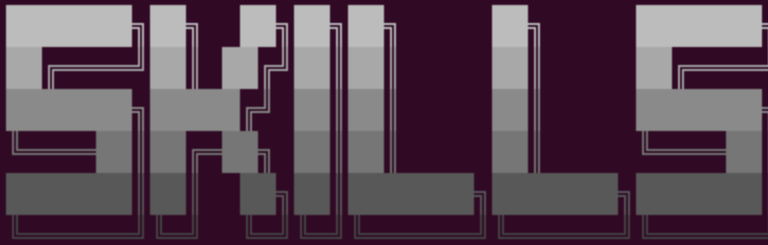
DEMO

Cowork Skills

GitHub Copilot CLI Skills

- Easiest way is to use the "skills" CLI program to install skills directly from internet
- You can then leverage the skills in GitHub Copilot CLI directly

```
~/code npx skills add https://github.com/github/awesome-copilot --skill workiq-copilot
```



The screenshot shows the 'skills' CLI interface. At the top, the command `npx skills add https://github.com/github/awesome-copilot --skill workiq-copilot` is entered. Below the command, the word 'SKILLS' is displayed in a large, stylized, blocky font. The interface then shows a list of steps for installing the 'workiq-copilot' skill:

- Source: `https://github.com/github/awesome-copilot.git`
- Repository cloned
- Found 354 skills
- Selected 1 skill: `workiq-copilot`
- 71 agents
- Installing to: `GitHub Copilot`
- Installation scope: Global

Below these steps, there is an 'Installation Summary' section with a box containing the following text:

```
~/.agents/skills/workiq-copilot  
copy → GitHub Copilot, Amp, Antigravity, Antigravity CLI, Cline +12 more
```

Below the summary, there is a 'Security Risk Assessments' section with a box containing a table of security checks:

	Gen	Socket	Snyk
workiq-copilot	Safe	0 alerts	Low Risk

At the bottom, there is a link to the details: `https://skills.sh/github/awesome-copilot`

DEMO

GitHub Copilot CLI Skills

SharePoint AI Skills

- Skills stored as Markdown files in the Agent Assets library
- Enables version control, governance, and team-wide editing
- Update skills by prompting SharePoint or editing markdown directly
- Whole team can share, review, and improve knowledge

```
4 ---
5 # List Site Folders
6
7 ## Purpose
8 When the user asks to see folders in the site, find folders, or list folder creators,
  this skill retrieves all folders across document libraries on the current SharePoint
  site and presents them with their creator. Document Sets are excluded.
9
10 ## Steps
11 1. Discover all document libraries on the current site using `discover_sharepoint_lists`
  with `filterType` set to `userCreatedDocumentLibraries`.
12 2. For each library, retrieve folder items using `get_list_item_metadata` with a CAML
  query that filters for folders (`FSObjType = 1`) and excludes Document Sets
  (`ContentType` not equal to `Document Set`):
13   ```xml
14   <Query><Where><And><Eq><FieldRef Name='FSObjType' /><Value Type='Integer'>1</Value>
  </Eq><Neq><FieldRef Name='ContentType' /><Value Type='Computed'>Document Set</Value></Neq>
  </And></Where></Query>
  ```
15
16 Set `rowLimit` to 100 and `fetchAll` to true.
17 3. For each folder found, retrieve the creator by calling `list_item_versions` with
 `top: 1` to get the earliest version. The editor of version 1.0 is the folder creator.
 Batch all items per library into a single `list_item_versions` call using the `items`
 array.
18 4. Present the results as a table with columns: Folder Name, Library, Created
 By, Created Date.
19 5. If no folders are found, inform the user.
20
21 ## Example
22
23 User: "Show me all folders and who created them"
24
25 Response: A table listing each folder, which library it's in, who created it, and
 when.
26
27 | Folder Name | Library | Created By | Created Date |
28 |---|---|---|---|
29 | Q1 Reports | Documents | Jane Smith | Jan 15, 2025 |
30 | Marketing Assets | Brand Assets | Alex Lee | Mar 3, 2025 |
31
32 ## Constraints
33 - Only scan user-created document libraries (skip system libraries).
34 - Always exclude Document Sets using the ContentType filter in the CAML query.
35 - Use `FSObjType = 1` to identify folders.
36 - If a library has many folders, note the count and display up to 100 per library.
37 - Use `list_item_versions` (not qna_on_list) to reliably get the Created By information.
```

## Purpose

When the user asks to see folders in the site, find folders, or list folder creators, this skill retrieves all folders across document libraries on the current SharePoint site and presents them with their creator. Document Sets are excluded.

## Steps

1. Discover all document libraries on the current site using `discover_sharepoint_lists` with `filterType` set to `userCreatedDocumentLibraries`.
2. For each library, retrieve folder items using `get_list_item_metadata` with a CAML query that filters for folders (`FSObjType = 1`) and excludes Document Sets (`ContentType` not equal to `Document Set`):

```
<Query><Where><And><Eq><FieldRef Name='FSObjType' /><Value
Type='Integer'>1</Value></Eq><Neq><FieldRef Name='ContentType' /><Value
Type='Computed'>Document Set</Value></Neq></And></Where></Query>
```

- Set `rowLimit` to 100 and `fetchAll` to true.
3. For each folder found, retrieve the creator by calling `list_item_versions` with `top: 1` to get the earliest version. The editor of version 1.0 is the folder creator. Batch all items per library into a single `list_item_versions` call using the `items` array.
  4. Present the results as a table with columns: **Folder Name**, **Library**, **Created By**, **Created Date**.
  5. If no folders are found, inform the user.

## Example

User: "Show me all folders and who created them"

Response: A table listing each folder, which library it's in, who created it, and when.

| Folder Name      | Library      | Created By | Created Date |
|------------------|--------------|------------|--------------|
| Q1 Reports       | Documents    | Jane Smith | Jan 15, 2025 |
| Marketing Assets | Brand Assets | Alex Lee   | Mar 3, 2025  |

## Constraints

- Only scan user-created document libraries (skip system libraries).
- Always exclude Document Sets using the `ContentType` filter in the CAML query.
- Use `FSObjType = 1` to identify folders.
- If a library has many folders, note the count and display up to 100 per library.
- Use `list_item_versions` (not `qna_on_list`) to reliably get the Created By information.



# Scenario 1

*Quick-fire • Easy*

Your company's legal department has a SharePoint site packed with compliance policies, contract templates, and regulatory updates. The team lead wants a quick way for employees to ask questions about these documents without leaving the SharePoint experience. Nobody on the team writes code.

**Which product would you choose?**

A) SharePoint Agent B) Agent Builder C) Copilot Studio D) M365 Agents Toolkit E) Microsoft Foundry



# Scenario 2

*Story + choices • Easy–Medium*

An HR team at a mid-sized company needs an employee benefits chatbot. Employees should be able to ask about holiday policies, submit leave requests, and get answers grounded in internal HR documents stored in SharePoint and Azure AI Search.

## Requirements:

- Available on Teams, mobile, and web
- Curated topics for common HR workflows (e.g. leave requests)
- Connectors to a ServiceNow ticketing system
- The team has low-code skills only



# Scenario 3

*Quick-fire • Easy–Medium*

A department head wants a simple agent they can configure themselves — no involvement from IT or developers. It should answer questions about team processes and project timelines using data already in M365. They want to share it with their immediate team inside the Copilot experience.

**Which product would you choose?**

A) SharePoint Agent B) Agent Builder C) Copilot Studio D) M365 Agents Toolkit E) Microsoft Foundry



# Scenario 4

*Detailed case • Hard*

An insurance company is building a claims processing system. They need specialised agents for car, health, dental, and travel claims — each owned by a different business unit with its own authentication and data. A central orchestrator agent should route customer queries to the right specialist. They want to use Anthropic Claude as the foundation model and deploy the experience on their public website, not just inside Teams.

**Key decision factors:**

- Multi-agent with separate auth per specialist → Connected agents pattern
- Non-Microsoft model (Claude) → Rules out M365 Copilot declarative agents
- Deploy anywhere (public website) → Rules out Teams-only options



# Scenario 5

*Detailed case • Hard — Deliberately ambiguous!*

A retail company wants an inventory management agent for store managers. It must pull product info from SharePoint documents AND call an external inventory API via MCP to check real-time stock levels. When stock drops below a threshold, the agent should autonomously trigger a reorder flow via Power Automate. The team is a mix of low-code and pro-code developers. It needs to work in Teams and on the web.

## Why this one sparks debate:

- Copilot Studio: Built-in MCP servers, autonomous triggers via Power Automate, multi-channel, low-code friendly
- M365 Agents Toolkit: MCP support, pro-code flexibility, deep debugging visibility
- Microsoft Foundry: Full control, any model, deploy anywhere

## Scenario 6 - Field Engineers Maintaining Critical Infrastructure

A utilities company employs hundreds of field engineers who spend most of their time on-site maintaining substations and network equipment. Connectivity is inconsistent, and engineers rely on mobile devices to access manuals, historical maintenance records, safety guidance, and job notes. Much of the most valuable knowledge lives in free-text reports, photos, voice notes, and informal messages sent back to the office.

Engineers frequently encounter situations that are “similar but not identical” to past jobs and want quick answers while on site: Has this fault happened before? What workaround was used? Were there any safety concerns noted? Calling colleagues often interrupts others and still leaves gaps. After visits, engineers are required to write detailed reports. These are time-consuming and often delayed until the end of the week, reducing accuracy. Office-based planners and asset managers want clearer insight into emerging issues and trends, but don’t want to overload engineers with extra admin.

There is interest in better support before, during, and after site visits, improving collaboration between mobile staff and office teams, and gradually standardising how knowledge from the field feeds back into the organisation.

## Scenario 7 - Customer Service Team Scaling Beyond Office Hours

A mid-sized financial services firm handles around 400 customer queries a day across phone, email, and Teams. During business hours, a small support team manages well enough, but evenings and weekends see a sharp drop in response times. Customers increasingly expect instant answers about account balances, transaction disputes, and product eligibility.

The firm's knowledge base lives across a SharePoint site (product guides, FAQs, compliance notes) and a Dataverse instance (customer records, case history). When a query involves sensitive financial data, regulations require a human to review before any action is taken. The compliance team insists on full audit trails and the ability to replay any conversation.

The support team has one Power Platform developer but no pro-code engineers. They want to start with a text-based agent on their website and in Teams, with a plan to add voice later. The agent should handle straightforward queries autonomously, escalate anything flagged as high-risk to a human via Teams, and log every interaction for regulatory review.

Leadership also wants weekly analytics on resolution rates, customer satisfaction, and escalation patterns to justify the investment to the board.

## Scenario 8 - Multi-Department Knowledge Hub for a Global Org

A multinational company with 15,000 employees across six countries wants a single “ask anything” assistant that employees can reach from Teams. Behind the scenes, queries need to be routed to the right specialist: HR policies for one region differ from another, finance operates under different reporting standards per jurisdiction, and IT support varies by office location.

Each department already manages its own SharePoint sites and has started building simple agents independently. The IT governance team is worried about agent sprawl - there are already 23 ungoverned agents across the tenant. They want a central orchestrator that coordinates these specialist agents, but each department insists on owning and publishing its own agent with its own authentication and data boundaries.

The company has a mix of capabilities: the IT team has pro-code developers comfortable with TypeScript, but the HR and Finance teams rely entirely on low-code tools. The solution must work for both groups. There is no appetite to move away from the Microsoft ecosystem, and the Copilot Studio licence is already in place across the organisation.

The CISO requires full audit trails, DLP policy enforcement, and the ability to monitor all agent-to-agent interactions from a single dashboard.

## Scenario 9 - Startup Building a Customer-Facing AI Product

A 30-person healthtech startup is building an AI-powered triage assistant that patients interact with before booking a GP appointment. The assistant asks about symptoms, cross-references clinical guidelines stored in a vector database, and recommends urgency levels. It must run on the startup's own web app and a branded mobile app — not inside Teams or any Microsoft surface.

The clinical team wants to evaluate multiple foundation models (GPT, Claude, and an open-source medical model) and run A/B tests to measure which produces the safest, most accurate triage recommendations. The engineering team needs full observability: token-level tracing, latency dashboards, and the ability to replay any patient conversation for audit.

Behind the triage agent, a second agent handles appointment scheduling by calling the clinic's booking API via MCP, and a third agent generates post-consultation summaries by pulling from the patient record system. The startup wants all three agents orchestrated as a single workflow, with deterministic handoff points and human-in-the-loop approval before any booking is confirmed.

Regulatory compliance under the UK Medical Devices Regulations is non-negotiable. The CTO wants the entire agent stack version-controlled, with CI/CD pipelines for testing prompt changes before they reach production.



# Key Takeaways

- 01** Different tools for different tasks
- 02** Stay up to date
- 03** Security for design
- 04** Effective prompting drives better agent outcomes
- 05** Multi-agent beats monolith - orchestrate specialists
- 06** MCP enables vendor-neutral tool integration
- 07** Governance and observability are non-negotiable in production

# Q&A

*We would love to hear your questions and feedback*

# Thank you.

See you on **11–12 June 2026** in London.