

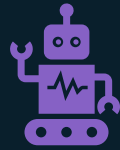
Agent Tech Talk November

2025-11-26

Agent Tech Talk



En session varje
månad



Fokus på AI & agenter
för teknisk målgrupp



Syfte att dela med oss
av nyheter, best-
practices och
inspiration



Schemat går att hitta
på Cloud Champion:
[Agent Tech Talk Series](#)
[– Sweden Cloud](#)
[Champion](#)



Alla inspelningar
publiceras på Cloud
Champion



Scaling Governance: Admin Strategies for Copilot Studio

Webinar 2025-11-26

Marica Lagerheim

Your presenter today



Marica Lagerheim

- ❖ Solution Engineer - Power Platform and Copilot Studio
- ❖ 12+ years of working with Dynamics 365 and Power Platform
- ❖ Background from consulting, sales and implementation

Agenda

- Introduction
- Environments
- Data Loss Prevention
- ALM
- Cost control



Introduction

The background of the slide is a light blue gradient. On the right side, there are several curved, glowing blue lines that sweep across the frame. These lines are composed of many small, bright blue dots, giving them a digital or particle-like appearance. The lines curve from the top right towards the bottom right, creating a sense of motion and depth.

A network diagram with star-shaped nodes connected by lines, set against a dark blue background. The nodes are colored in a gradient from teal to light green. A central green rounded rectangle contains the text.

1.3 Billion

AI agents by 2028

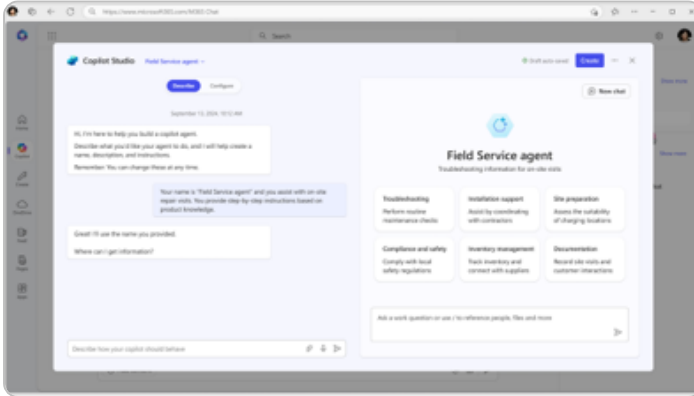
Source: IDC Info Snapshot, 1.3 Billion AI Agents by 2028, doc #US53361825, May 2025

A range of tools for agent creation

Simple



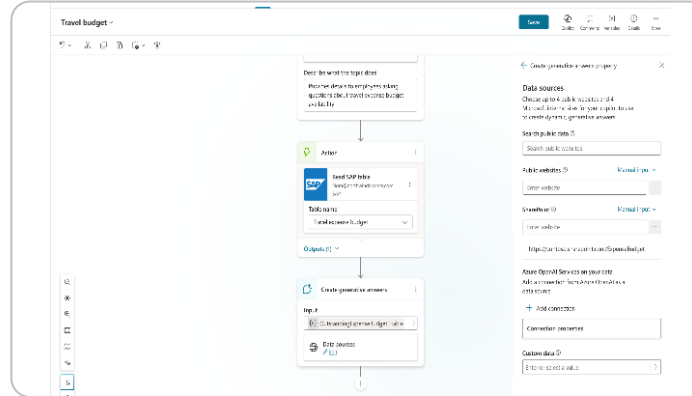
For end users



Agent Builder



For makers

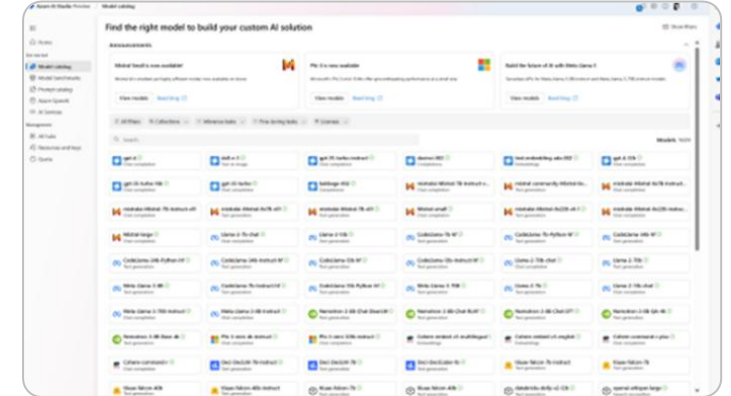


Copilot Studio



Advanced

For developers



Visual Studio Code, Copilot Studio,
Azure AI Foundry

Governance for Copilot Studio





Power Platform



Power Apps

Web and mobile app development



Power Automate

Process and workflow automation



Copilot Studio

Customize & create copilots



Power Pages

Secure, data-centric business websites



Power BI

Data exploration, analytics and reporting



Data connectors



AI Builder



Microsoft Dataverse



Power Fx

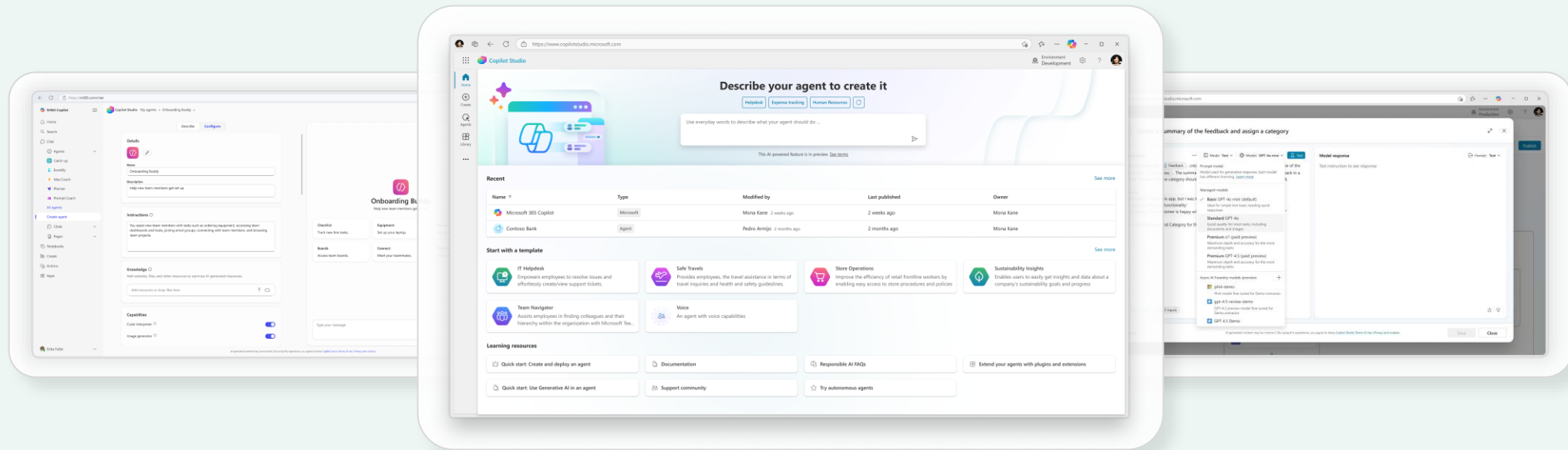


Managed Environments



Microsoft Copilot Studio

Build, manage and secure AI agents



M365 Copilot agent builder

Build agents with natural language right inside Microsoft 365 Copilot

Copilot Studio

Access a complete set of intuitive tools and capabilities for building agents

Advanced extensibility

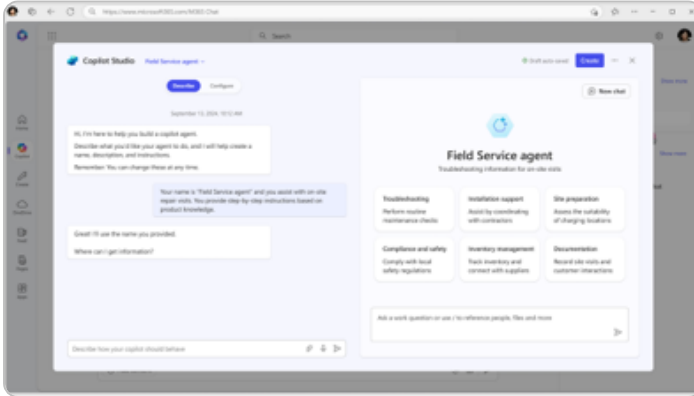
Customize agents using pro dev tools like Microsoft 365 Agents SDK, VS code & Microsoft Foundry

A range of tools for agent creation

Simple



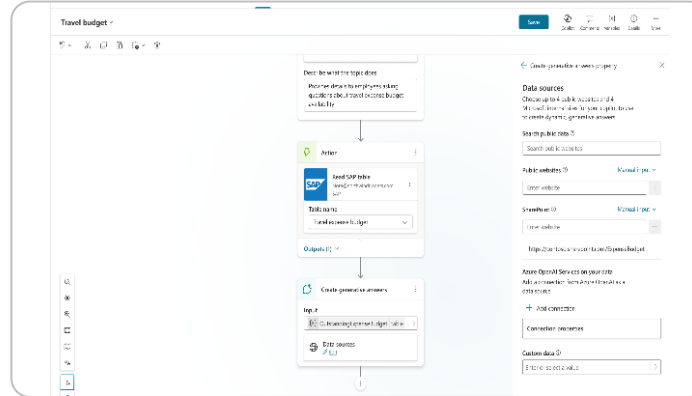
For end users



Agent Builder



For makers

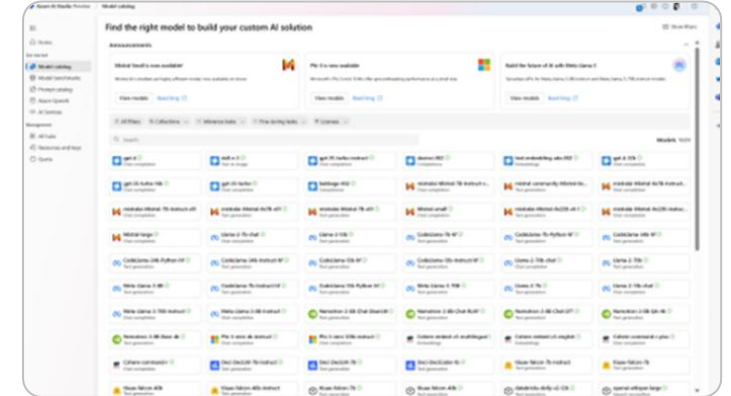


Copilot Studio



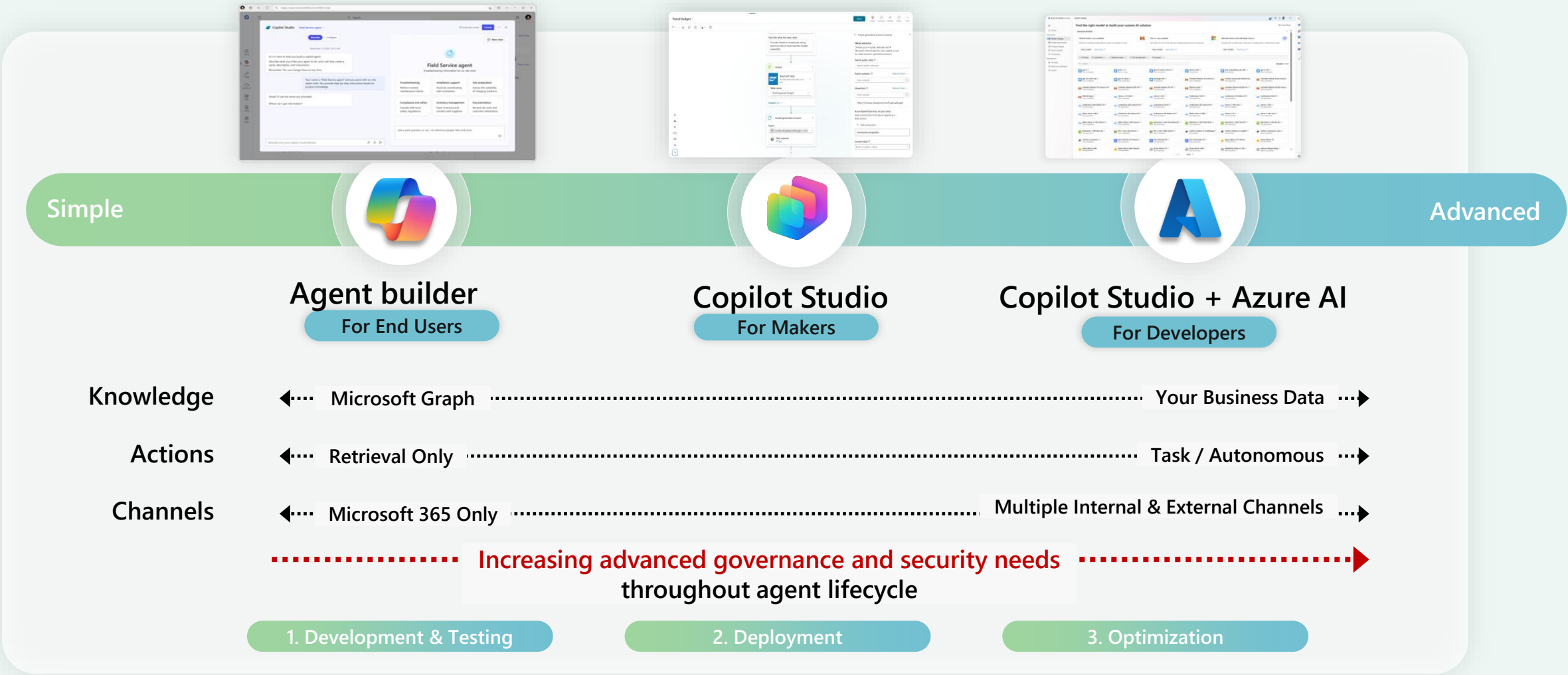
Advanced

For developers



Visual Studio Code, Copilot Studio,
Azure AI Foundry

Advanced agents require more advanced governance and security



Top security and governance concerns with generative AI

Data oversharing
and data leaks

80%

of leaders cited leakage of sensitive data as their main concern¹

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 implement²

AI governance and
risk visibility

84%

Want to feel more confident about managing and discovering data input into AI apps and tools²

1. First Annual Generative AI study: Business Rewards vs. Security Risks, Q3 2023, ISMG, N=400

2. [Microsoft data security index 2024 report](#)

What is Governance?

Governance \neq Risk Management

If it was, we should just call it risk management!

The word “**govern**” means “**to steer**”, so it is fundamentally about opportunity realization as well!

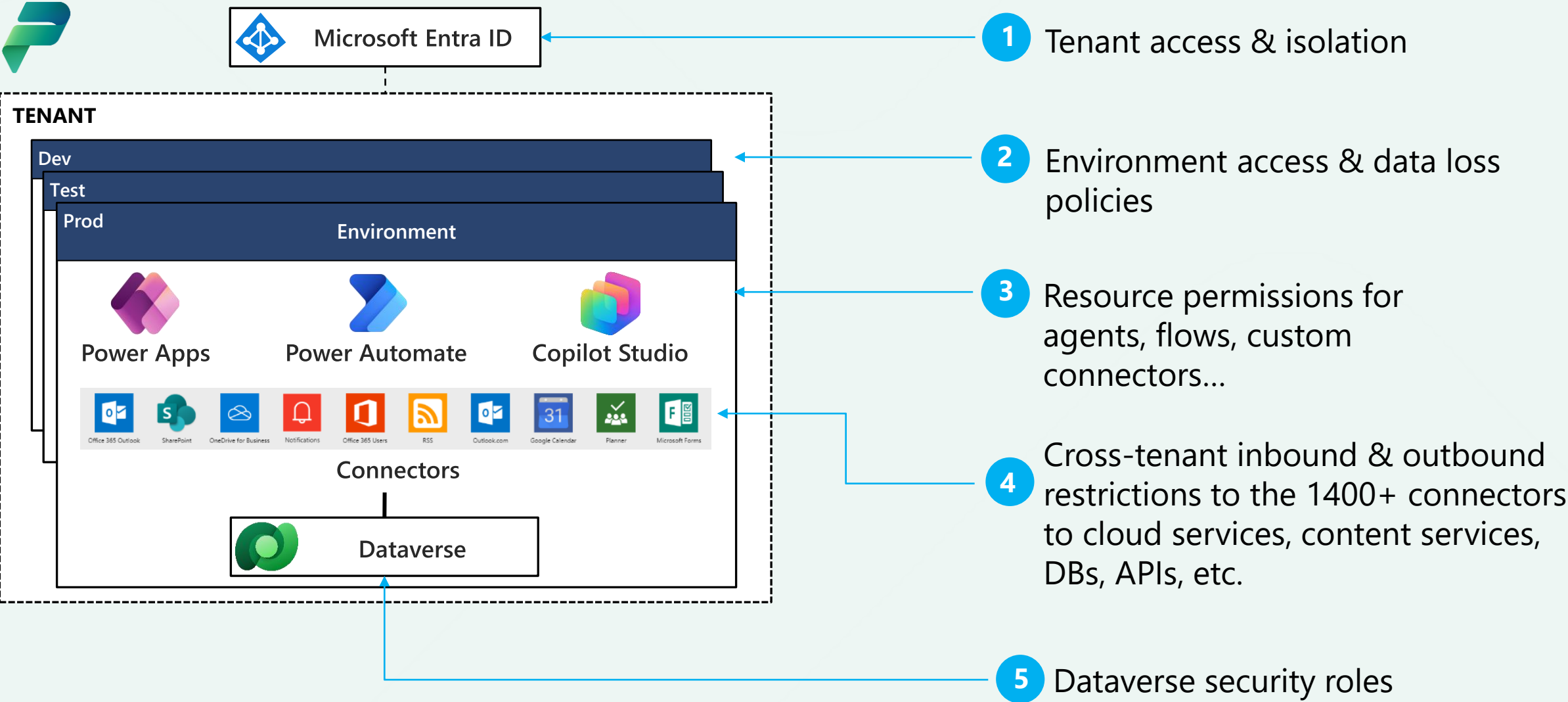
To effectively govern you need

Goal Clarity

Role Clarity

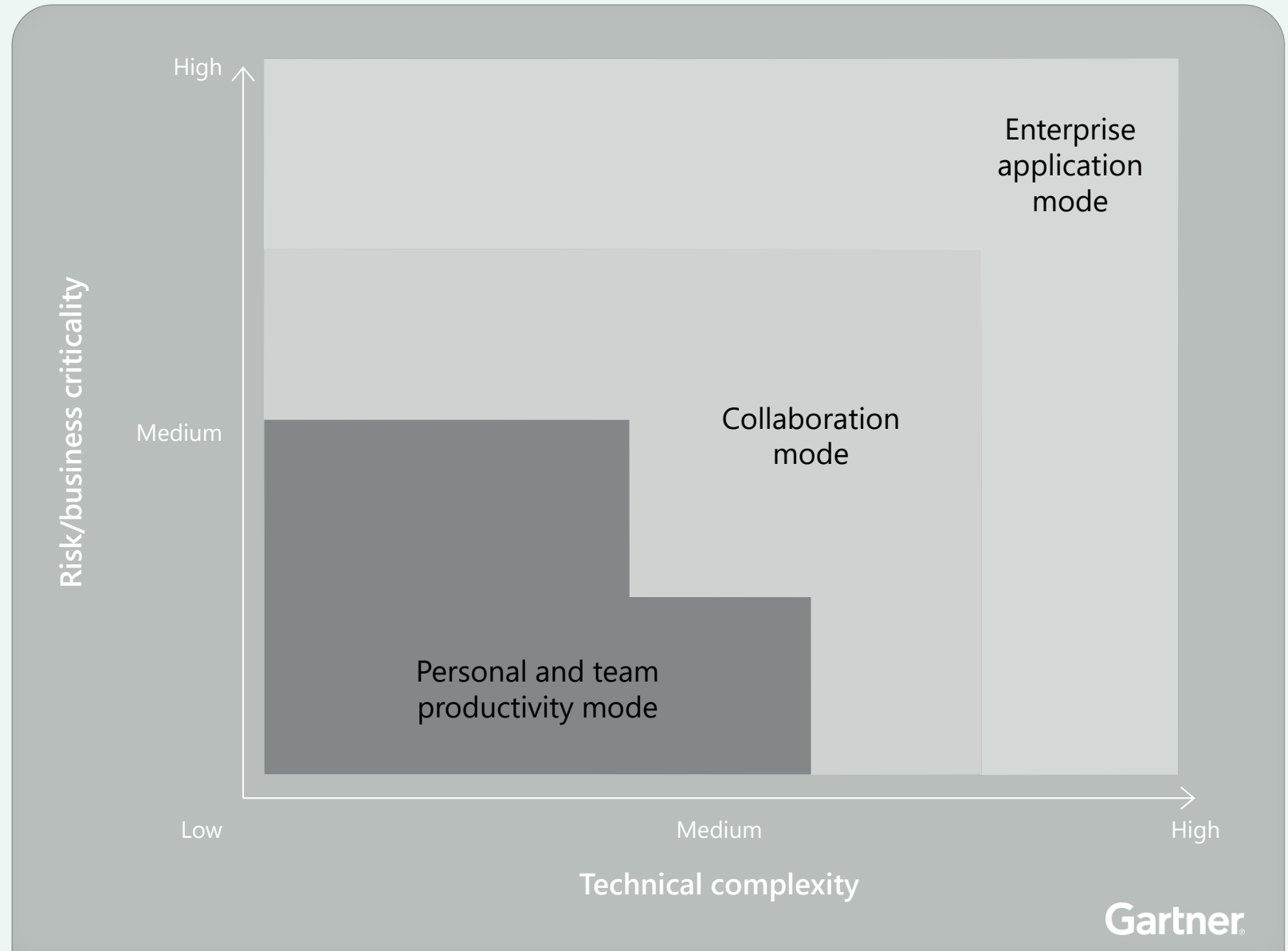
Task Clarity

Governance & Security Overview



Implementing Zone Strategy

Governing agents by segmenting by audience + exposure and complexity + risk into zones.

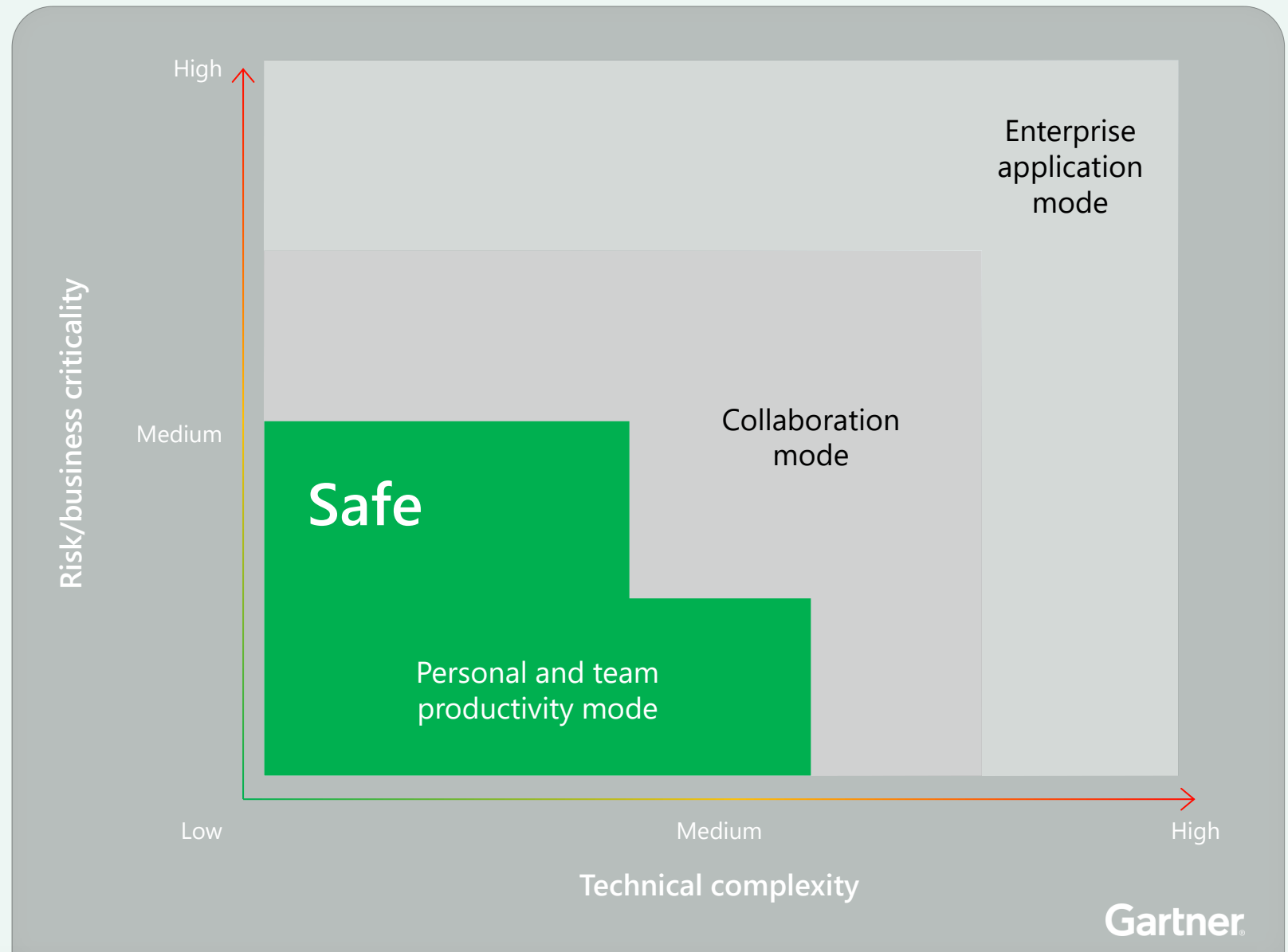


Implementing Zone Strategy



Safe Innovation Zone (Green)

Self-service “sweet spot” for rapid AI agent experimentation with minimal oversight

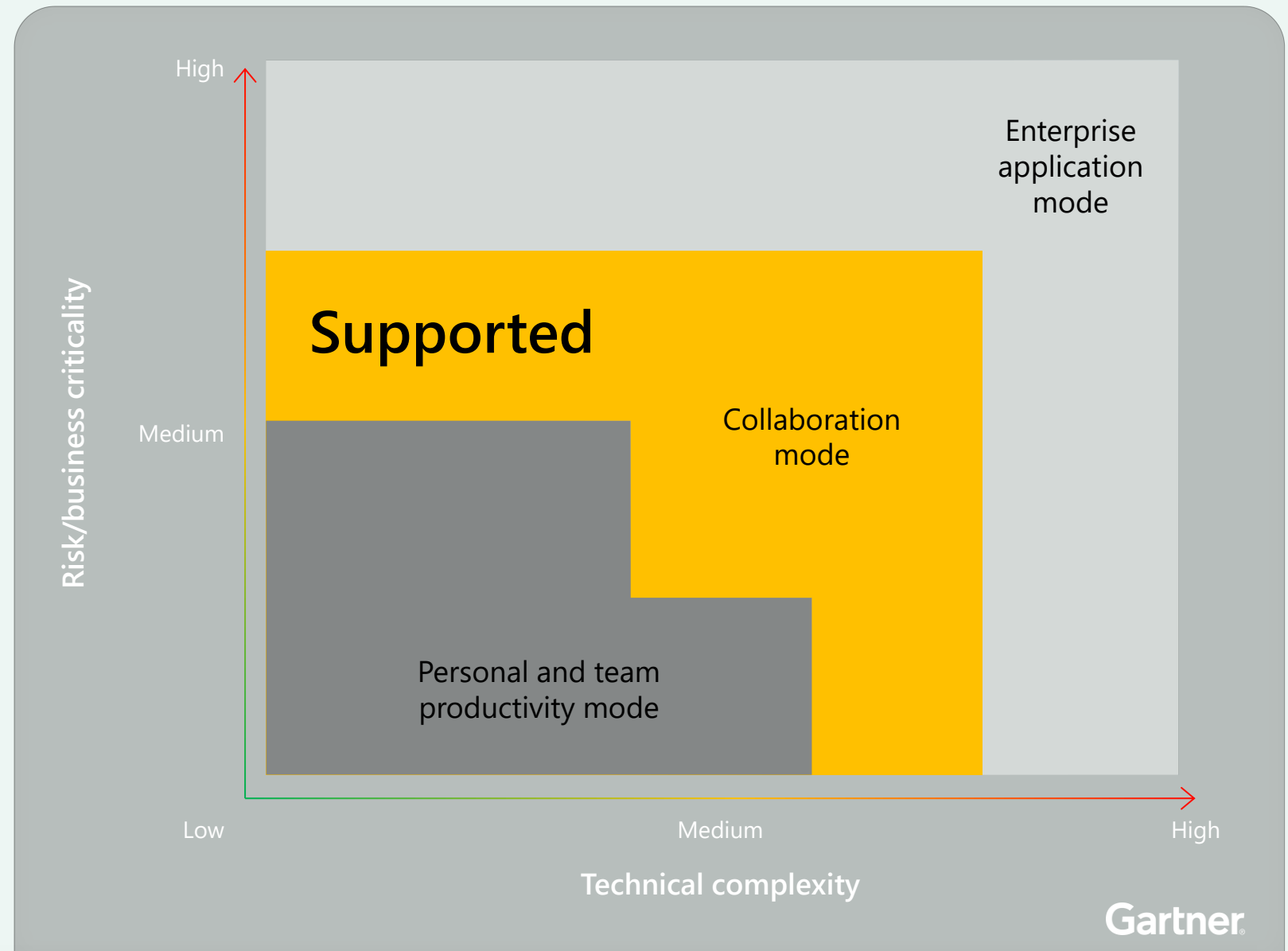


Implementing Zone Strategy



Collaboration Zone (Yellow)

Medium-risk scenarios
(Department-level).
Requires some admin
governance

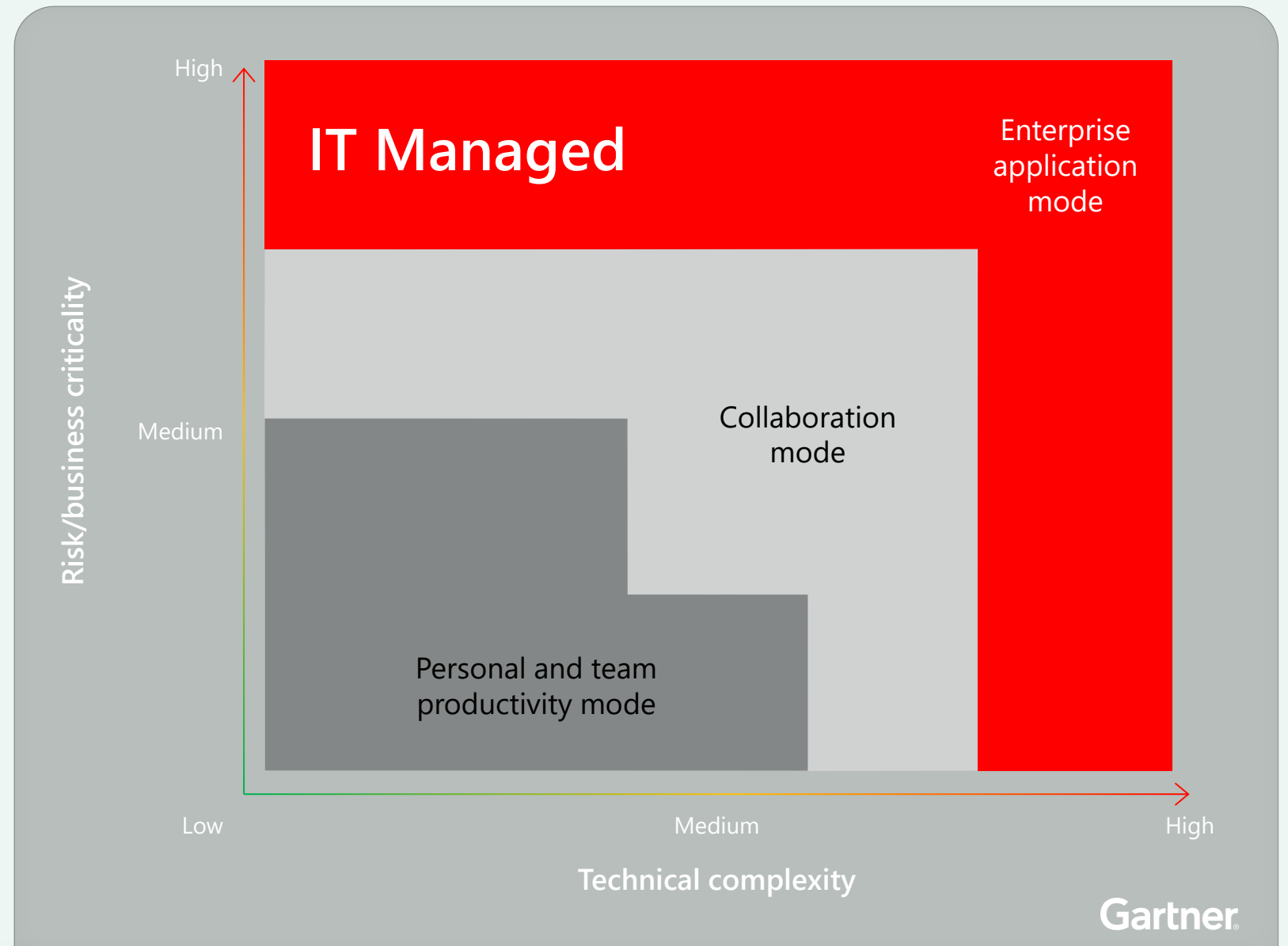


Implementing Zone Strategy



Enterprise Zone (Red, Black)

High-risk, mission critical scenarios. Demands strict IT/Management control



Why the Safe Innovation Zone Matters

1. **Empower Makers:** Quick creation of low-risk agents with minimal friction
2. **Scale Innovation:** Identify the high value scenarios emerging from early experiments that are growing in adoption
3. **Admin Efficiency:** Safeguards must be in place so admins can dedicate effort where risk is higher

Today, *Default Environment and Developer Environment* empower Makers to get started, but it requires Admin setup to ensure safeguards are in place. Without them, all environments behave like the "Yellow Zone"



DEFAULT ENV

Shared Environment for everyone in the Company

Allows for low risk Agents, flows, Apps to be shared with others in the company



DEVELOPER ENV

Personal environment per Maker

Allows for Makers to build personal agents, flows, apps with richer functionality



OTHER ENVs

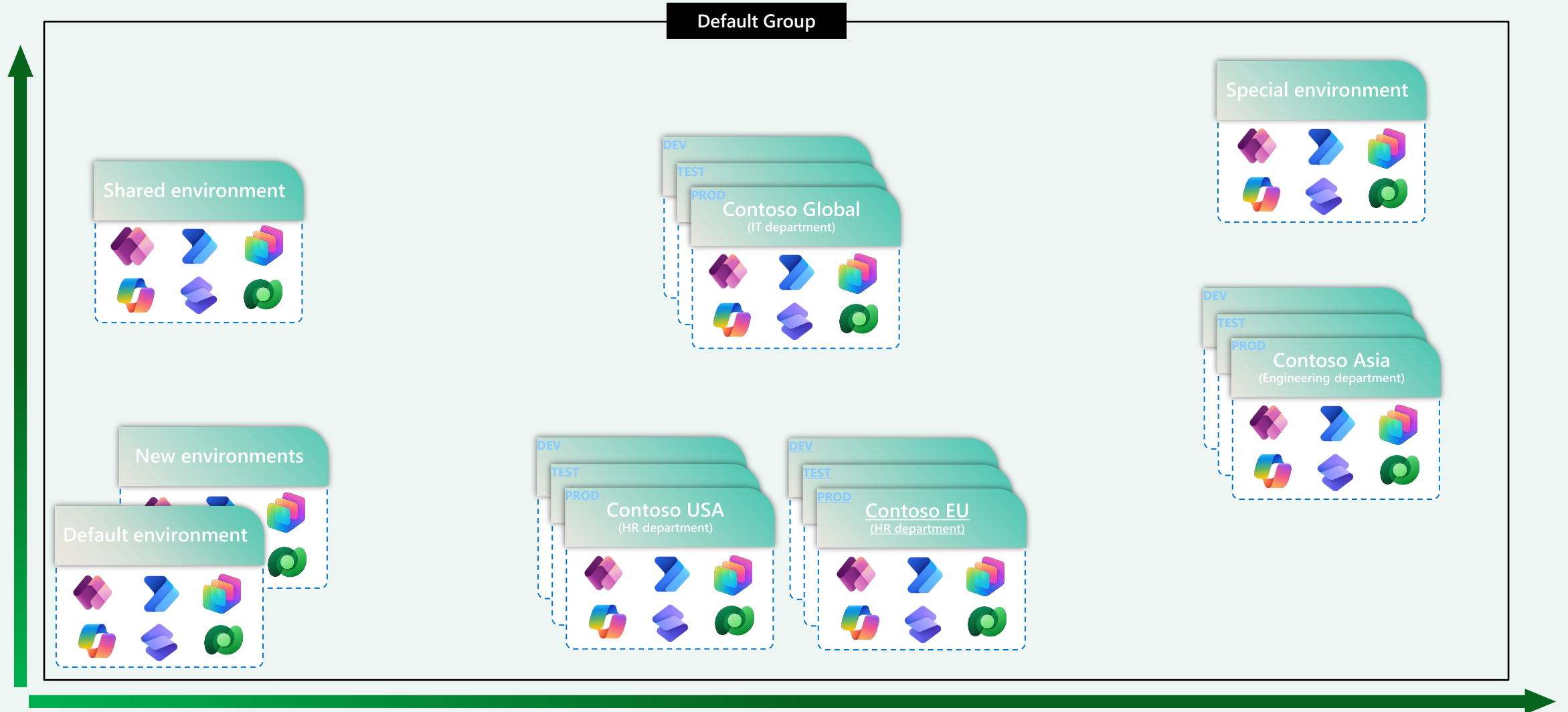
Trial, Sandbox, Production

Allows Makers who can create or acquire other environments full access to create custom agents, apps, flows

COLLABORATION ZONE (YELLOW ZONE) IF NO SAFEGAURDS ARE IN PLACE

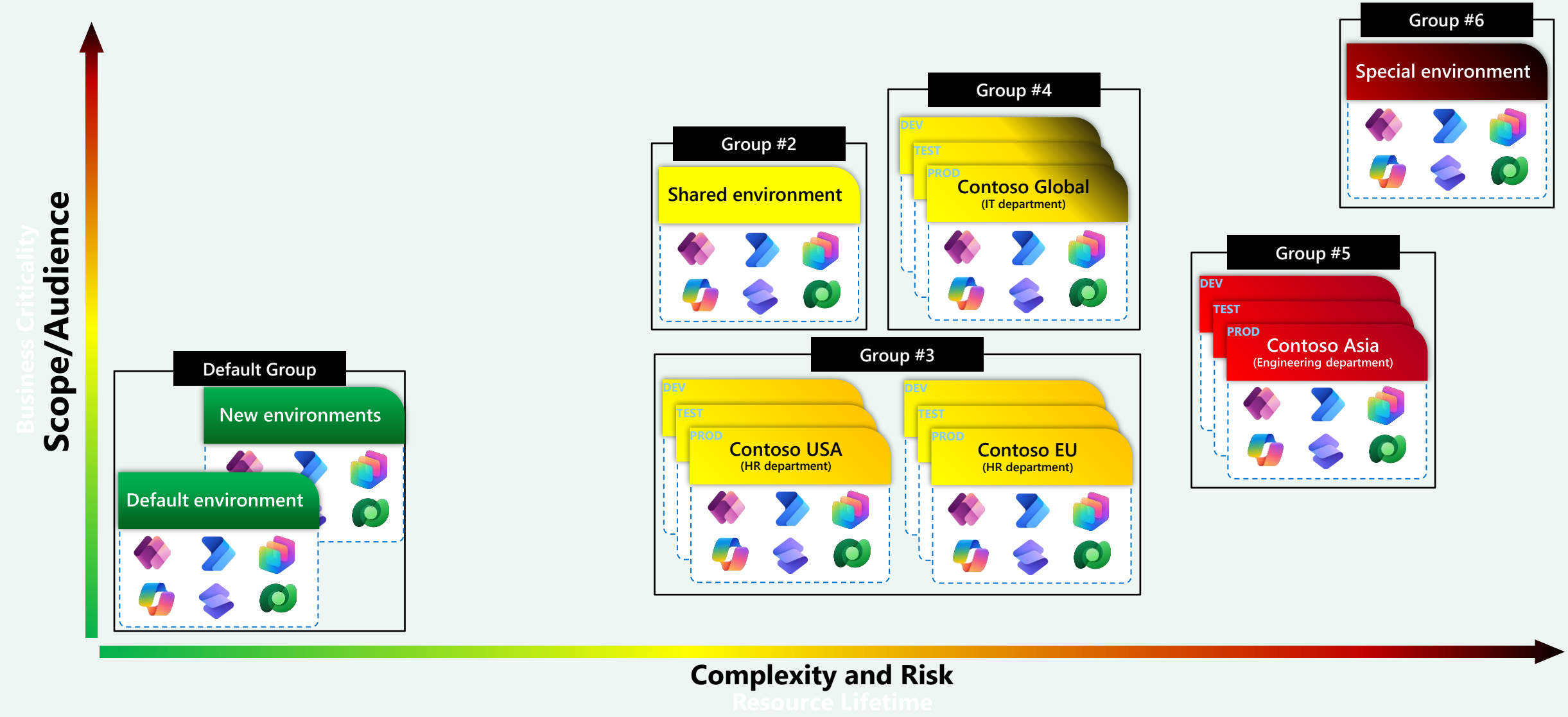
Empowerment through Zoned Governance

An example of an empowered, yet fully governed approach



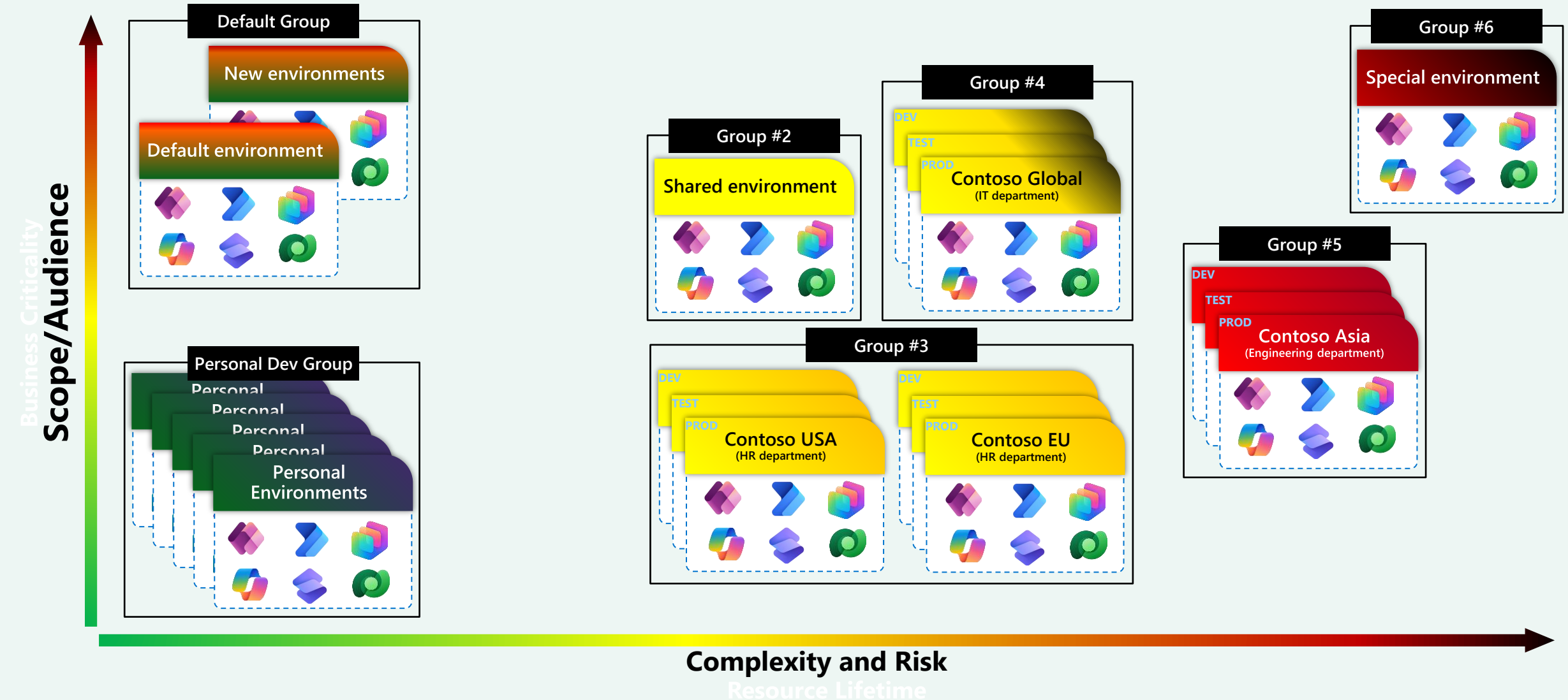
Empowerment through Zoned Governance

An example of an empowered, yet fully governed approach



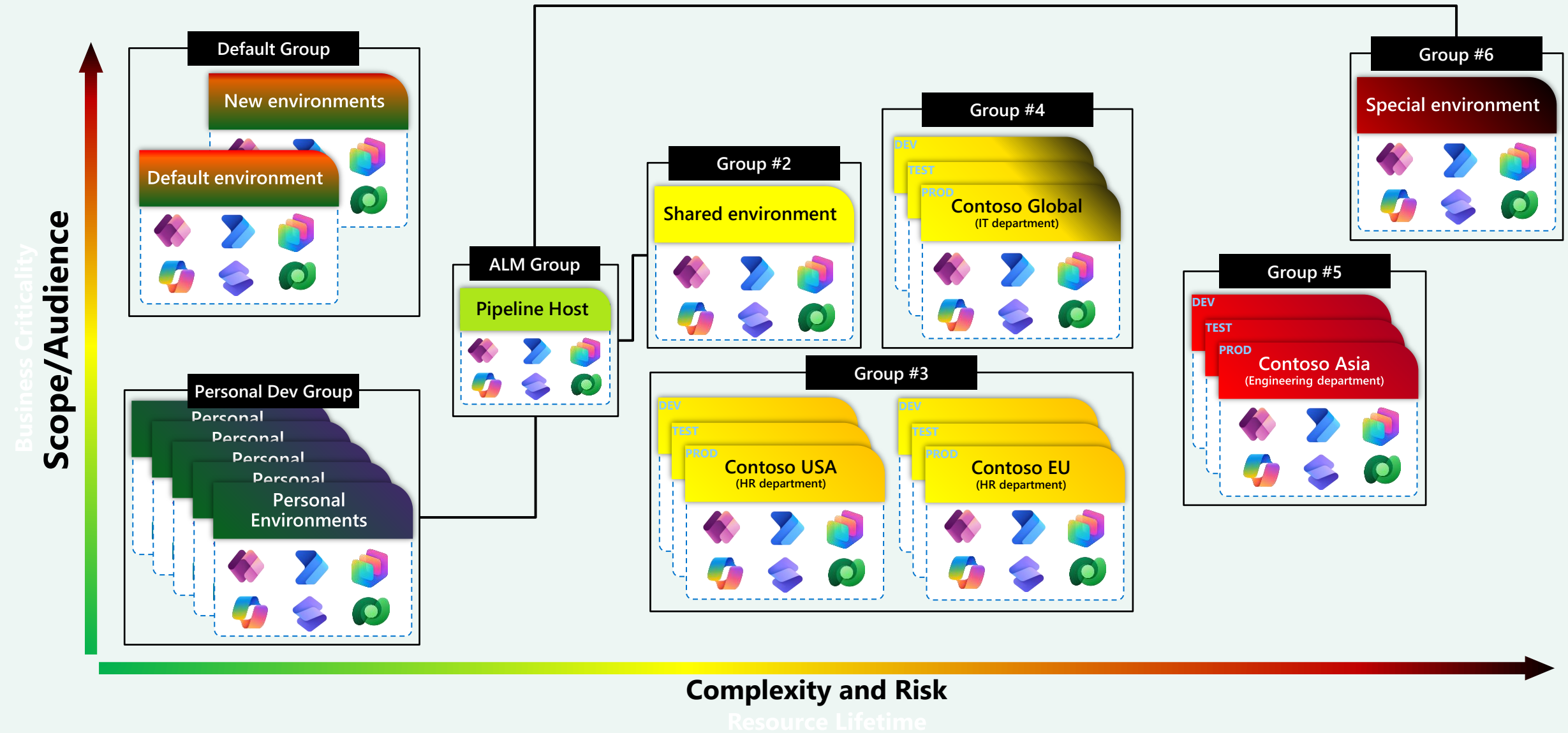
Empowerment through Zoned Governance

An example of an empowered, yet fully governed approach

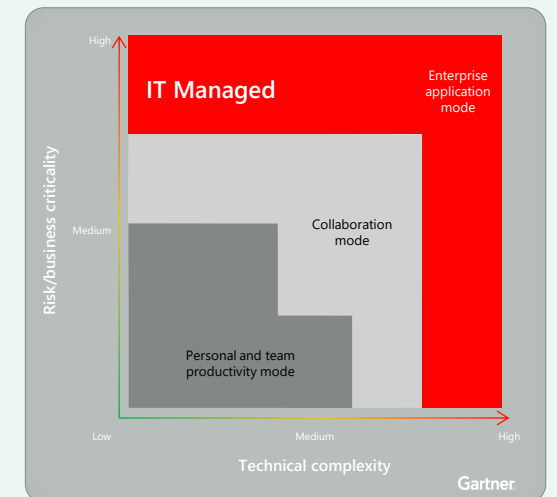
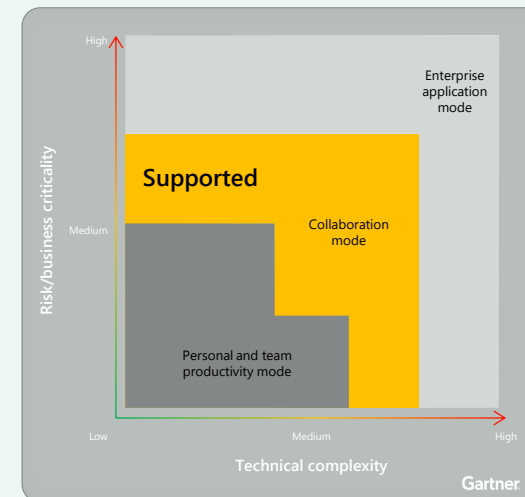
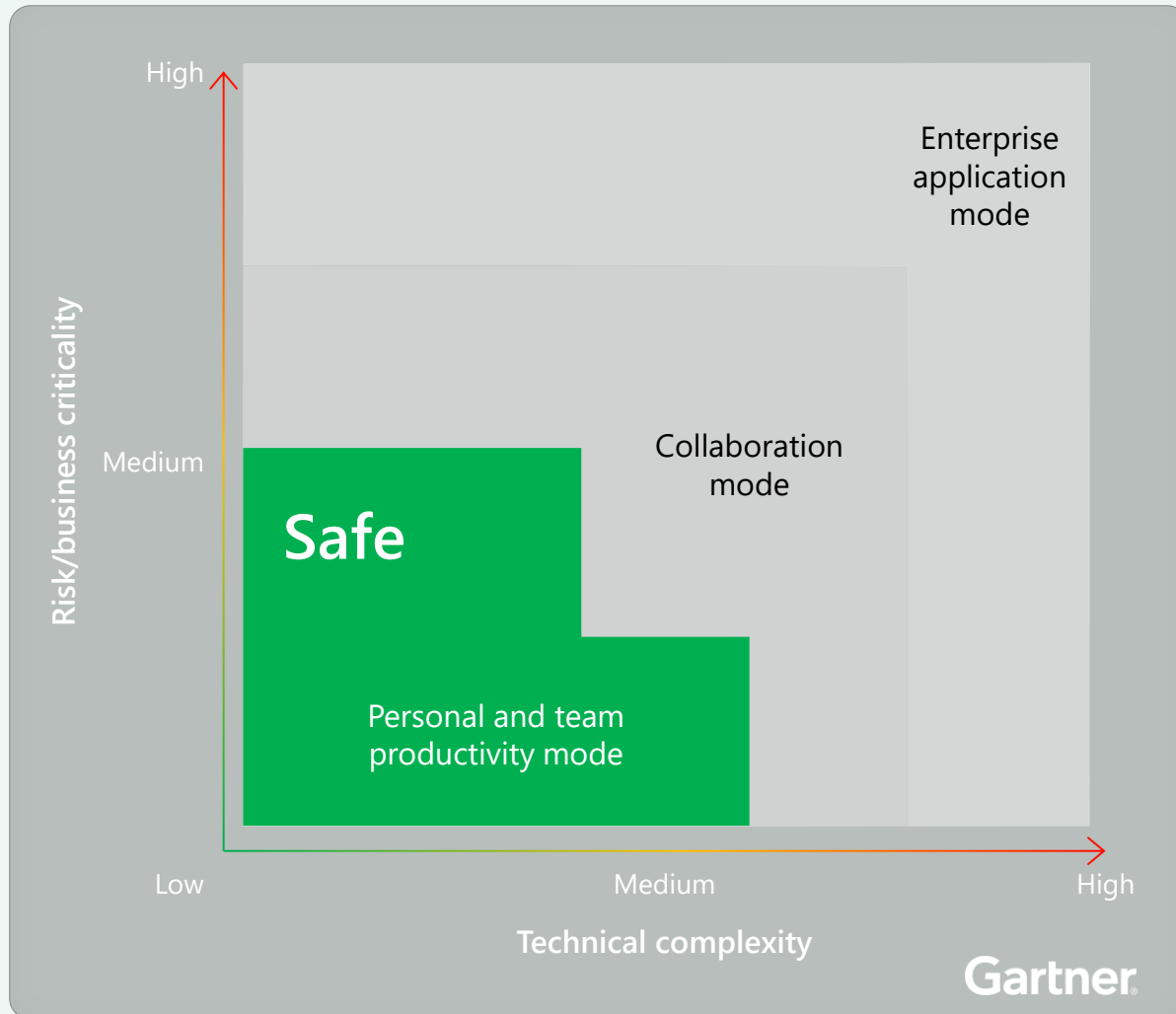


Empowerment through Zoned Governance

An example of an empowered, yet fully governed approach

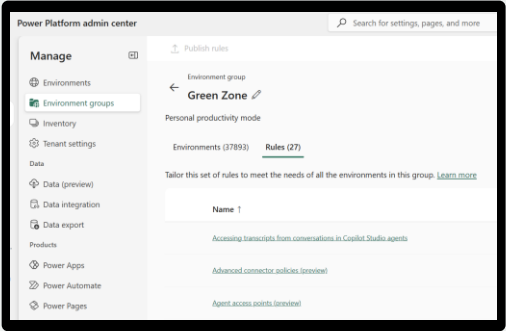


The Green zone

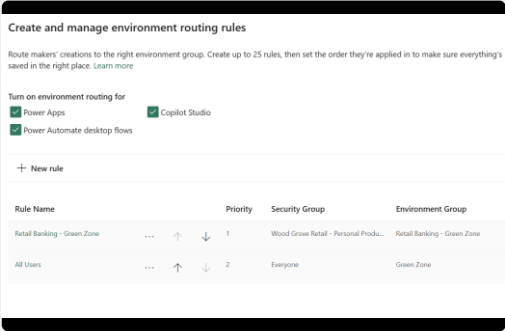


Go Green: Building your zone

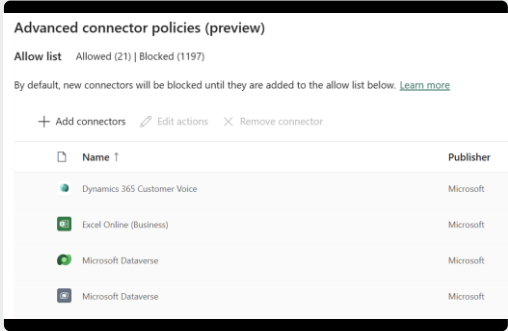
Environment Groups aka.ms/EnvironmentGroups



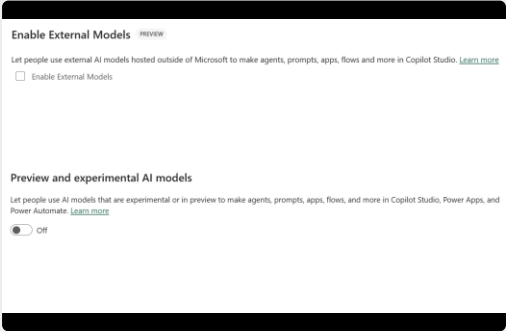
Environment Routing aka.ms/EnvironmentRouting



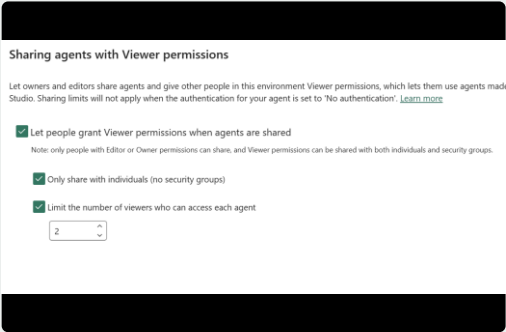
Rule: Advanced Connector Policies aka.ms/LearnACP



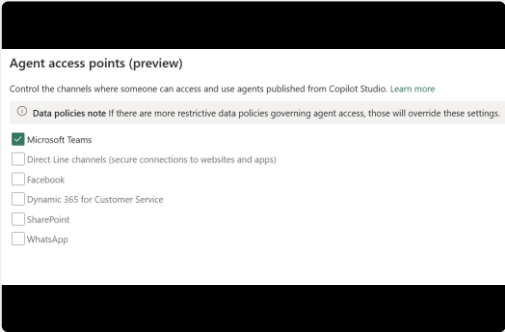
Rule: Agent AI models aka.ms/AgentModels



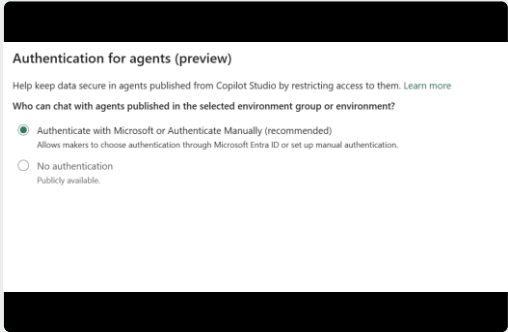
Rule: Agent Sharing aka.ms/LimitSharing



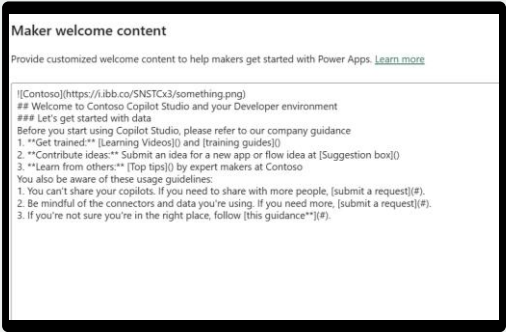
Rule: Agent Channels aka.ms/AgentChannels



Rule: Agent Authentication aka.ms/AgentAuth



Rule: Agent Onboarding aka.ms/MakerOnboarding





Power Platform Admin Center: Secure Agent Access

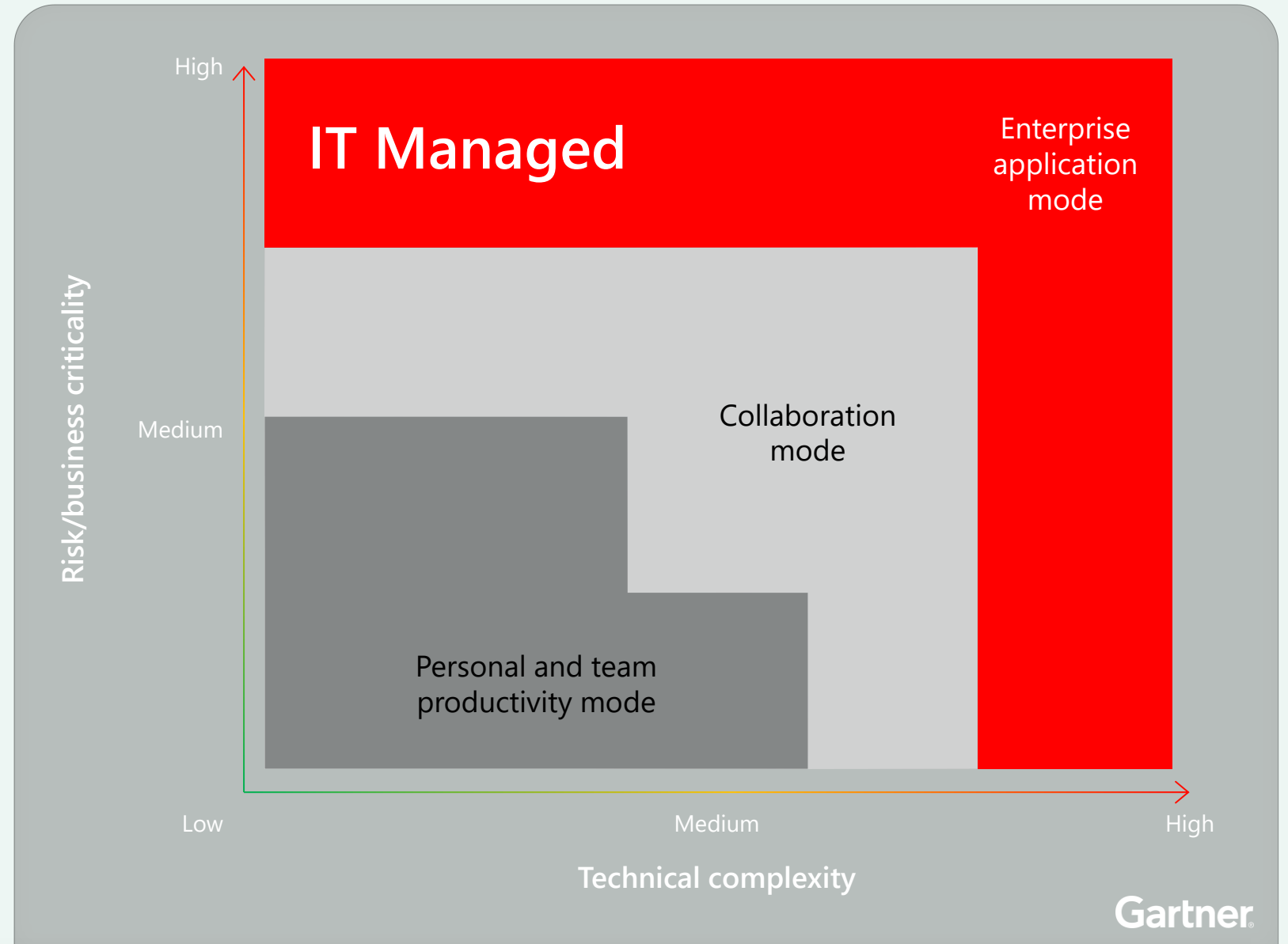
Secure agent access by disabling publish using connector management and by disabling access from internet to chat.

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

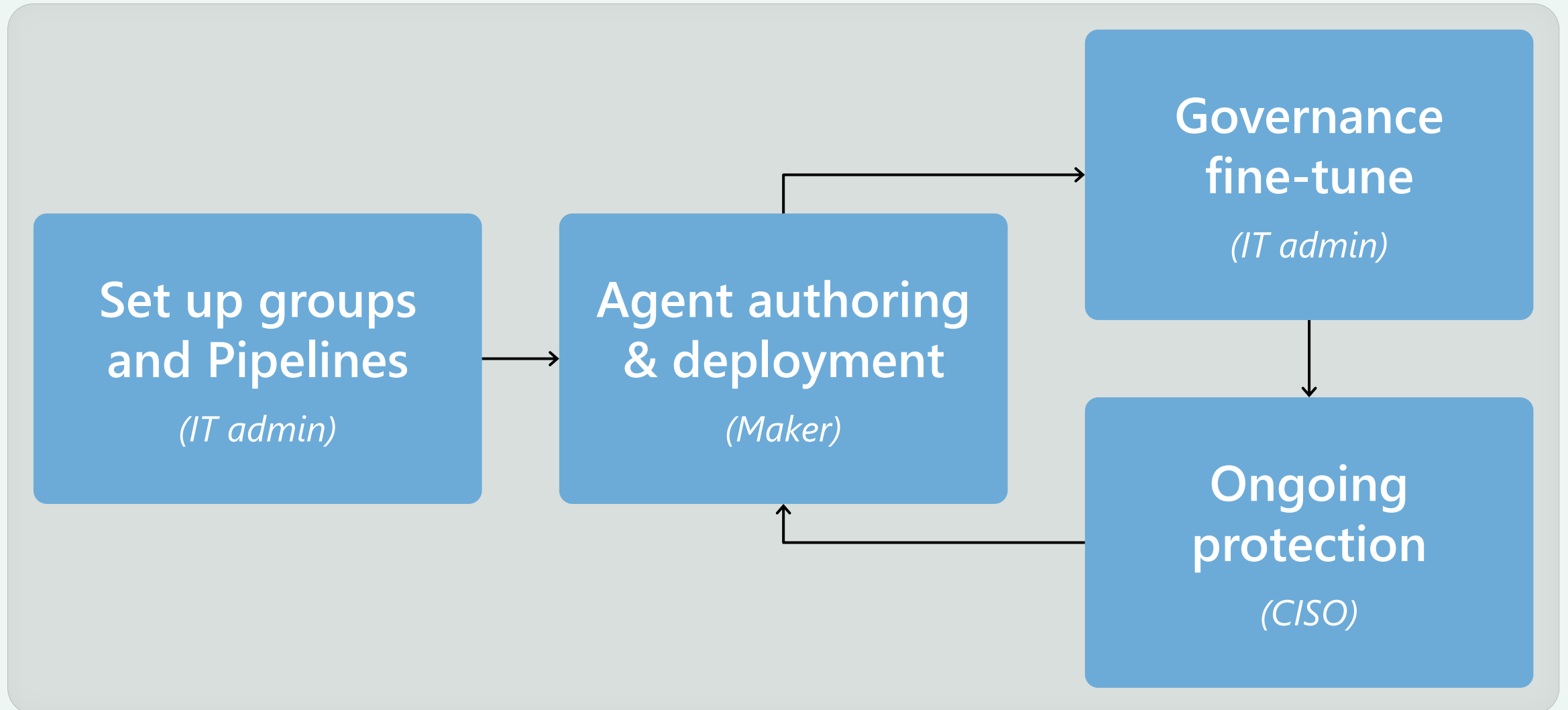
The screenshot displays the Power Platform Admin Center interface. The left sidebar shows the navigation menu with 'Security' selected. The main content area is titled 'DLP Policies > Edit Policy'. The 'Policy name' is 'MCAPSTechConnect2024 (Do Not Delete)'. The 'Prebuilt connectors' section is expanded, showing a list of connectors that are blocked by the policy. The 'Assign connectors' section shows a list of connectors that are blocked by the policy, with a search bar and a 'Set default group' button. The table lists the following connectors:

| Name | Blockable |
|--|-----------|
| Chat without Microsoft Entra ID authentication in Copilot Studio | Yes |
| Microsoft Teams + M365 Channel in Copilot Studio | Yes |
| Direct Line channels in Copilot Studio | Yes |
| Facebook channel in Copilot Studio | Yes |
| Omnichannel in Copilot Studio | Yes |

Living in the Red Zone



The steps of Red Zone governance

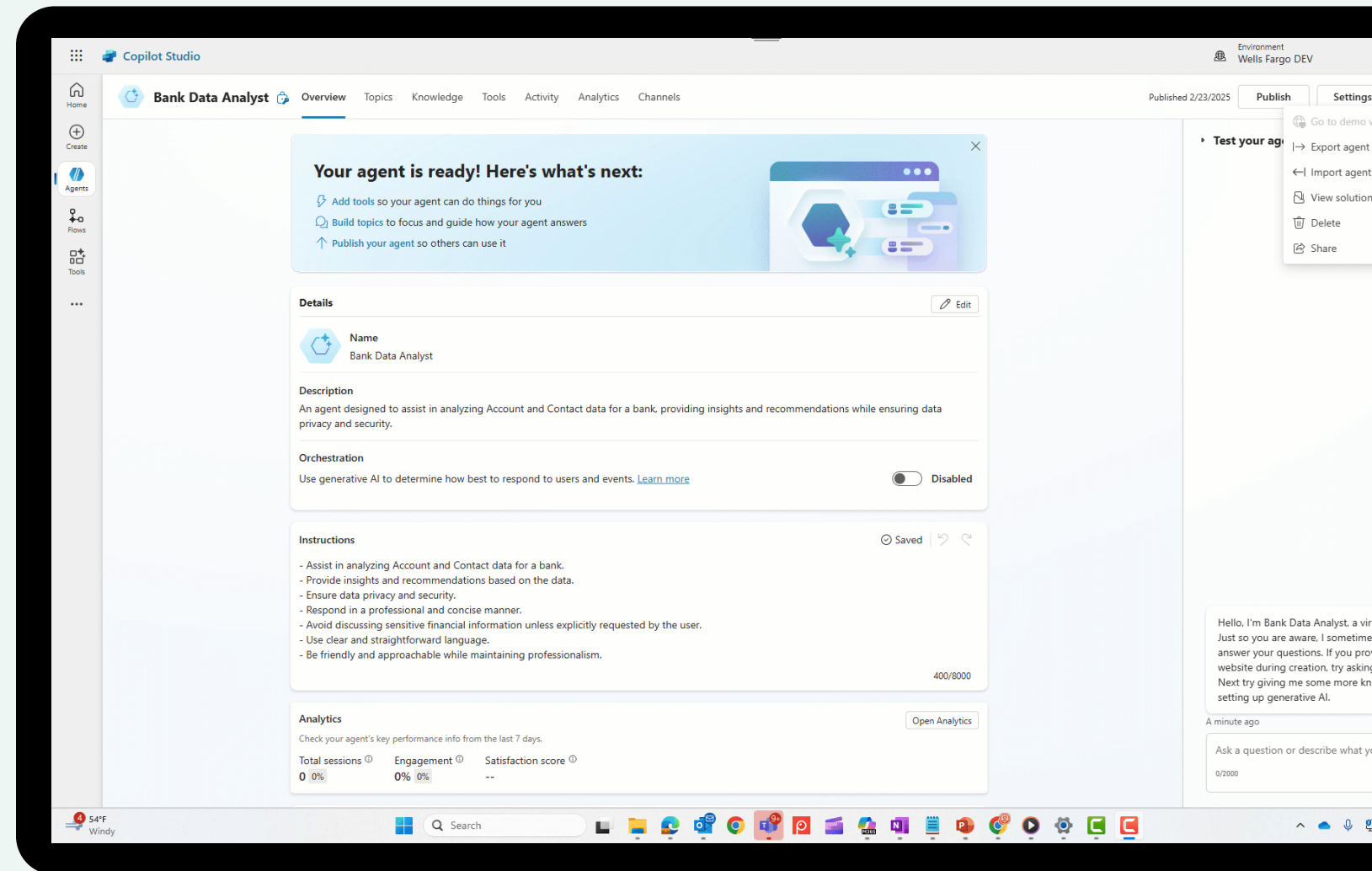




ALM

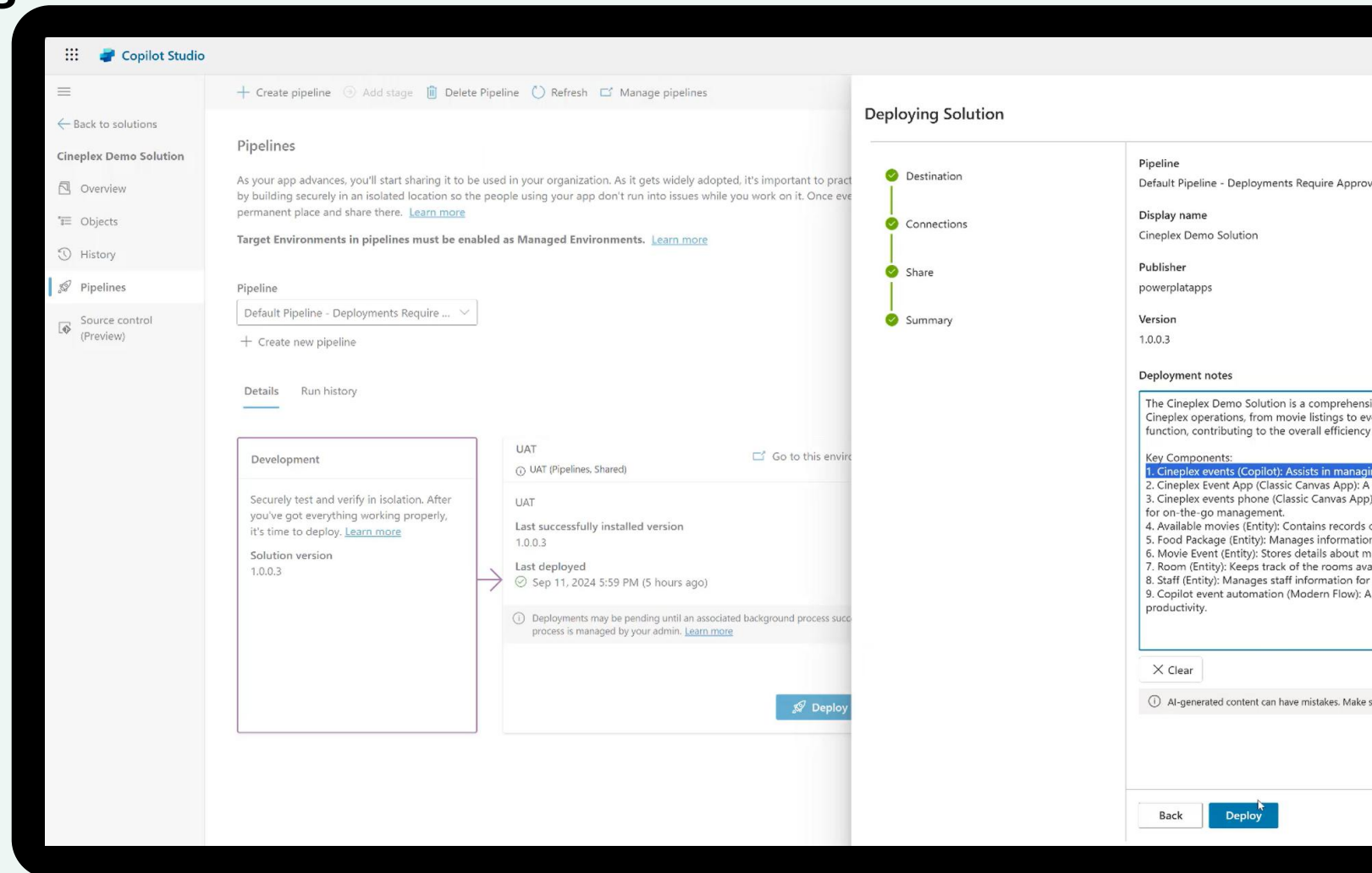
Power Platform Admin Center Pipelines + Onramps

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



Power Platform Admin Center Agent Deployment notes

- 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!



Copilot Studio Kit



The Copilot Studio Kit is a comprehensive set of tools designed to augment Microsoft Copilot Studio.

The kit includes features that help with the development, testing and long-term performance monitoring of custom agents.

Dynamics 365

Copilot Studio Kit

Search

Quick links

Home

Configure

Agents

Test

Test Sets

Test Runs

Conversation KPIs

Dashboard

Details

Tools

Prompt Advisor


Adaptive Cards

Webchat Playground


Copilot Studio Kit

The Copilot Studio Kit is a comprehensive set of capabilities designed to augment Microsoft Copilot Studio. The kit helps makers test agents, use large language model to validate AI-generated content, track aggregated key performance indicators, and design advanced functionalities through a user-friendly interface.


Features



Configure agent test
Configure agent configurations and their associated test sets.



Test runs history
View test execution history for evaluation of their conversational capabilities and



Prompt advisor
Fine-tune your prompt crafting with real time feedback and guidance.

Latest Test Runs

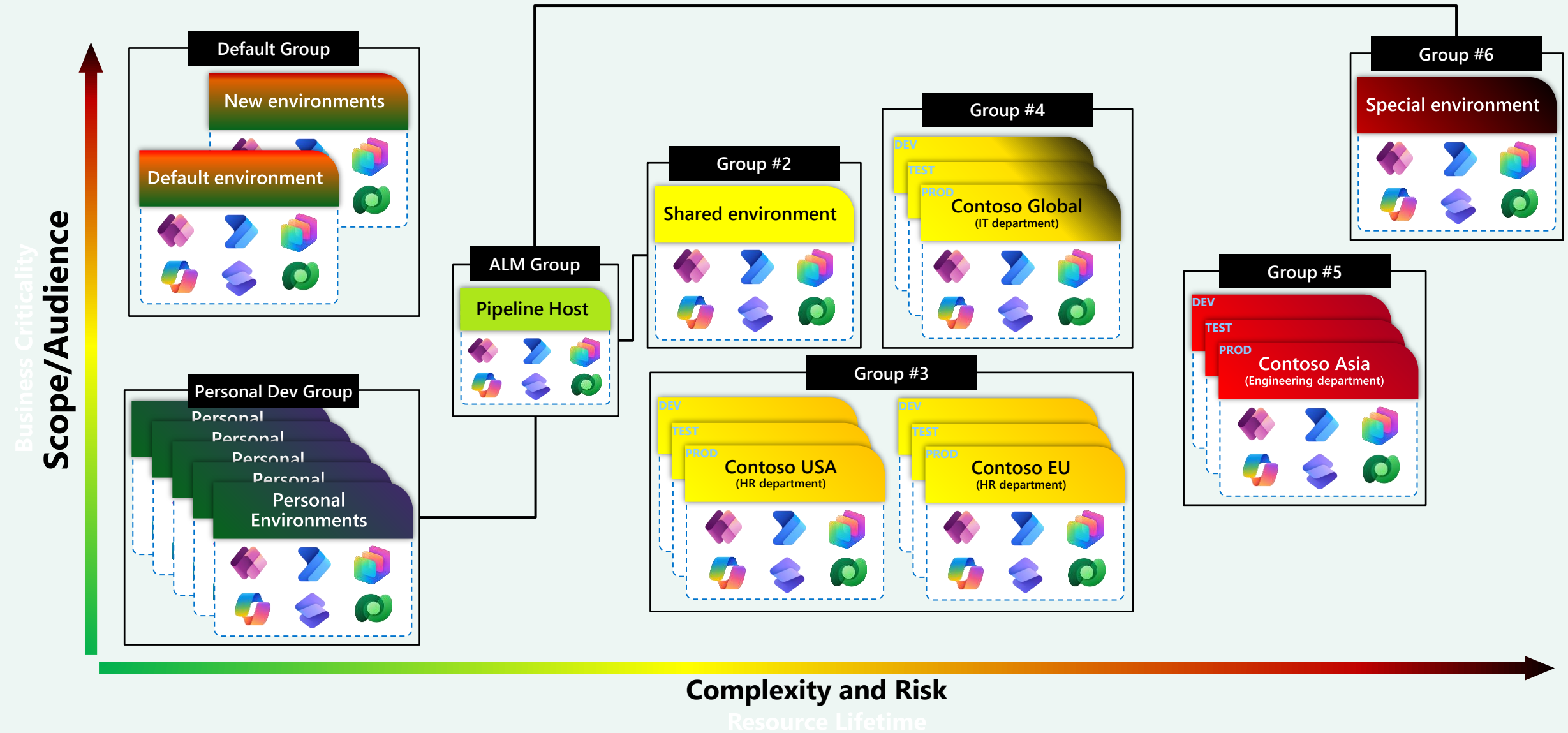
| Name | Run Status | Success Rate | # Tests |
|---------------------|------------|--------------|---------|
| Smoke test set 3 | Complete | 0 | 5 |
| Smoke test set 2 | Complete | 0 | 5 |
| Smoke test set 1 | Complete | 0 | 3 |
| Store Operations 01 | Complete | 100 | 2 |

aka.ms/CopilotStudioKit

Empowerment through Zoned Governance

An example of an empowered, yet fully governed approach

aka.ms/environmentstrategy



Cost Controls

Copilot Studio Agent Consumption Estimator

Estimate Agent Message Consumption

Preview

- Forecasts message consumption using data driven trends and assumptions
- Customizes estimates based on licensing options and feature usage
- Accessible from within Copilot Studio, Power Platform admin center, and public website

aka.ms/copilotstudioestimator

Copilot Studio agent usage estimator (preview)

Use this estimator to forecast your agent's message volume. Select from licensing options, agent types, and the features your agent leverages to respond to your end users. See the message consumption impact based on these selections. This provides a monthly message estimate for a single agent and makes no guarantees of final costs. This isn't a pricing calculator, so we can't provide total costs or make any definite forecasts around your monthly expenses.

1 Message = \$.01

Go [here](#) to convert to your currency.

Estimator type

Configure monthly agent message estimation in two ways

- ☒ An estimate based on common telemetry data and assumptions
- ☐ An estimate based on manual entries for my agent

Agent traffic

Agent traffic quantifies the activity an agent supports by assessing the number of end users accessing the agent and their monthly engagement frequency

How many users? *

e.g. 1000

On average, how many times per month will your users interact with your agent?

e.g. 30

Agent type

Agent type specifies whether the agent is deployed internally for employee interactions or externally for customer and partner conversations. Deployment location impacts usage trends, aiding in accurate consumption forecasting. [Learn more](#)

What is your agent type?

- ☐ Employee-facing agent
- ☐ Customer or partner-facing agent

Agent orchestration

Orchestration involves managing and coordinating an agent's capabilities and actions to effectively respond to user queries and perform tasks. [Learn more](#)

What type of orchestration will you require?

- ☐ Generative
- ☐ Classic

Agent knowledge

Knowledge sources enable agents to provide relevant information and insights. Published agents use configured knowledge sources to ground their responses. [Learn more](#)

Total estimated messages

Messages driven by knowledge

- Messages consumed for tenant graph grounding (10 messages) + generative answers (2 messages)
- Messages consumed for non-tenant graph grounding (2 messages): Dataverse, web, files

Messages driven by actions and topics

- Number of messages that charge for actions and topics
- Number of messages that charge for agent flows

Messages driven by agent autonomous triggers

Messages driven by optional modifiers

Basic GPT-4o mini

1 message per every 10 responses

Standard GPT-4o

15 messages per every 10 responses

Premium GPT-o1

150 messages per every 10 responses

Agent Cost Optimization in PPAC

Understand and optimize agent costs

Generally Available

- **View messages consumption** by environment, by agent, by product, and by feature
- **Allocate** messages to environments to split costs, and optionally **burst to PAYG**

Preview June 2025

- Set **agent level** message limits and track against those limits
- Set **automatic triggers** against capacity limits (warning email when close to limit followed by shut off)

The screenshot shows the Power Platform admin center interface. The left sidebar contains navigation links: Home, Actions, Manage, Security, Copilot, Monitor, Deploy..., Licensing (selected), Support, and Dev tools. The main content area is titled 'Licensing' and includes a search bar. Below the search bar, there are tabs for 'Summary' (selected) and 'Environments'. The 'Summary' tab displays the following sections:

- Copilot Studio**: A row of buttons for 'Manage billing plans', 'Manage messages', 'Manage sessions', 'Manage Agents', and 'Download report'.
- Recommendations**: A section titled 'Create a billing plan' with a subtext 'To use agents that you've created and to track usage, you'll need to set up a billing plan.' and a '+ New billing plan' button.
- Capacity summary**: Two summary cards for the current month:
 - Pay-as-you-go messages**: Shows 2.00 Billing plans and 0.00 Total messages.
 - Prepaid capacity**: A table showing capacity usage.
- Capacity consumption by product**: A section for 'Messages capacity' and 'Sessions capacity'.
- Total capacity consumption trend**: A section showing 'Pre-paid messages used' (0.00) and 'Pay-as-you-go messages' (0.00) for the 'Month to date' period.

| License type | Category | Purchased | Assigned | Consumed |
|--|-------------------|---------------|----------|----------|
| Capacity Manage capacity | Messages capacity | 3,125,250,000 | 7,000 | 0 |
| Capacity (Legacy) Manage capacity | Sessions capacity | 0 | 0 | 0 |

Focusing Admin Oversight WHERE IT counts

Manage higher risk zones

Safe Innovation Zone: Safe defaults reduce continuous monitoring. Admins can be hands off

Collaboration/Enterprise Zone: Focus your governance efforts (approvals, DLP, Tighter policies) on Dept level and Enterprise critical agents

Strengthen oversight & lifecycle management

Inventory & Audits: Keep reviewing agents inventory in Power Platform Admin Center.

Retirement of obsolete Agents: Proactively remove or archive to manage costs and remove clutter

Refine Continuously

Adapt based on usage: As agent adoption grows, revisit environment policies and connector classifications

Educate & Empower: Provide training and best practices so makers can stay aligned with organizational rules

RESULT

Innovation at Scale

Reduced Risk

Cost & Compliance
Management

Early access

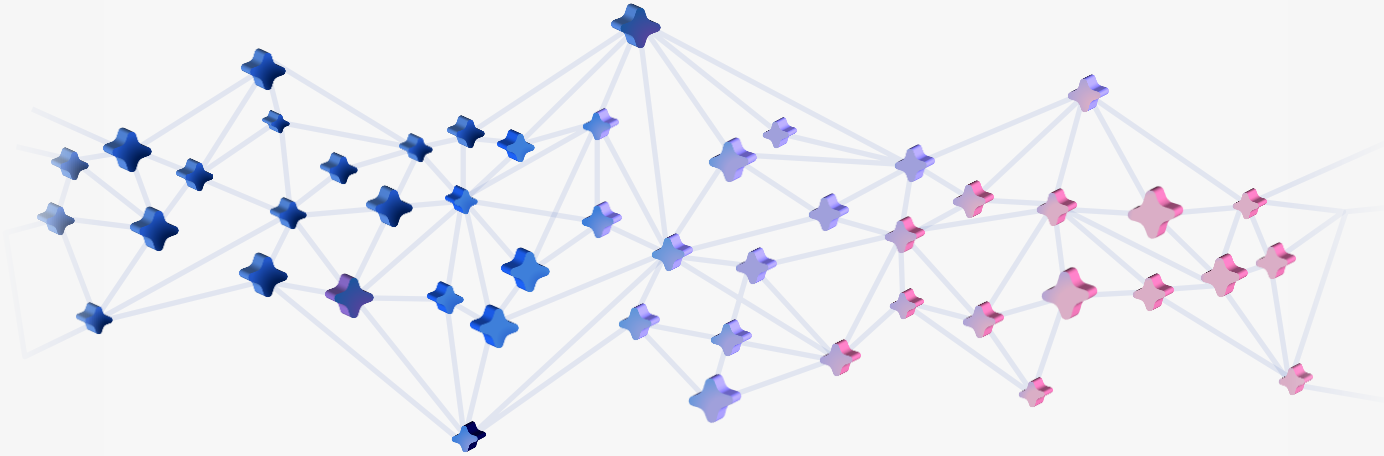


Microsoft Agent 365

The control plane for agents

Microsoft Agent 365

The control plane for agents



Registry



Access Control



Visualization



Interoperability



Security

Learn more



Breakout Sessions at Ignite:

- **BRK264:** From Risk to Resilience: Secure your AI Agents with Microsoft Defender.
- **BRK307:** Best practices to secure and govern low code agents, apps, and flows.
- **BRK310:** Deploying and operating Power Platform solutions with DevOps.

| | | |
|----|---|---|
| 1 | Maker Onboarding | aka.ms/MakerOnboarding |
| 2 | Environment Routing | aka.ms/EnvironmentRouting |
| 3 | Environment Groups | aka.ms/EnvironmentGroups |
| 4 | Limit Sharing | aka.ms/LimitSharing |
| 5 | M365 Copilot Control Settings | aka.ms/M365CCS |
| 6 | Power Platform Copilot Hub | aka.ms/PowerPlatformCopilotHub |
| 7 | Power Platform Inventory | aka.ms/PowerPlatformInventory |
| 8 | Default Pipeline | aka.ms/default-pipeline |
| 9 | Monitor Alerts | aka.ms/MonitorAlerts |
| 10 | Monitoring Hub | aka.ms/MonitoringHub |
| 12 | Manage MCS Credit | aka.ms/ManageMCSCredit |
| 13 | Power Platform Admin Center (PPAC) | aka.ms/PPAC |
| 14 | Learn Advanced Connector Policies | aka.ms/LearnACP |
| 15 | Agent Channels | aka.ms/AgentChannels |
| 16 | Copilot Studio Runtime Protection | aka.ms/CopilotStudioExtendedProtection |
| 17 | Microsoft Information Protection in MCS | aka.ms/MIPinMCS |
| 18 | Monitoring Overview (Docs) | aka.ms/MonitoringHub |

Get started today



aka.ms/trycopilotstudio



Learn more

Copilot Studio website: [aka.ms/**copilotstudio**](https://aka.ms/copilotstudio)

Blog: aka.ms/copilotstudioblog

Public Demo: [aka.ms/**copilotstudiodemodemo**](https://aka.ms/copilotstudiodemodemo)

Learn Docs: [aka.ms/**copilotstudiodocs**](https://aka.ms/copilotstudiodocs)

Community page: [aka.ms/**copilotstudiocommunity**](https://aka.ms/copilotstudiocommunity)

Copilot Studio Resources: aka.ms/copilotstudio/resources

Copilot Studio
Implementation Guide: [aka.ms/CopilotStudio/Implementa
tionGuide](https://aka.ms/CopilotStudio/ImplementationGuide)