Microsoft 365
COMMUNITY CONFERENCE

Supercharge Your Agents with Computer Use in Copilot Studio

Sravani Seethi & Phi-Lay Nguyen

Apr 22, 2026

© Copyright Microsoft Corporation. All rights reserved.

Microsoft

Sravani Seethi
Sr Product Manager
CAD (Copilot Agent Development) / CAT

Phi-Lay Nguyen
Sr Product Manager
CAD (Copilot Agent Development) / CAT

CAD
COPILOT AGENT DEVELOPMENT

What You'll Learn

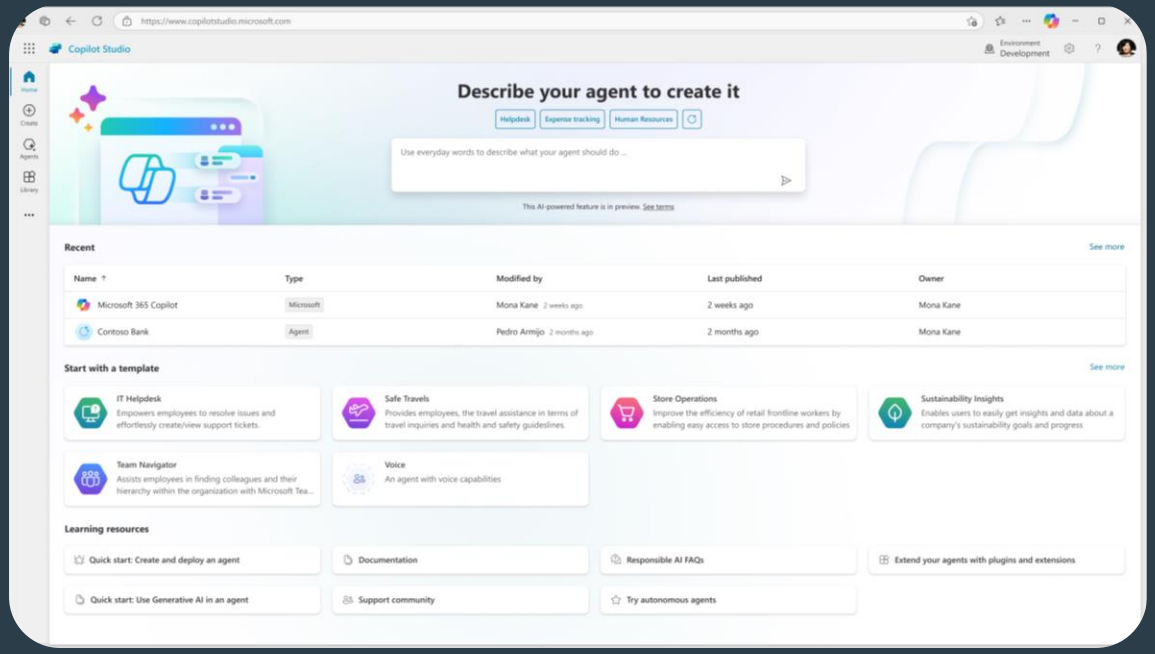
- What: is a Computer Using Agent (CUA)?
- How:
  - Does it work?
  - Build a Computer Using Agent
- When: Use cases
- Safety first: Enterprise guardrails
- Resources

What is a Computer Using Agent (CUA)?

Microsoft

Copilot Studio

Copilot Studio is Microsoft's low-code platform for **building custom AI agents**



- Meet your users where they already are
- Access everything in one place
- Automate your workflows
- Integrate with your external apps
- Connect to your data in Microsoft 365

Microsoft 365 Copilot

Make every information worker more productive

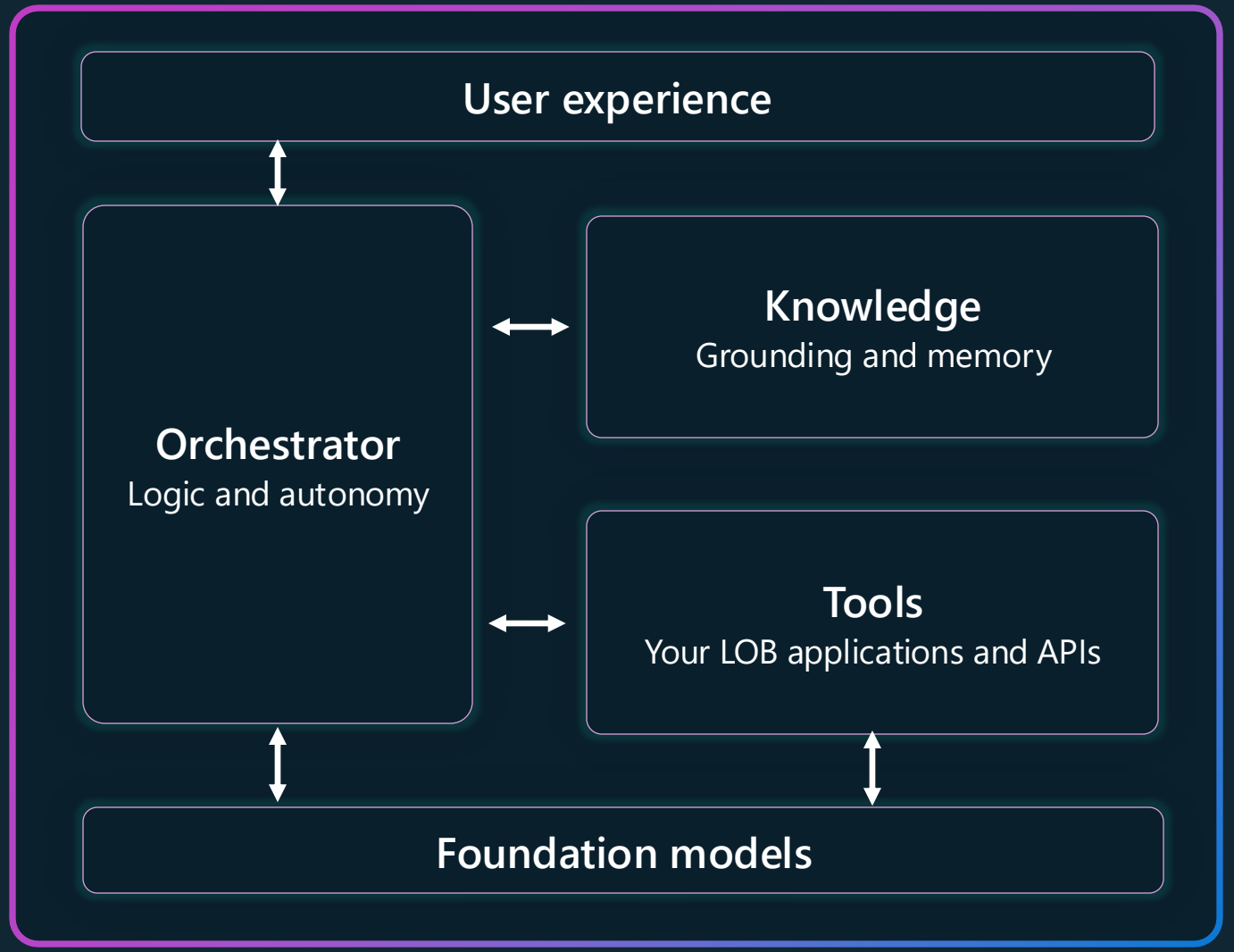
Microsoft Copilot Studio

Implement and manage teams of agents
to run every business process more efficiently

Microsoft Foundry

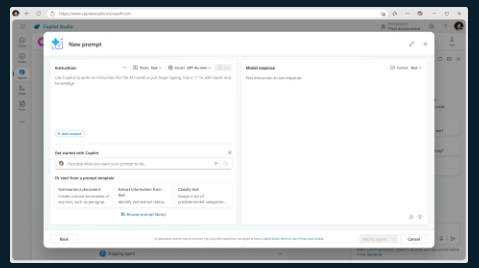
Professionally manage and fine-tune AI models

Anatomy of an agent



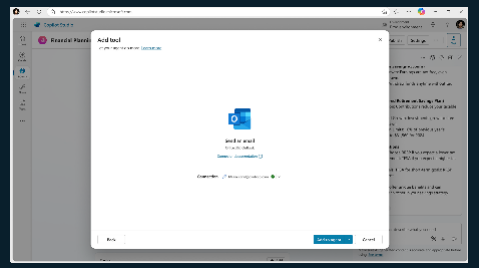
Tools

Your LOB applications and APIs



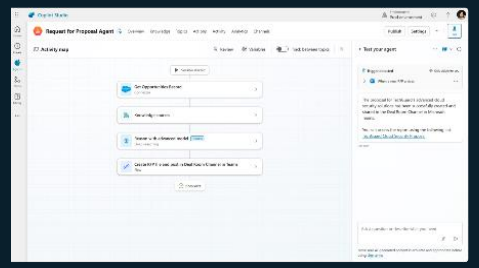
Prompts

Provide structured instructions to guide the LLM to perform specific tasks



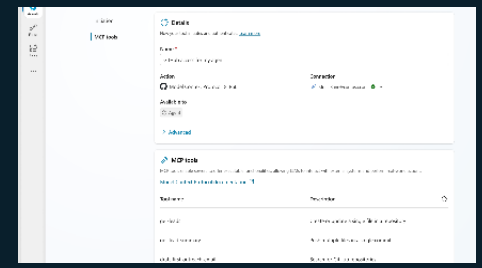
Connectors

Choose from 1,500+ prebuilt Power Platform connectors to popular data sources and apps or create a custom connector for any publicly available API



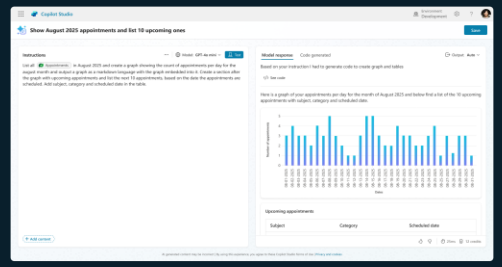
Deep reasoning

Instruct agents to perform complex reasoning tasks



Model Context Protocol (MCP)

Connect directly to existing knowledge servers and APIs for automatic updates to actions and knowledge



Code interpreter

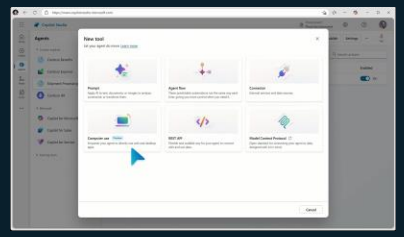
Enable your agent to write and run Python code to perform complex tasks

Document generation

Instruct your agent on how to generate a structured doc

Rest API

Connect with your external systems



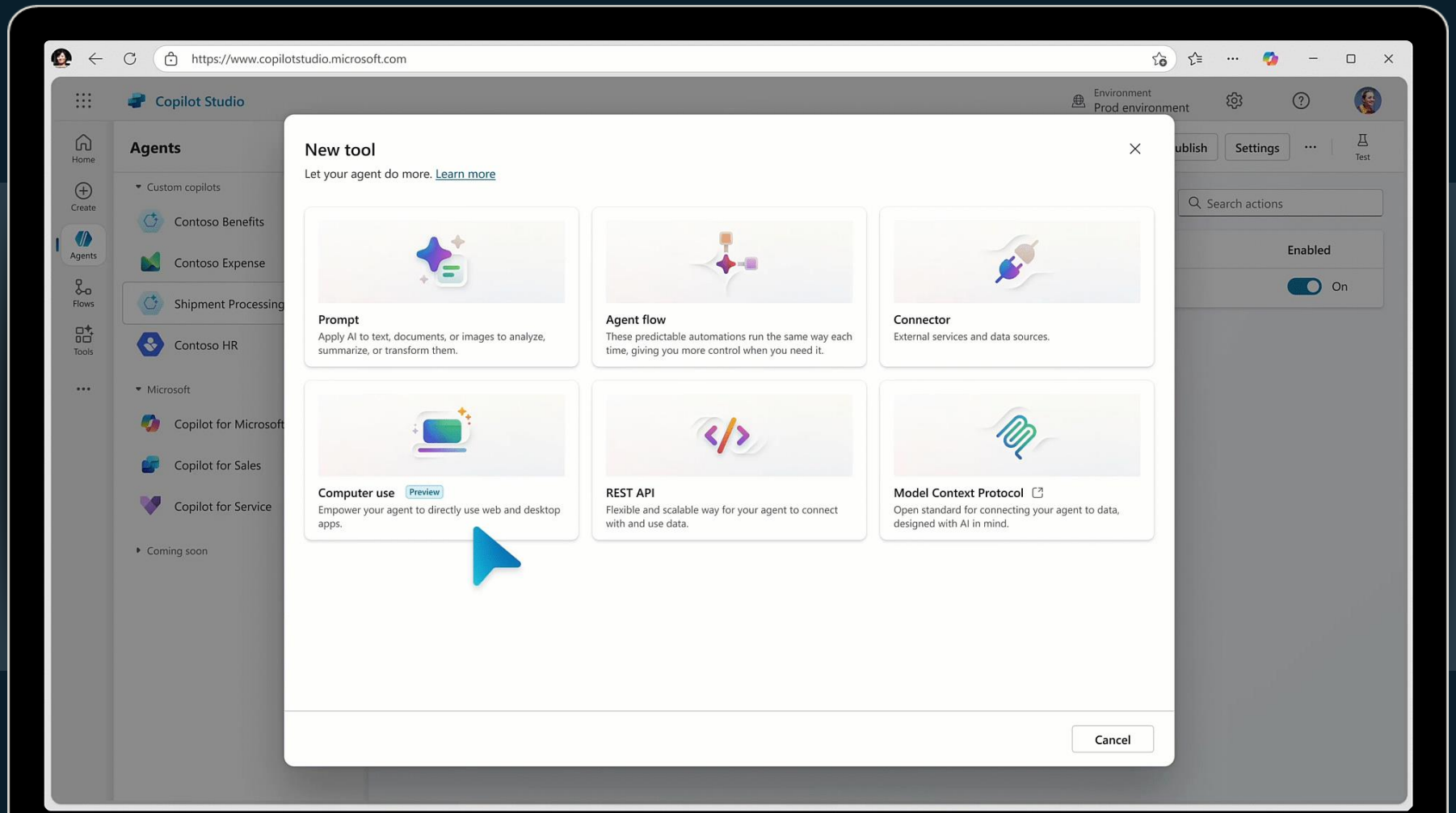
Computer Use

Enable your agents to interact with web / desktop apps and APIs

Computer Use in Copilot Studio

Agents can now interact with any system that has a graphical user interface

Public preview

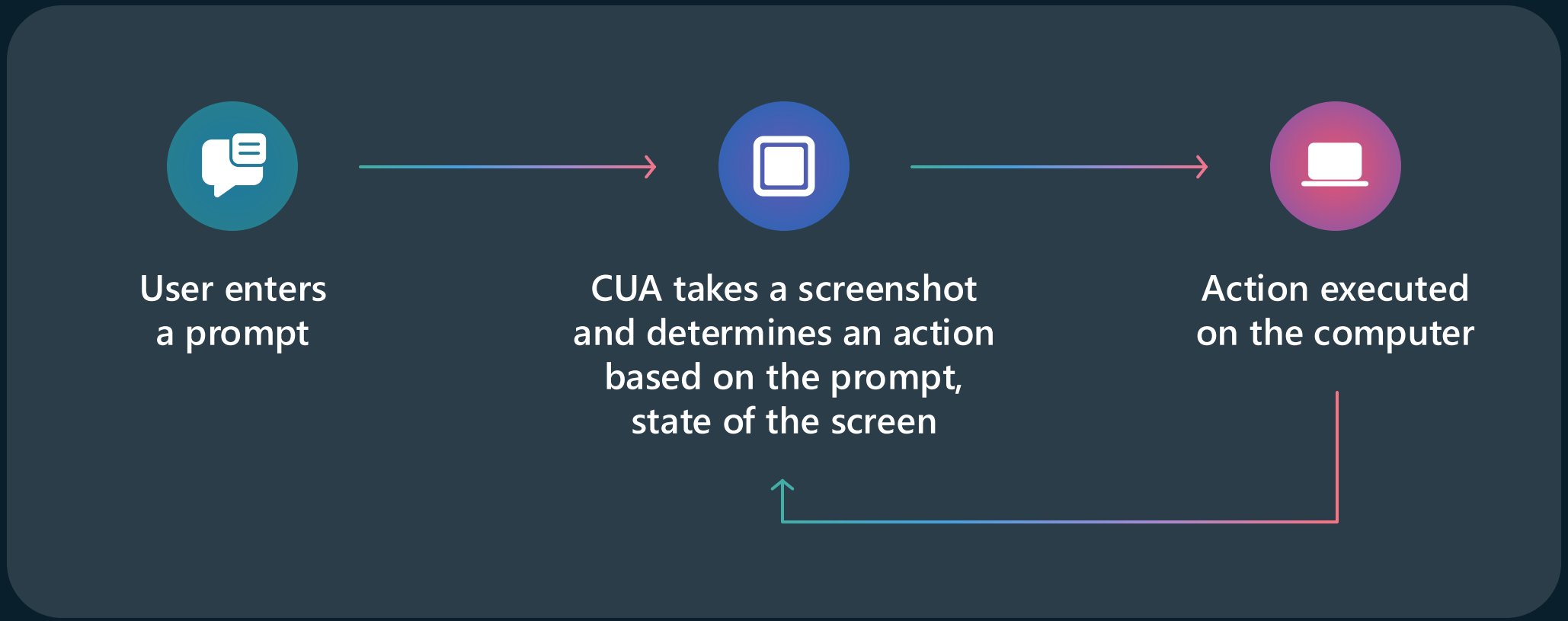


The How..

Microsoft

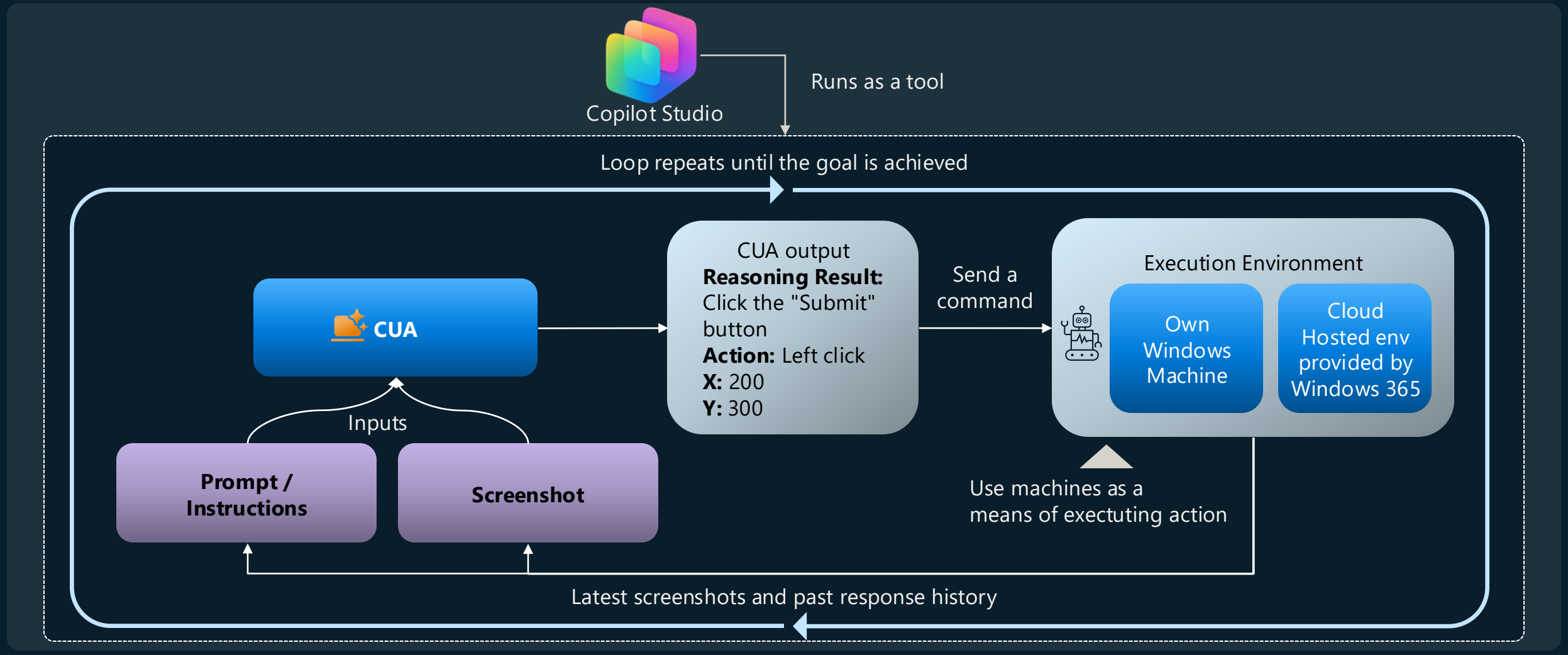
How it works

Computer Using Agents (CUA)



How it works – Deep Dive

Runs automation in a full Windows environment



UI Automation – RPA and CUA

Aspect	RPA	CUA
Automation type	Rule based	LLM driven
Interact via	UI tree	Vision
Authoring	Script	Natural language instructions
Decision making	Predefined rules	Autonomous decisions
Flexibility	Limited	High
Error Handling	Static	Self-correcting on visual feedback

RPA & CUA

Today, use RPA when	Today, use CUA when
UI is stable The screens, fields, and selectors hardly change	**UIs shift or vary widely** Frequent redesigns, unpredictable user experience
Rules are clear Decisions can be captured in rules	**Decisions may vary** The agent must think to pick the next step or self-correct
Speed matters High-volume where every second counts	**Vision matters** The task depends on what's visible on screen (charts, colors, dynamic layouts)
An RPA team owns it Existing RPA development and management knowledge	**Increase personal productivity** Needing an easier way to build UI automation
Needing production now For mission critical systems at scale	**Tolerance for errors** "Misclicks" or retries are ok. E.g., read only scenarios

Use both where CUA covers RPA
Self-heal after a failure or step is too dynamic

Machines

Hosted browser

Best for web-only tasks

Ready-to-use machines with Microsoft Edge and Windows apps

Cannot access internal resources

Powered by Windows 365 for agents

Bring-your-own-machine

Best for automation requiring specific machine configurations not covered by other options

Full control over your infrastructure

New

Cloud PC pool

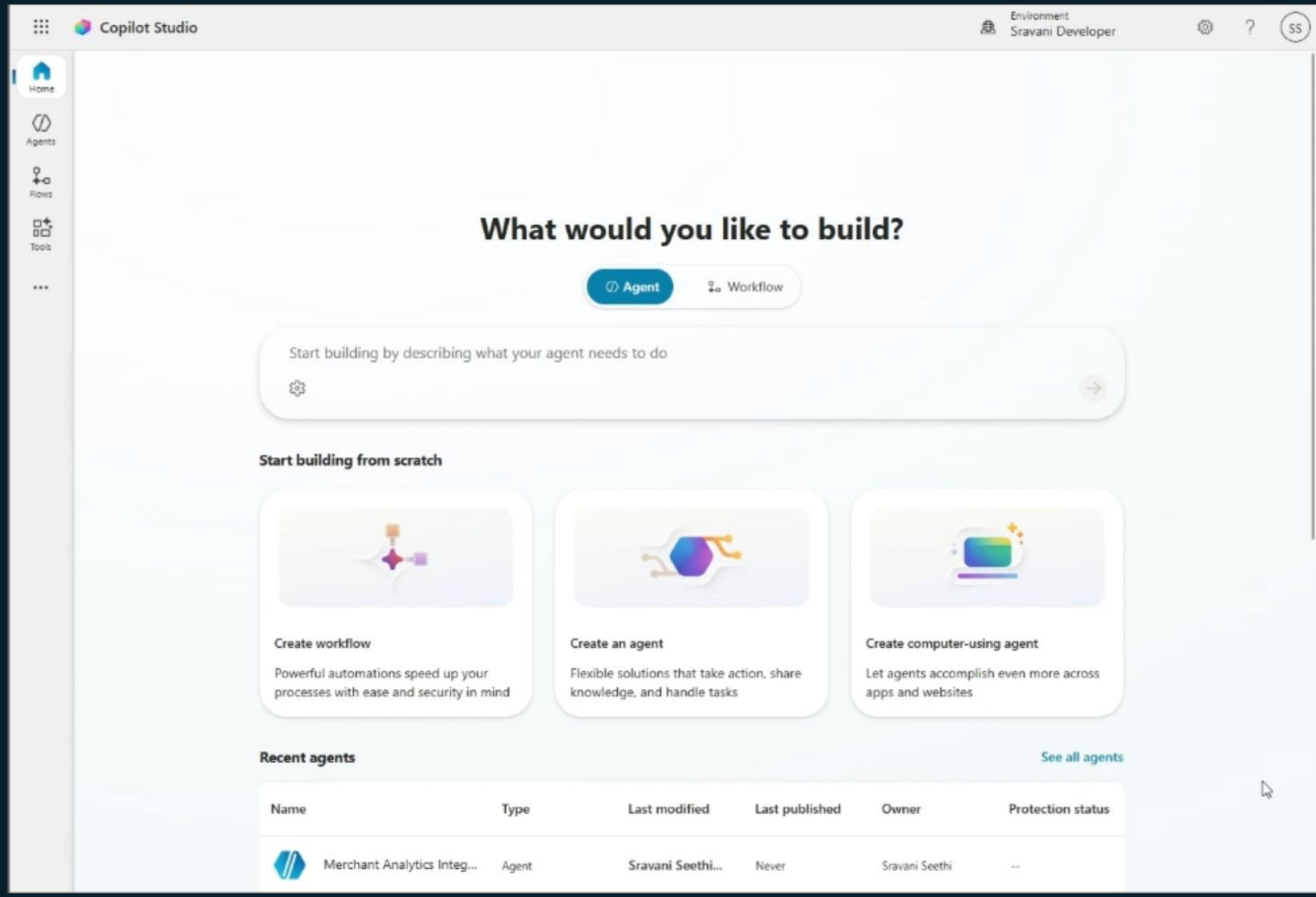
Best for tasks using internal systems, resources and apps

Scalable Cloud PC pools Entra-joined to your tenant

Single sign-on to enterprise resources

Powered by Windows 365 for Agents

Building a Computer-Using Agent



Applications of Computer Using Agents (CUA)

Microsoft

Scenarios

Data entry

Create sales orders in SAP for each row in the incoming CSV, then write the generated order ID back to the file

Data extraction

Access supplier portals, search for SKUs, extract price, stock, and lead time, and insert results into the database

Visual interpretation

Navigate dashboards, capture key KPIs, and generate email reports

Across Apps

Export the day's transactions from the desktop finance client, navigate QuickBooks, post each entry to the correct account

Demo scenario

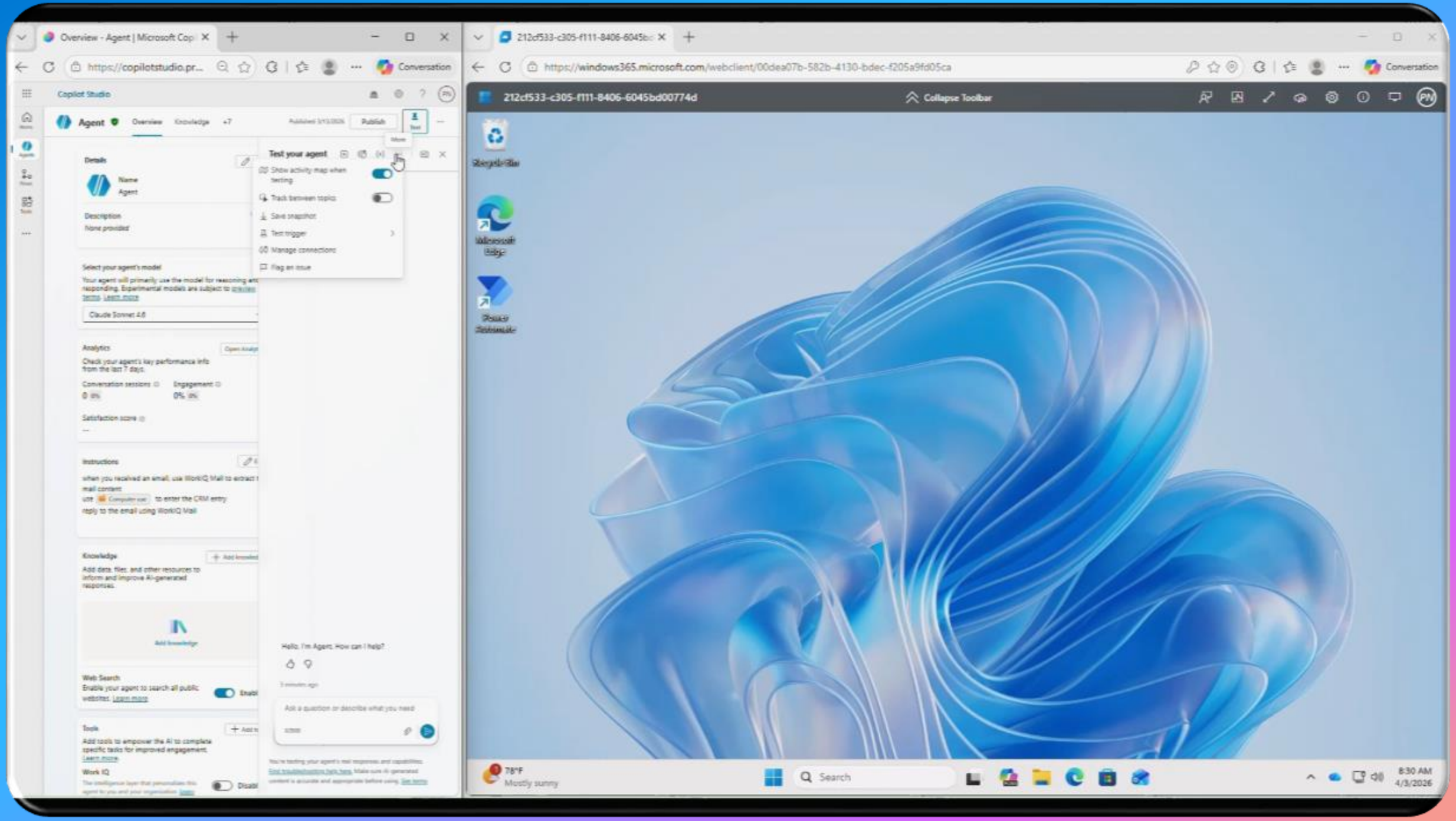
Scenario

An autonomous agent built with Copilot Studio is demonstrated, triggered by an incoming email event to automate CRM updates when no API is available, replicating end-to-end human interaction with the system.

The agent processes the email, understands the context, and executes actions directly through the application interface, ensuring high accuracy and resilience even in dynamic environments.

Steps of the agent

1. Receives and analyzes the email to extract relevant details and build an execution plan.
2. Navigates through a browser, accesses the CRM website, and enters information step by step, validating each action before proceeding.
3. Adapts navigation in real-time based on screen content for accuracy and resilience.
4. Validates the CRM record for completeness, then responds to the user with appropriate information.
5. Orchestrates multiple tools, switching to generate and send an email response, combining reasoning, computer use, and tool orchestration for streamlined business processes.


Overview - Agent | Microsoft Cop
https://copilotstudio.pr...
Conversation
Copilot Studio
Agent
Overview
Knowledge
Publish
Test
Details
Name
Agent
Description
None provided
Test your agent
Show activity map when testing
Track between topics
Save snapshot
Test trigger
Manage connections
Flag an issue
Select your agent's model
Claude Sonnet 4.6
Analytics
Check your agent's key performance info from the last 7 days.
Conversation sessions
Engagement
Satisfaction score
Instructions
Knowledge
Add data, files, and other resources to inform and improve AI-generated responses.
Web Search
Enable your agent to search all public websites.
Tools
Add tools to empower the AI to complete specific tasks for improved engagement.
Work IQ
Hello, I'm Agent. How can I help?
Ask a question or describe what you need
212cf533-c305-f111-8406-6045bd00774d
https://windows365.microsoft.com/webclient/00dea07b-582b-4130-bdec-f205a9fd05ca
212cf533-c305-f111-8406-6045bd00774d
Collapse Toolbar
Conversation
78°F
Mostly sunny
Search
8:30 AM
4/3/2026

Enterprise Guardrails

Microsoft

CUA & Security

Within the Azure boundaries

Runs on the OpenAI CUA model hosted in Azure OpenAI - kept entirely within Microsoft's Azure boundary.

Your data is your data

Your data is not used to train or improve the model.

Encryption

All data is encrypted both in transit and at rest.

Audit trail

Screenshots and messages related to CUA are saved in Agent history. Only the agent owner can access them.

Machine controls

Intune policies can control which websites and applications CUA is allowed to operate on.

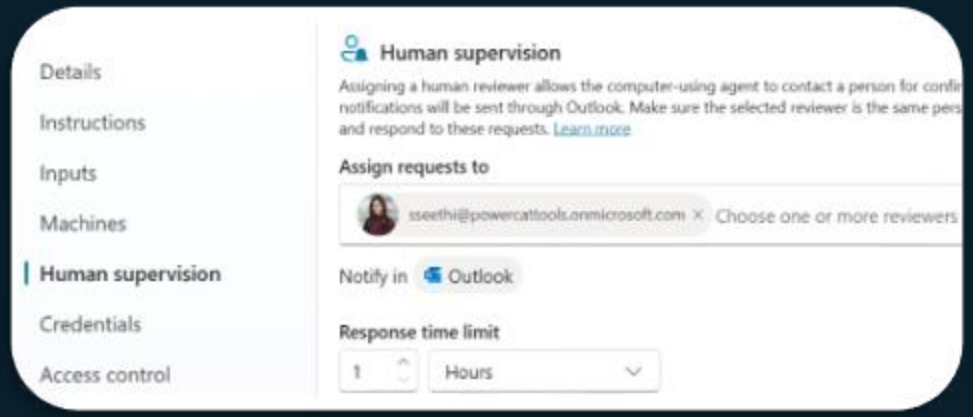
Thorough Responsible AI reviews

Applies to all Microsoft AI features, including this one.

Public preview

Human supervision

Computer use will reach out to you whenever it needs more information to continue



Public preview

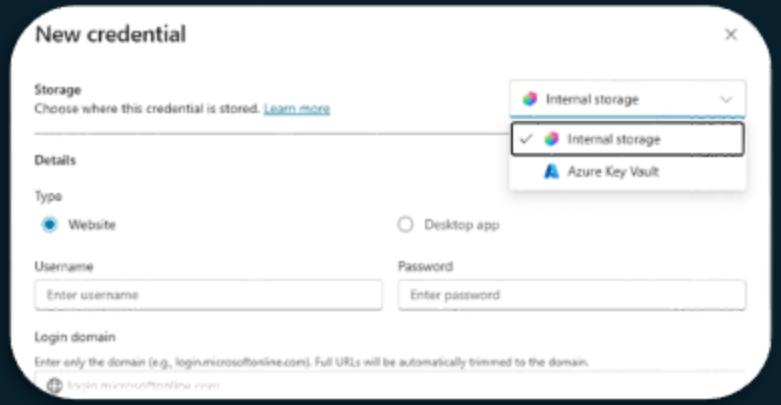
Observability

Rich activity feed with full audit logs available in Microsoft Purview

Public preview

Credentials

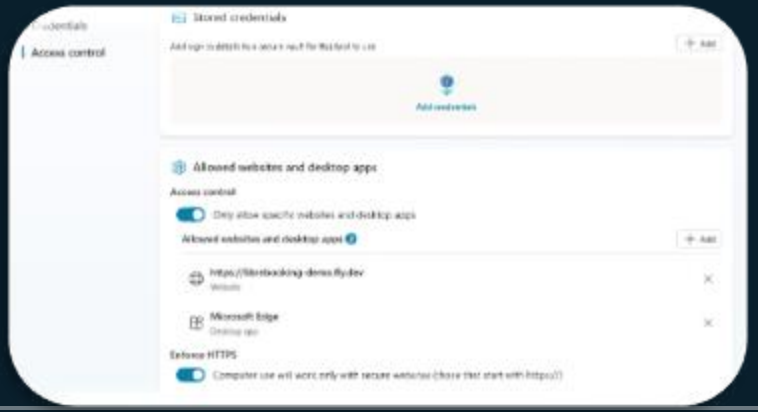
Secure credential storage directly stored within Copilot Studio or via Azure Key Vault



Public preview

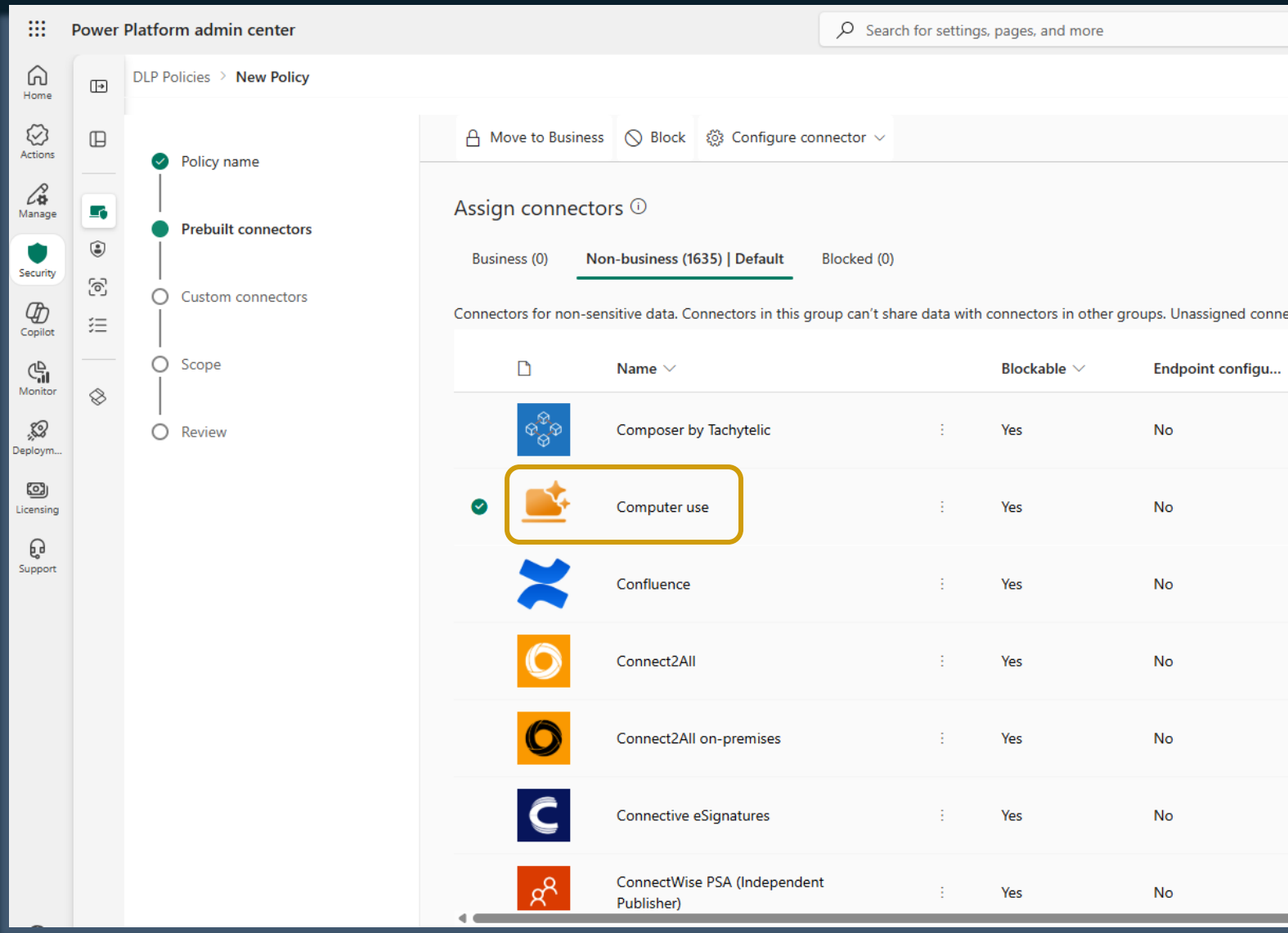
Allowlist

Restrict which websites and desktop applications are allowed to operate



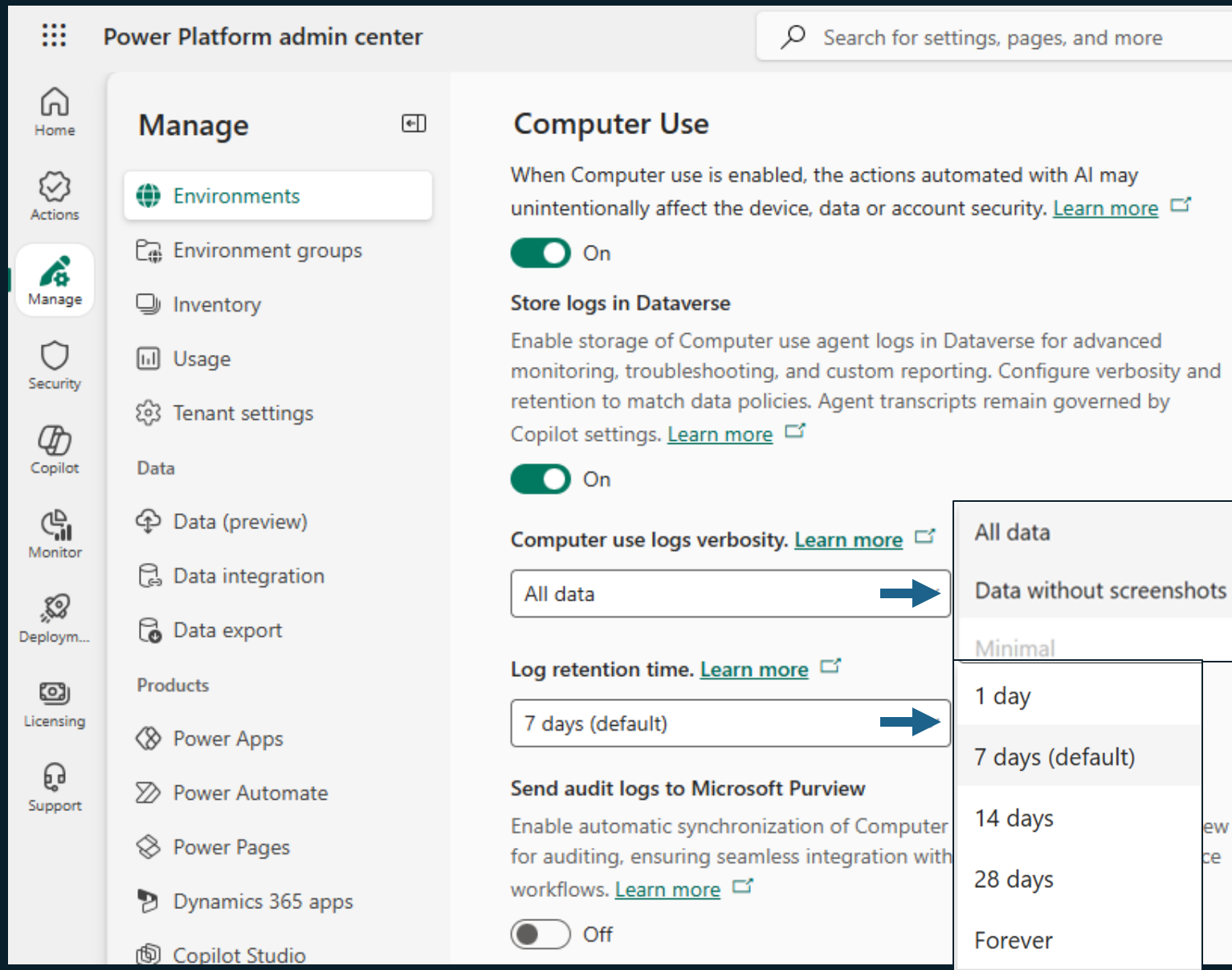
DLP policies for computer use

Tenant Level Data Loss Prevention (DLP) policies to enable or disable CUA tool/connector



Environment Controls

- Enable / Disable CUA for each environment
- Manage Logs and retention
- Send audit logs to Purview



What’s Next!

Microsoft

Best Practices

Security

- Use dedicated, isolated machines for computer use
- Apply least-privilege access to user accounts
- Allowlist trusted websites only
- Restrict desktop apps to essentials for the workflow

Instructions

- Be explicit: include full URLs and exact app names
- State actions clearly (submit, send, save)
- Break down complex UI steps
- Use step-by-step formatting for longer tasks

Data

- Explicitly describe what data to extract
- Specify output format: text or JSON
- Structure JSON clearly when passing data to other tools
- Include downstream tool (e.g., email) in instructions

High level Roadmap

Jan-Feb'26

New Anthropic and OpenAI models

Instructions builder

Human in the loop

March'26

New Anthropic models

Geo Expansion

Admin level machine & allow list controls

Apr-May'26

Human in the loop

CUA General Availability

Get Started!

Try computer use in Copilot Studio today!

https://aka.ms/mcs-cua

We have an exciting future ahead.

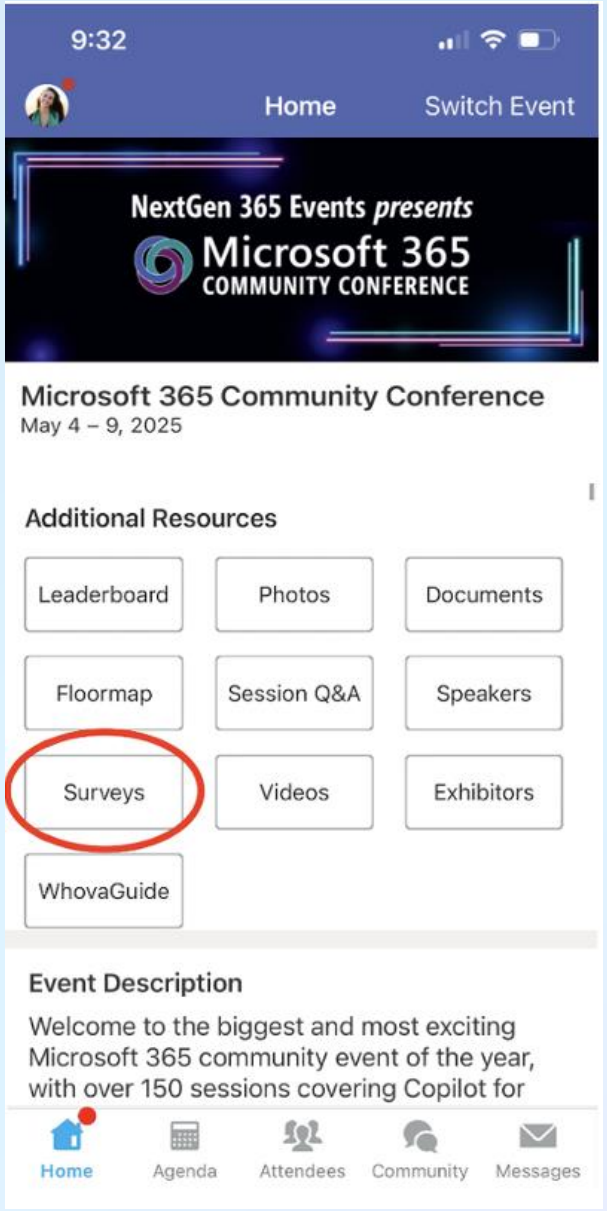
Whova

The official event app for the
Microsoft 365 Community Conference

Event invitation code: Orlando2026

Join the event app to access:

- Event announcements
- Personalized agenda, session details
- Speaker & attendee profiles
- Networking, meet-ups, messages
- Event documents



Session feedback surveys

We want to hear from YOU!

Share your feedback to make next years conference even better!

Here's how –

- Simply go to the Whova App on your smartphone.
- Scroll down on the M365 Community Conference Homepage to 'Additional Resources' to click "Surveys'.
- Click Session Feedback.
- Scroll down to find this session title.
- Complete the session feedback survey.
- Finally, click 'Submit'.

It's just that easy!