Microsoft

Getting Governance Right

Considerations for Enterprise Agent Adoption

Master SERIES

Jeffrey Bennett | Sr. Solution Engineer | AI Business Solutions

Microsoft

Agenda

1. Spectrum of Copilot Agents and Controls
2. Copilot Control System (CCS): Agent Management
3. Agent Measurement and Reporting
4. Data Protection
5. Agent 365

Microsoft

Spectrum of Copilot Agents and Controls

Top security and governance concerns about generative AI

Data oversharing and data leaks

80%

of leaders cited leakage of sensitive data as their main concern

Identification of risky AI use

41%

of security leaders cited that the identification of risky users based on queries into AI was one of the top AI controls they want to implement

AI governance and risk visibility

84%

want to feel more confident about managing and discovering data input into AI apps and tools

Copilot Control System

Copilot + Agents

Security & Governance	Management Controls	Measurement & Reporting
Data Security	Copilot licensing	Readiness and adoption
AI Security	Agent lifecycle	Productivity shifts
Compliance & privacy	Metering controls	Business value & ROI

Balancing Governance and Innovation

Agent Creator/Maker

- How can I **build a conversational agent** that will answer on my behalf?
- How can I build agents that can **drive efficiency and save efforts and costs** for our enterprise?

CISO

- How can I understand all my **data security risks**?
- How can I **discover** all agents and **protect my data** from external threats?
- How can I ensure agents have the right access to data and **prevent data exfiltration**?
- How can I **stay compliant with regulations**?

CIO

- How can I ensure that solutions people are building **follow guidelines?**
- How can I gain **visibility** to what is getting used?
- How can I get **experts to review agents** before they get shared broadly?
- How can I drive **cost efficiency and ROI?**

Agent Controls Model

Individual

Organizational

Zone 1

Citizen Development Zone

IT restricts makers to personal agents with read-only access based on content permissions

Zone 2

Partnered Development Zone

IT-approved makers build agents in secure, IT-managed environments and deploy them department-wide

Zone 3

Professional Development Zone

Pro developers build and deploy enterprise-grade agents with org-standard ALM

Data protection, agent sharing & usage limits, and reporting & cost management

Spectrum of Agents and Controls

	Agent Users – Agent Creators	Makers	IT Catalog
Tool	Agent Builder, SharePoint	Copilot Studio	Any Tool
Capabilities Available	Scoped subset of functionality available through Copilot	Triggers, connections to external systems, workflows	Full set of platform capabilities
Tool Controls	Copilot controls	Power Platform environment controls	M365 Admin Center Integrated Apps
Content Controls	Content permissions, Microsoft Purview, SharePoint Advanced Management		
Reports and Controls	Agent usage reports, inventory and block, agent metered consumption reports and controls		

Zoned security, governance, and operations

	Zone 1	Zone 2	Zone 3
Purpose	Citizen Dev agent creation (DIY) for personal use and experimentation with safe defaults	Team or Department Agents in the partnered DIY zone require formal assistance and oversight from a DIY coach, but are built by trained citizen developers	Large, potentially risky agents in the professional development zone are reserved for pro dev & IT-led development only
Secure	Only M365 and Power Platform Connectors Agents run in user's context only	Zone specific Advanced Connector policies in Power Platform Admin Center Teams share access to approved Data sources Scale with Environment groups + rules	Zone specific Advanced Connector policies in Power Platform Admin Center + Purview
Govern	Personal use agents in Developer Environments. Environment routing keeps agents isolated to maker. Sharing disabled and scoped to just Maker use	Admin approved environments provisioning Scoped roles and sharing policies ALM Pipelines for agent versioning IT-admin approval to publish agents	Manage sharing via Integrated Apps in Microsoft Admin Center
Monitor	Review agent usage in Copilot Hub in Power Platform	Track agent usage and security posture in Microsoft Admin Center, Microsoft Purview, and Power Platform Admin Center	

Spectrum of Copilot Agent Capabilities

Zone 1

Zone 3

Retrieval

Retrieve information from grounding data, reason, summarize, and answer user questions

Generally available

Task

Take actions when asked, automate workflows, and replace repetitive tasks for users

Generally available

Autonomous

Operate independently, dynamically plan, orchestrate other agents, learn and escalate

Preview

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

Agent data

Models
1900+ Azure AI Foundry

Bring your own models with Azure AI Foundry integration to tailor agent responses using 1,900+ models including Phi-4, Grok 3, and Hugging Face.

Knowledge
Context aware agents

Unify and operationalize content from files, Dataverse tables, and more using patterns that range from simple read operations to advanced vector-based retrieval.

Tools
1500+ connectors

Enable agents to take real action, whether it's automating workflows through MCP, or connecting to third-party systems, so your solutions go beyond insights to impact.

Orchestration
Agent to agent

Build multi-agent systems where agents collaborate to complete complex, business-critical tasks across systems, teams, and workflows.

Agent Knowledge and Tools

Data connectors

External systems

Microsoft Graph

Productivity data (Microsoft 365)

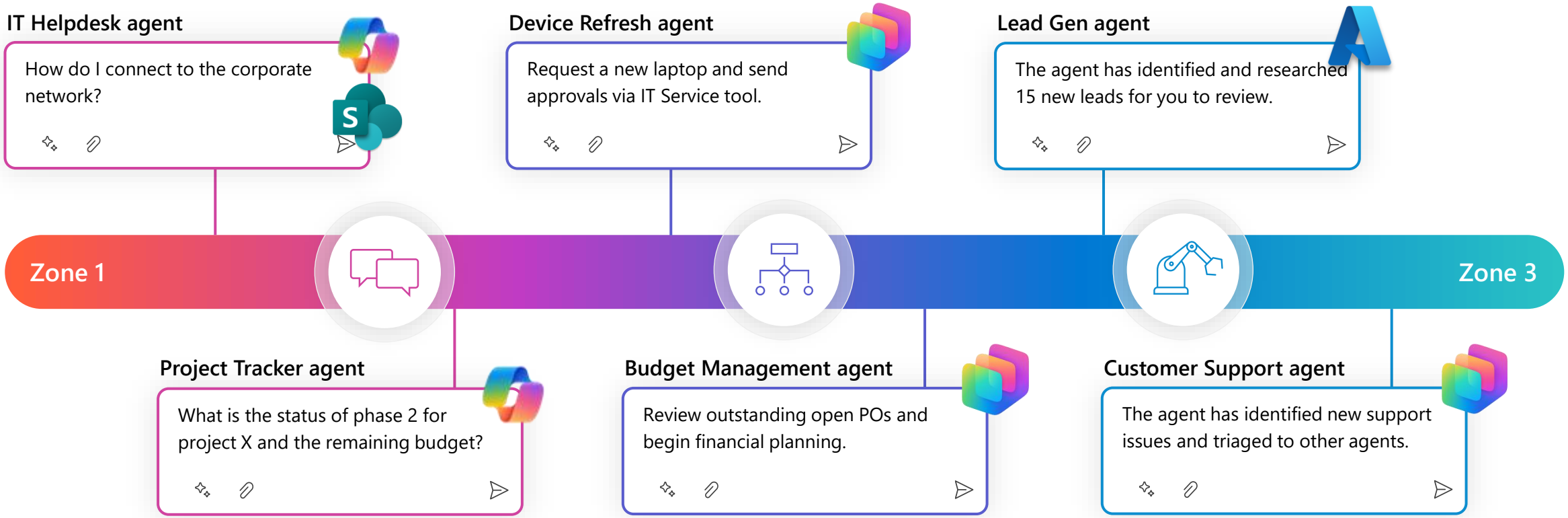
Microsoft Dataverse

Business data

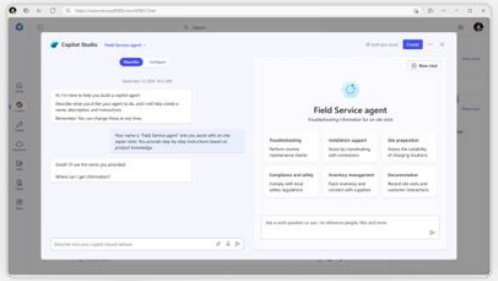
Microsoft Fabric

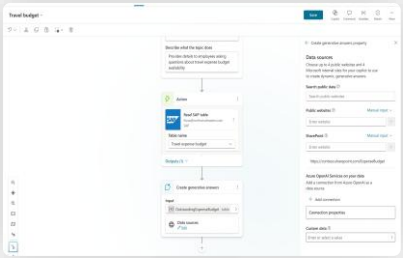
Analytics

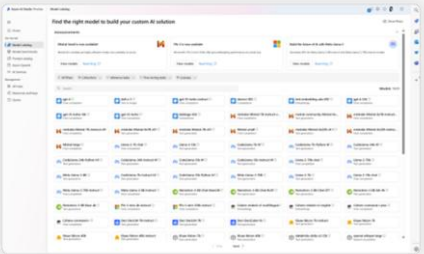
Explore a continuum of solutions



Advanced agents require more advanced governance and security







Conversational

Advanced

	Agent builder	Copilot Studio	Copilot Studio + Azure AI
	Users/Creators	Makers	Developers
Knowledge	Microsoft Graph		Your Business Data
Actions	Retrieval Only		Task / Autonomous
Channels	Microsoft 365 Only		Multiple Internal & External Channels

Increasing advanced governance and security needs throughout agent lifecycle

1. Development & Testing

2. Deployment

3. Optimization

Tools to secure and govern your Copilot use

Security and Governance

- Prepare your environment to implement secure Copilot Studio adoption
- Identify risks related to data, users, and agents to prevent sensitive data leakage and ensure agents do not process sensitive files.
- Prevent data loss and insider risks by securing sensitive files, agent interactions, and providing alerts and reports on risky behavior and AI usage.
- Govern AI use to meet regulations and policies by inspecting interaction content and audit logs, investigating for compliance and ethical violations, and enforcing lifecycle policies and legal holds.

Management Controls

- Establish clear guidelines and policies for agent behavior to ensure consistency and compliance across all interactions.
- Evaluate agent performance regularly using key performance indicators (KPIs) to identify areas for improvement and give prompt feedback.
- Implement agent policies to restrict oversharing of agents and manage publishing channels.
- Enhance the manageability of agents across various environments and ensure precision with application lifecycle management features.

Measurement and Reporting

- Track agent performance metrics in real-time to ensure timely and accurate reporting of key performance indicators (KPIs).
- Analyze data collected from agent interactions to identify trends, areas for improvement, and opportunities for training and development.
- Share reports with relevant stakeholders to facilitate informed decision-making and continuous improvement in agent performance and customer service.

Microsoft

Copilot Control System (CCS)

Agent Management

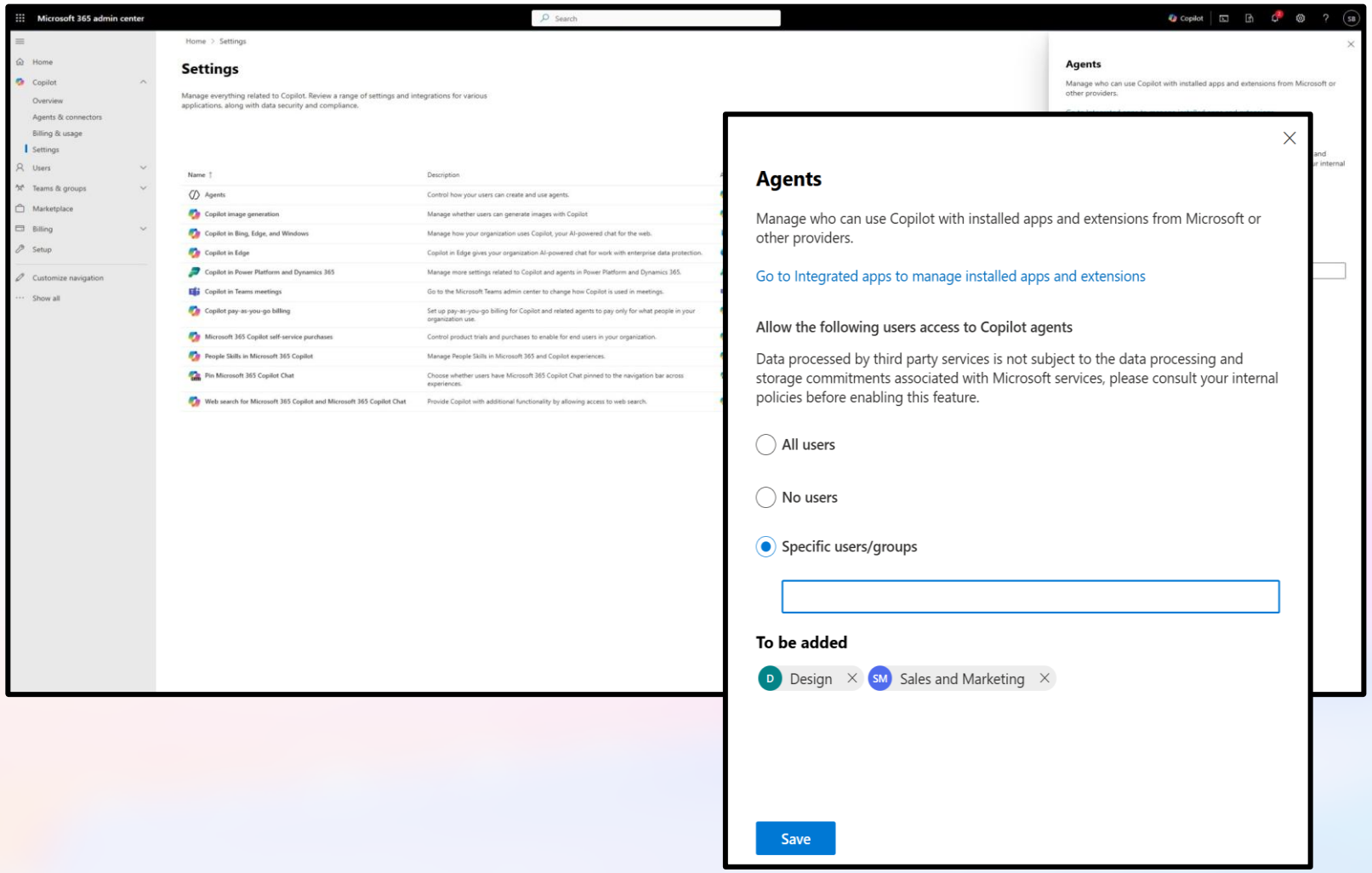
Manage who can create and use agents

Generally Available

AI admins can manage who can create and use agents in M365 Copilot Chat

Options to enable agents for all users, no users, or specific users and groups

Enables staged rollout of agents by security groups



Product images subject to change

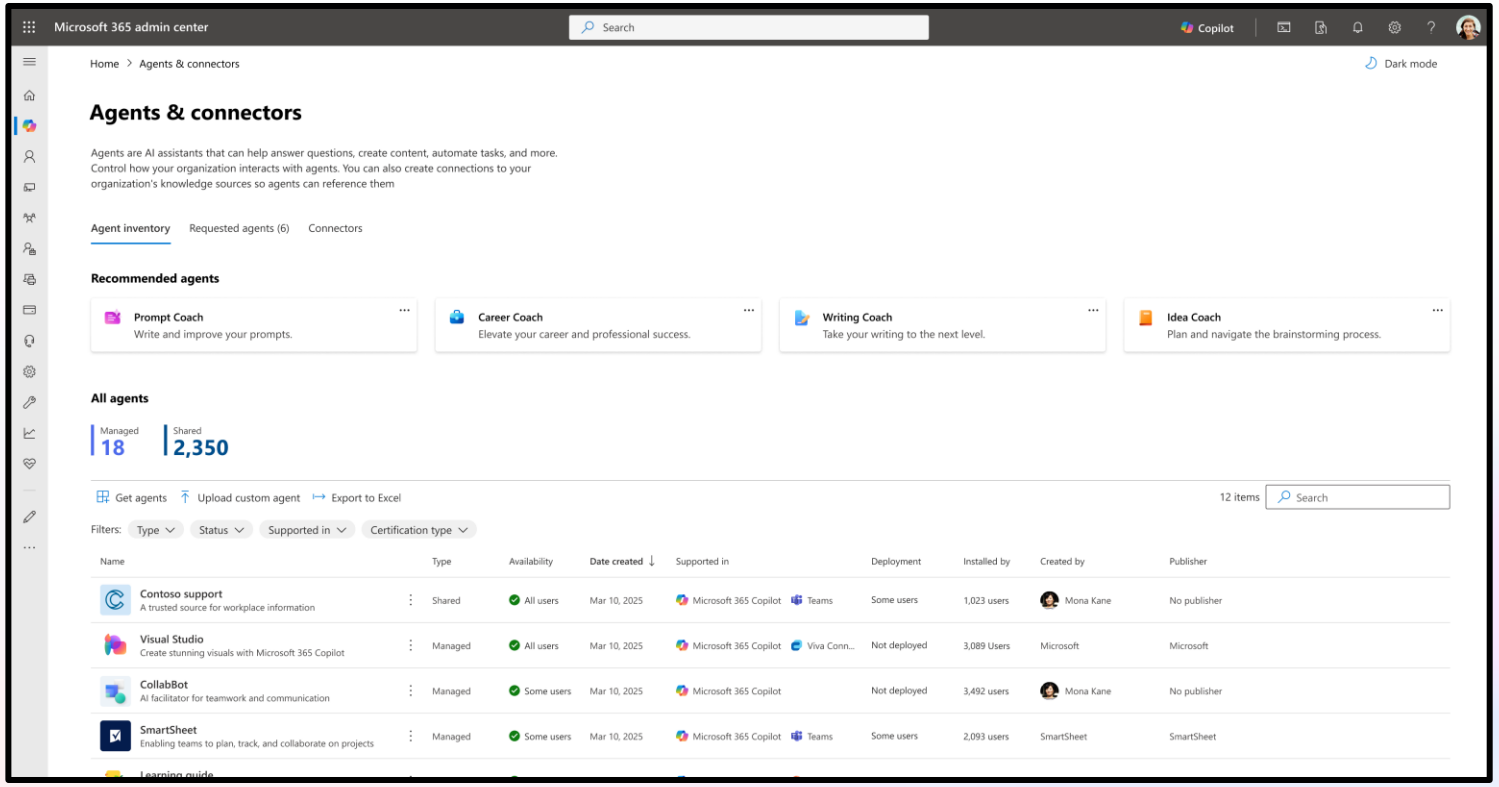
Central management of agents in M365 Copilot Chat

GA: Q2CY2025

Agent inventory - rich agent metadata, capabilities, data sources, custom actions, certification details and more

Deploy and block agents, review and approve requested agents

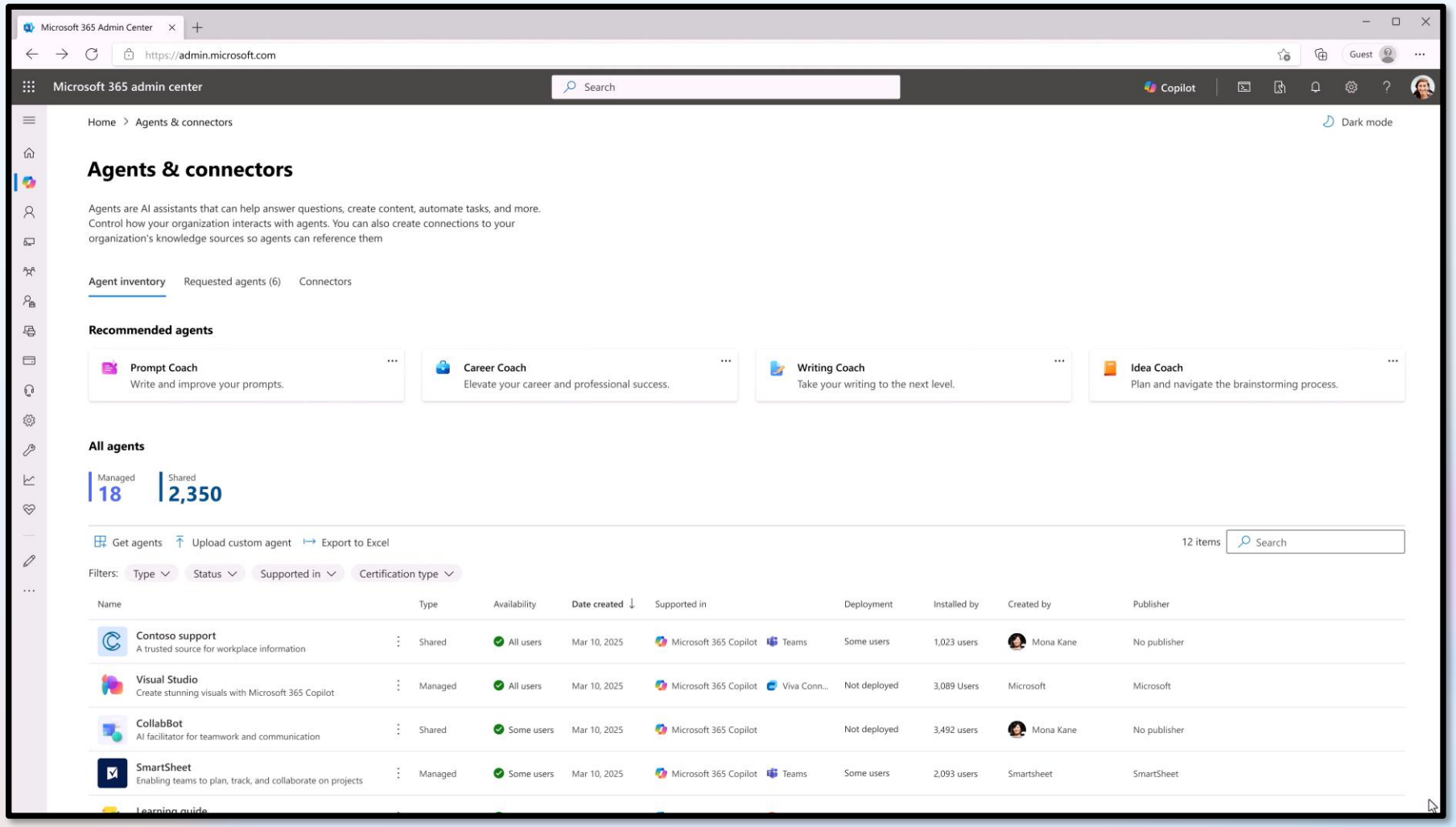
Agent-level user access controls



Product images subject to change

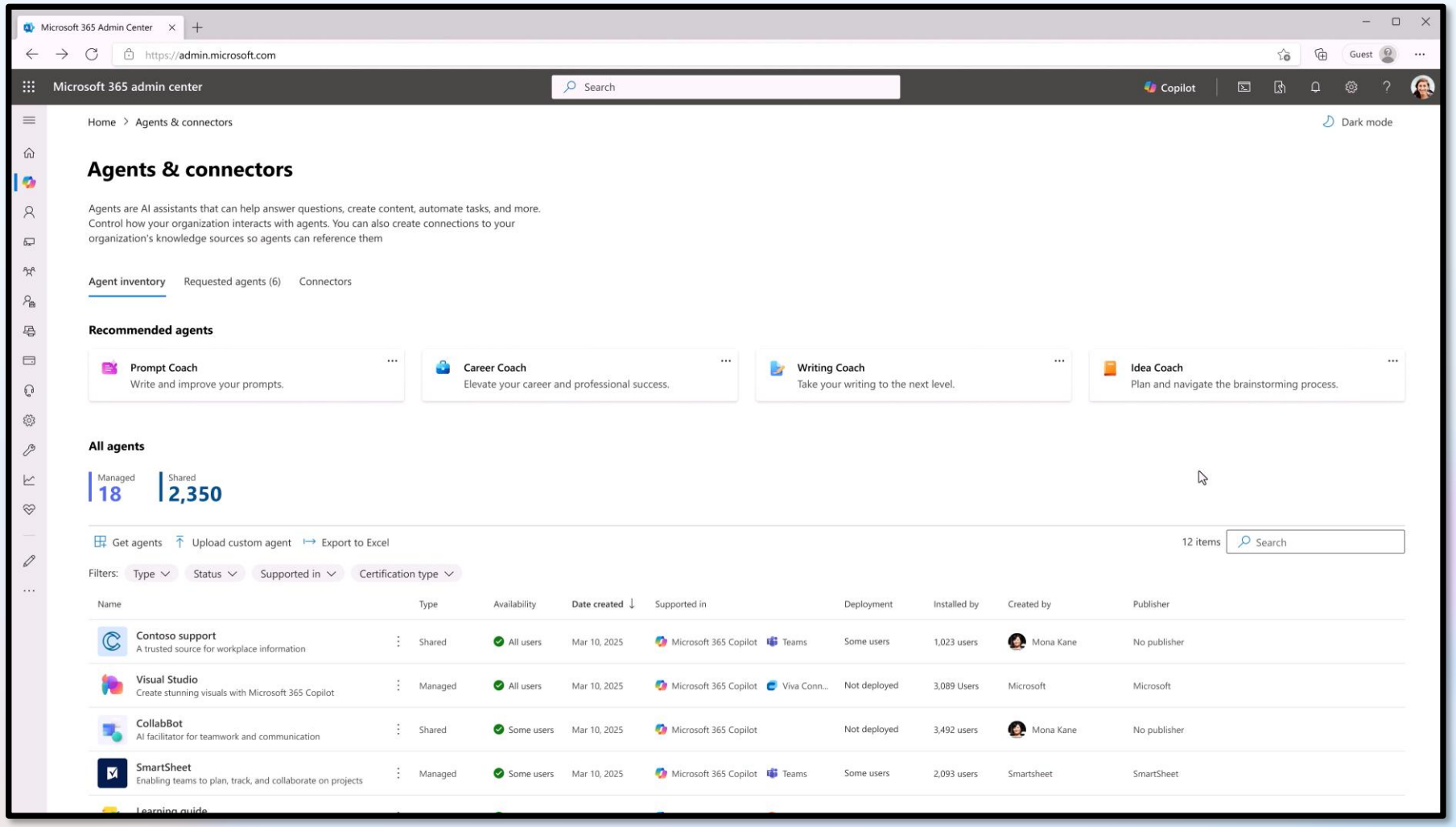
CCS – Agent Management

Deploying a recommended agent to all users



Product images subject to change

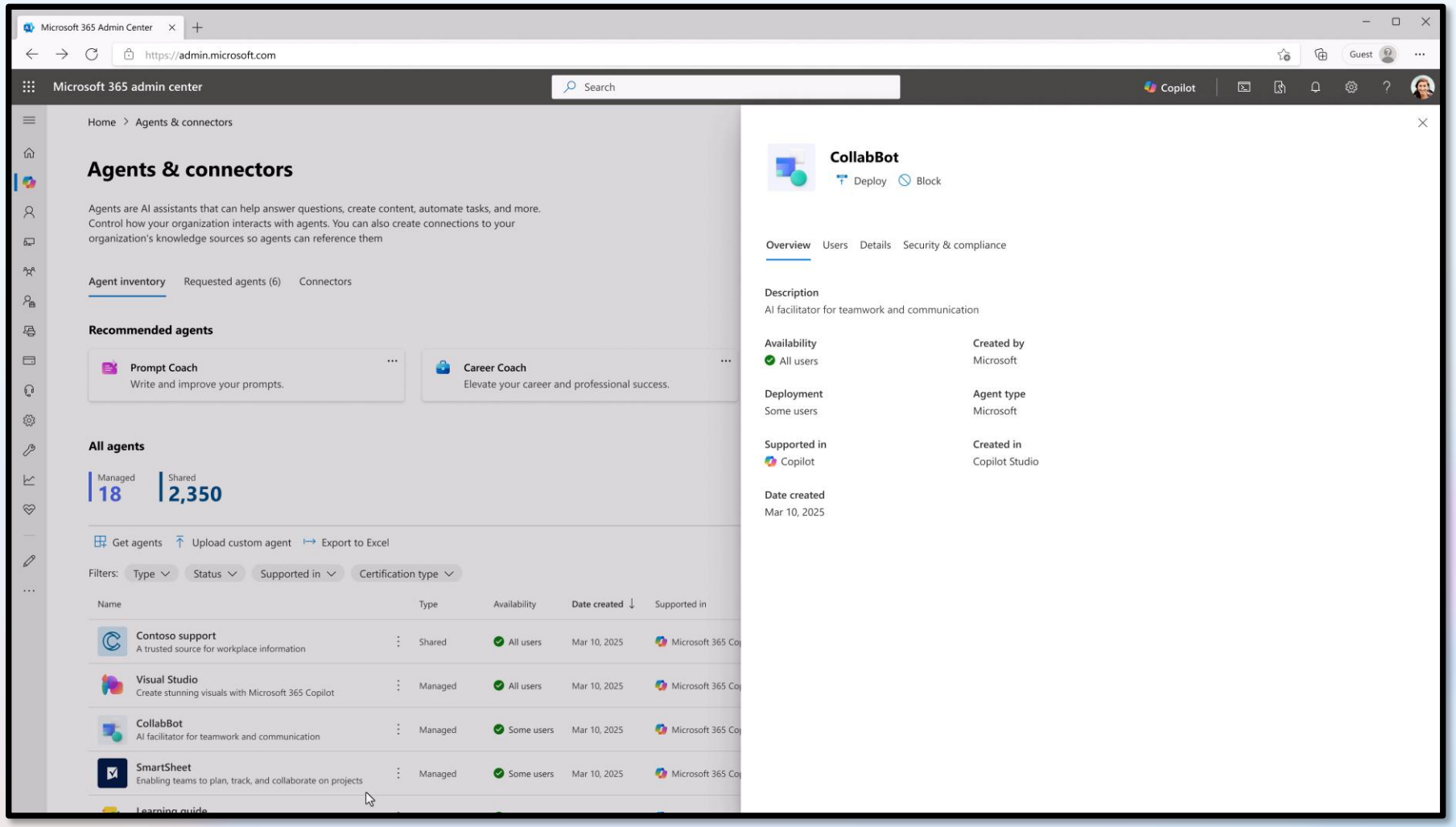
Deploying an agent to a group of users



Product images subject to change

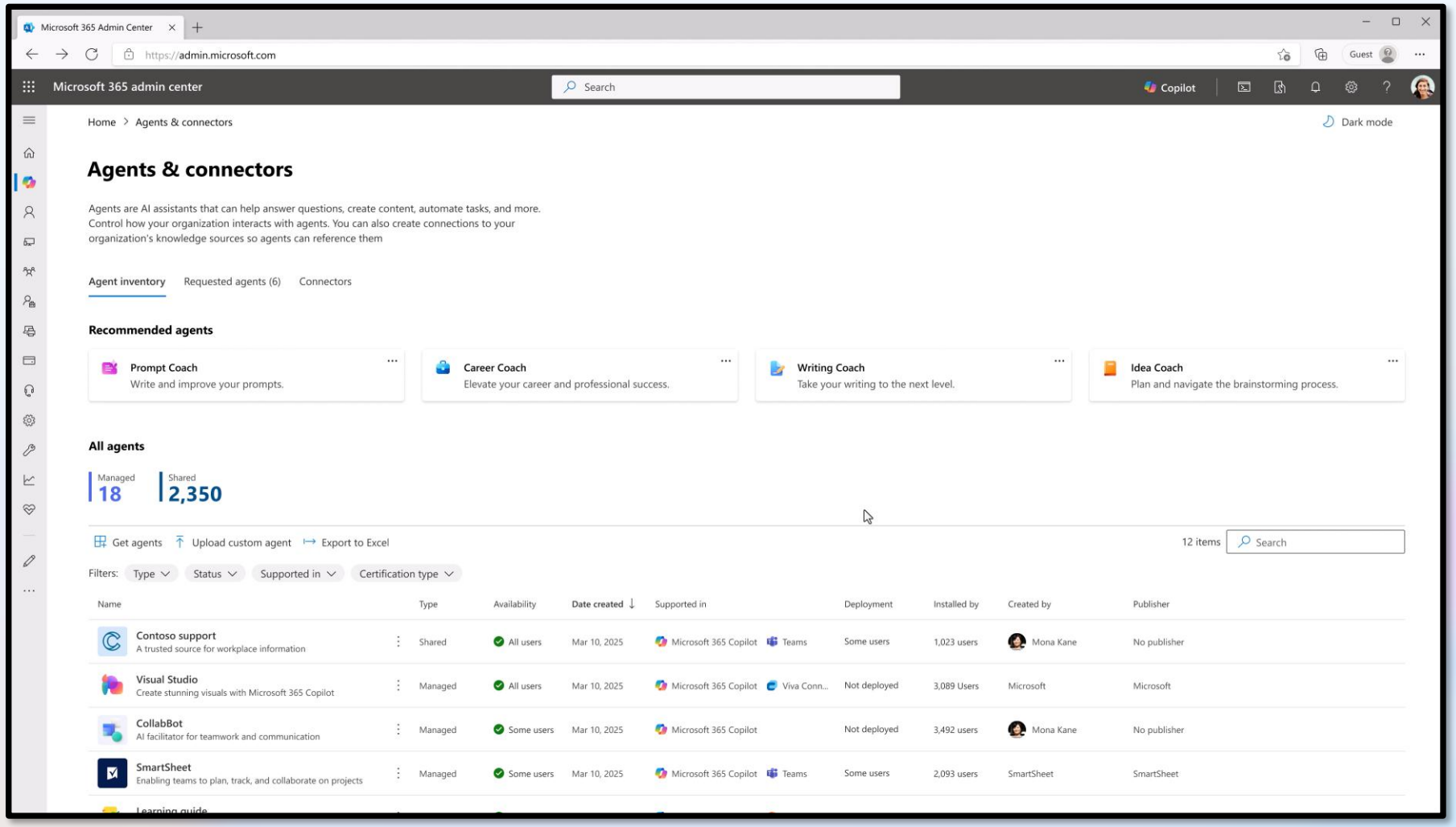
CCS – Agent Management

Remove user access to an agent



Product images subject to change

Block an agent



Product images subject to change

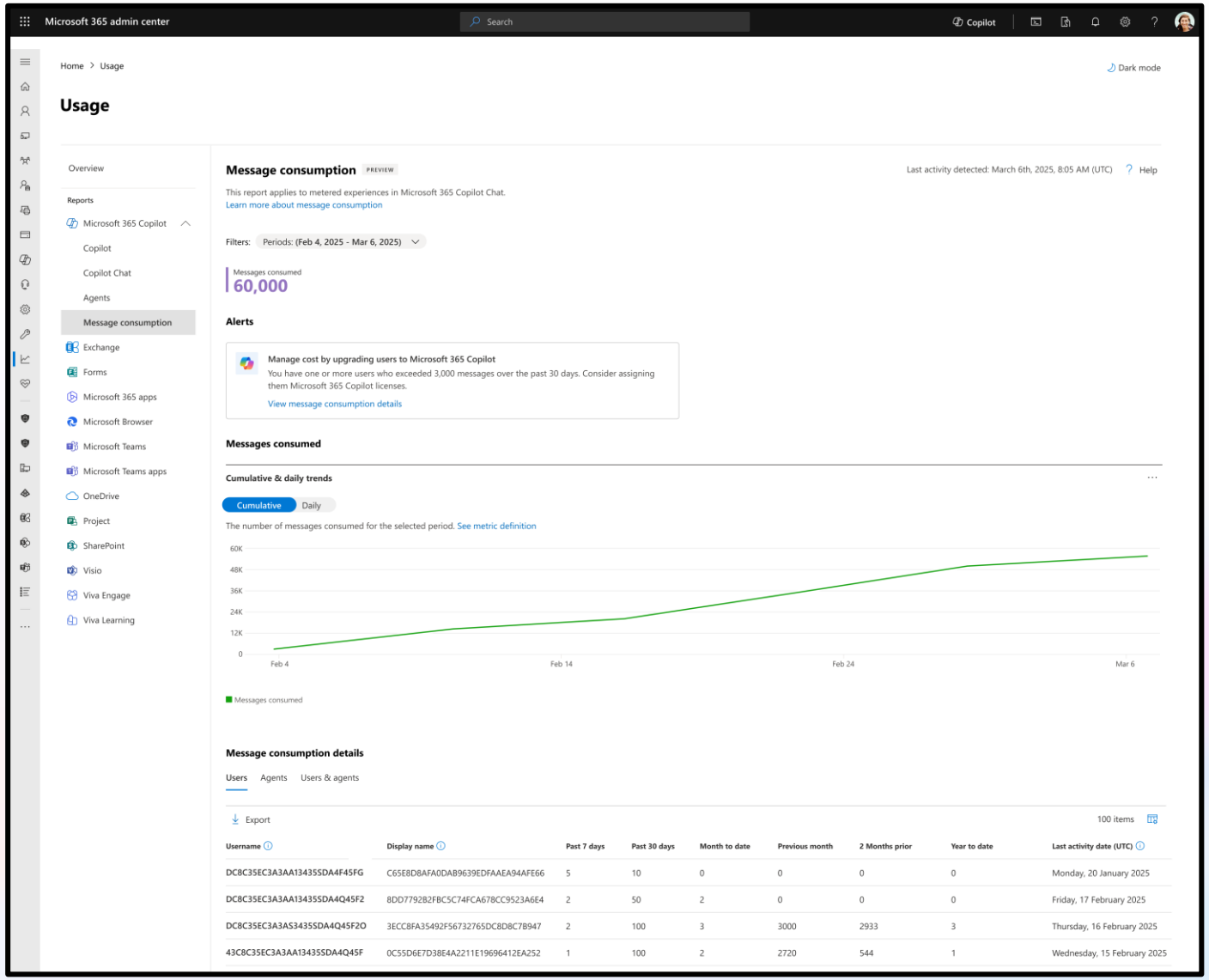
Track message consumption

Public preview: Q2CY2025

Near real-time visibility into metered message consumption

Total messages consumed for the selected period with cumulative and daily trends

Line-level consumption details per user, agent, billing policy*, and user-agent pair



**Consumption per billing policy planned for Q3CY2025*

Assess agent usage

Public preview: Q2CY2025

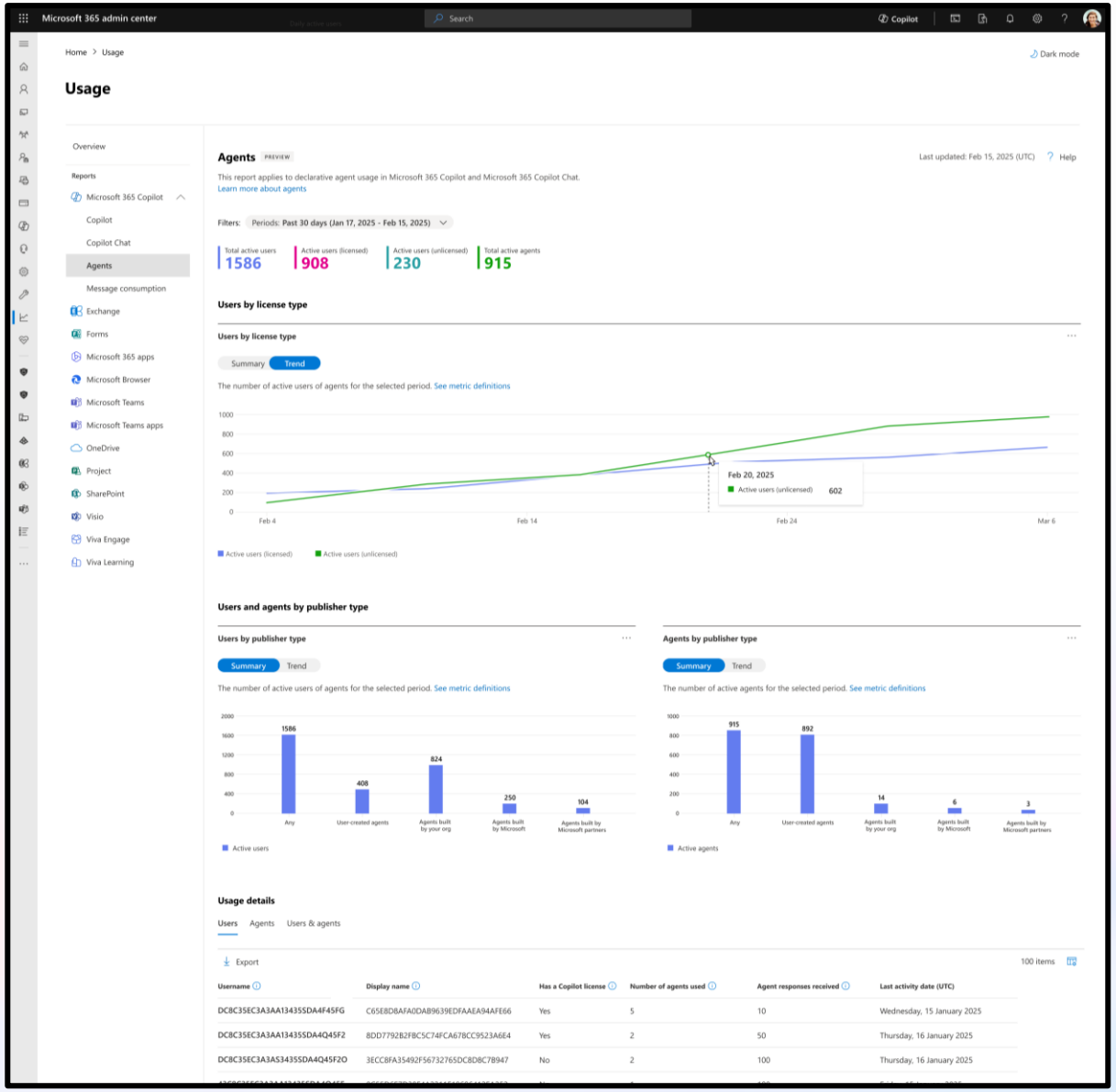
Inform agent management and adoption strategy decisions with insight into agent usage

Total active users with segmentation by M365 Copilot licensed and unlicensed users

Total active agents

Active users and active agents by publisher type i.e. user-created, built by your org, built by Microsoft, built Microsoft partners

Line-level details per user, agent, and user-agent pair



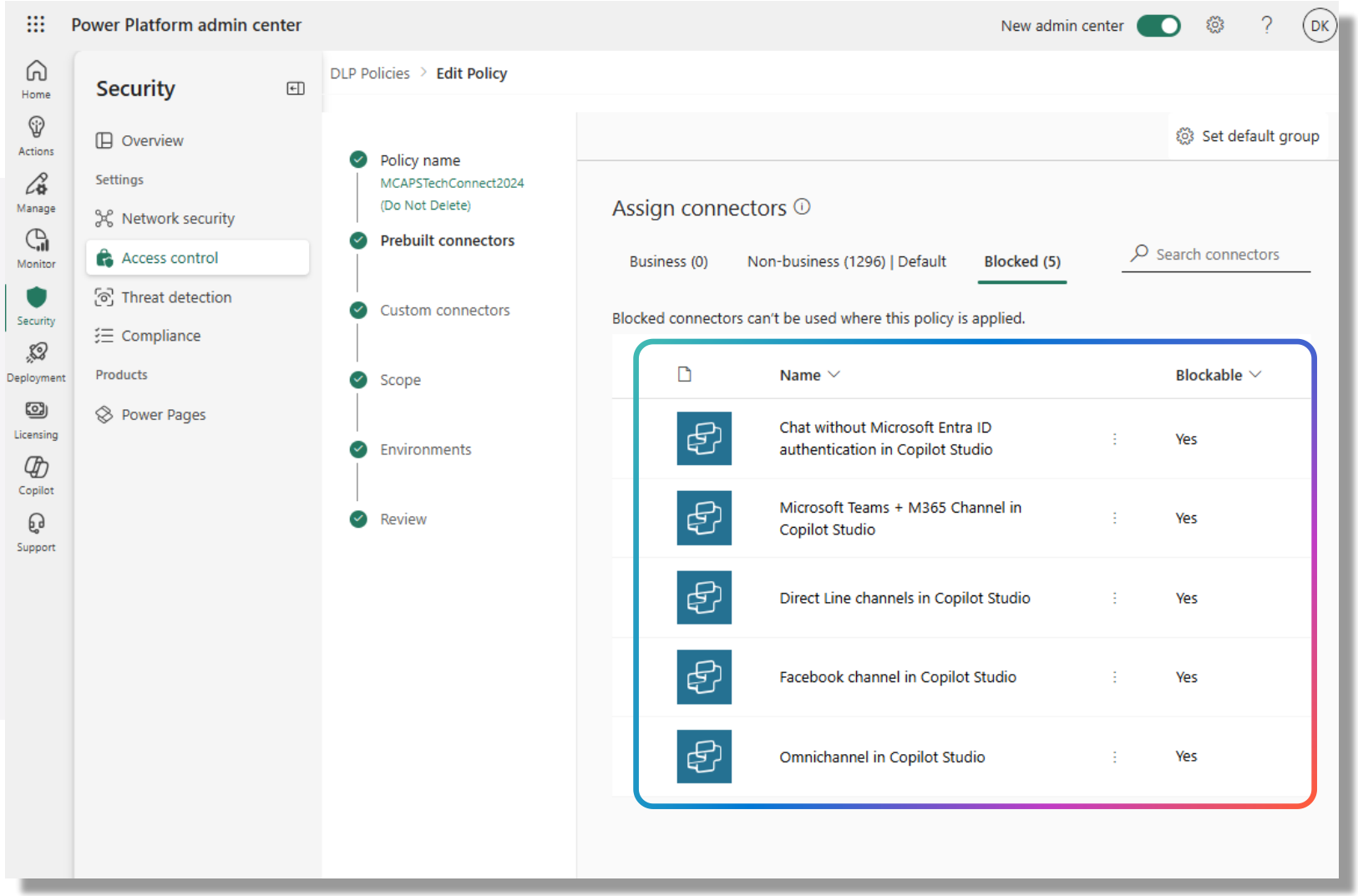
Product images subject to change

Copilot Studio

Power Platform Admin Center: Secure Agent Access

Secure agent access by disabling publish using connector management and by disabling access from internet to chat.

Limit agent sharing to co-authors or end users who chat.



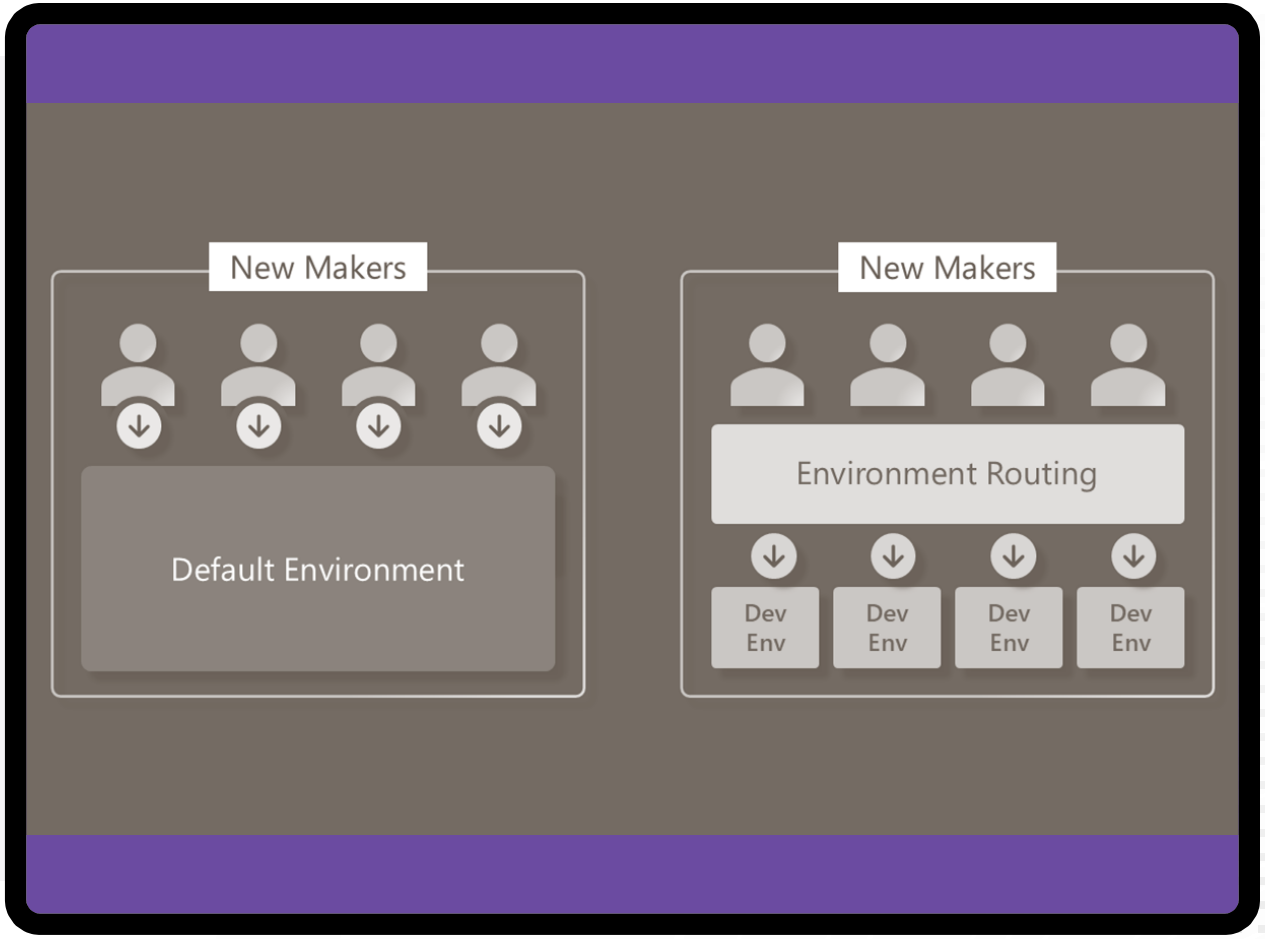
Copilot Studio

Power Platform Admin Center: Environment Groups

Secure by default: Makers build in their own secure, pre-configured environment instead of default.

Enhanced manageability: It is easier to govern when users and assets are distributed across environments.

Healthy ALM: Avoids clutter in the default environment. Only relevant assets are promoted.

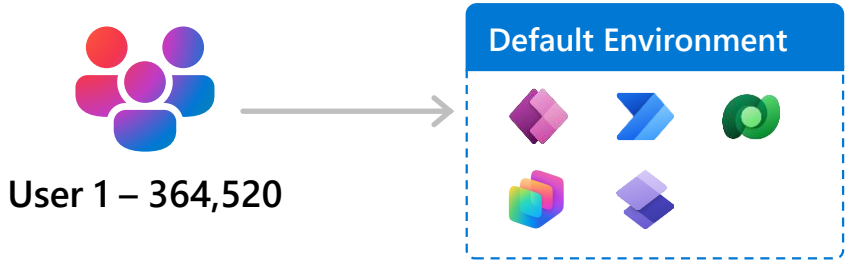


Available for: Power Apps Copilot Studio Power Automate

Power Platform Admin Center: Environment Groups & Rules

Bulk management of environments

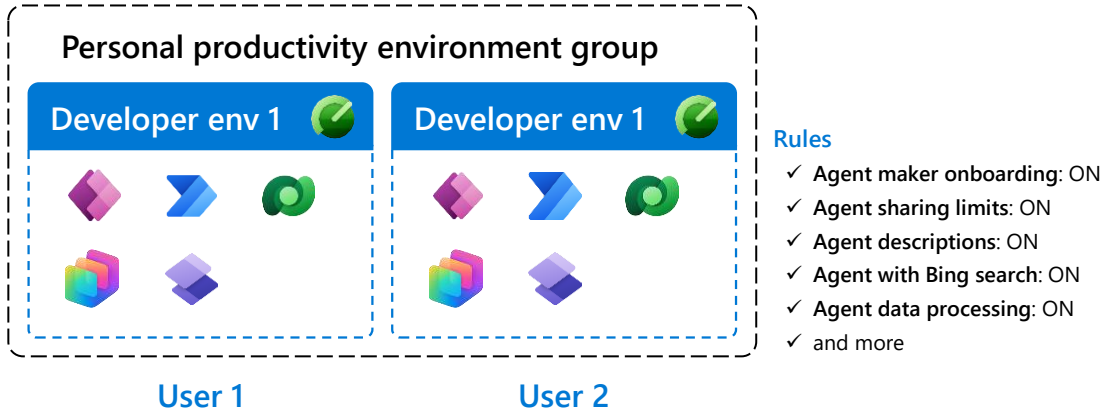
Environment groups manages 30,000+ identically configured environments.



Before

Lock the settings of environments

Lower-level admins and users cannot override the environment group's rules.

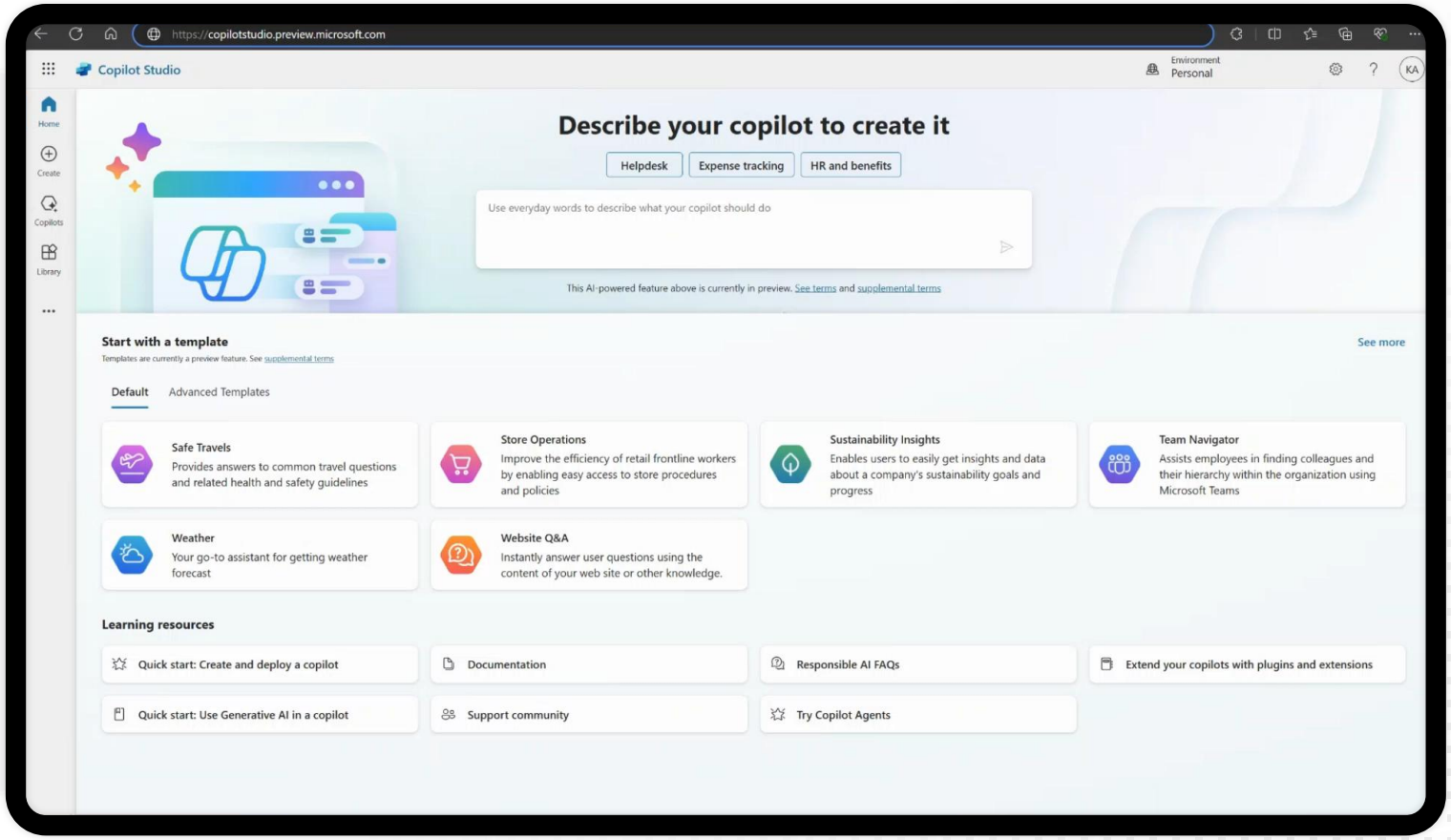


After

Power Platform Admin Center: Environment Groups + Rules + Environment Routing

When paired with Environment Routing…

- Provision **new developer environments** into specified groups
- **Route Copilot Studio makers** to their own developer environments
- Configure **new environments** based on predefined rules
- Welcome Copilot Studio makers with **Maker Onboarding**



Copilot Studio

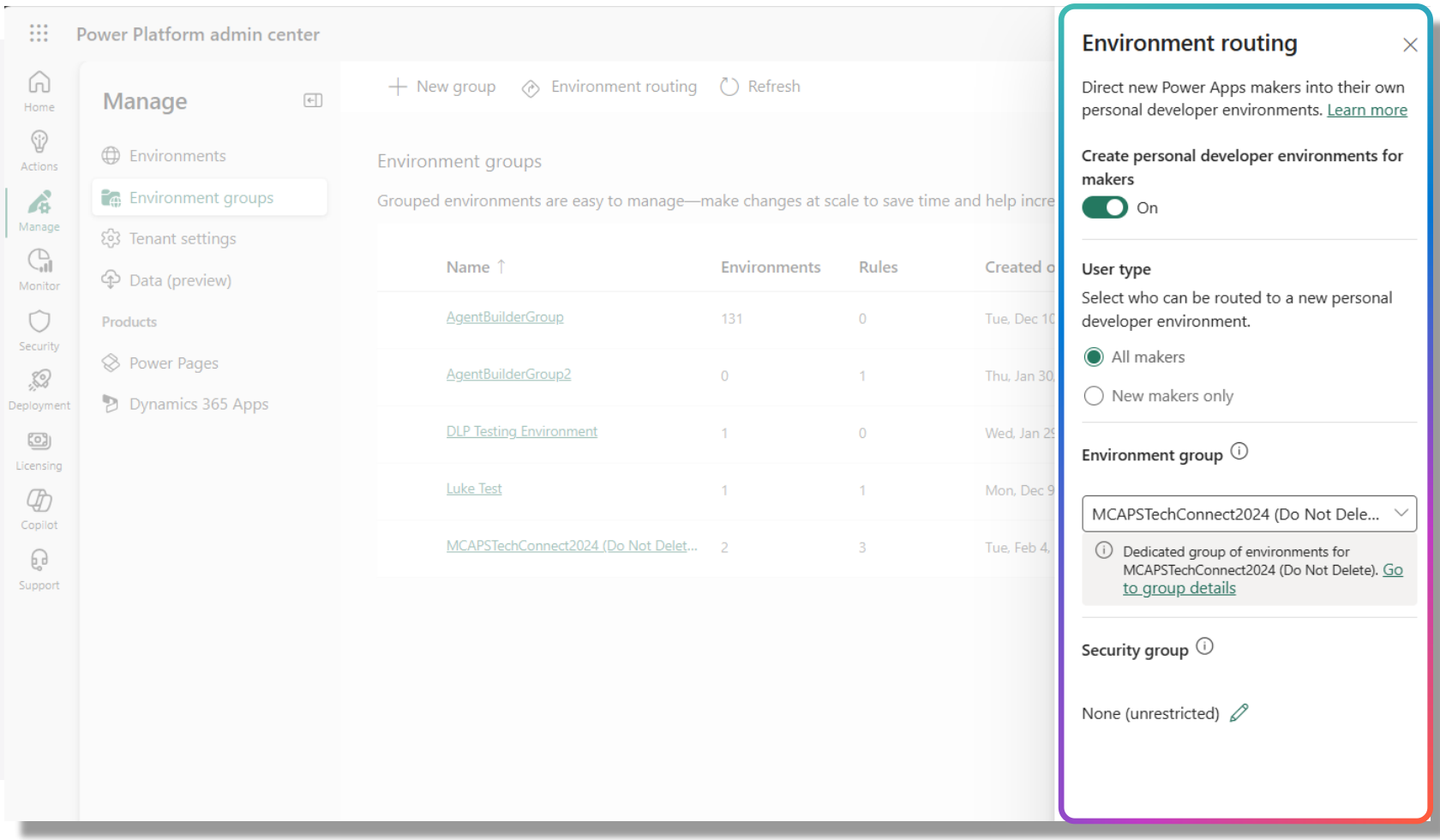
Power Platform Admin Center: Govern Agents at Scale

Generally available

Makers can build agents in personal environments without the fear of others accessing their agents.

Deploy and certify agent solutions using Pipelines from development to production environments.

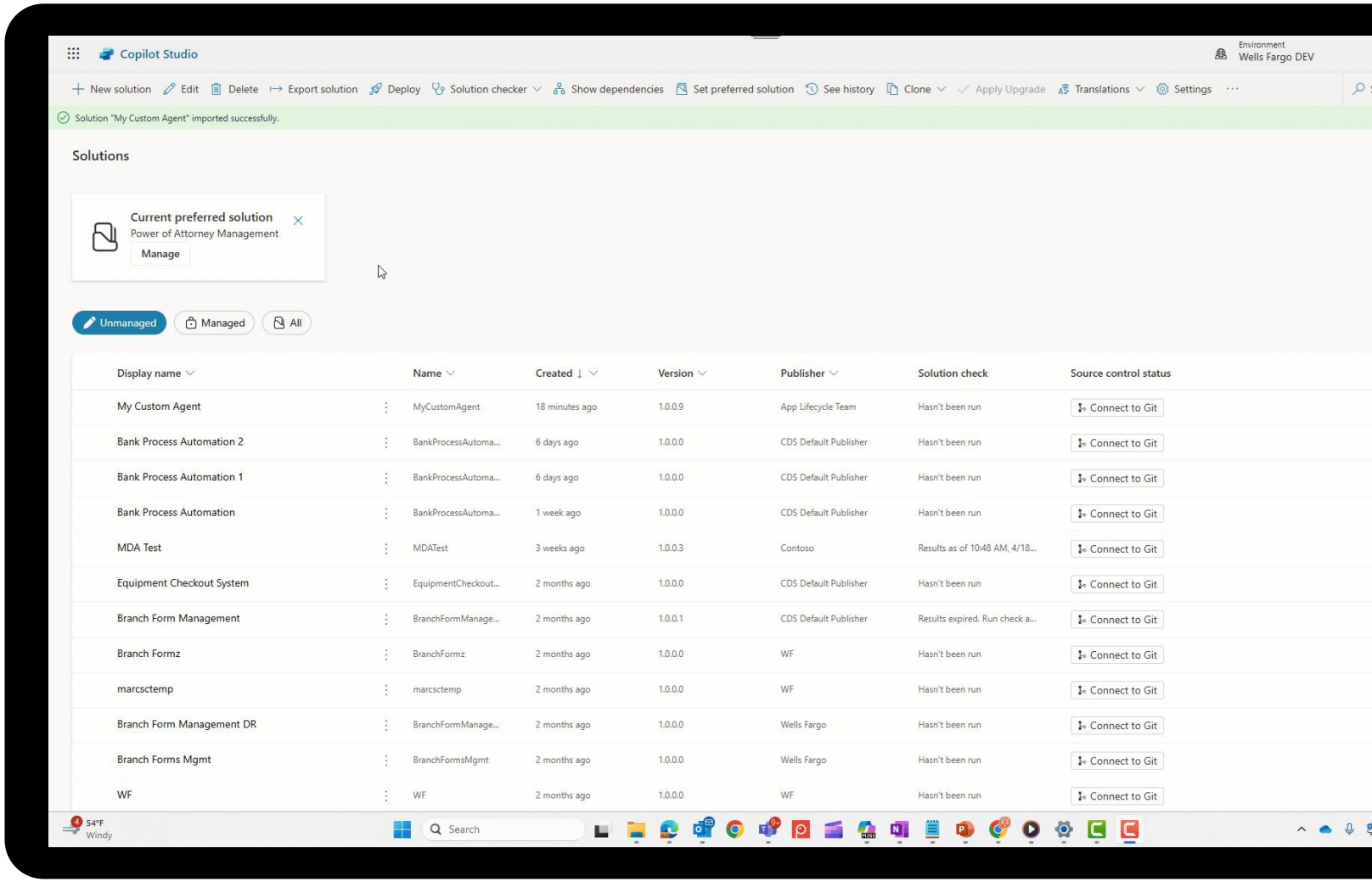
Maker welcome message to inform agent authors about important privacy and compliance requirements.



Power Platform Admin Center: Preferred Solution

Generally Available

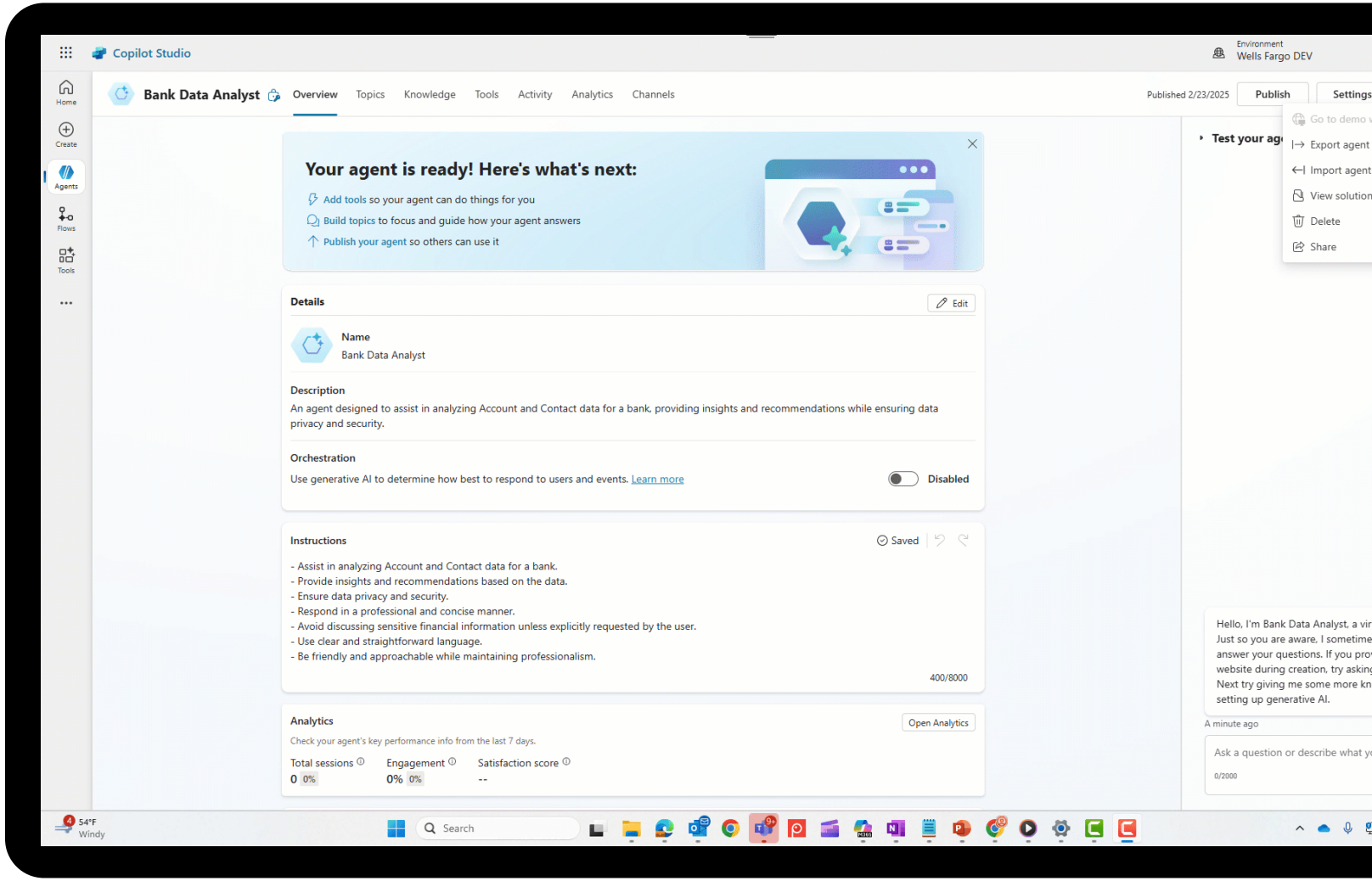
- Keeps customizations organized
- Works across all maker experiences
- Starts every maker with “healthy” ALM



Power Platform Admin Center Pipelines + Onramps

Generally Available

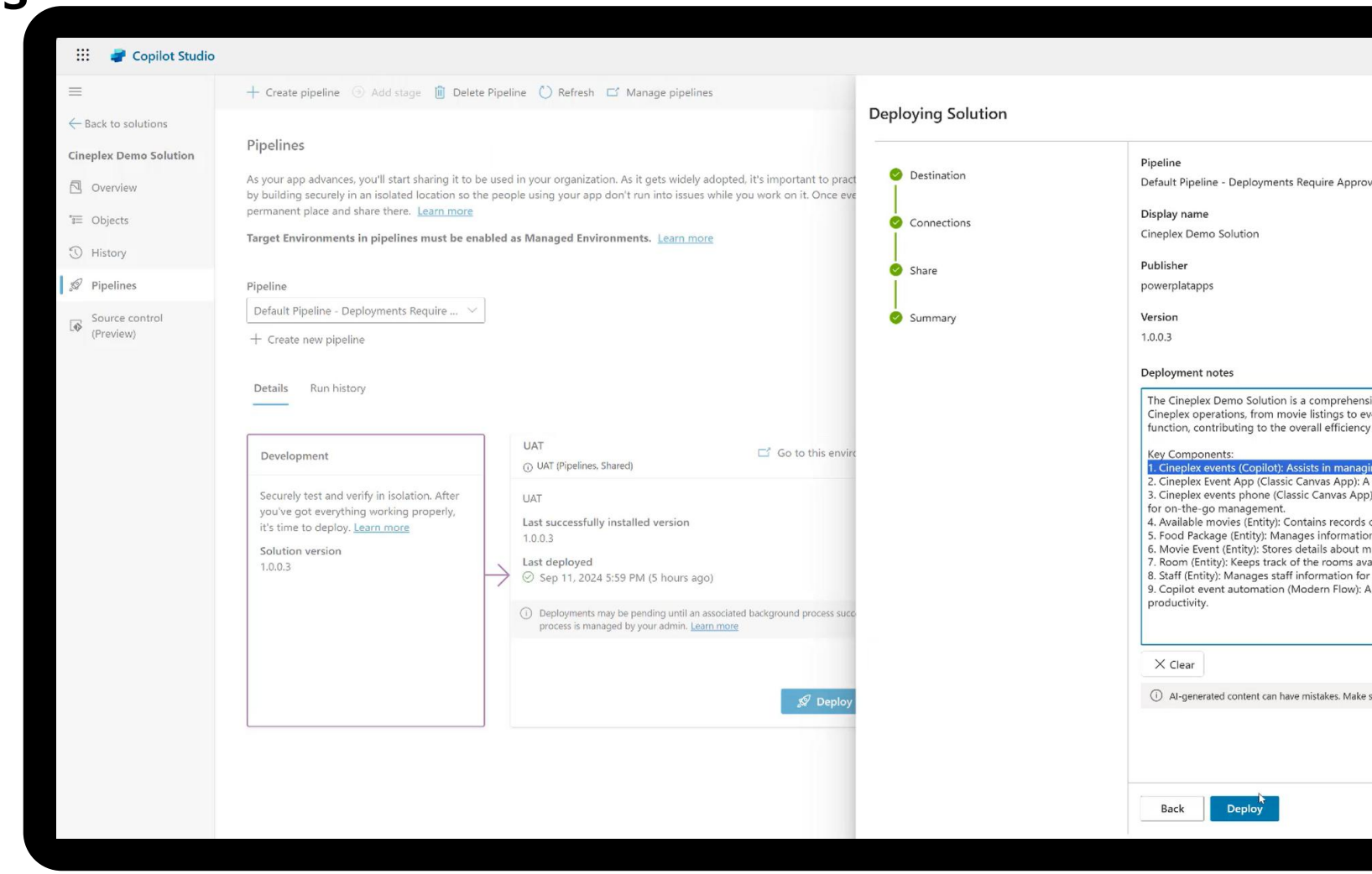
- Traverses “sharing limits” cliff
- Directs users to deploy to production environments
- Seamlessly connects the Maker ALM journey



Power Platform Admin Center
Agent Deployment notes

Generally Available

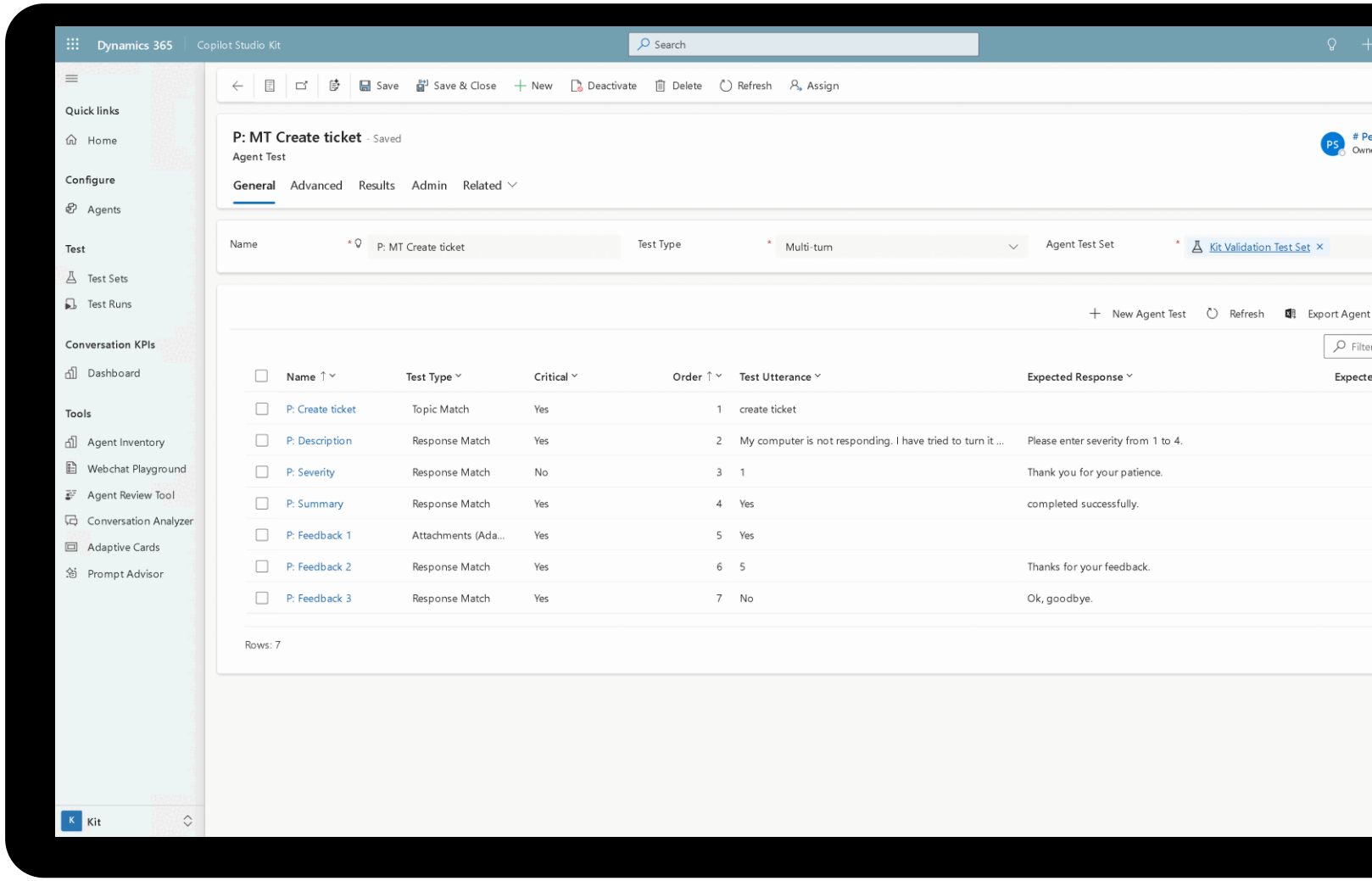
- Copilot generates deployment notes for pipelines deployments
- Gives makers insights into every deployed version with less effort
- Streamlines the approval process
- **Agents** now included in key components!



Test Automation with Copilot Studio Kit

Generally Available

- Build test cases using multiple validation methods - including using AI model to validate the response
- Easily validate the core scenarios of your custom agent
- Automatically perform hundreds of test cases with a click of a button



Introducing Foundational Governance with Copilot

Provided with SharePoint Advanced Management [1,2]

Reduce site sprawl

Identify patterns and potential issues with reporting and receive actionable recommendations.

Run automated, rule-based policies to manage and retire inactive sites and their content.

Create and leverage AI-powered policies and reports to govern content at scale.

Control site oversharing

View reports that identify sites that contain potentially overshared or sensitive content.

Enforce stringent access conditions when users access SharePoint sites with access policies.

Prevent sites and content from being discovered with restricted content discovery control.

Manage site lifecycle

Review and monitor changes you've made to a SharePoint site's properties.

Use broad reports to review changes to SharePoint site properties.

Leverage policies to ensure proper content ownership and manage unused content across the organization.

[1] Capabilities which require Microsoft Purview (Extended SharePoint Permissions or Default Sensitivity Label for a SharePoint Document Library) require separate licensing of those products
[2] SharePoint Advanced Management is available as a standalone offer (3 PUPM) for customers without a Copilot license

SharePoint admin center

Your SharePoint Advanced Management subscription is enabled.

- Home
- Sites
  - Active sites
  - Archived sites
  - Deleted sites
- Containers
- Policies
- Settings
- Content services
- Migration
- Reports
- Advanced
- More features
- Advanced management PRO
- Customize navigation
- Show all

Home > Advanced management

Advanced management

Manage and govern SharePoint and OneDrive with advanced tools and enhanced Microsoft 365 secure collaboration abilities.

Learn more about SharePoint Advanced Management

What's included

Feature ↑	Location	Purpose
Block download policy for SharePoint and OneDrive	Microsoft PowerShell	Prevent download for both external and internal users
Change history	Reports > Change history	Find who made particular site or organization setting changes and when
Conditional access policies for SharePoint and OneDrive	Microsoft Entra conditional access	Control whether users can access sensitive sites based on conditions like location or operating system
Data access governance reports	Reports > Data access governanace	Discover potential oversharing and keep track of sites that have sensitive files
Default sensitivity labels for document libraries	Library settings and Create document library panel	Help make sure sensitive project files are appropriately labeled
OneDrive access restriction	Policies > Access control > OneDrive access restriction	Allow only particular groups of users to use OneDrive
Recent actions	Active sites > Recent actions	Review recent site changes you made

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

Microsoft

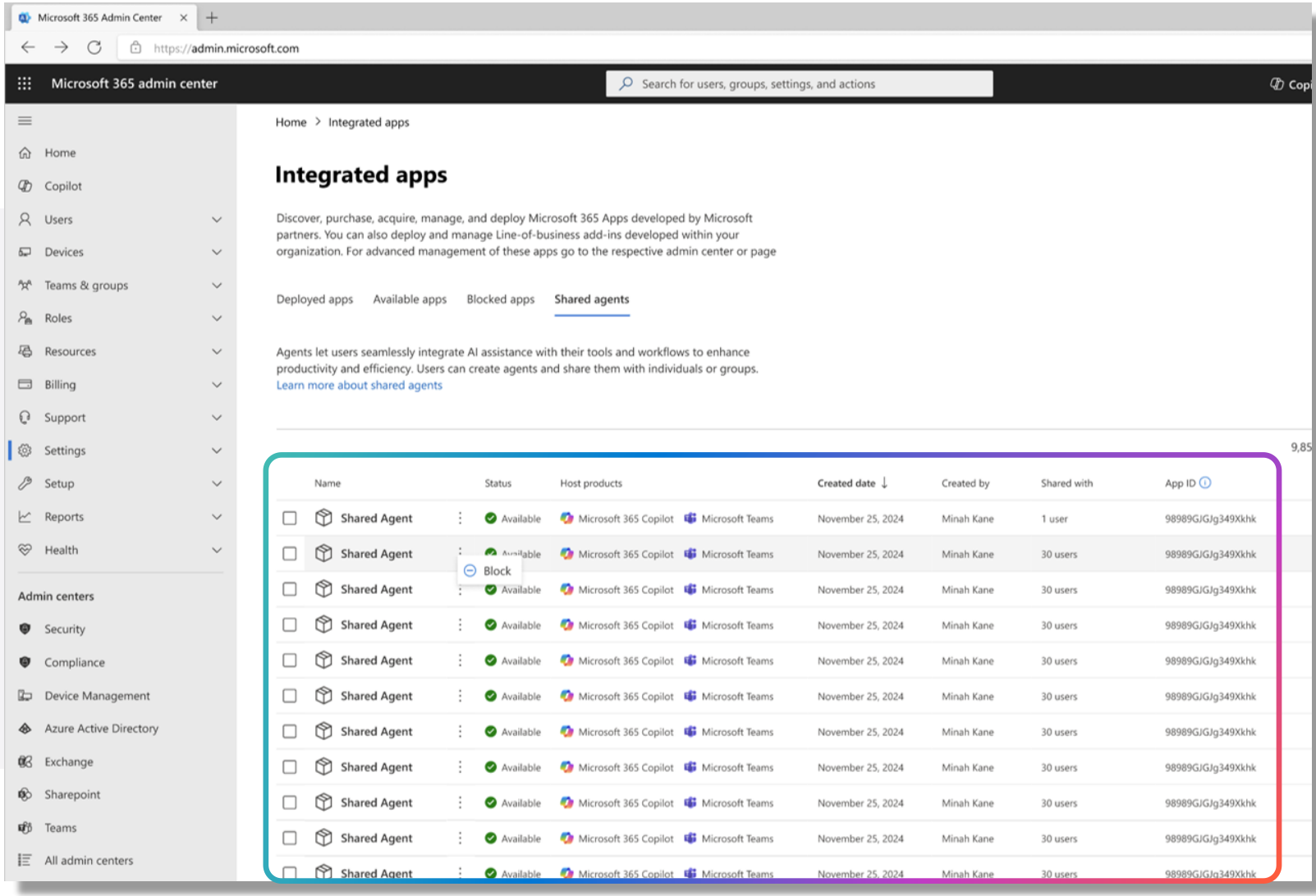
Agent Measurement and Reporting

Agent Builder

Microsoft 365 Admin Center: Agents Inventory Management

Generally available

View the **inventory of shared agents** in my tenant from custom agents and agent builder.



Copilot Studio

Agent Builder

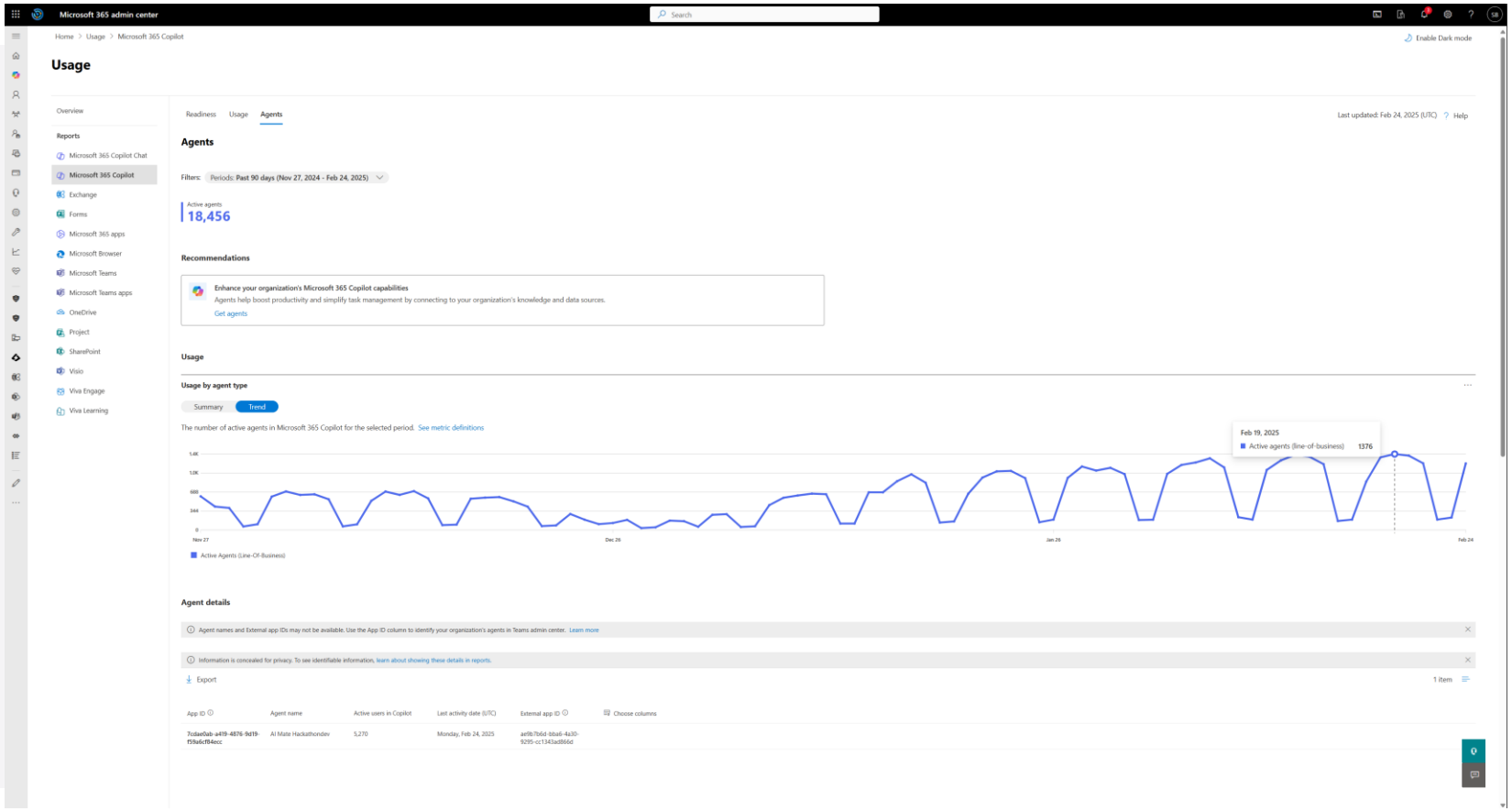
Microsoft 365 Admin Center: Agent reporting

Generally available

Report shows distinct **count of users** in your org who used agents.

New **Agents tab** shows active agents built by your org using Copilot Studio, Agent Builder, and Teams Toolkit.

Export report as csv.



Learn more: aka.ms/MACAgentReport

Copilot Page

A centralized location for documents, insights, and controls for Power Platform in PPAC

Readiness

- Data and security guidance
- Copilot FAQ
- What's new in Copilot
- Getting started guides

Insights

- Usage across Copilots
- Apps created using Copilot
- Makers using Copilot
- Copilot ROI

Governance

- Responsible AI insights
- Visibility to Copilot enablement
- Centralized Copilot settings

Power Platform admin center

Search

New admin center

SF

Home
Actions
Manage
Monitor
Security
Deployment
Licensing
Copilot
Support
Admin centers

Welcome, Sean

Construction zone: the new Power Platform admin center

We're building you an admin center that's easier to navigate and intuitive to use.

See what's new

+ Add cards Share feedback

Service health

0 incidents or advisories.

Message center

30 unread messages

- Finance and Operations Apps - Dataverse will be mandatory for all new and existing deployments
- Power Platform – Create and Use Power Fx Functions Public preview
- Copilot Studio - Removal of the 'New Analytics' toggle on the Analytics page in Custom copilot agents
- Finance and Operations Apps – Information regarding security enhancements for managed storage accounts

Show all

Documentation

- Power Platform admin center
- Activate Managed Environment
- Licensing overview for Microsoft Power Platform

Advisor

Recommendation may show for up to a week once acted on.

3 recommendations

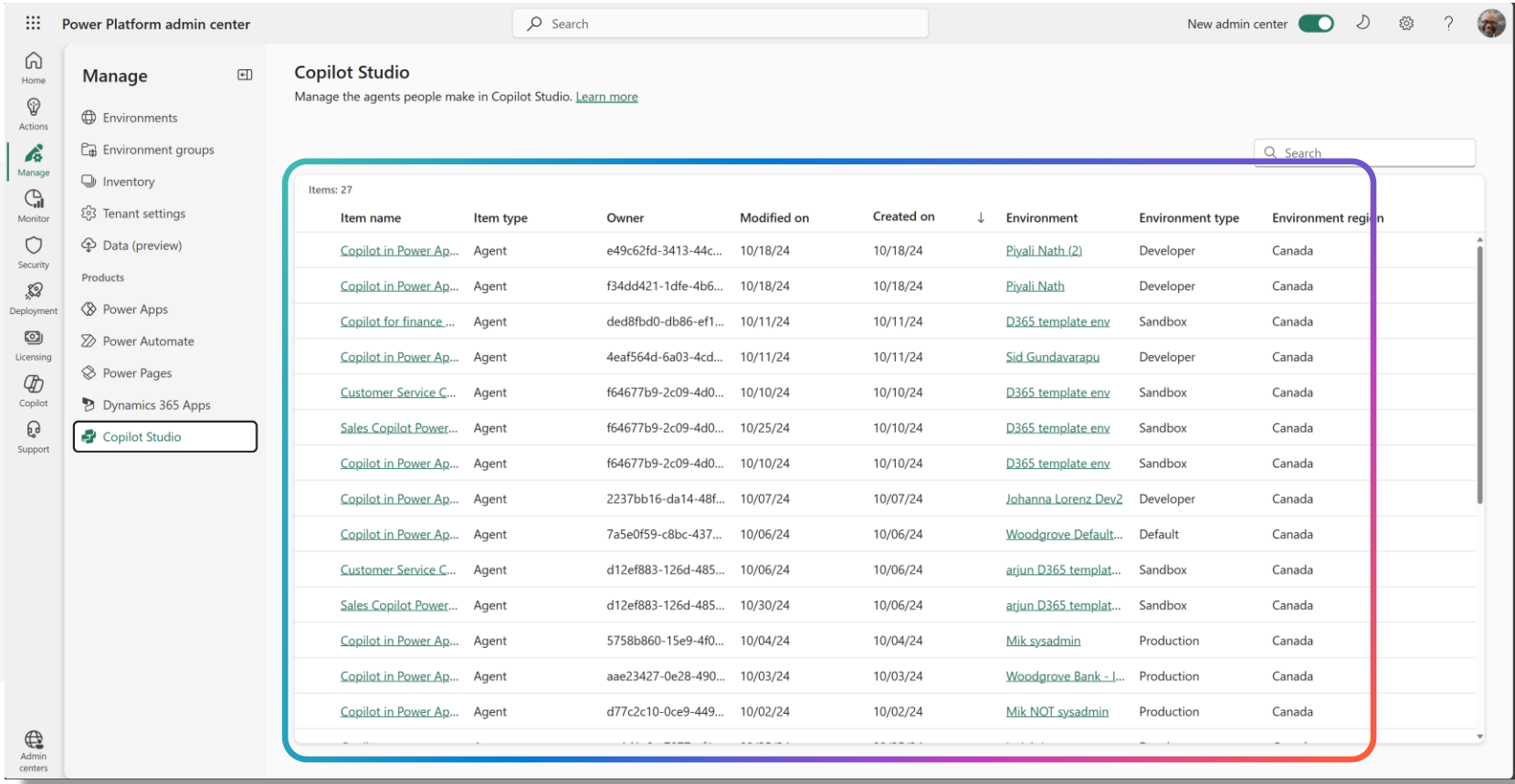
Set up IP firewall View details

Copilot Studio

Power Platform Admin Center: Agents Inventory

Preview

Showing agents **inventory** in Power Platform Admin Center for custom agents



Item name	Item type	Owner	Modified on	Created on	Environment	Environment type	Environment region
Copilot in Power Ap...	Agent	e49c62fd-3413-44c...	10/18/24	10/18/24	Piyali Nath (2)	Developer	Canada
Copilot in Power Ap...	Agent	f34dd421-1dfe-4b6...	10/18/24	10/18/24	Piyali Nath	Developer	Canada
Copilot for finance ...	Agent	ded8fbd0-db86-ef1...	10/11/24	10/11/24	D365 template env	Sandbox	Canada
Copilot in Power Ap...	Agent	4eaf564d-6a03-4cd...	10/11/24	10/11/24	Sid Gundavarapu	Developer	Canada
Customer Service C...	Agent	f64677b9-2c09-4d0...	10/10/24	10/10/24	D365 template env	Sandbox	Canada
Sales Copilot Power...	Agent	f64677b9-2c09-4d0...	10/25/24	10/10/24	D365 template env	Sandbox	Canada
Copilot in Power Ap...	Agent	f64677b9-2c09-4d0...	10/10/24	10/10/24	D365 template env	Sandbox	Canada
Copilot in Power Ap...	Agent	2237bb16-da14-48f...	10/07/24	10/07/24	Johanna Lorenz Dev2	Developer	Canada
Copilot in Power Ap...	Agent	7a5e0f59-c8bc-437...	10/06/24	10/06/24	Woodgrove Default...	Default	Canada
Customer Service C...	Agent	d12ef883-126d-485...	10/06/24	10/06/24	arjun D365 templat...	Sandbox	Canada
Sales Copilot Power...	Agent	d12ef883-126d-485...	10/30/24	10/06/24	arjun D365 templat...	Sandbox	Canada
Copilot in Power Ap...	Agent	5758b860-15e9-4f0...	10/04/24	10/04/24	Mik sysadmin	Production	Canada
Copilot in Power Ap...	Agent	aae23427-0e28-490...	10/03/24	10/03/24	Woodgrove Bank - I...	Production	Canada
Copilot in Power Ap...	Agent	d77c2c10-0ce9-449...	10/02/24	10/02/24	Mik NOT sysadmin	Production	Canada

Microsoft

Data Protection

Data Security Admin

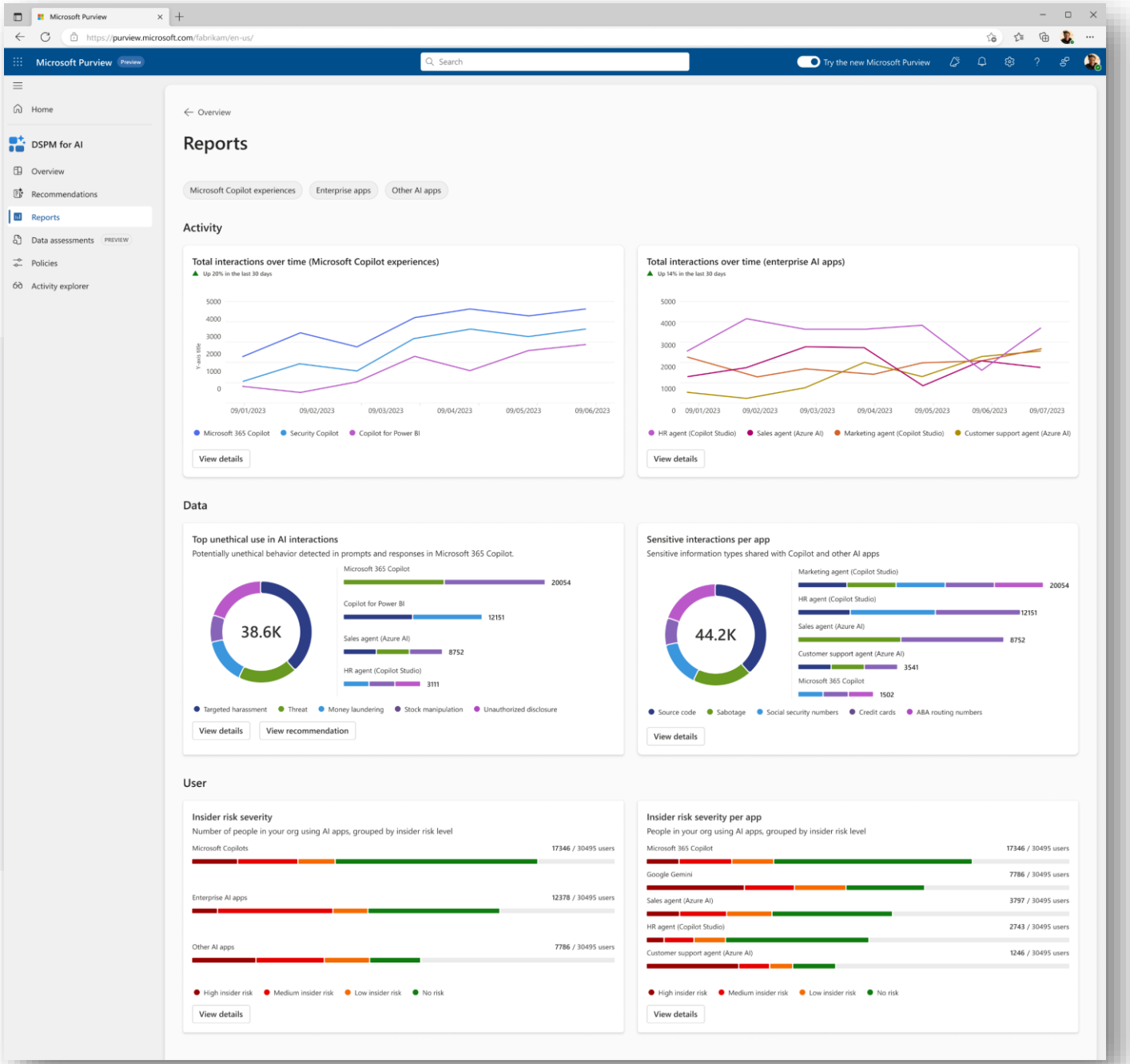
Microsoft Purview:

Data Security Posture Management for AI

General Availability

Data Security Posture Management (DSPM) for AI helps customers to **gain visibility into AI usage** and provide data **risk analytics** across agents and AI apps including:

- Sensitive data shared with AI interactions
- Risky usage with AI interactions
- Unethical use in AI interactions
- Compliance with AI regulations



* Free Preview for Copilot Studio until May 2025, then Paid Preview

Purview + Copilot Agents

	End Users	Makers		Developers	
Difficulties	No code	Low code		Pro code	
Builder Tools	Agent builder, SPO agent	Copilot Studio		VS code + TTK, Azure AI(Foundry), Semantic Kernel, etc.	
RAG+LLM	Sydney	Sydney	Samba (MCS Standard)	Sydney	Custom RAG +LLM
Host	M365 Apps, Copilot Chat, Teams, SPO	Copilot Chat, Teams	Teams	Copilot Chat, Teams	Teams
Publishing	For individual use, share with link for specific people	Share with link for specific people IT admin approval for org-wide use (M365 app catalog)	IT admin approval for org-wide use (M365 app catalog)	IT admin approval for orgwide use (M365 app catalog)	IT admin approval for orgwide use (M365 app catalog)
Knowledge	Custom instructions SPO External web Graph connectors	Custom instructions SPO External web Graph connectors	Custom instructions SPO External web Graph connectors Files Dataverse PP connectors AOAI on your data	Custom instructions SPO External web Graph connectors	Custom instructions AOAI on your data
Skills/Actions	Code Interpreter Image generator	PP Connectors (read-only) Power Automate flow Rest API	PP Connectors (read/write) Power Automate flow Rest API Azure bot framework Skills	Rest API	Code Interpreter Rest API Azure Functions Function calling
IT admin portal/controls	M365 Admin portal (usage report)	Power Platform Admin Center (Block connectors) M365 Admin portal (approval/reject)	Power Platform Admin Center (Block connectors) M365 Admin portal (approval/reject)	M365 Admin portal (approval/reject)	M365 Admin portal (approval/reject)
Purview capabilities	Discover • DSPM for AI (*under Microsoft Copilot Experiences*) Protect • IRM (risky prompt/responses) • Honoring label (SPO) • DLP for Copilot (SPO) • Oversharing data assessments (Copilot Chat) Govern • Compliance for AI (Audit, eDiscovery, Data Lifecycle Management, Communication Compliance)	Discover • DSPM for AI (*under Microsoft Copilot Experiences*) Protect • IRM (risky prompt/responses) • Honoring label (SPO) • DLP for Copilot (SPO) • Oversharing data assessments (Copilot Chat) Govern • Compliance for AI (Audit, eDiscovery, Data Lifecycle Management, Communication Compliance)	Discover (Public Preview) • DSPM for AI (*under MCS agents*) Protect (Public Preview) • IRM (risky prompt/responses) • Honoring label (SPO) Govern (Public Preview) • Compliance for AI (Audit, eDiscovery, Data Lifecycle Management, Communication Compliance)	Discover • DSPM for AI (*under Microsoft Copilot Experiences*) Protect • IRM (risky prompt/responses) • Honoring label (SPO) • DLP for Copilot (SPO) • Oversharing data assessments (Copilot Chat) Govern • Compliance for AI (Audit, eDiscovery, Data Lifecycle Management, Communication Compliance)	Discovery (PrPr) • DSPM for AI (*under AzureAI*) Protection (PrPr) • IRM (risky prompt/responses) • Honoring label (SPO) Governance (PrPr) • Compliance for AI (Audit, ED, DLM, CC)

*SPO – SharePoint Online

Microsoft

Agent 365

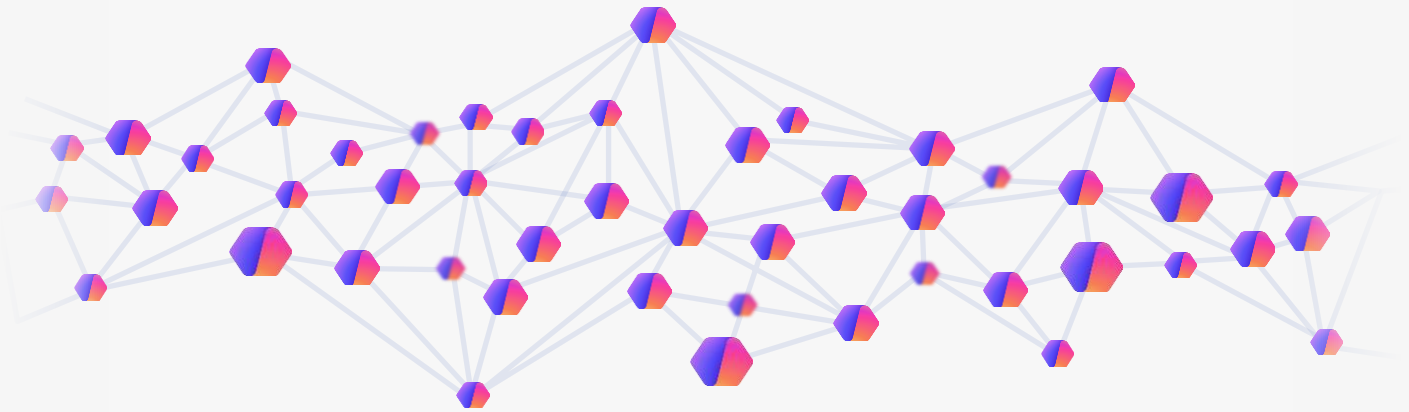
Early access

Microsoft Agent 365

The control plane for agents

Microsoft Agent 365

The control plane for agents



Registry

Access Control

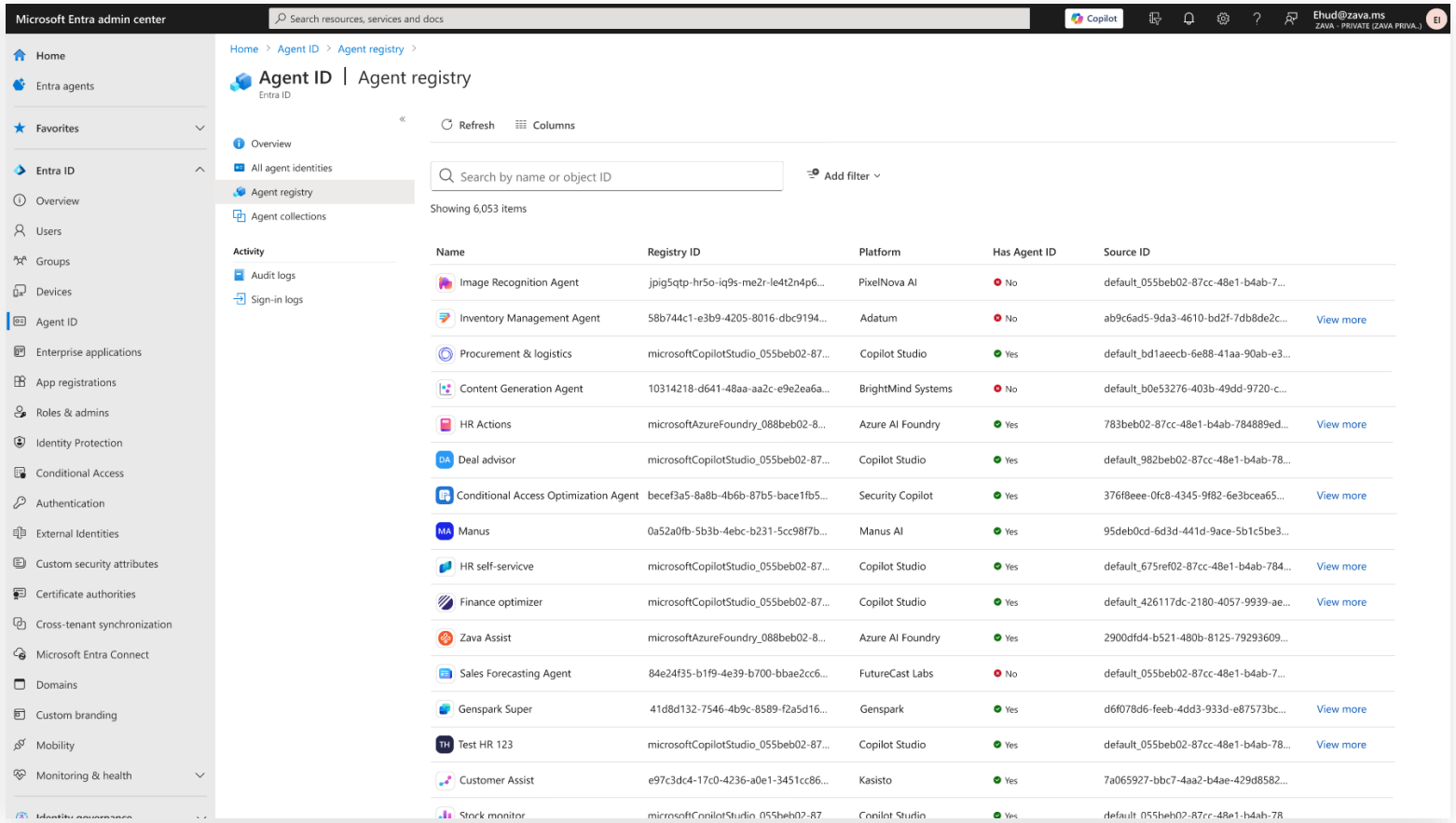
Visualization

Interop

Security

Registry

Get the complete view of all agents that are being used in your organization, including agents with agent ID, agents you register yourself and shadow agents.

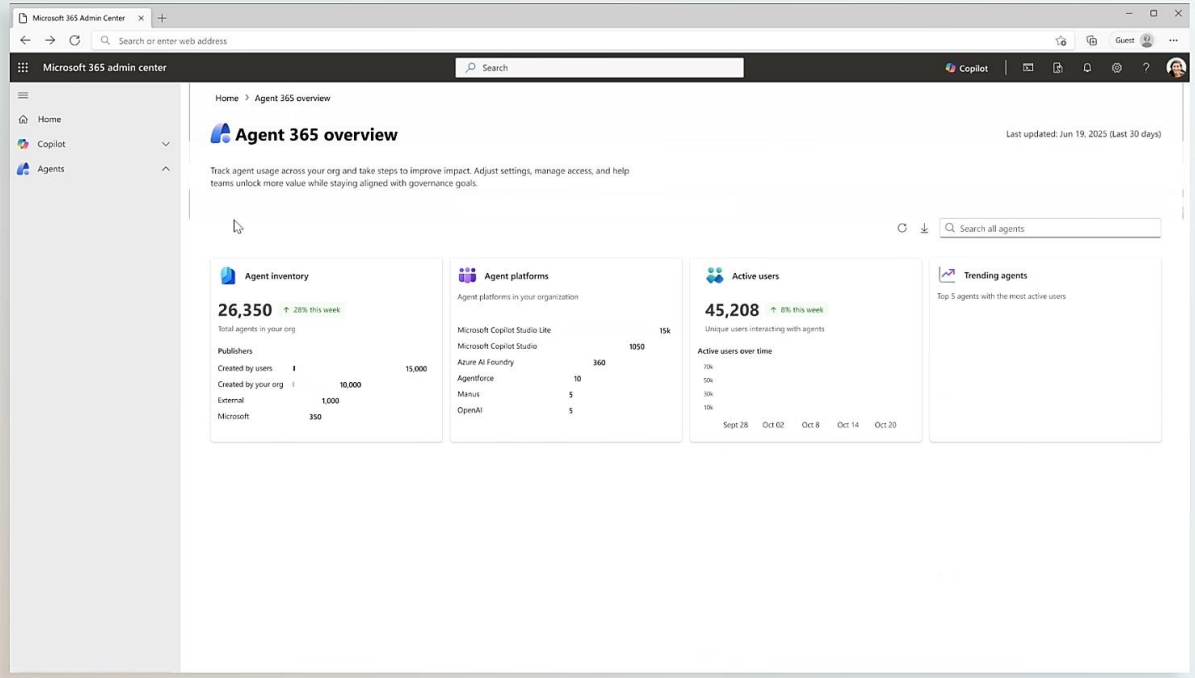


Access control

Bring agents under management and limit their access to only resources they need. Prevent agents compromise with risk-based conditional access policies.

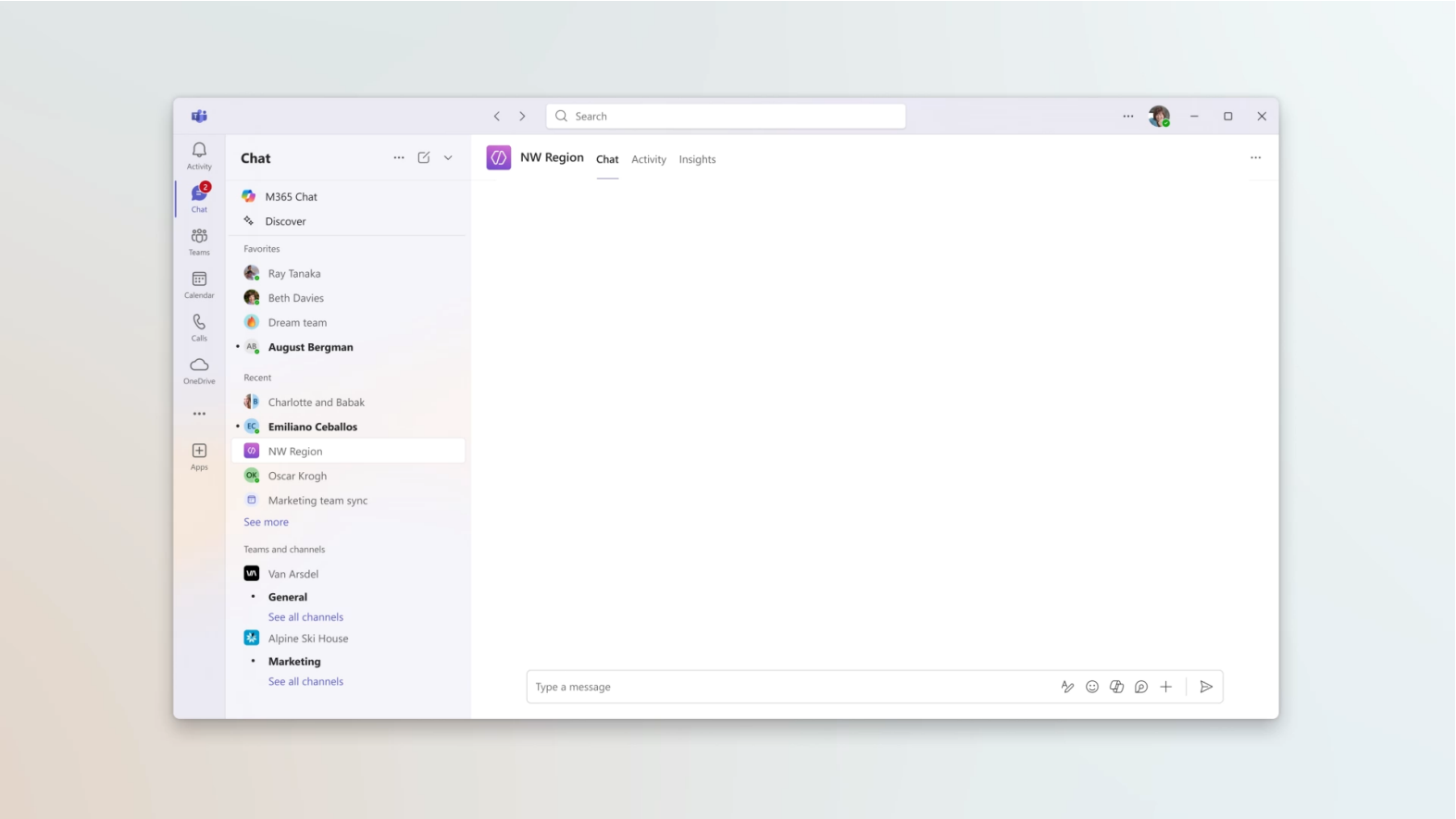
Visualization

Explore connections between agents, people and data and monitor agent behavior and performance in real time to assess their impact on your organization.



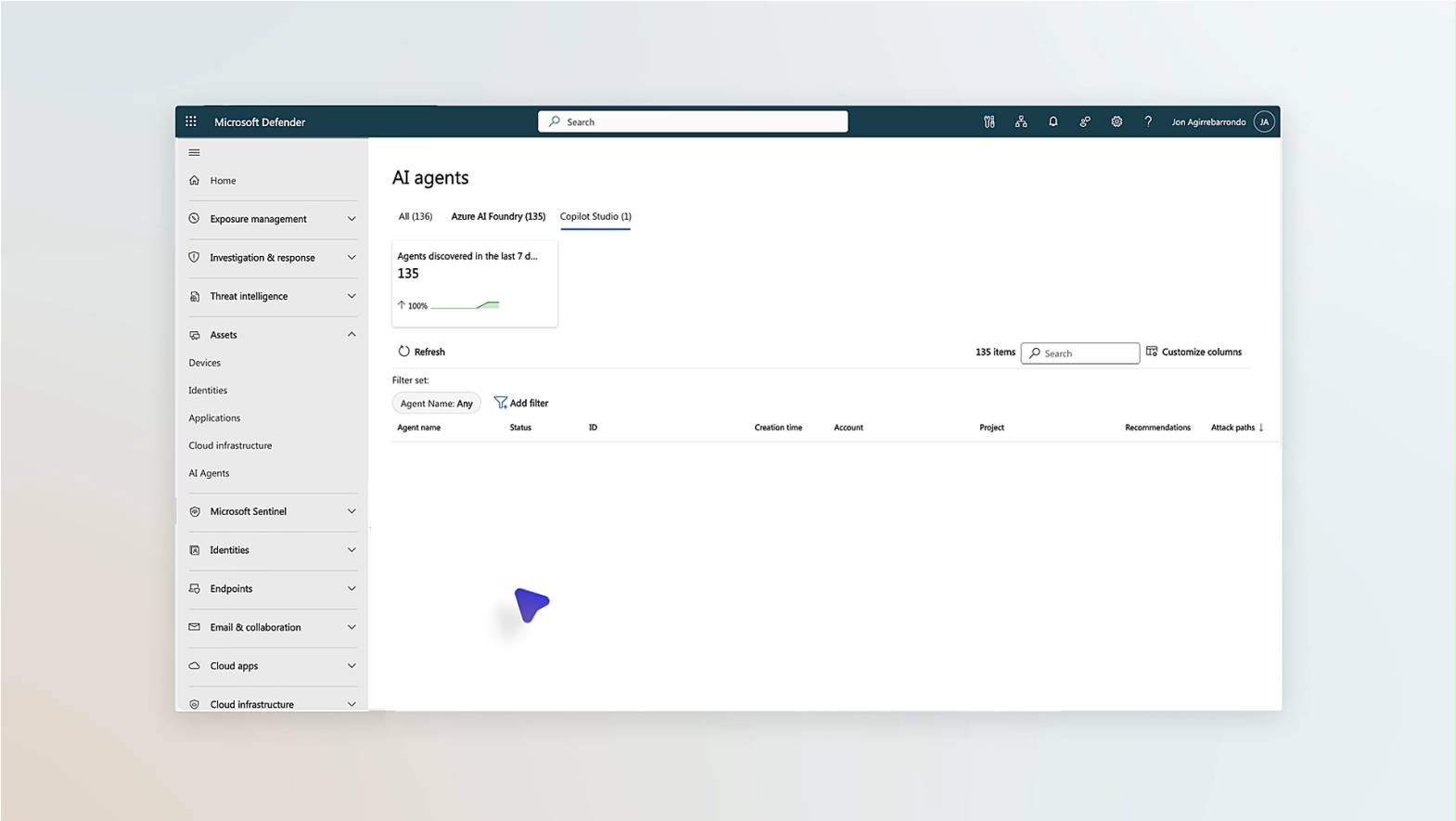
Interop

Equip agents with the same apps to simplify human-agent workflows. Connect them to organizations' data to provide context of work for effective integration into business processes.



Security

Protect agents from threats, detect and remediate attacks that target agents. Protect data that agents create and use from oversharing, leaks, and risky agent behavior.



Agent 365 Ecosystem
aka.ms/AgentShowcase
Cognition
LexisNexis
PolyAI
crewai
Adobe
ANTHROP\C
SAP
workday
servicenow
perplexity
Microsoft Copilot Studio
Microsoft Foundry
OpenAI
BlueYonder
Seismic
Genspark
glean
Microsoft 365 Copilot
LangChain
box
WorkOS
kore.ai
CURSOR
manus
n8n
databricks
ZENSAI
SOPHOS
NVIDIA
Kasisto
zendesk
Vercel
EGNYTE

Get started with Agent 365

Join early access in Frontier

Agent 365 is available starting today in Microsoft 365 Admin Center with Frontier, Microsoft's early access program for the latest AI innovations.

Microsoft

Thank you

Jeffrey Bennett
Sr. Solution Engineer
Microsoft | Oil, Gas, & Energy

https://aka.ms/LinkedIn/JBennett