

**HITACHI**



Hitachi Solutions Europe

# Agents In A Day

Hands-on workshop

# Today's Presenters

HITACHI



**David Reid**  
Solution Architect  
AI Business Solutions  
**Hitachi Solutions**



**Dana Hasan**  
Architect  
AI and Analytics  
**Hitachi Solutions**



**Kyle Smith**  
Consultant  
AI Business Solutions  
**Hitachi Solutions**



**Amy Matrai**  
Senior Project  
Manager  
**Hitachi Solutions**



**Sam Bartlett**  
Data and AI Lead  
Regulatory Services  
Programme  
**Environment Agency**



**Will Corfield**  
Go To Market Lead  
Low Code  
**Microsoft**



**Phil Wiltshire**  
Lead Solution Architect  
**Defra**

# Event Agenda

HITACHI

**09:00-09:30**

*Check-In & Breakfast*

---

**09:30-10:30**

**Welcome and Microsoft Presentation – the Frontier Firm**

---

**10:30-11:15**

**Introduction to Agents in Microsoft Copilot chat (demo) and Copilot Studio**

---

**11:15-11:30**

*Coffee break*

---

**11:30-12:15**

**Lab Session 1: Building Conversational Agents in Copilot Studio**

---

**12:15-13:15**

*Lunch break*

---

**13:15-14:00**

**Environment Agency and Hitachi: Responding to ministerial priorities through AI-enabled transformation**

---

**14:00-15:00**

**Lab Session 2: Enhancing Agents with Tools and Knowledge**

---

**15:00-15:15**

*Coffee break*

---

**15:15-16:00**

**Lab Session 3: Expanding to Autonomous Agents and advanced behaviours in Copilot Studio**

---

**16:00-16:30**

**Managing Security and Governance in the Agentic era**

---

**16:30- 17:00**

**Conclusion, Q&A, Feedback session and networking**

---

# Hitachi Overview

HITACHI



# Hitachi has been a leader in innovation since 1910

HITACHI

All companies under the Hitachi name operate today based on the principle our founder Namihei Odaira recognized over 110 years ago: "Companies are their people."

Hitachi remains at the forefront of innovation today, delivering new innovations to benefit both society and organisations.

## Digital Innovation & Transformation

Accelerating digital and business transformation within organisations across the globe through AI, IoT, cloud computing, digital engineering and data analytics.

\$17B USD

107,000 employees

## Green Energy & Mobility

Sustainable innovation through renewable energy, smart grids, electric transportation, and advancing carbon neutrality and efficient infrastructure for a greener future.

\$20.2B USD

82,000 employees

## Connective Industries

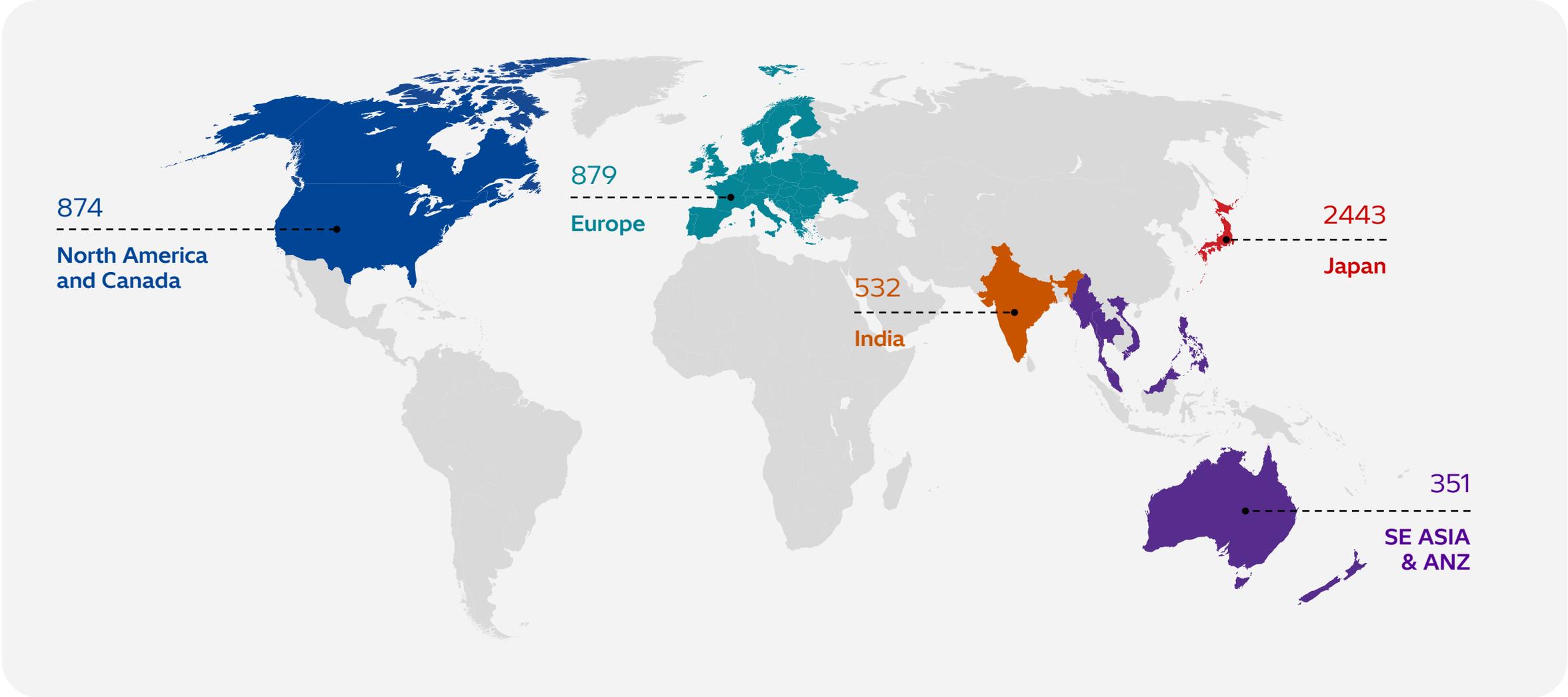
Integrates digital, IoT, and AI solutions to enhance efficiency, sustainability, and productivity across manufacturing, logistics, energy, and urban development.

\$21.2B USD

62,000 employees



# We're global, yet local



# 20 years of partnership with Microsoft

HITACHI

We work exclusively alongside Microsoft, leveraging 20 years of collaboration to drive end-to-end digital transformation to organisations across the globe.

Our mission to contribute to society through the development of superior, original technology and products aligns with Microsoft's goal of empowering people and organizations worldwide

“

Our expanded partnership with Hitachi will bring together the power of the Microsoft Cloud – including Microsoft Copilot – with Hitachi’s industry expertise to **improve the productivity** of 270,000 Hitachi employees and help **address customers’ biggest challenges**, including sustainability.”



**Satya Nadella**  
Chairman and CEO, Microsoft

A handwritten signature in black ink that reads "Satya N.".

# Our Microsoft awards

55x

Microsoft Partner of  
the Year Award Winner

100

Partner  
Contribution  
Index Score  
*out of 100*

19

Years on  
Microsoft's  
Partner Advisory  
Council

22

Years in  
Microsoft's  
Inner Circle



2025 Microsoft Partner of the Year  
**Winner for Finance**

2025 Microsoft Partner of the Year  
**Winner for Government**

2025 Microsoft Partner of the Year  
**Finalist for Build and Modernize AI Apps Award**

2025 Microsoft Partner of the Year  
**Finalist for Dynamics 365 Sales & Customer Insights Award**

2025 Microsoft Partner of the Year  
**Finalist for Dynamics 365 Supply Chain Award**

2025 Microsoft Partner of the Year  
**Finalist for Low Code Application Development Award**

2024 Microsoft Partner of the Year  
**Winner for Low Code Application Development**

2024 Microsoft Partner of the Year  
**Finalist for Intelligent Automation**

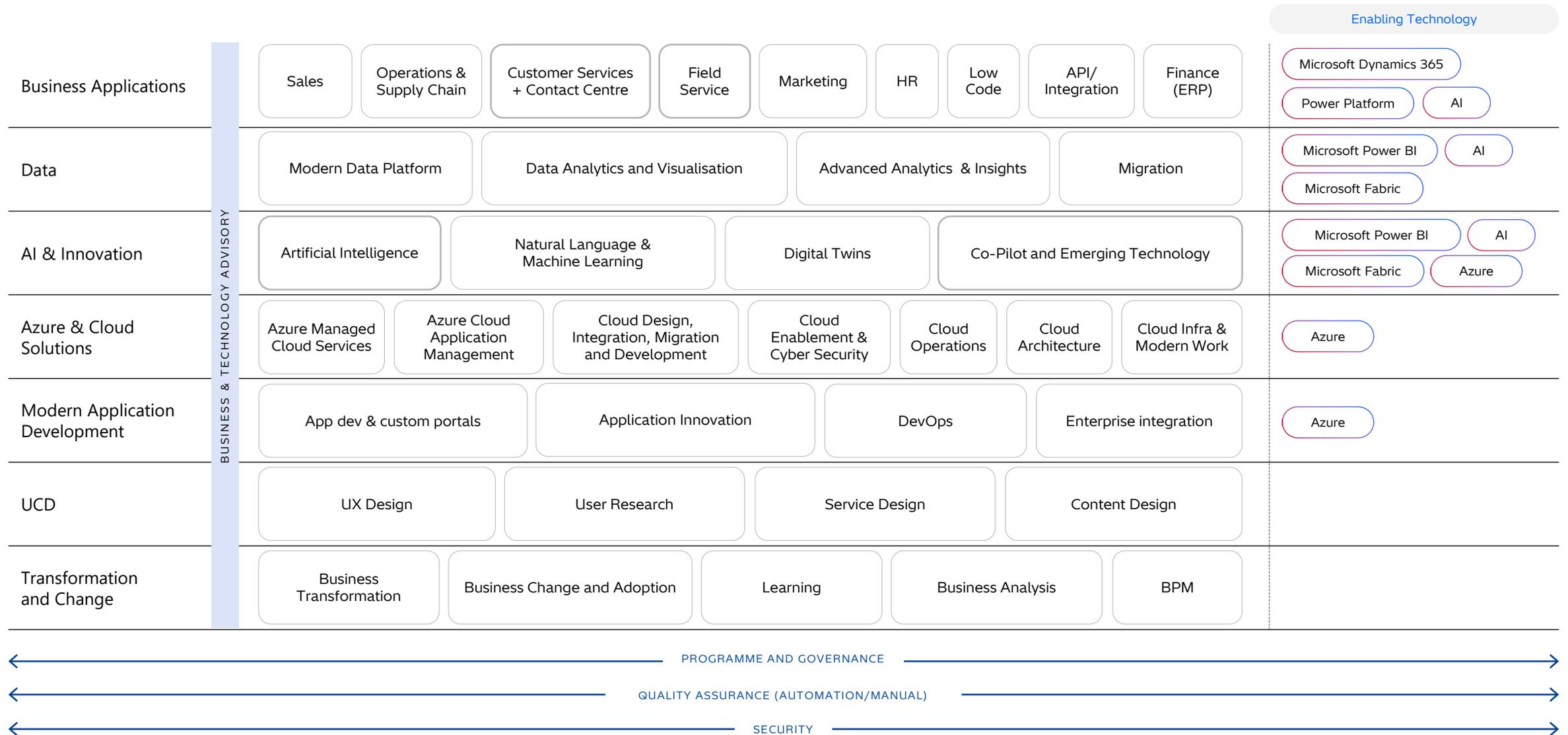
2023 Microsoft Partner of the Year  
**Winner for Dynamics 365 Services**

2023 Microsoft Partner of the Year  
**Winner for Dynamics 365 Supply Chain Management**

2022 Microsoft Partner of the Year  
**Winner for Dynamics 365 Supply Chain Management**

2021 Microsoft Partner of the Year  
**Winner for Dynamics 365 Field Service**

# Our overall services



# Transformation Advisory



Our Advisory services align you to the correct entry point based on current state. We enable you to understand how the implementation of Microsoft capability can support the achievement of your strategic objectives.

We develop an understanding of your **Strategic objectives** and **organisational challenges**

We enable teams to develop and **understanding** of challenges, ideate solutions and **prioritise** potential innovations

We develop a roadmap **vision** for Microsoft enabled transformation with clearly defined **value** opportunities

## Engagement Types

- ✔ **Strategic Alignment**  
Develop an understanding of how Microsoft capabilities can enable your transformation strategy
- ✔ **Transformation Mapping**  
Understand, prioritise and identify the value potential of transformation opportunities
- ✔ **Design Sprints**  
Rapidly understanding a challenge and potential solutions based upon Microsoft capability



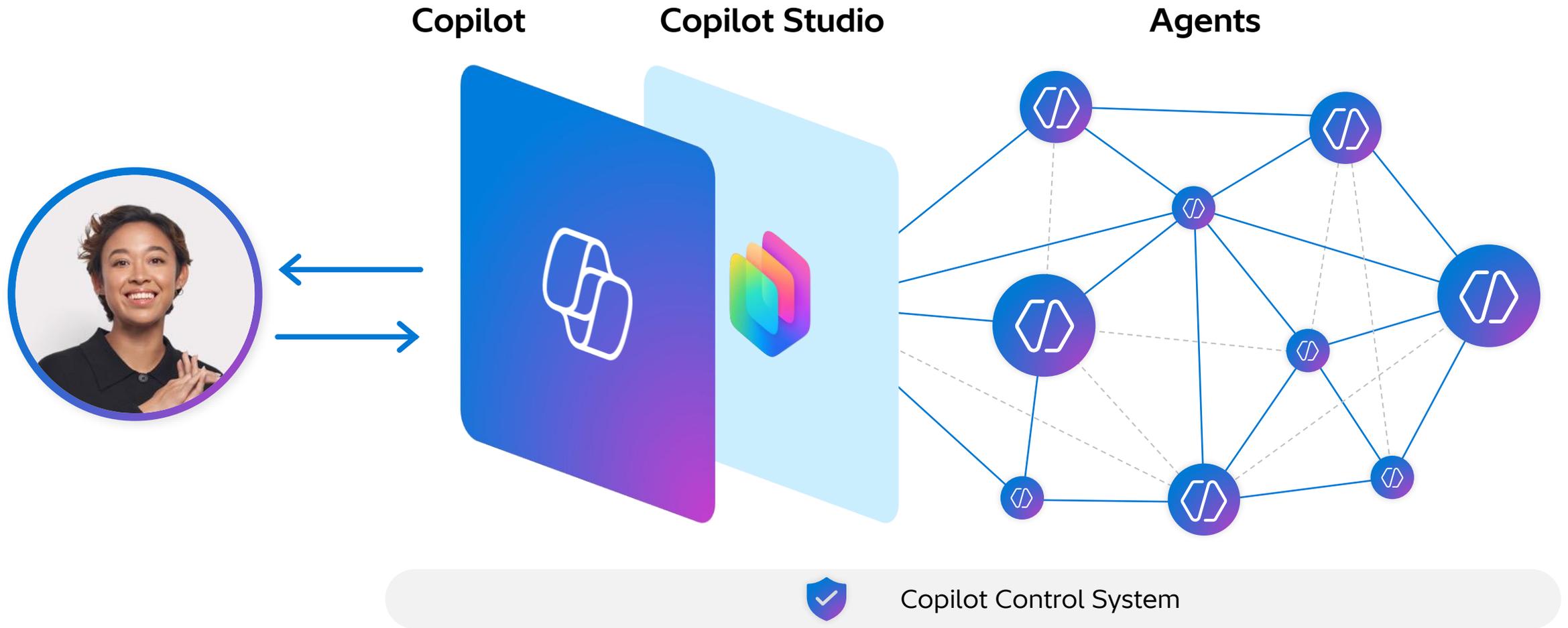
# Introduction to Agent in Microsoft Copilot chat and Copilot studio

HITACHI

10:30 - 11:15

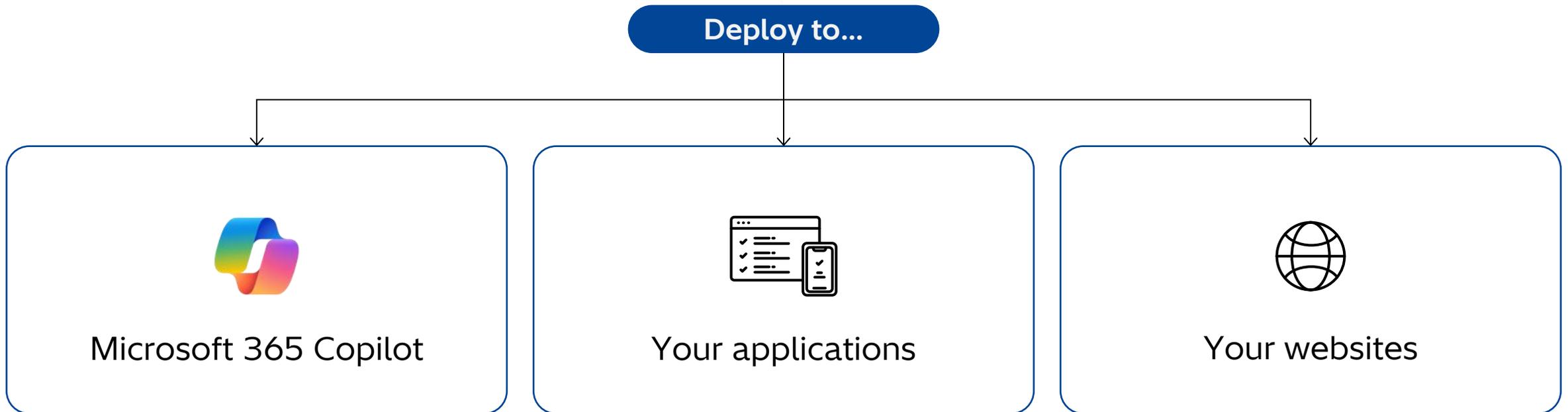
45 Min

# Copilot is the UI for AI

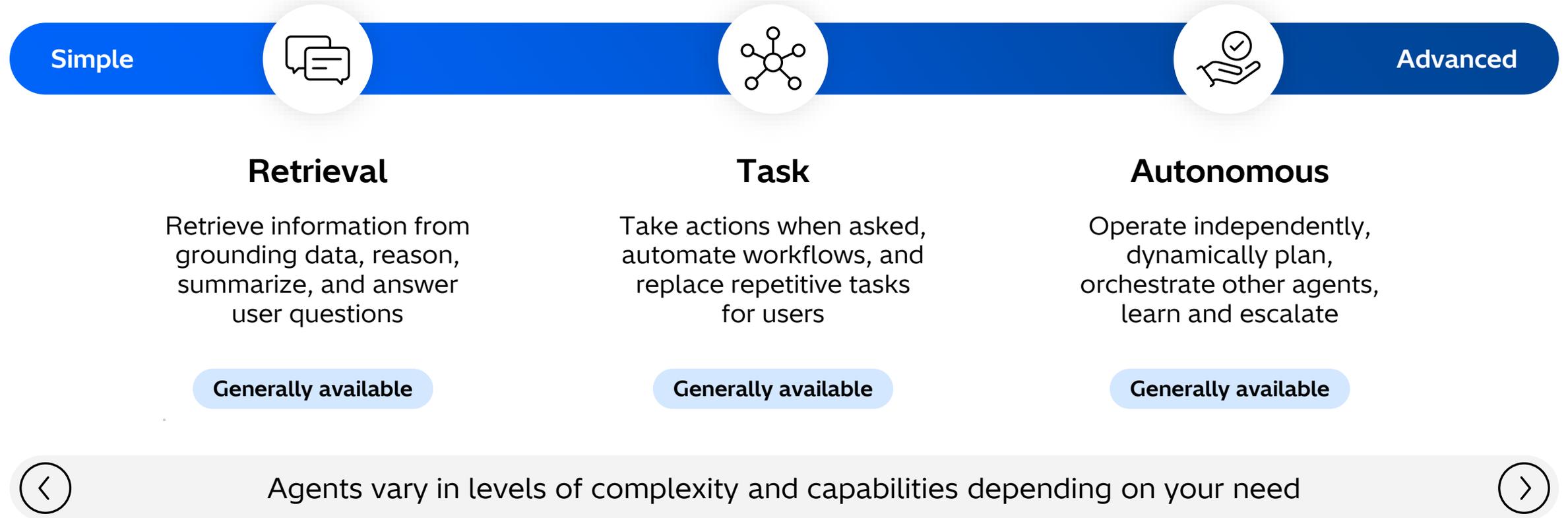


# What is an agent?

Agents use AI to automate and execute business processes, working alongside or on behalf of a person, team, or organization.



# Spectrum of agents

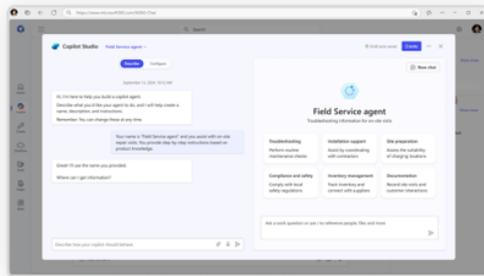


# A range of tools for agent creation

and a range of agent scenarios to create



## For End Users

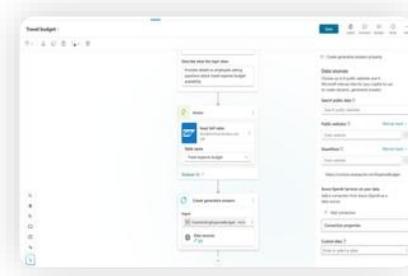


### Agent builder

Employee facing coach/knowledge scenarios

Helpful agents in M365 Copilot and apps

## For Makers



### Copilot Studio

Copilot Agents using web and company data

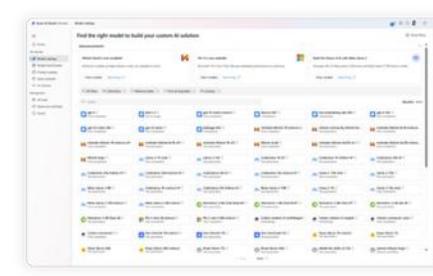
Customer-facing conversational chat agents

Autonomously triggered agentic processes

Embedded agents in D365 Sales and Service

Legacy integration – connect and automate

## For Developers



### Visual Studio Code, Copilot Studio, Azure AI Foundry

Pro-code and dev/testing patterns

Multi-agent orchestration

Agent service and Azure AI search

Specialist AI models – Azure AI Foundry

# Delivered Use Cases

## HR Recruitment

Prototype

Transform the process by automating essential tasks.



## AI HR Policy

Production

Answering questions about HR policies.



## RFQ Automation

POC

Build a quote based on an RFQ document.



## Charities Finder

POC

Conversational agent linked to a Power BI dashboard to select relevant charity.



## Sales Order Automation

Production

Captures data from sales order documents and integrates with ERP systems.



## Recruitment Process agent

Hitachi Solutions

Prototype

Improve end-to-end process with AI.



## App User guide assistant

POC

Improve adoption with a conversational agent.



## Document analysis

POC

Extract essential data from a notarial document.



## Environmental reports and Q&A

POC

Part of a broader initiative to modernize regulatory services using AI.



## Employee Onboarding

POC

Enhance onboarding process ensuring a smooth transition and reducing integration risks.



## IT Helpdesk

Production

Conversational agent linked to Service Now and Salesforce.



# When to use what M365 Copilot Or Copilot Studio



## Use a **M365 Copilot** for...

- Enhancing individual productivity and creativity at work
- Assisting with writing, analysis, and communication tasks
- Helping employees save time and focus on higher-value work



## Use a **Copilot Studio** for

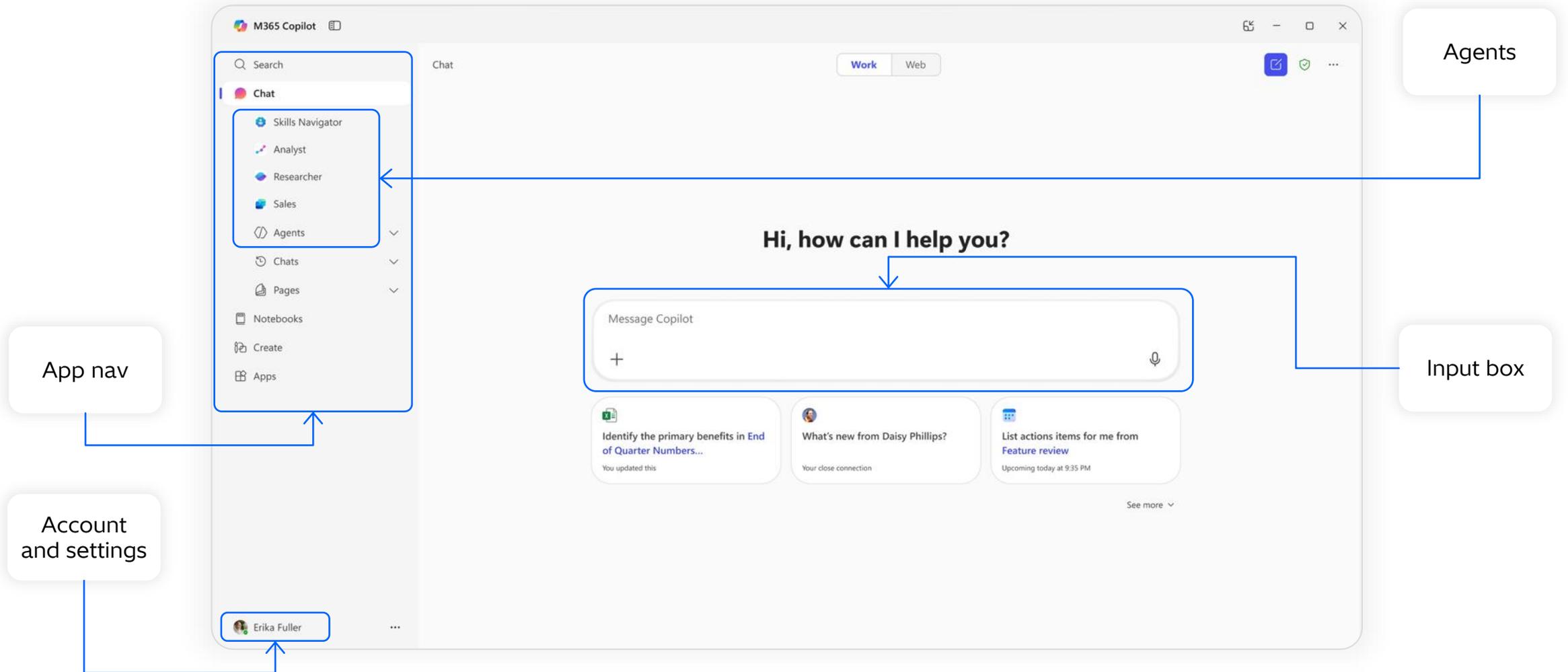
- Creating tailored assistants for teams or departments
- Guiding users through structured workflows or decisions
- Delivering consistent answers and experiences across the organization

# Microsoft Copilot chat

HITACHI



# Accessing agents in Copilot Chat

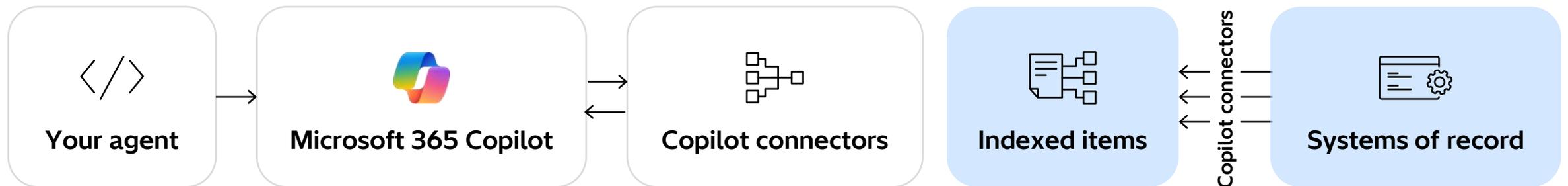


# Copilot connectors

Add new knowledge to Microsoft 365 Copilot

Generally Available

Copilot connectors (formerly Graph connectors) make it easier to bring external knowledge into Microsoft 365 Copilot. They enable Copilot to understand context and relationships in your data, delivering more relevant and secure responses. Over 65 Microsoft built connectors are now generally available or in preview in the Microsoft 365 Admin Center, including Gong, PagerDuty, Unily, and more. Full list will be updated here for Build: [https://aka.ms/Copilot\\_connectors\\_learn](https://aka.ms/Copilot_connectors_learn)



# Creating helpful agents using M365 Copilot

These agents can be easily built using Copilot Studio “lite” agent builder in Copilot Chat. Once shared, users with access can add the agent by selecting [Get Agents](#) in Copilot Chat.

Agent Name	Description
 <b>Onboarding Buddy</b>	Assists new hires with onboarding processes, provides training, answers questions, and sets up meetings.
 <b>Contract/Legal review</b>	Automates review and analysis of legal documents, identifies key clauses and assesses compliance.
 <b>Research Assistant</b>	Retrieves research materials from company databases, enhances productivity by providing relevant information.
 <b>Policy Search</b>	Offers comprehensive policy lookup capabilities, answers inquiries about company policies.

# Demo: HR Policy Assistant



Our fictitious company, Hisole Energy, is planning to build an AskHR agent to answer common questions by retrieving answers from existing SharePoint site.

**Example description/What would you like it to make:** You are an Ask HR Agent that can provide HR related information such as answering holiday, leave related queries. You should answer questions about PTO policy, the holiday calendar, and parental leave using only verified and approved HR information.

Use the name "HR Policy Assistant" for the agent.

You should always cite the source document and also provide step-by-step instructions for HR processes referencing the documents

**Naming confirmation:** HR Policy Assistant

To be emphasized/avoided: Please be clear and concise and avoid long answers. Where possible, refer primarily to the knowledge shared with you. If you don't know the answer, please refer users to the HR Team

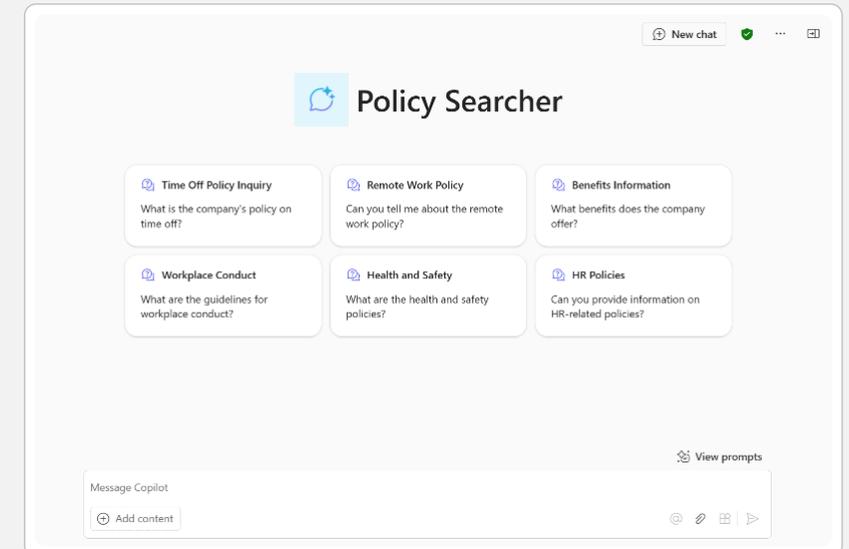
**How to communicate:** Friendly and professional

**Starter prompts:** Leave as is

**Knowledge:** Use a SharePoint site that stores company HR policies

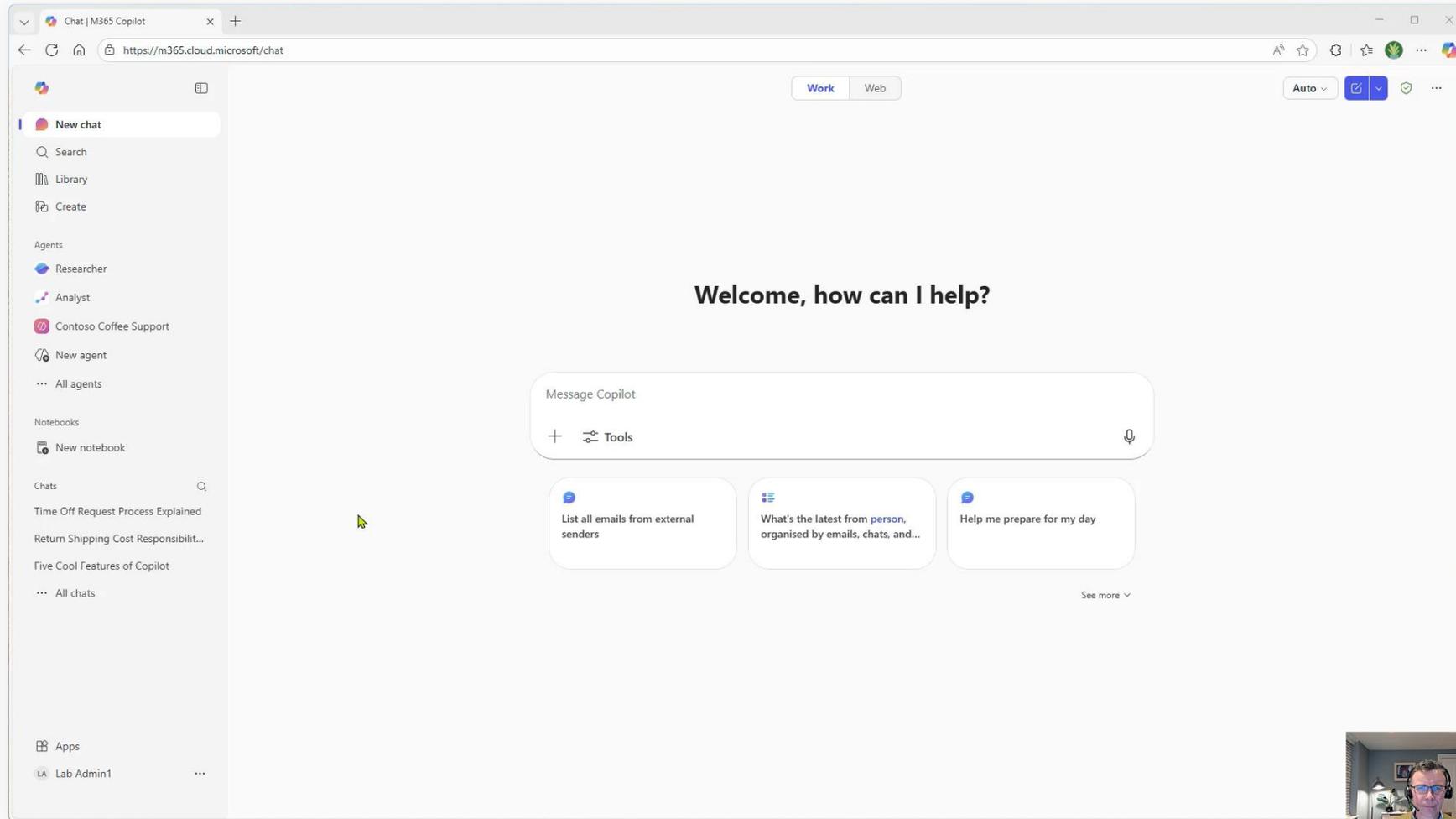
**Example questions to ask:**

- What is our PTO policy
- Where can I find holiday calendar
- How do I apply for a parental leave?
- Are public holidays different in Scotland?



# DEMO

## Creating an HR Policy Assistant in M365 Copilot Studio Lite experience



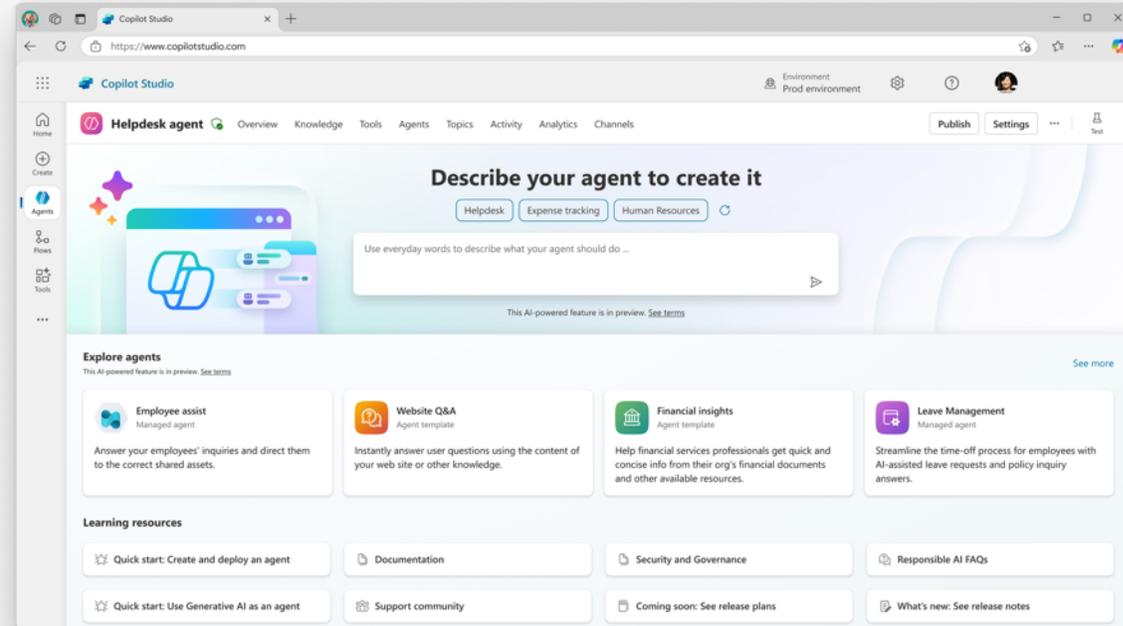
# Copilot Studio

HITACHI



# Copilot Studio

Copilot Studio is a **low code tool** for **building agents** and extending Microsoft 365 Copilot.



- ✔ 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

# Create chat experiences that are...



## Intelligent

Remember and understand user context and intent



## Secure

Maintain industry standards for governance, security and lifecycle management



## Automated

Dynamically complete tasks and automate workflows



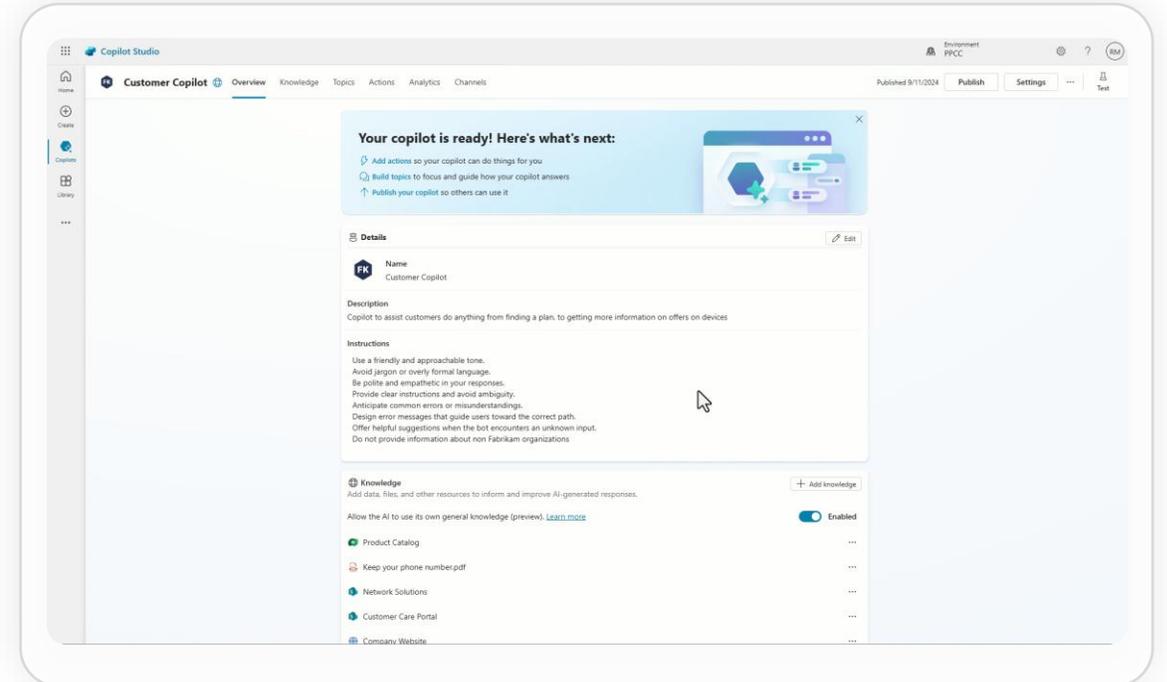
## Customizable

Connect to your data and legacy systems, extend across Microsoft's ecosystem and more



## Collaborative

Interact with agents as if they were another member of the team



## Evolution

2023

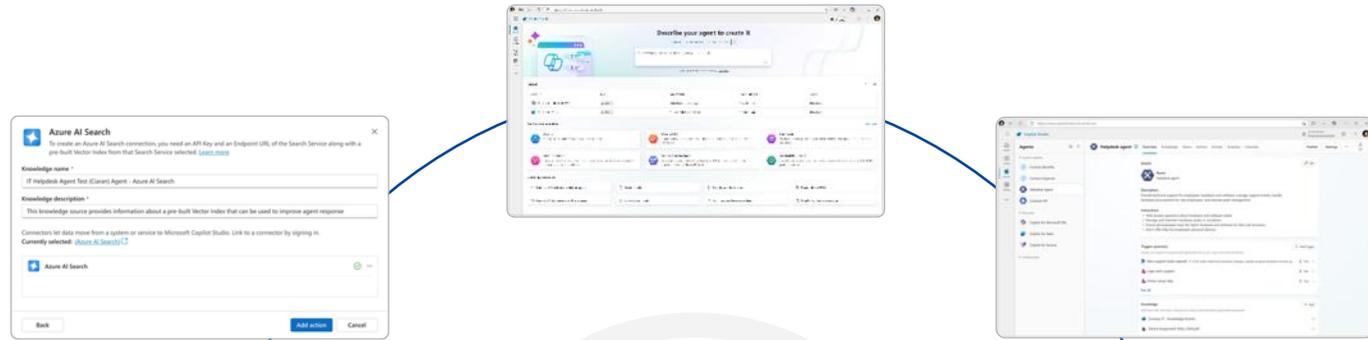
Search • Summarization • Generation

2025+

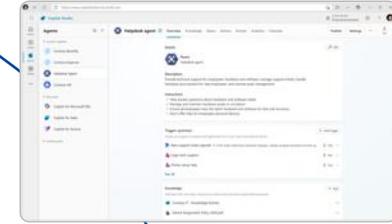
Customization • Collaboration • Automation

Build agents and workflows  
by simply describing what you want

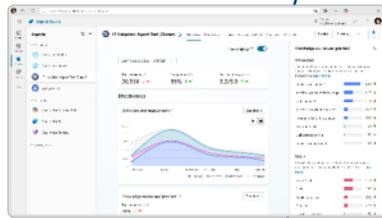
Integrations  
Integrate with Microsoft Foundry



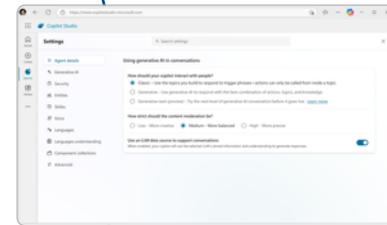
Trigger your agents and workflows  
interactively through a chat, or  
autonomously through events



Monitor and Improve  
with rich analytics,  
observability, and  
custom evaluations



Chat over your knowledge  
Provide generative answers  
over your knowledge –  
wherever it is - in M365,  
in Dataverse, in 3rd party  
systems and more

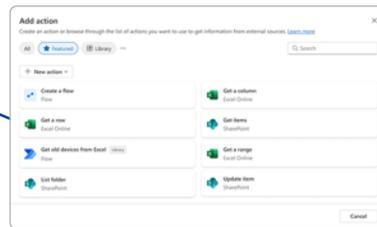
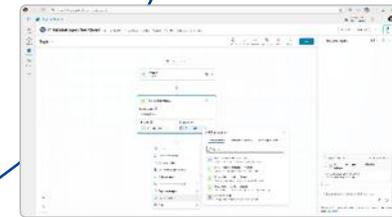


Publish to multiple channels,  
and go live instantly

Govern and manage your  
agents with sophisticated  
capabilities



Use workflows  
Create your own agent workflows and  
deterministic processes – allow your  
agents to use them and (soon) allow  
workflows to call your agents



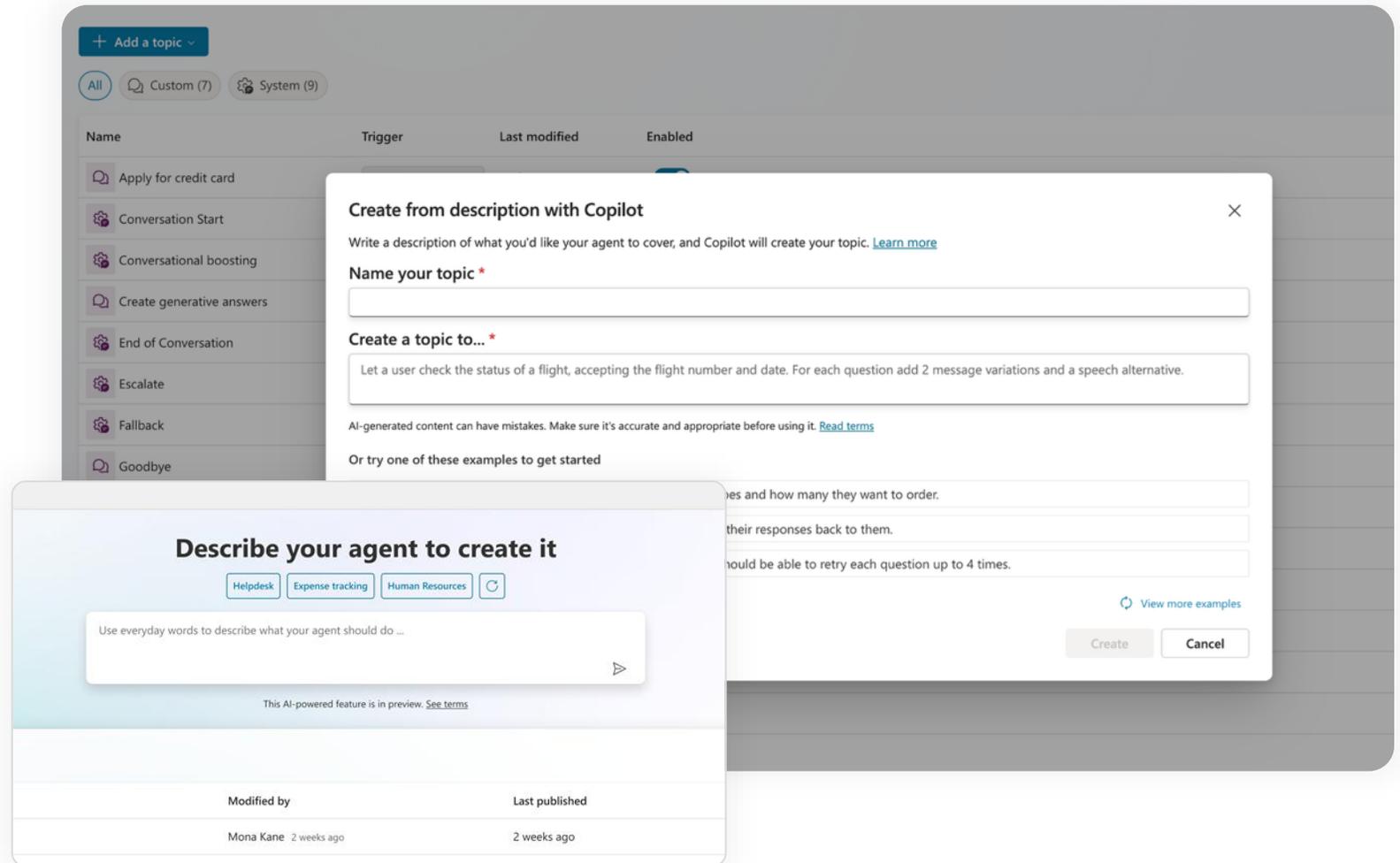
Orchestrate over multiple agents and tools such as  
APIs, PP connectors, MCP servers, and powerful  
built-in tools such as Computer Use Agents

# Generative building

Build a complete custom agent by describing what you want your agent to do in natural language.

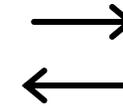
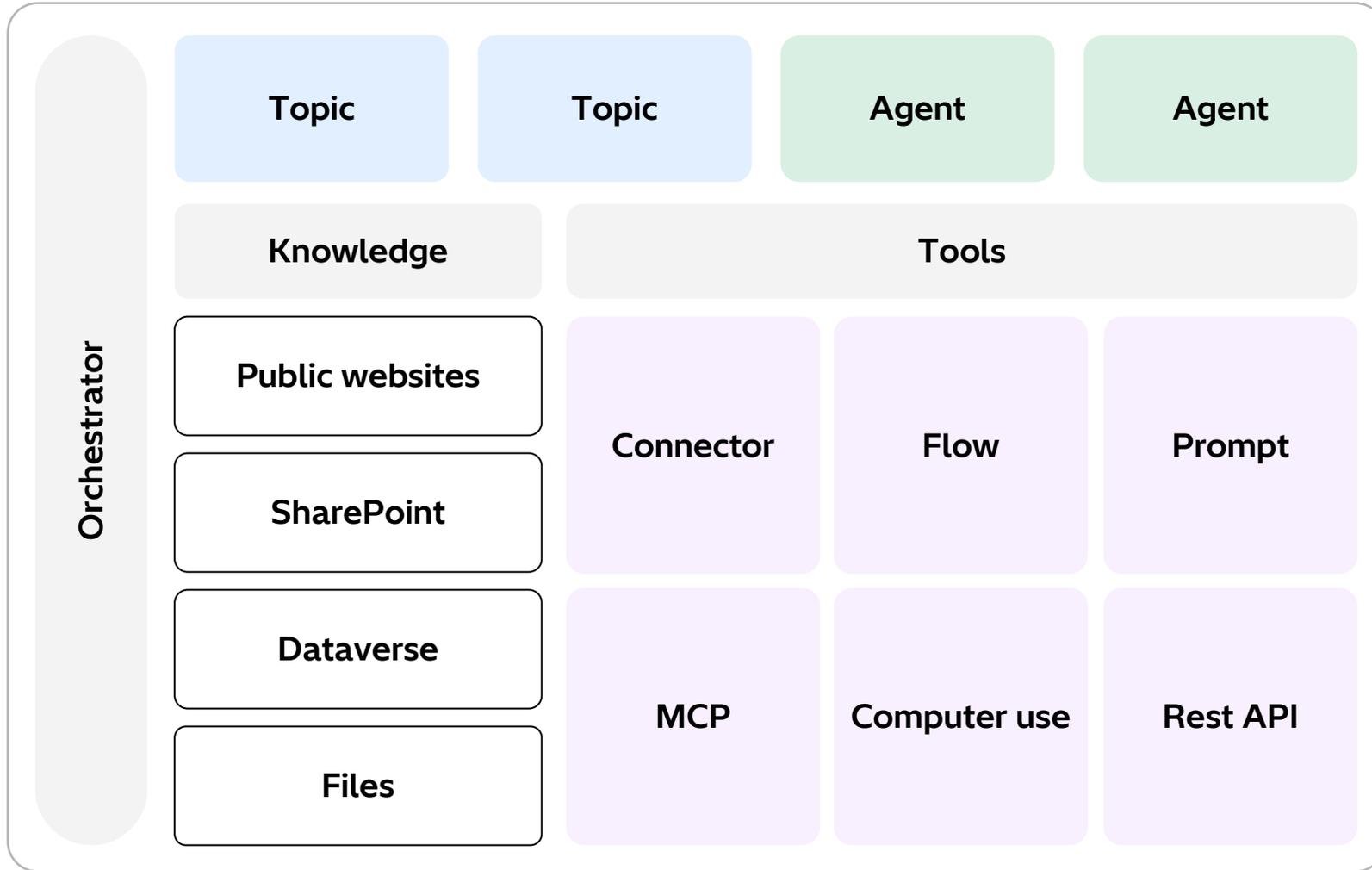
Use the in-product embedded Copilot experience for:

- Topic creation
- Topic iteration
- Response generation
- Adaptive Card generation
- Topic improvement suggestions
- Suggested trigger phrases, topic names, topic descriptions
- Transcript generation
- Topic suggestions



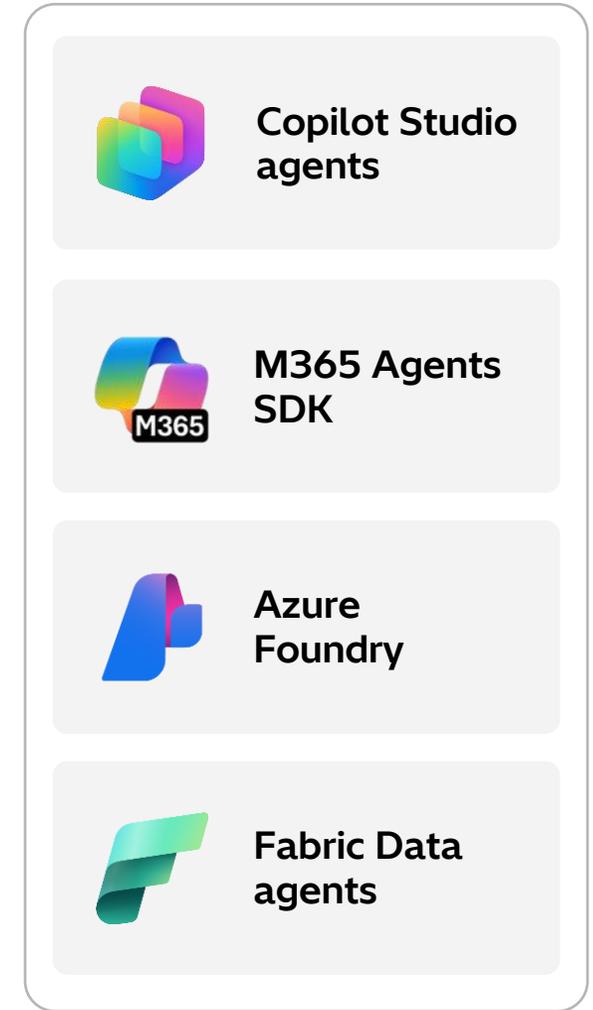


# Copilot Studio agent



HITACHI

## Connected agents



# Knowledge

Add your **public and enterprise data** sources using connectors.

Your agent will be able to **dynamically generate multi-turn answers** in real time using your enterprise data.

Allows you to create an **immediately useful agent**.

## Supported data sources include:

Public websites	SharePoint / OneDrive
Dataverse	Microsoft Fabric <i>(coming soon)</i>
File uploads	Copilot connectors
Open web search <i>(public preview)</i>	

### Add knowledge

Add knowledge so your agent can provide more relevant information and insights. Once set up, other people with edit permissions for this agent can reuse these knowledge sources for additional topics. [Learn more about knowledge sources](#)



Upload file

Drag and drop or [select to browse](#). Files can be up to 512 MB, and can't be labeled Confidential or Highly Confidential or contain passwords.

★ Featured    ⚙️ Advanced    [See suggestions](#)

Public websites

SharePoint

OneDrive

Azure AI Search

Dataverse

Dynamics 365

Salesforce

ServiceNow

Azure SQL

Cancel

33

Hitachi Solutions

©Hitachi Solutions Europe, Ltd. All rights reserved.

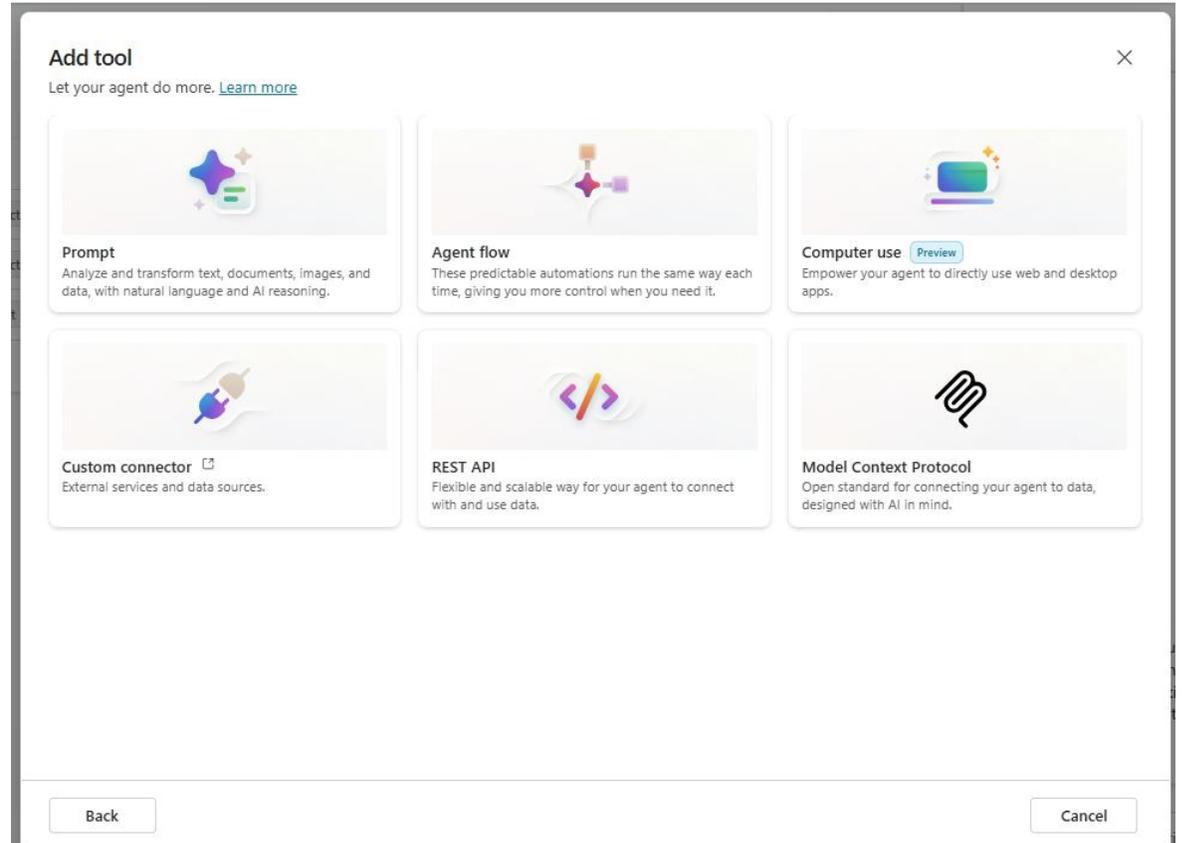
# Tools

Easily connect to your **key line of business systems**.

Enable your agent to **automate your business processes** and complete tasks.

<b>Prebuilt connectors</b>	Choose from 1500+ prebuilt Power Platform connectors to popular data sources and apps
<b>Custom connectors</b>	Create a custom connector for any publicly available API
<b>Agent flows</b>	Enhance your agents with predefined logic that executes repetitive tasks quickly
<b>Prompts</b>	Provide custom instructions to the agent model (standard or deep reasoning)
<b>Skills</b>	Add a bot built using Azure Bot Framework as a skill
<b>REST API</b>	Connect with your external systems
<b>Computer use <sup>1</sup></b>	Allow your agent to interact with websites and desktop apps
<b>Model Context Protocol</b>	Connect directly to existing knowledge servers and APIs for automatic updates to actions and knowledge
<b>Code Interpreter <sup>2</sup></b>	Enable your agent to write and run Python code to perform complex tasks
<b>Document generation <sup>3</sup></b>	Instruct your agent on how to generate a structured doc

<sup>1</sup>Frontier only | <sup>2</sup> Paid public preview | <sup>3</sup> Private preview



# Agent flows

Generally Available

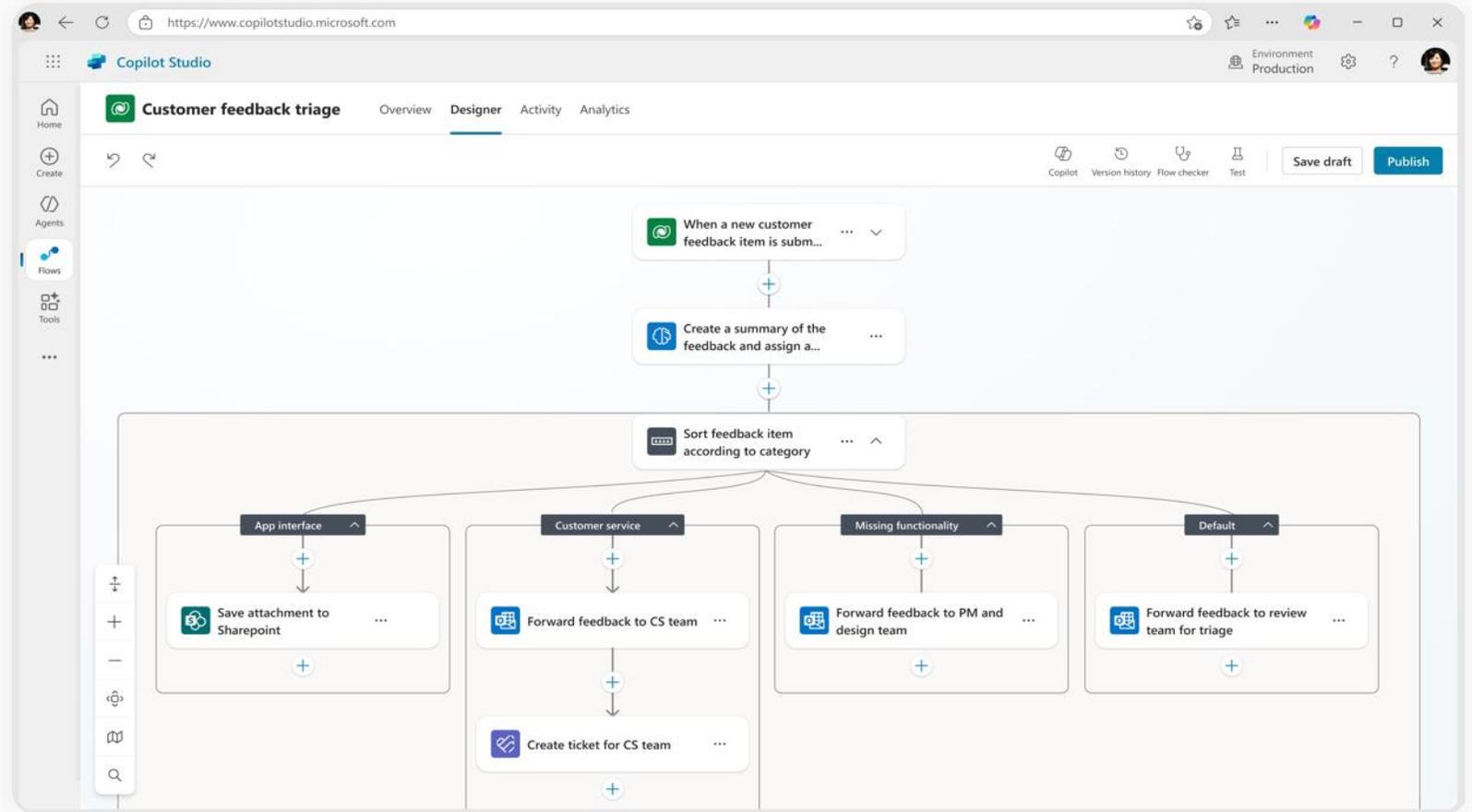
## Accelerate your agents with fixed automation pathways

Enable your agents to **accomplish objectives faster** by equipping them with fixed automation pathways that don't rely on agent reasoning and orchestration at every step.

Agent flows **execute repetitive tasks** quickly by precisely following a predefined sequence of agent flow actions.

Enhance agent flows with targeted use of **intelligent actions** for processing information, making decisions, simplifying complex steps, and more.

Leverage advanced new features such as **multi-stage and conditional approvals** to manage complex approval workflows that align with your real business processes.



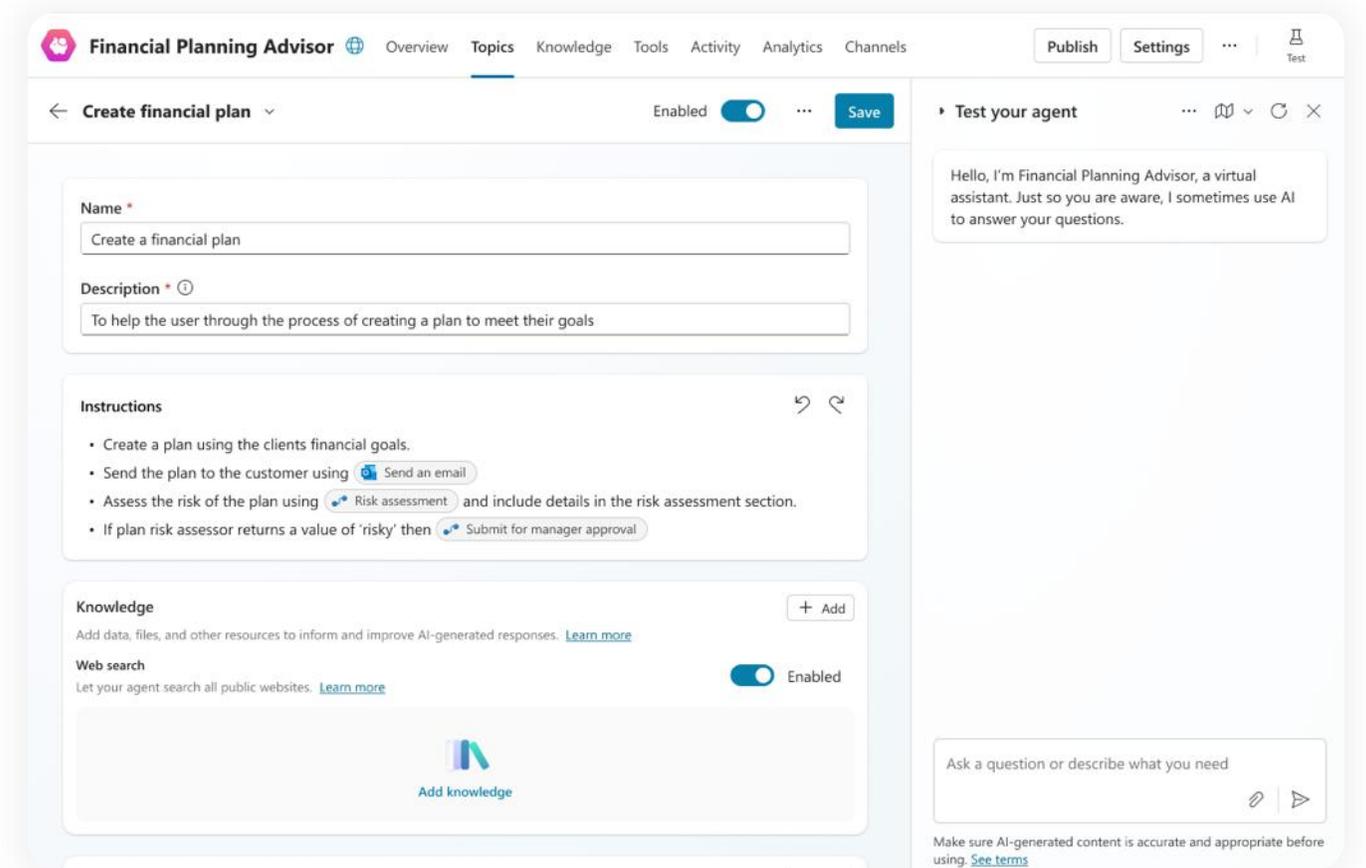
# Orchestrator

Have complete control over critical scenarios by designing specific step-by-step topics.

Provide instructions and human guard rails, adapting them as needed.

Use autonomous triggers so your agent can independently begin work and dynamically reason over its capabilities without human intervention.

Easily mix and manage both generative and custom dialog in one system.



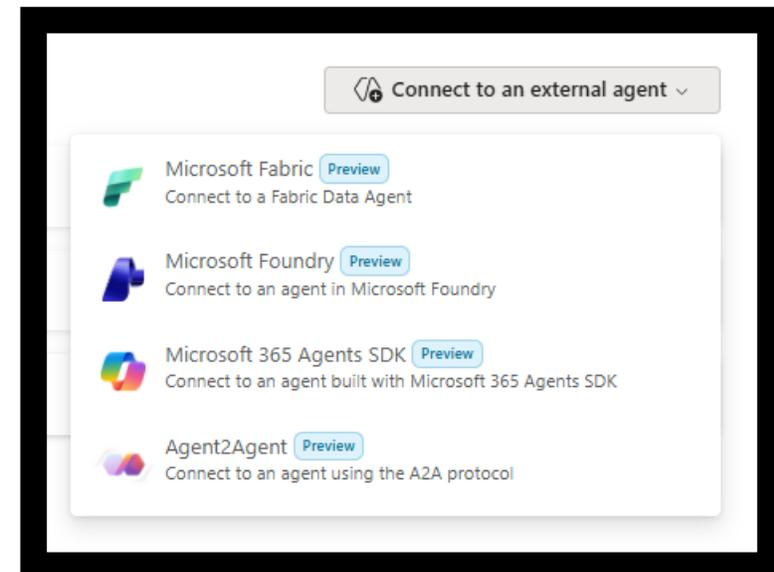
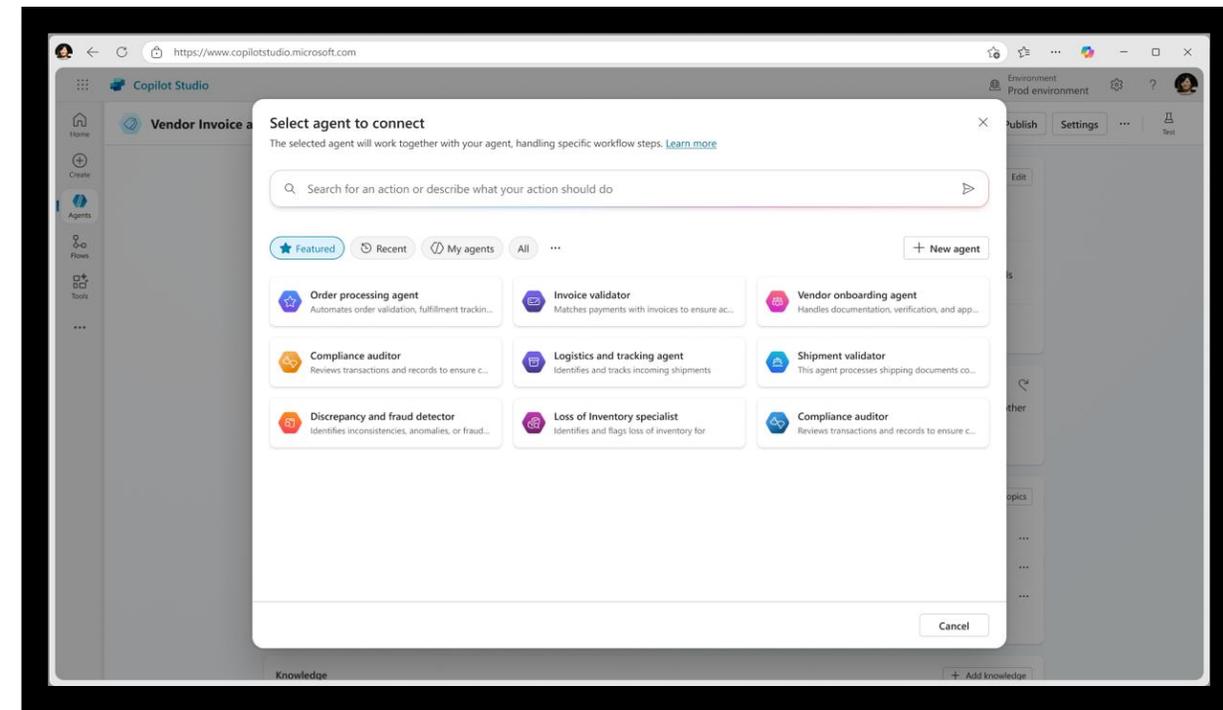
# Multi-agent orchestration

Help boost productivity by enabling your agents to connect with other agents

Agents can exchange data, collaborate on tasks, and distribute work based on their specializations

Together, agents can complete processes more effectively than a single agent.

Agents can be utilised across teams and connected to help scale business processes and solve business problems.

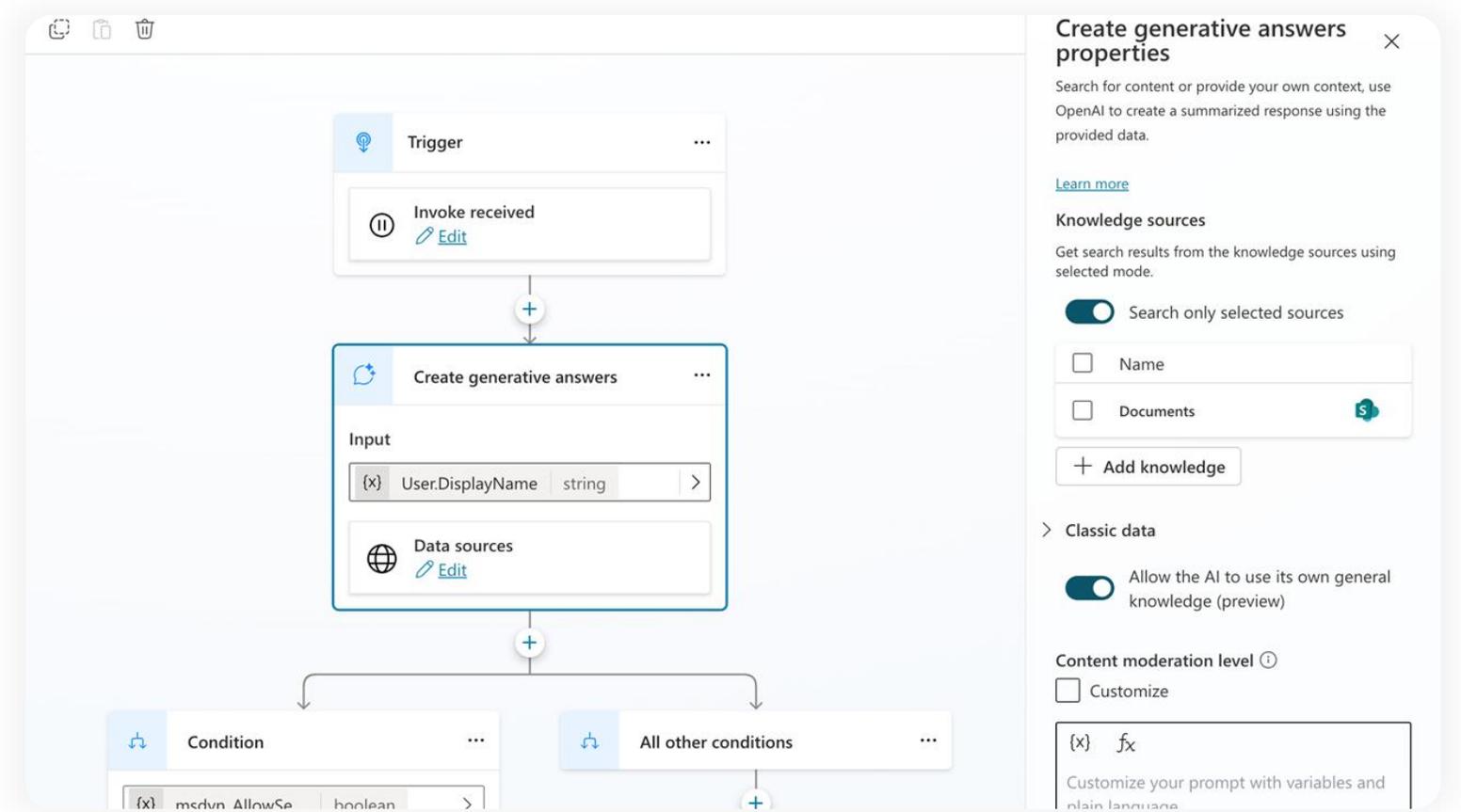


# Generative answers

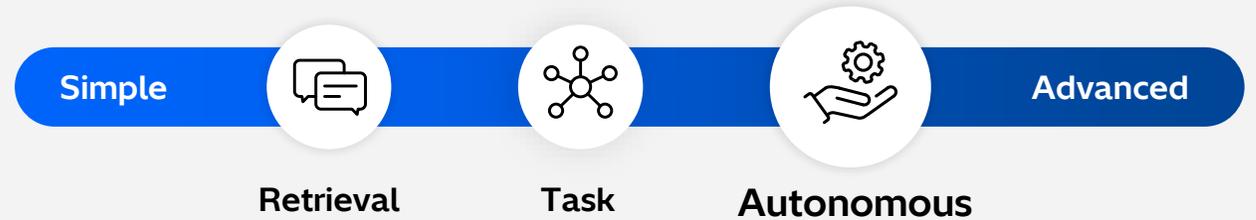
Enable multi-turn chat over your own internal and external knowledge sources and sites with generative answers.

Agents can answer thousands of questions out of the box in seconds.

You can even pull data from an API or other backend system and enable generative chat over it.



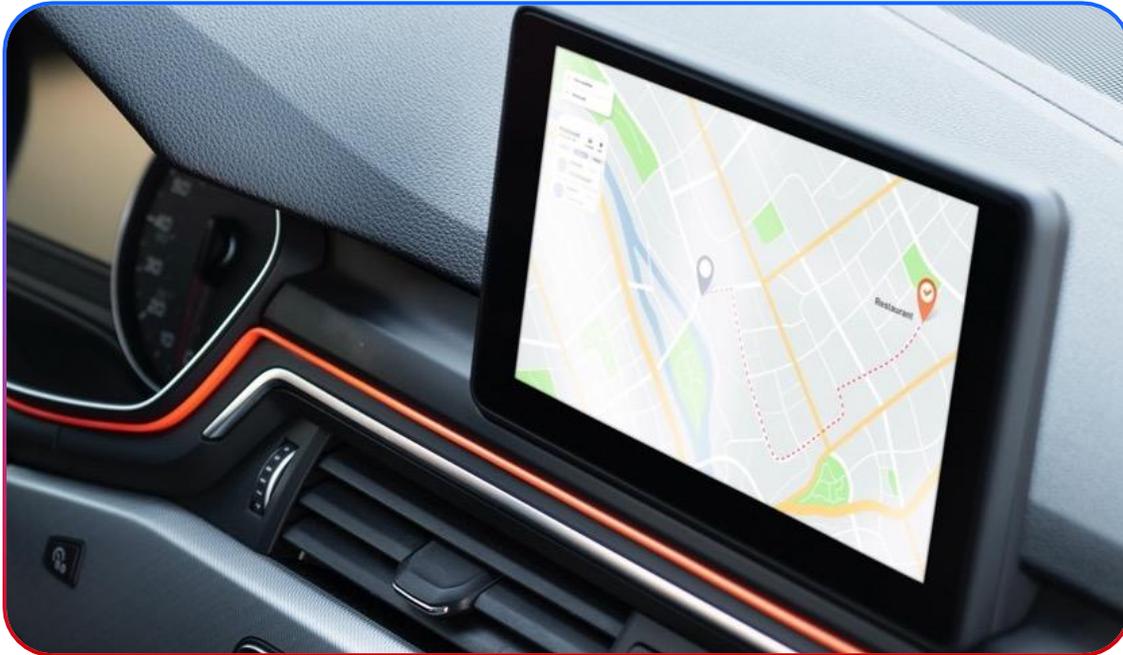
## A spectrum of agents



Expert systems that **manage and automate complex business tasks**, enhancing efficiency and innovation across your organization.

By 2028, at least **15% of day-to-day work decisions** will be made autonomously through agentic AI, up from 0% in 2024.\*

# Conversational vs Autonomous Agents



## Conversational Agents are like using GPS

You tell it where you want to go and navigate accordingly.  
You need to keep interacting with it to make it useful.



## Autonomous Agents are like using a self driving car

Once it knows the destination, it makes decisions independently – no input needed.

# Change the way you work with autonomous agents



## Agility

### Modernize automation

---

Optimize existing business processes with agents that can improve legacy technology.



## Efficiency

### Innovate with new processes

---

Unlock untapped business value by connecting across data silos to automate new problems.



## Scalability

### Empower everyone with agents

---

Enable end users in every function and department to address their individual business problems.

# Planning integrations

Provide an overview of all integrations with other systems/expected volumes

## Example answers:

Connected system	Called by	Called with	Expected daily volume	Expected peak	Details / purpose
ServiceNow	Service Desk KB topic	Agent flow	5,000	1,000	The user query is used as an input to run a query on ServiceNow knowledge base using the standard connector. A JSON of results is returned to Copilot Studio for generative actions custom data.
Contoso website	Conversational Boosting topic	Generative answers	1,000	100	<a href="https://contoso.com/en-us/FAQ">https://contoso.com/en-us/FAQ</a> with /en-us/ being dynamically set based on the user locale variable.
Internal Directory API	Conversation Start topic	Agent flow	15,000	5,000	Use of the on-premises data gateway to connect to an internal API.
Weather API	Weather topic	HTTP	500	100	GET request to a REST-based API
Teams	Meeting Booking topic	Action	1,500	300	Create a Teams meeting based on conversation inputs.
Bot Framework Skill	Travel topic	Skills	2,000	400	Leveraging existing Bot Framework Skill to book travels.
SAP	Every 24h	Agent flow	20,000	-	Daily batch synchronization of the product catalogue from SAP to Dataverse.

# Prompt Engineering

HITACHI

Instructions are how we program our agent and provide it with a mission.



# Building blocks of writing agent instructions



## Role

What's the purpose of the agent?

"You are a customer service agent for an online shoe store. Your goal is to assist customers with product recommendations and order issues."



## Scope

What should it do? What should it avoid?

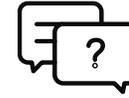
"You can provide product details and troubleshoot common issues, but do not handle refund requests."



## Context

What does the agent need to know?

- Use our product catalog
- Reference our FAQ doc
- If return is needed, submit an item in our return system and notify the sales team



## Tone

How should the agent respond?

"Be friendly, concise, and professional. Use casual language when assisting customers."



## Error Handling

What does it do if it's unsure?

"If you are unsure of an answer, provide helpful alternatives or escalate to a human agent."

# Guiding Generative Behaviour in Copilot Studio

Only respond to requests to provide information about educational, legal, wellness, wellbeing, health, dental care, and newborn benefits for employees and dependents.  
Respond to benefit types with details, health plan comparisons available for employees and dependents in tabular format.  
Answer in bold and underline fonts as necessary.

## Constraints

Use the FAQ documents only if the question is not relevant to Hours, Appointments, or Billing.  
Only use the ticket creation topic for creating tickets.  
For other requests related to fixing issues, use the troubleshooting topic.

## Tools and knowledge to call

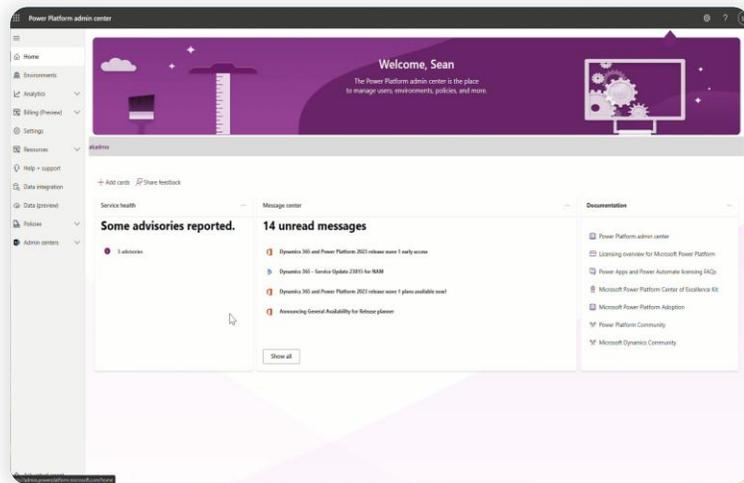
Search only within specific country folders relevant to the employee's country.

## Guidance

Only respond to messages that are relevant to Contoso corporation and ordering coffee.  
Otherwise, tell the user you can't help with their inquiry..

## Help the agent generate a response

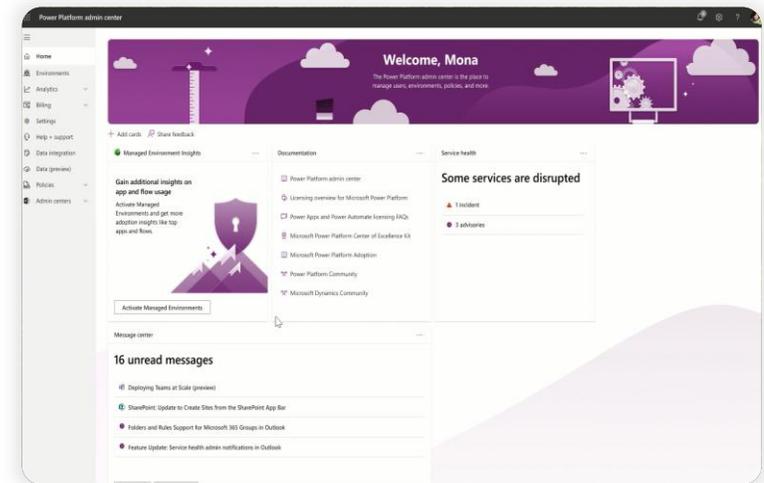
## Power Platform Admin Center



### Standard governance offering:

- Build guardrails around data, apps, and environments
- View analytics on low code assets across your organization

## Managed Environments for Power Platform



### Premium governance offering:

- Enable governance-at-scale without additional IT resources
- Proactively build and enforce best practices while gaining key insights and analytics

# Coffee Break

11:15 - 11:30

HITACHI

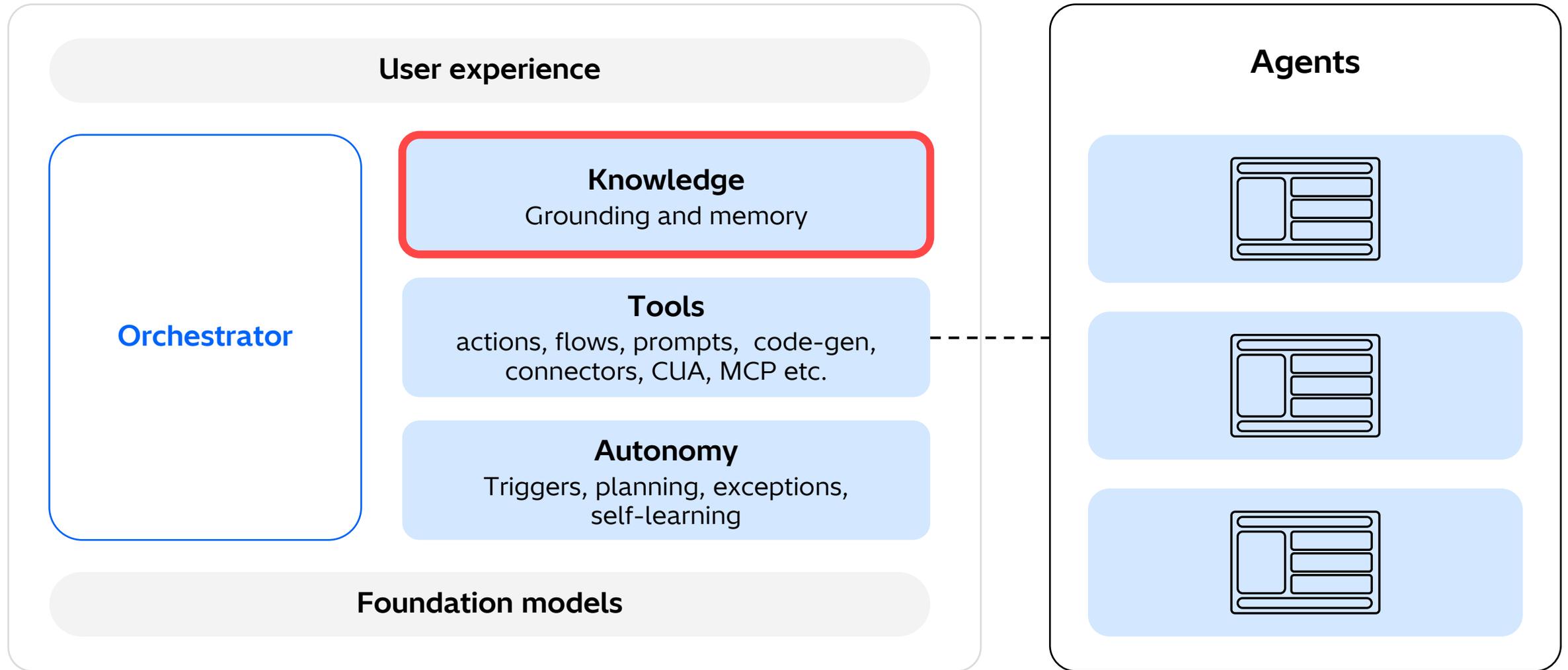
15 Min

# Lab Session 1: Building Conversational Agents in Copilot Studio

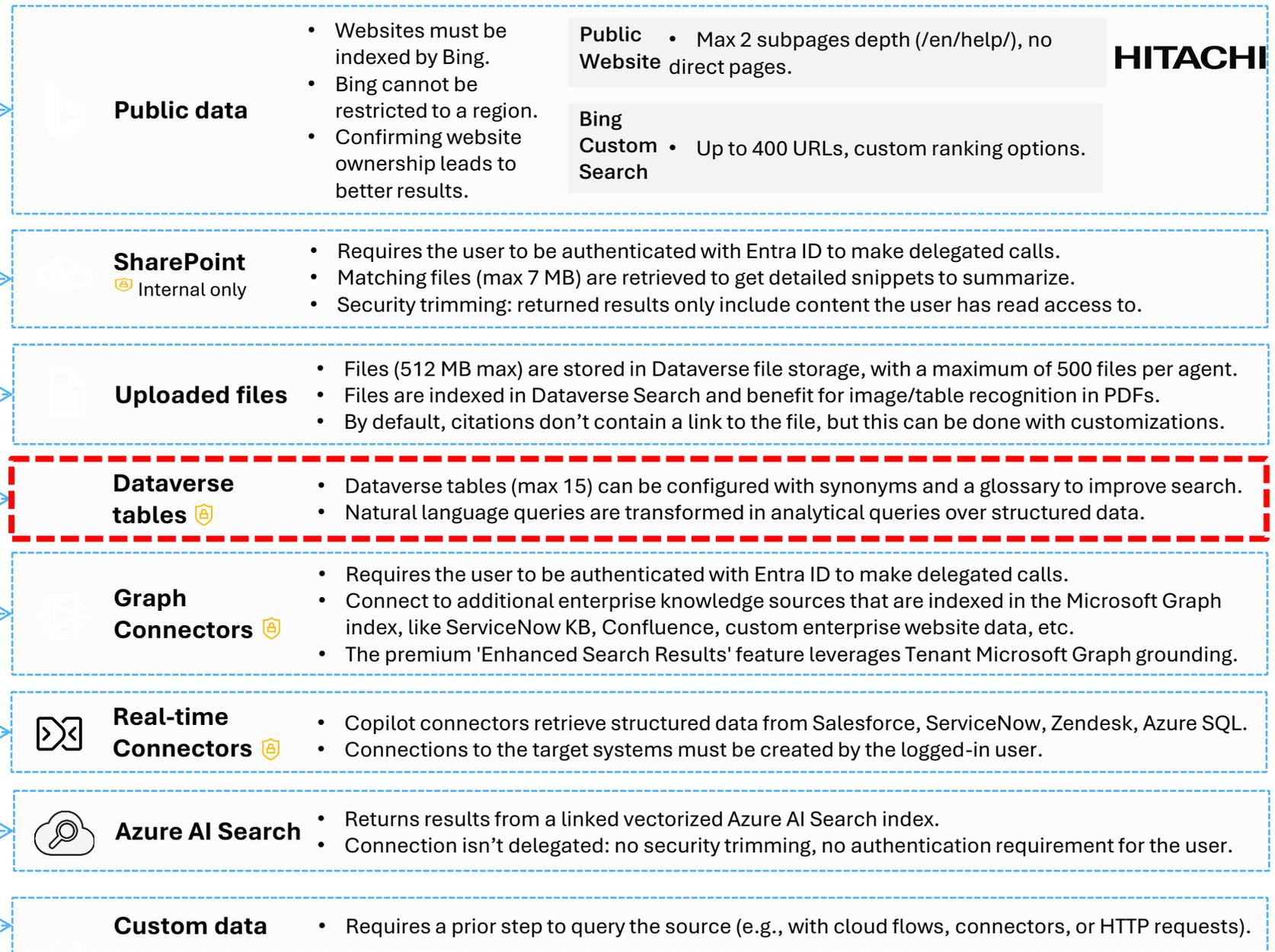
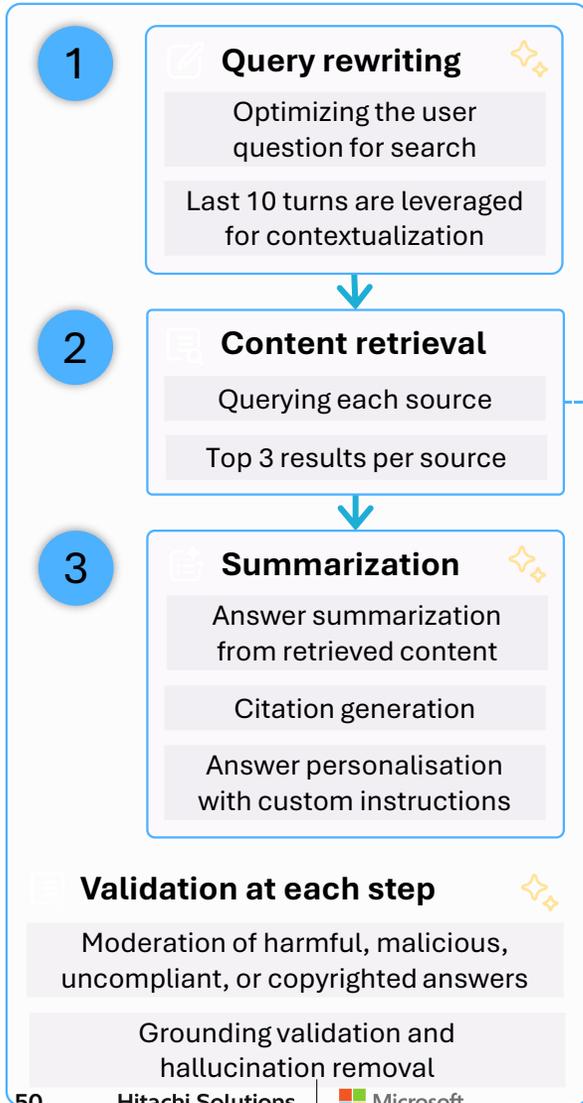
11:30 - 12:15

45 Min

# Key Agent Components



# Knowledge sources & Generative AI



**HITACHI**

# Introducing Contoso Coffee

HITACHI



Welcome to Contoso Coffee! At Contoso Coffee, we are passionate about providing efficient, environmentally sustainable, and innovative coffee products, barista experiences, and services.



Customer support costs have continued to rise as the customer base has grown, and the company can no longer continue to expand the Customer Support team. You have been tasked with finding a solution using Copilot Studio.

# Lab Session 1: Building Conversational Agents in Copilot Studio

11:30 - 12:15

<https://bit.ly/4k6lyJ4>



[Build a conversational agent in Copilot Studio - Online workshop - Training | Microsoft Learn](#)

45 Min

<https://aka.ms/AgIADStudentFiles>

# Lunch

12:15 - 13:15

HITACHI

60 Mins

# Environment Agency and Hitachi: Responding to ministerial priorities through AI-enabled transformation



**Amy Matrai**

Senior Delivery Manager  
**Hitachi Solutions**



**Sam Bartlett**

Data and AI Lead  
**Environment Agency**



**Phil Wiltshire**

Lead Solution Architect  
**Defra**

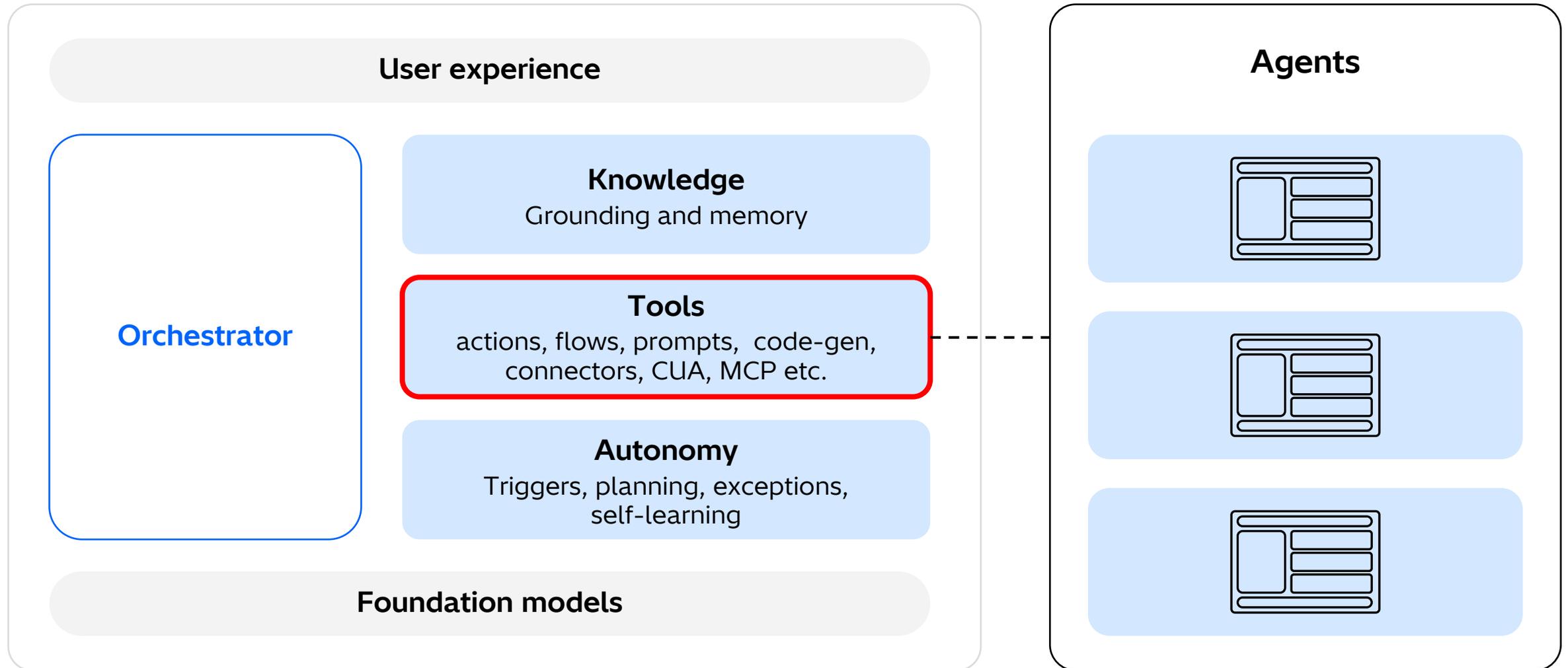
45 Mins

# Lab Session 2: Enhancing Agents with Tools and Knowledge

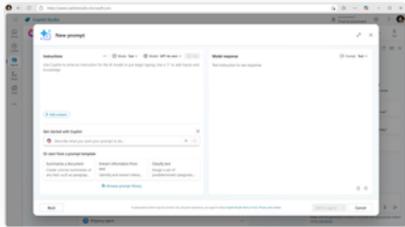
14:00 - 15:00

60 mins

# Key Agent Components



# Popular agent tools



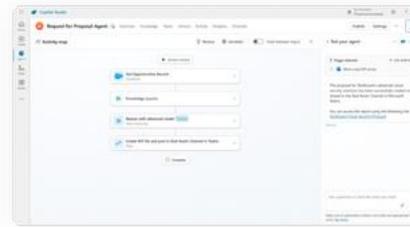
## Prompts

Provide structured instructions to guide the LLM to perform specific tasks.



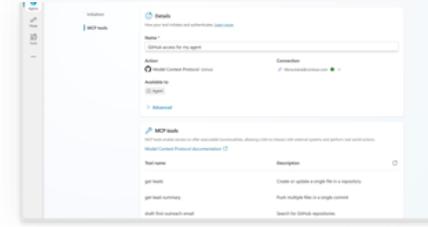
## Connectors

Choose from 1500+ prebuilt Power Platform connectors to popular data sources and apps or create a custom connector for any publicly available API.



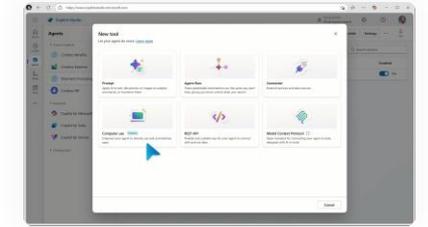
## Deep reasoning

Instruct agents to perform complex reasoning tasks.



## Model Context Protocol

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



## Computer Use<sup>1</sup>

Enable your agents to interact with websites and desktop apps.



## Code interpreter<sup>2</sup>

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



## Agent flows

Enhance your agents with predefined logic that executes repetitive tasks quickly

## Skills

Add a bot built using Azure Bot Framework as a skill

## REST API

Connect with your external systems

## Document generation<sup>3</sup>

Instruct your agent on how to generate a structured doc

<sup>1</sup> Frontier only | <sup>2</sup> Paid public preview | <sup>3</sup> Private preview

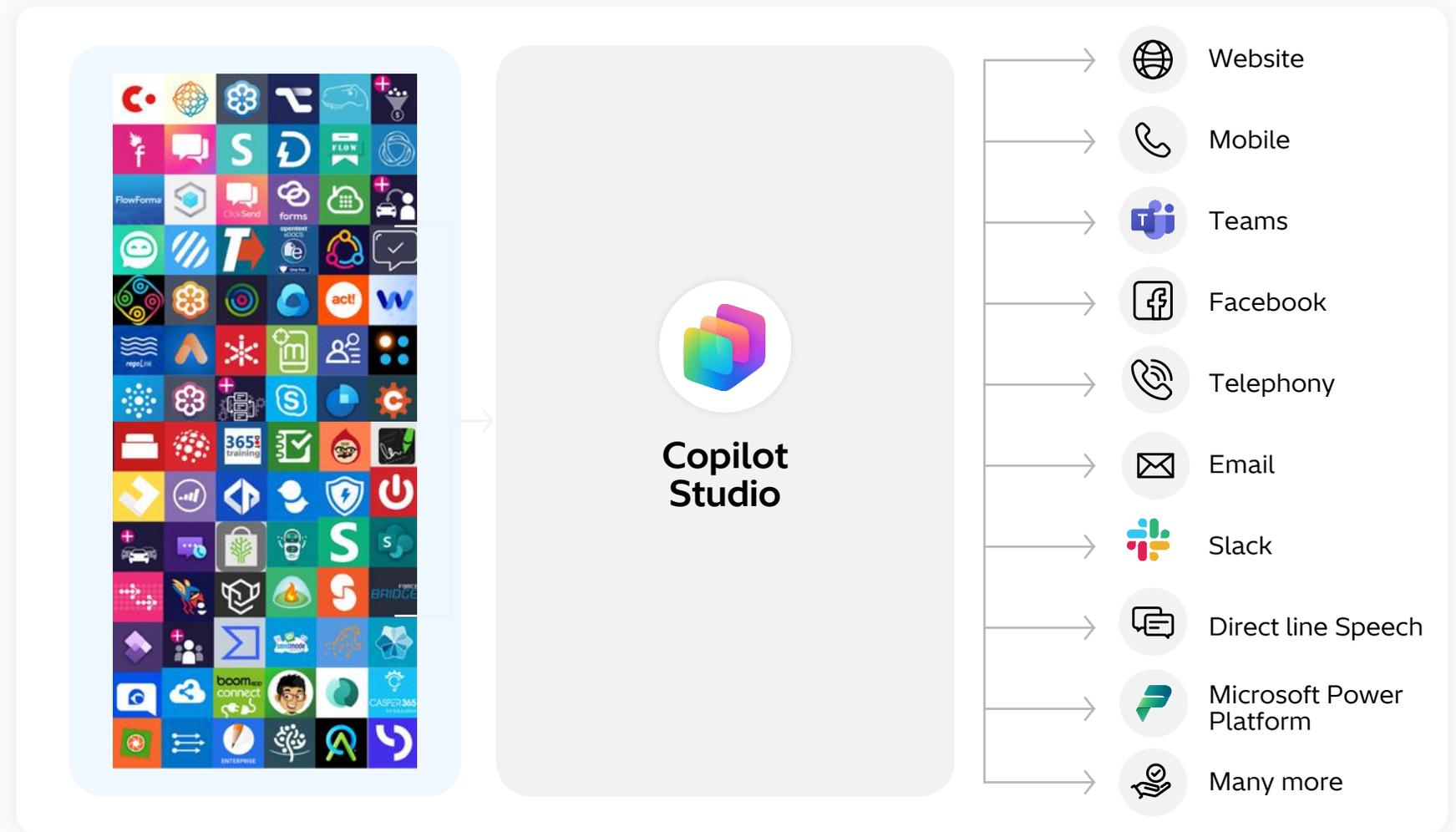
# Agent flows and connectors

Use agent flows to build, edit, and extend automation with 1,500+ pre-built connectors or custom APIs.

For a smooth user experience, agent flows triggered with your agent to execute quickly to minimize delays in response times.

Agent flows from Copilot Studio have a 100-second limit to return results before timing out.

Make HTTP requests directly from Copilot Studio to bypass agent flows and enhance efficiency.



1500+ prebuilt data connectors

# Lab Session 2: Enhancing Agents with Tools and Knowledge

14:00 - 15:00

<https://bit.ly/3YZUuBz>

45 Min



Use tools in Copilot Studio -  
Online workshop - Training |  
Microsoft Learn

# Coffee Break

15:00 - 15:15

HITACHI

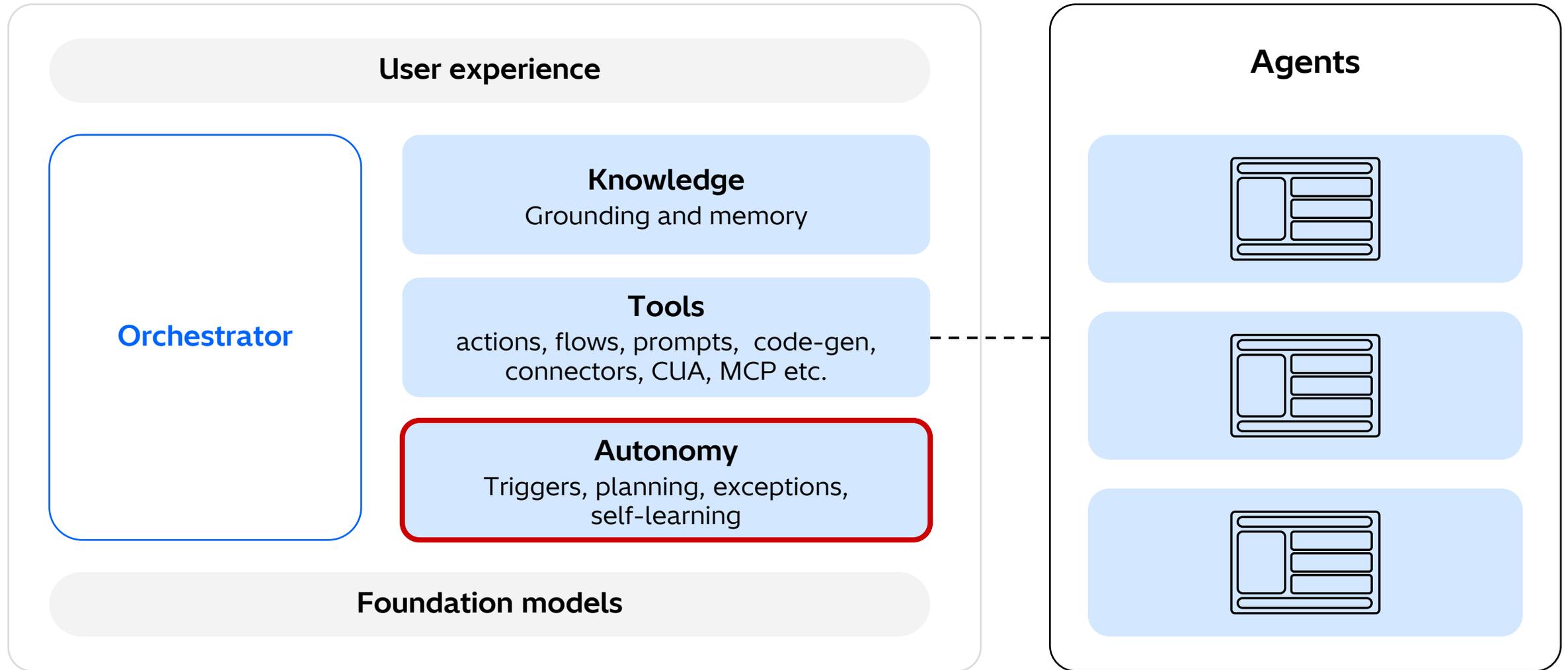
15 Min

# Lab Session 3: Expanding to Autonomous Agents and advanced behaviours in Copilot Studio

15:15 - 16:00

45 Min

# Key Agent Components



# Autonomous agents

Handle variability and complexity at infinite scale

Generally Available

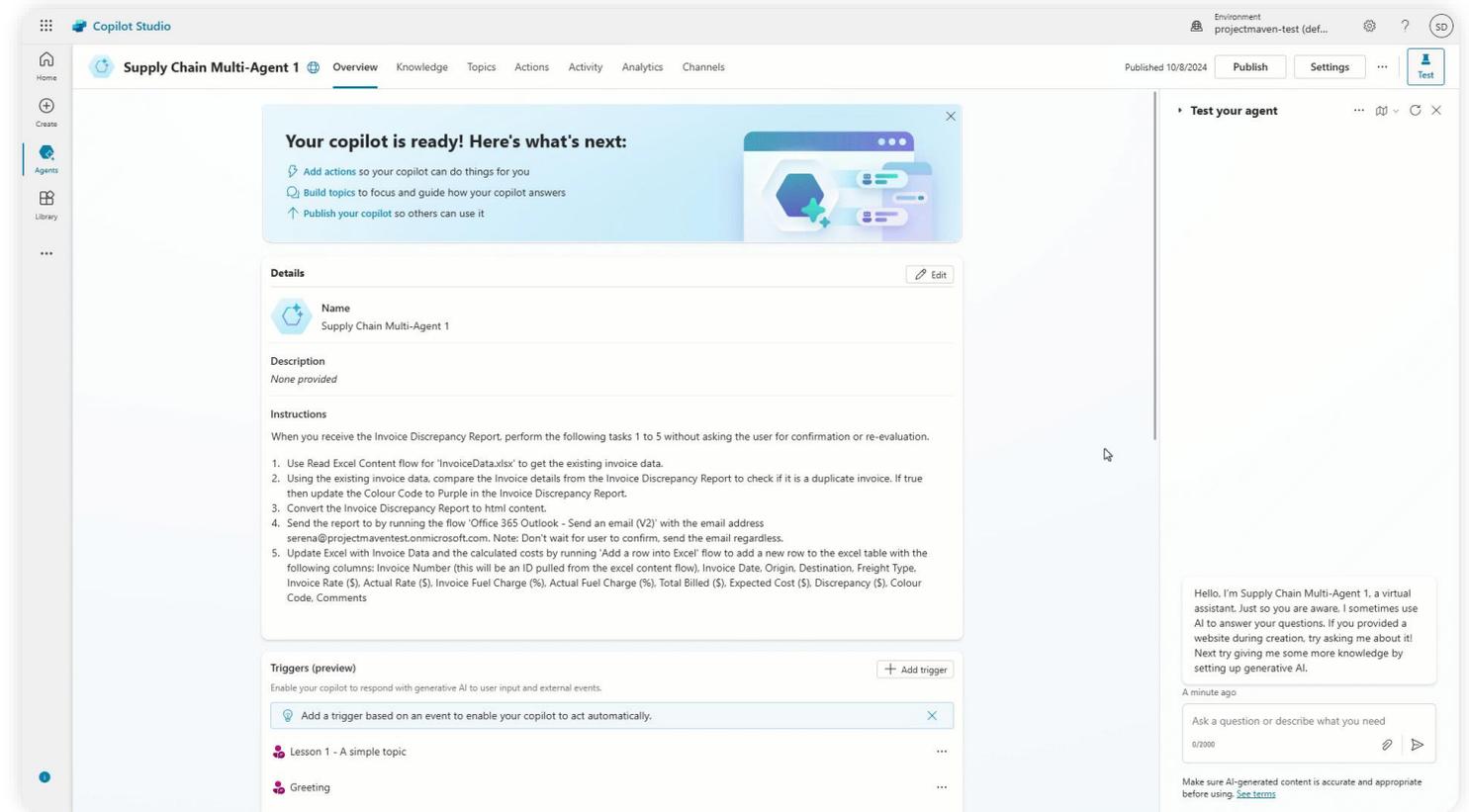
Independently begins work based on autonomous triggers.

Automates long running processes.

Dynamically reasons over its capabilities.

Follows human guard rails and asks for help.

Orchestrate other agents.



# Model Context Protocol

Simplify integration with AI

**HITACHI**

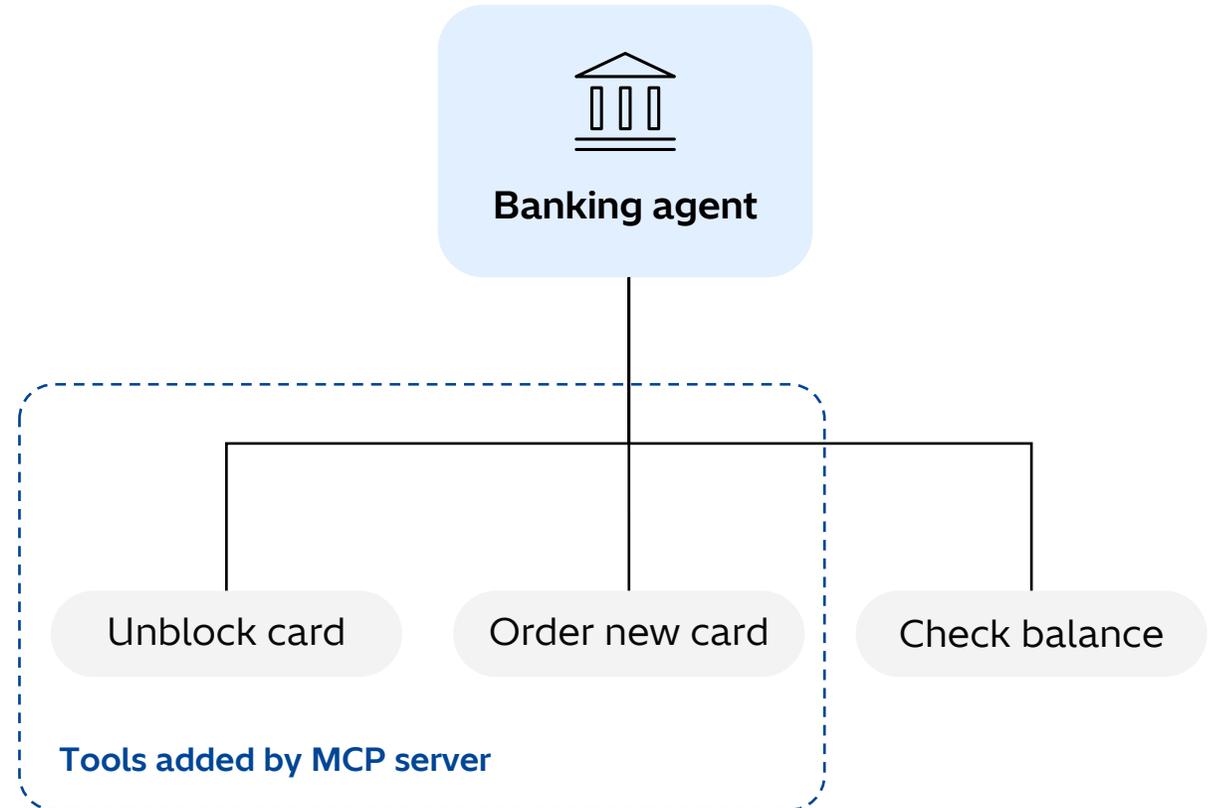
Generally Available

**MCP Support, a standardised way to connect agents to your data and tools, is now Generally Available in Copilot Studio. It's like a USB-C port for your agents.**

Connect your agents to MCP-enabled connectors, unlocking the latest actions and knowledge made available.

Apply enterprise security and controls to your connectors including data loss prevention, authentication, and virtual networks.

Access a marketplace of servers from the growing library of pre-built, MCP-enabled connectors showing list of tools available for your agents to use.



# Built-in MCP servers in Copilot Studio

## ❑ Dynamics 365

- Sales
- Finance
- Supply Chain
- Service
- Enterprise Resource Planning (ERP)
- Contact Center

## Microsoft MCP Servers

- Microsoft Outlook Mail MCP
- Microsoft 365 User Profile MCP
- Microsoft Outlook Calendar MCP
- Microsoft Teams MCP
- Microsoft SharePoint and OneDrive MCP
- Microsoft SharePoint Lists MCP
- Microsoft 365 Admin Center MCP
- Microsoft Word MCP
- Microsoft 365 Copilot (Search) MCP

## ❑ Fabric

- ❑ Office 365 Outlook
- ❑ GitHub
- ❑ Learn docs MCP

The screenshot shows the 'Add tool' interface in Copilot Studio. At the top, it says 'Add tool' and 'Let your agent do more. [Learn more](#)'. Below this, there are several filter tabs: 'All', 'Connector', 'Prompt', 'Flow', 'REST API', and 'Model Context Protocol' (which is currently selected). A '+ New tool' button is in the top right. The main area displays a grid of MCP server cards, each with an icon and text. The cards include: Azure Databricks Genie, Bigdata.com MCP endpoint, Box MCP Server, CData Connect AI, Celonis MCP Server, Contact Management MCP S..., D365 Sales MCP Server, D365 Service MCP Server, Databricks Genie, Dataverse MCP Server, DocuSign MCP Server, Draup MCP Server, Dynamics 365 Business Cent..., Dynamics 365 Contact Cente..., Dynamics 365 Conversation ..., Dynamics 365 ERP Analytics MC..., Dynamics 365 ERP MCP, Dynamics 365 ERP MCP (Pre..., Dynamics 365 Sales MCP (Pr..., Email Management MCP Server, Enlyft MCP, Environment Management ..., Geni Actions for fetching an..., Github MCP Server, Intelix IOC Analysis, Jira MCP Server, Kusto Query MCP Server, and MCP server for Salesforce. At the bottom, there is a feedback prompt: 'How is your experience with adding tools?' with thumbs up/down icons, and a note: 'Suggestions and search will include AI-generated results. [See terms](#)' with a 'Cancel' button.

# Reinvent business processes

Autonomous agents use advanced logic to pick the best actions and knowledge available and adapt to changing criteria at run time.

## Traditional agents

Runs 1-5

## Autonomous agents

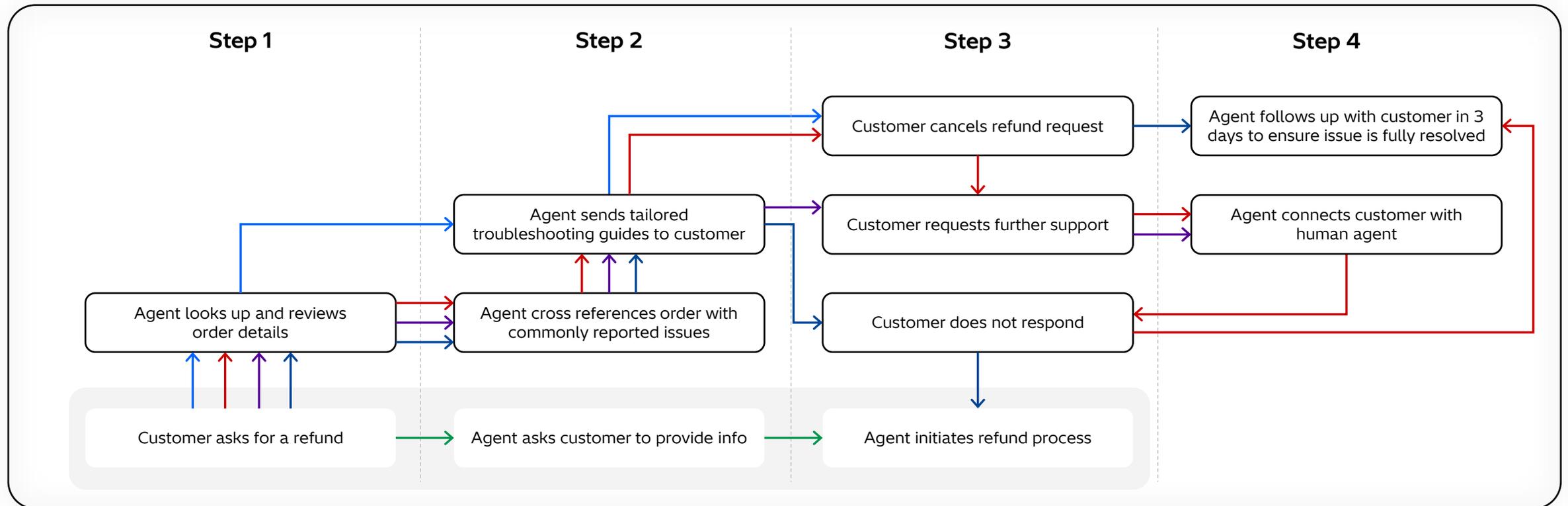
Run 1

Run 2

Run 3

Run 4

Run 5



# Lab Session 3: Expanding to Autonomous Agents and advanced behaviours in Copilot Studio

15:15 - 16:00

<https://bit.ly/4kd8kdC>

45 Min



Make your agent autonomous in  
Copilot Studio - Online workshop -  
Training | Microsoft Learn

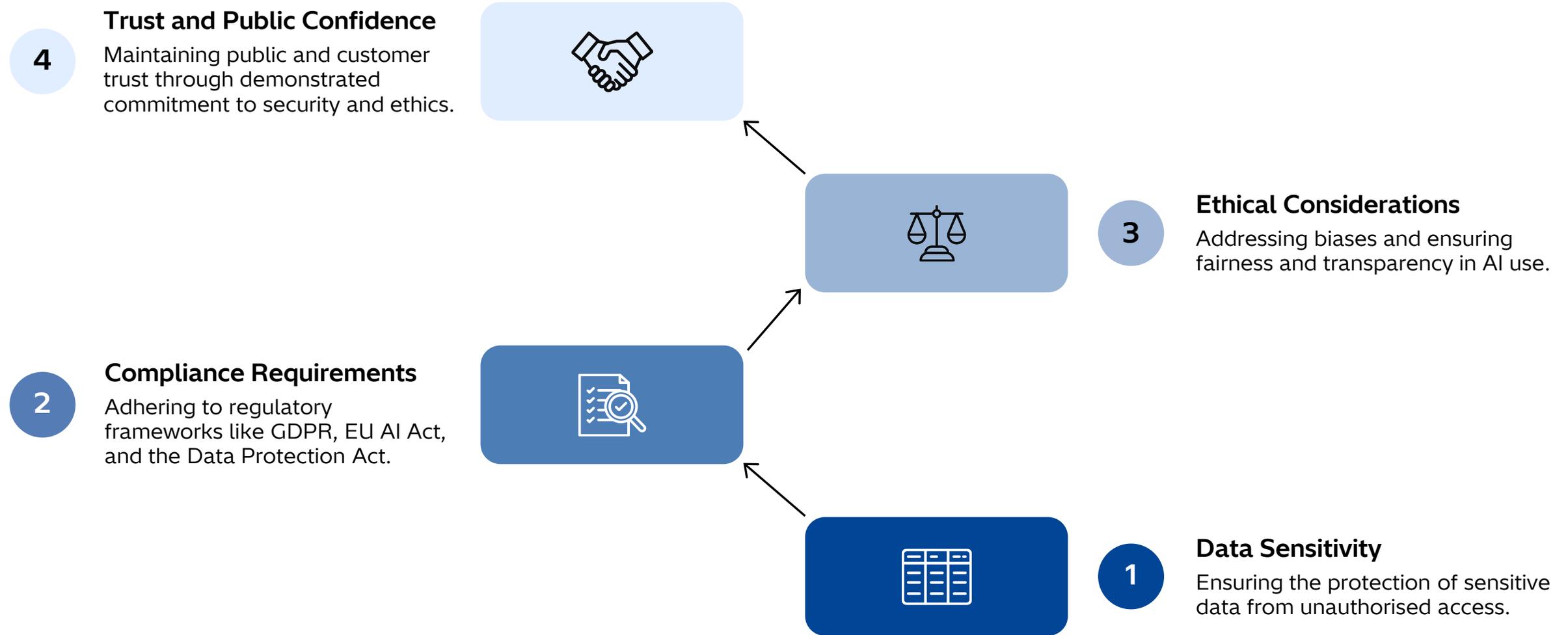
# Managing Security and Governance in the Agentic era

16:00 – 16:30

HITACHI

30 Min

# Why does AI security and privacy matter?



# Can I rely on Copilot in a high security setting?

## Copilot Security Foundations

**Built-In Compliance and Privacy**

 Respects sensitivity labels & sharing

 Complies with major industry standards and regulations including GDPR, HIPAA, FedRAMP

**Copilot Only Uses What You Can See**

 Can only access files and content you already have

 Access to MS Graph for context\*

 Prompts and responses are protected

**Your Identity and Data Are Protected**

 Sign-in with your work account

 Security rules like the rest of Microsoft 365

 Data remains in the Microsoft Cloud

**Data never leaves tenant or used to train models**

\* Available on the paid version only

# How is information kept secure in Copilot?



## Security and Governance Controls

- Data Security and Zero Trust
- Sensitivity and Data Loss Prevention (DLP)
- AI Security Safeguards
- Compliance and Privacy



## Management Controls

- Access governance
- Agent Lifecycle Management
- Policy Enforcement
- Environment Readiness

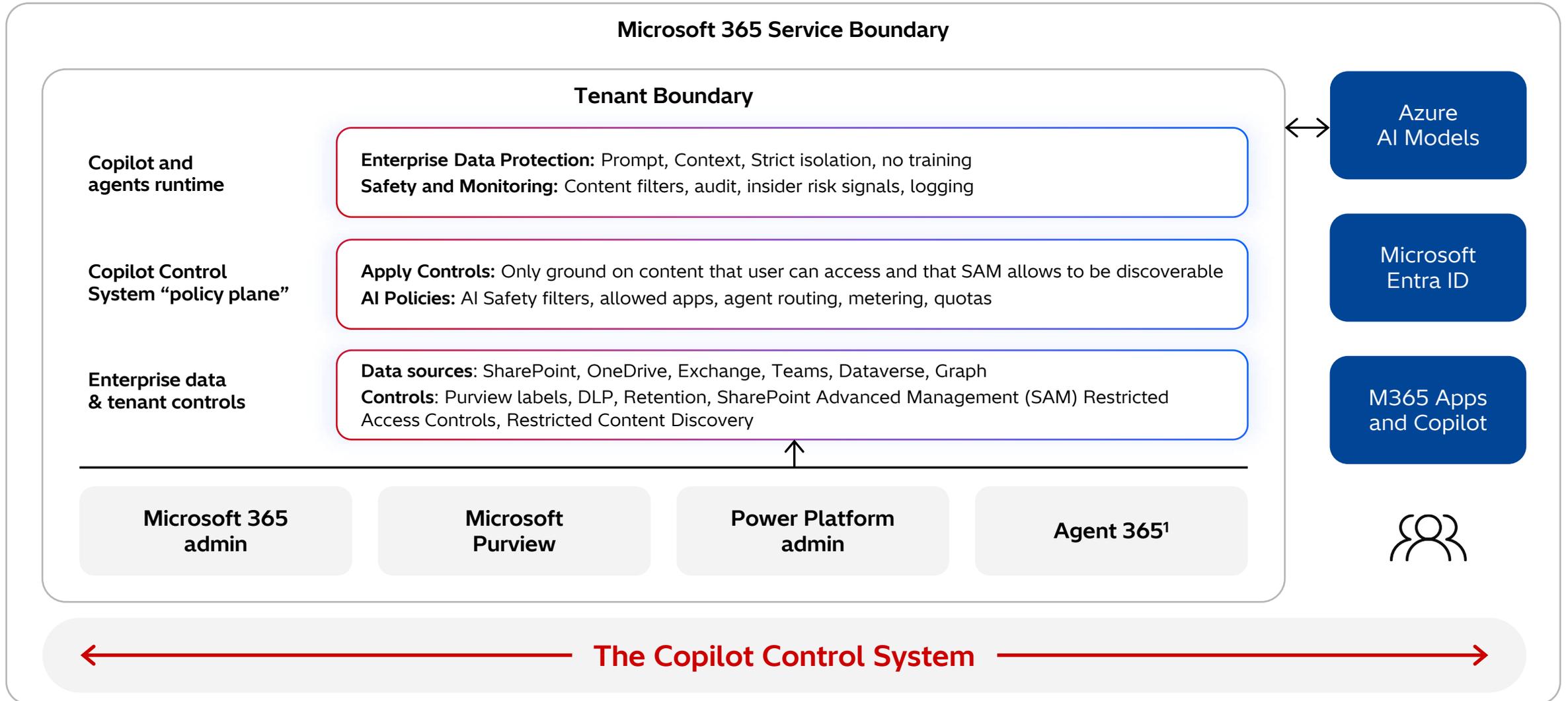


## Measurement and Reporting

- Readiness and Adoption
- Productivity Impact
- Business Value and Return on Investment (ROI)
- Risk and Compliance Reports

← The Copilot Control System →

# What Security Controls are available to help?



<sup>1</sup>Agent 365 currently in preview in Microsoft Frontier program

# Data Security - Know your Data Before you Deploy

What does Purview Data Security Posture Management (DSPM) do?

## Data Security

**Discover Sensitive Data:** Where sensitive data sits before Copilot starts surfacing it.

**Identify oversharing risk:** Generate oversharing reports to find files or sites with excessive access.

**Classify and label** content so Copilot respects OFFICIAL/OFFICIAL-SENSITIVE style boundaries and applies access controls.

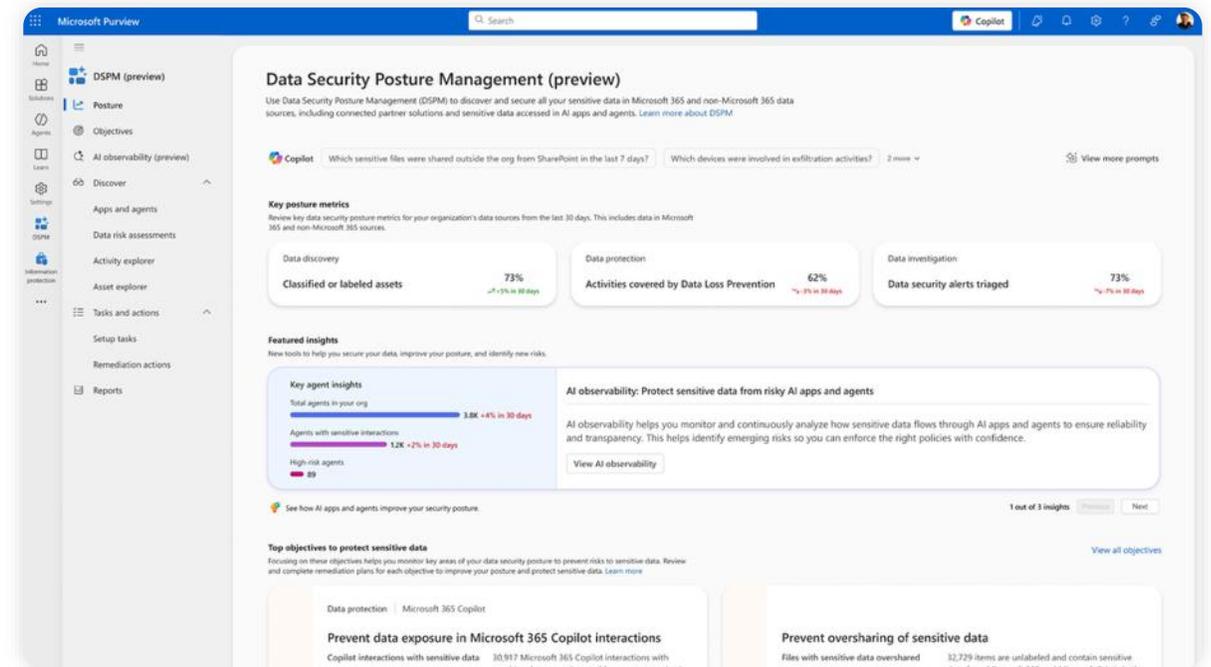
Data Privacy

Observability

Compliance

### Audience questions

- How does DSPM actually help me reduce risk before I enable Copilot?



Discover



Classify & Label



Protect

# Data Privacy – Prevent Oversharing and Data Leaks

## Sensitivity Labels and Data Loss Prevention Policies (DLP)

### Data Security

#### Data Privacy

Copilot respects your organisation's data boundaries - **but only if they're defined.**

Use Purview sensitivity labels to classify content (e.g. 'OFFICIAL', 'HR Only').

Apply DLP policies to

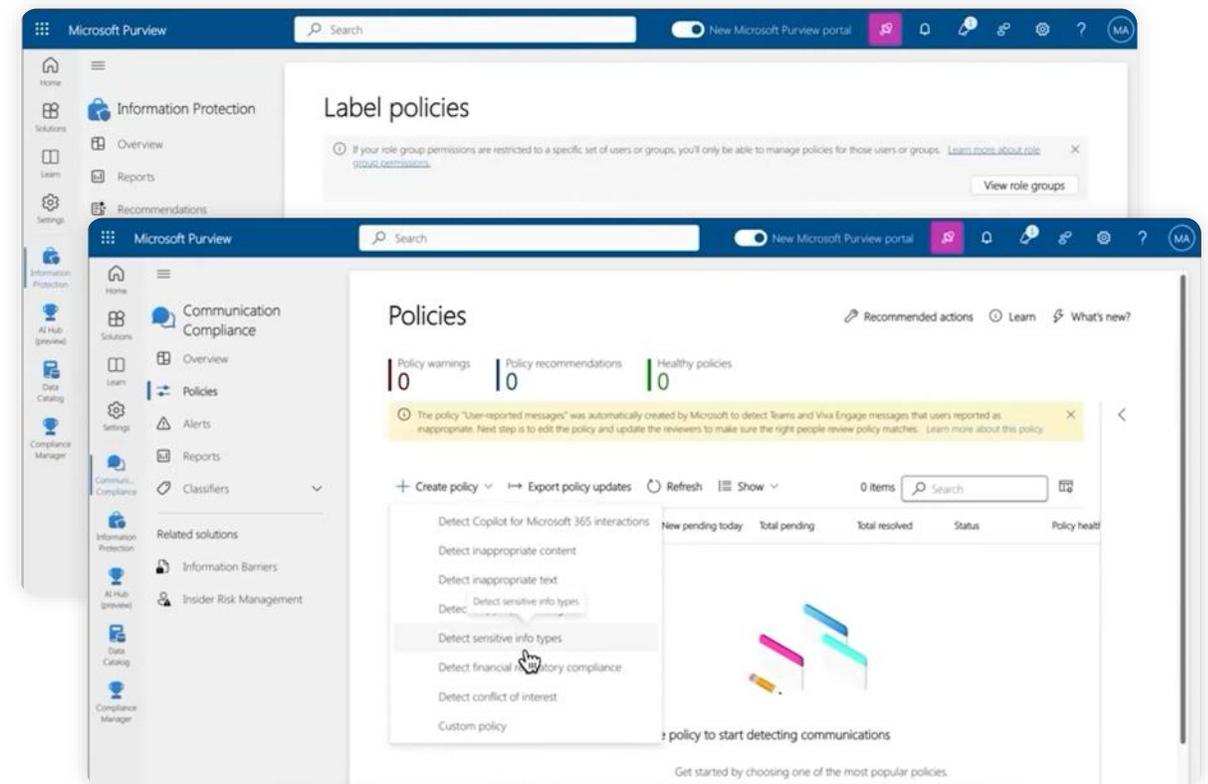
- Warn or block risky sharing
- Prevent Copilot from summarising sensitive content
- Detect and remediate oversharing

### Observability

### Compliance

#### Audience questions

- How do we make sure Copilot doesn't expose confidential or sensitive information to the wrong people?



# Observability – Monitor and Audit Copilot Activity

How do understand how Copilot and AI are being used, to mitigate risk and build trust?

Data Security

Data Privacy

## Observability

Copilot interactions are fully auditable — every prompt and response is logged

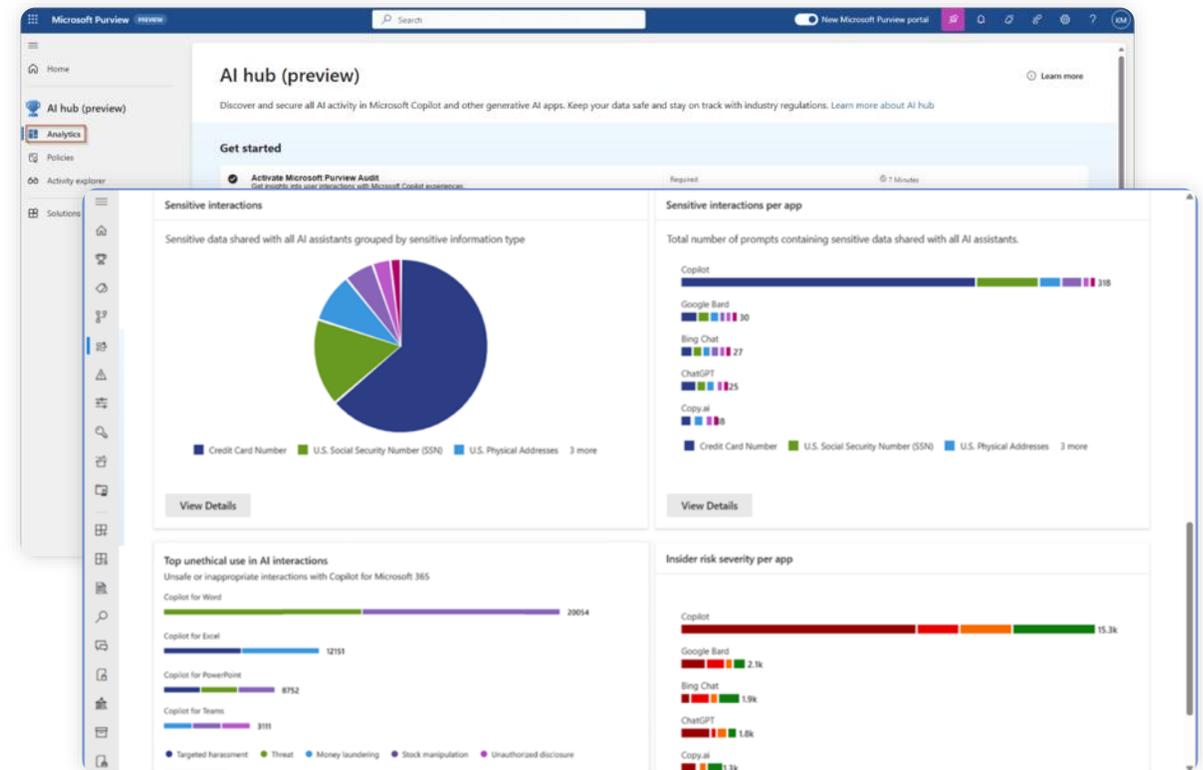
Microsoft Purview provides

- Audit logs for every Copilot interaction
- Alerts for risky behaviour (e.g. mass exports, sensitive prompts)
- Insider Risk Management and AI Hub for visibility into usage trends

Compliance

### Audience questions

- Can we see what users are asking Copilot and what responses they get?
- Can we block users or take action directly from AI Hub?



# What are the steps to securely implement Copilot?

What is our roadmap to Microsoft 365 Copilot adoption?

## Audience questions

- How long does it take to get Copilot ready for production?
- *Do we need E5 licensing for all these features?*

1

### Get the foundations right

- Enable **Purview Audit** logging
- Define a few core **sensitivity labels**
- Implement **basic DLP** rules
- Use **Conditional Access & MFA** to secure Copilot access

2

### Configure Purview guardrails specifically for Copilot

- Create AI-aware DLP policies
- Leverage sensitivity labels in prompts and outputs
- Configure retention and audit for Copilot interactions

3

### Monitor, investigate, and respond to AI risk

- Use activity explorer and audit to watch AI usage
- Enable Insider Risk Management for AI
- Investigate incidents and fulfil legal / FOI duties

4

### Tie it back to UK government AI/ M365 guidance

- Baseline DLP and labels on Secure Configuration Blueprint
- Map Purview controls to the UK Government AI Playbook themes
- Document decisions with business owner sign off

Foundational



Optimised

1

## Data and Compliance

Ensure agents use data safely, legally and appropriately

- ❑ Define approved data sources and connectors
- ❑ Enforce data residency, privacy and retention policies
- ❑ Prevent exposure of sensitive or restricted data

2

## Access & Security

Control who can build, deploy, and run agents

- ❑ Role-based access control for makers and admins
- ❑ Least-privilege permissions for agent actions
- ❑ Managed identities and secure authentication

3

## Responsible AI & Guardrails

Shape and constrain generative behaviour

- ❑ Clear instructions and system prompts
- ❑ Input/output filtering and content boundaries
- ❑ Disclosure that users are interacting with AI

4

## Oversight & Monitoring

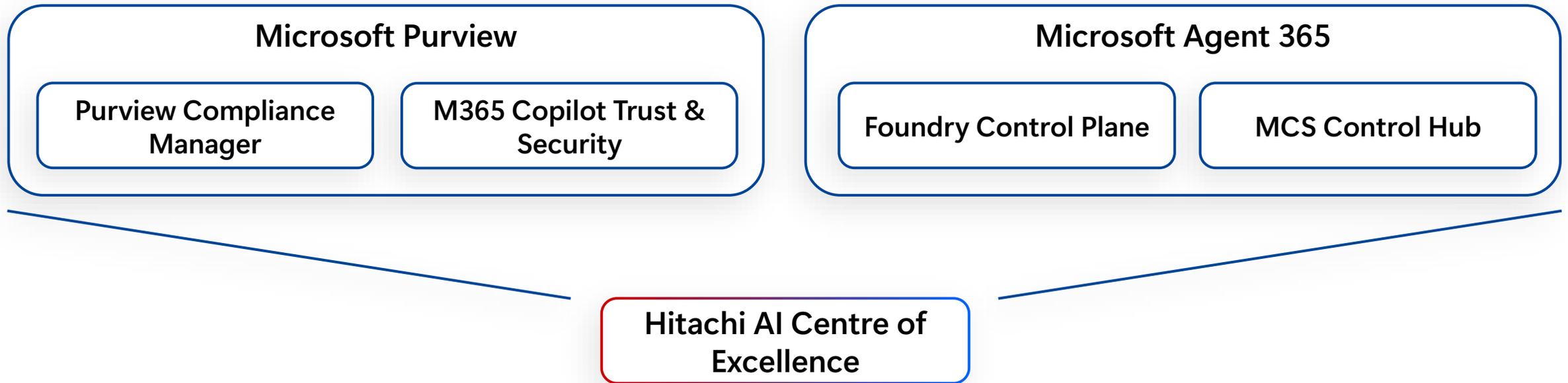
Maintain visibility, accountability and control

- ❑ Central inventory of all agents
- ❑ Logging, audit trails and usage tracking
- ❑ Cost monitoring and ongoing governance review

**Governance provides the guardrails that allow agents to scale safely and confidently.**

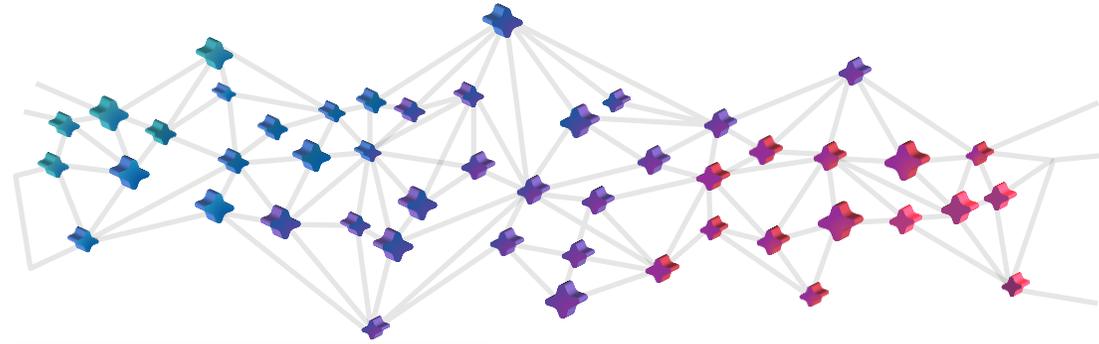
# Capabilities Enabling AI Governance

The shift from isolated AI experiments to large-scale, enterprise AI deployment. With that scale comes new risks and Governance and compliance are now fundamental, not optional. AI agents must be managed like human users (identity, permissions, observability, lifecycle) across the entire estate, and with a wholistic approach.



Hitachi's approach focuses on taking a wholistic approach to Agent observability and governance

# Governance for the Agentic / Copilot-enabled Enterprise



## Microsoft Agent 365

- Central registry of all agents.
- Unique Agent IDs, identity via Microsoft Entra.
- Fine-grained access control / risk-based conditional access.
- Visibility & telemetry (behaviour, performance, data usage).
- Integration with Microsoft Defender and Purview

## Purview Compliance

- Enforce data governance across Agent 365
- Monitor data access from intelligence layer
- Track agent observability and data usage (DSPM)
- M365 Copilot Trust and security configuration

## Foundry Control Plane

- Single point of control for provisioning, monitoring and scaling of Pro-code agents.
- Unified compliance posture across all agents (internal, external, third-party).
- Supports interoperability: agents across platforms can be tracked and governed centrally.

## Agent Control System

- A central Copilot Hub to manage your AI transformation.
- Discover new AI capabilities.
- Manage AI settings.
- Track adoption.
- Admin-Centric Design for ROI evaluation

# Next steps

HITACHI

16:00 – 16:30

30 Min

# Need organisation-wide Copilot adoption support?

Strengthen Adoption, Capture Learnings, and Prepare for Scale

## Microsoft 365 Copilot Change & Adoption

Preparing the business for secure, confident Microsoft 365 Copilot adoption for public sector organisations, driving productivity and responsible AI use.

### Key Pillars:

- Build trust and embed Copilot into daily workflows
- Develop practical skills and activate digital champions
- Prioritise governance, compliance and measurable impact

### Key Activities:

- Tailored learning journeys
- Champion-led engagement
- Continuous feedback and improvement
- Impact measurement with clear KPIs

### Outcome:

A scalable blueprint for sustainable transformation and productivity gains.

## Enterprise AI Governance

A strategic blueprint for secure, scalable AI governance across Microsoft Copilot, Azure and Power Platform, reducing risk and enabling confident innovation

### Key Pillars

- Comprehensive governance framework
- Centralised agent management and observability
- Integrated compliance and security controls
- Modular, blueprint-based approach

### Key Activities

- Maturity assessment and gap analysis
- Governance model and policy design
- Technology configuration and implementation

### Outcome:

A robust, compliant AI environment that accelerates adoption, minimises risk and delivers measurable business value.

# Copilot propositions

How we engage with customers

## AI Kickstart

2-day engagement

Education on Microsoft AI and Copilot.

Envisioning how it can be applied to **solve your business problems.**

STARTING

## AI Design Sprint

5-day engagement

Deep dive into your business problem for a use case that **Copilot can solve.**

Design and build a **Copilot prototype** to test with your users.

SENSING

## PT2Copilot

Convert your prototype into a production **Copilot asset.**

Roll-out to your business.

**Implement** the governance framework to support AI.

SHAPING

## Platform

Scale **your Copilot implementation.**

Enable automated deployments and testing.

**Develop** and govern multiple AI use cases.

SCALING

# Q&A

HITACHI

# Get started today

Learn more

<b>Copilot Studio website</b>	<a href="https://aka.ms/copilotstudio">aka.ms/copilotstudio</a>
<b>Blog</b>	<a href="https://aka.ms/copilotstudioblog">aka.ms/copilotstudioblog</a>
<b>Demo</b>	<a href="https://aka.ms/copilotstudiodemo">aka.ms/copilotstudiodemo</a>
<b>Product documentation</b>	<a href="https://aka.ms/copilotstudiodocs">aka.ms/copilotstudiodocs</a>
<b>Learning resources</b>	<a href="https://aka.ms/copilotstudiolearn">aka.ms/copilotstudiolearn</a>
<b>Community page</b>	<a href="https://aka.ms/copilotstudiocommunity">aka.ms/copilotstudiocommunity</a>
<b>Implementation guide</b>	<a href="https://aka.ms/copilotstudioimplement">aka.ms/copilotstudioimplement</a>
<b>Adoption Resources</b>	<a href="https://aka.ms/adoptcopilotstudio">aka.ms/adoptcopilotstudio</a>
<b>Scenario Library</b>	<a href="https://aka.ms/scenariolibrary">aka.ms/scenariolibrary</a>
<b>Copilot Connectors</b>	<a href="https://aka.ms/copilot_connectors_learn">aka.ms/copilot_connectors_learn</a>

[aka.ms/trycopilotstudio](https://aka.ms/trycopilotstudio)

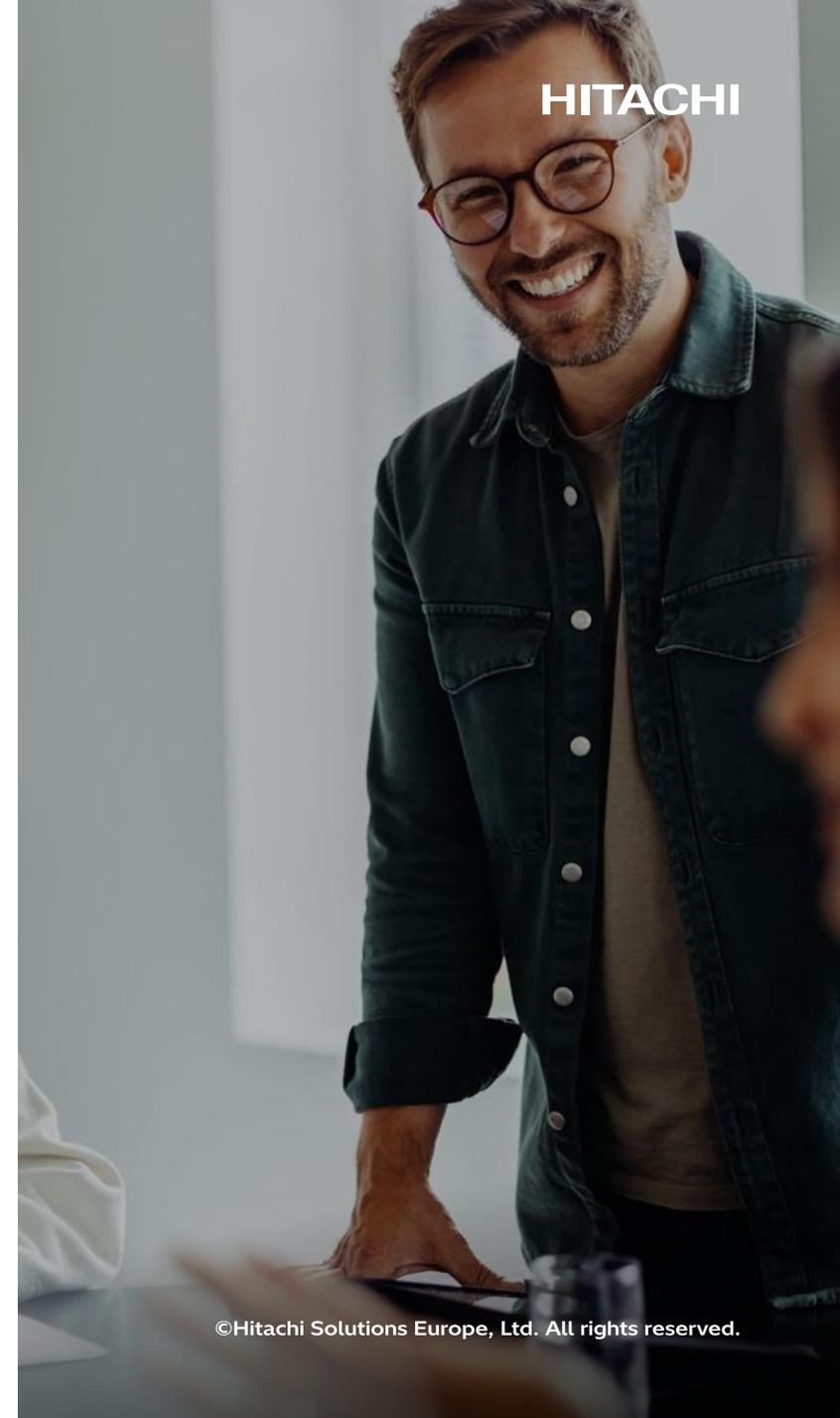


# Continue learning

## Other learning resources

<b>Copilot Studio Advanced HOL's</b>	<a href="https://aka.ms/CopilotStudioWorkshop">https://aka.ms/CopilotStudioWorkshop</a>
<b>AI Agents for beginners</b>	<a href="https://microsoft.github.io/ai-agents-for-beginners/">https://microsoft.github.io/ai-agents-for-beginners/</a>
<b>Microsoft Power Up Program</b>	<a href="https://aka.ms/PowerUp">https://aka.ms/PowerUp</a>
<b>Create a Monthly Business Review (MBR) Agent</b>	<a href="https://github.com/microsoft/mcs-labs/blob/main/labs/mbr-prep-sharepoint-agent/README.md">https://github.com/microsoft/mcs-labs/blob/main/labs/mbr-prep-sharepoint-agent/README.md</a>
<b>Transform Your Business Processes with Agents</b>	<a href="https://learn.microsoft.com/en-us/training/paths/implement-no-code-copilot-agents-microsoft-365-sharepoint">https://learn.microsoft.com/en-us/training/paths/implement-no-code-copilot-agents-microsoft-365-sharepoint</a>
<b>Dynamics 365 Agents</b>	<a href="#">Autonomous service agents, Sales Qualification Agent, Customer Insights agent</a>

[aka.ms/copilotstudiolearn](https://aka.ms/copilotstudiolearn)



How did  
we do?



# Thank you

Copilot Studio  
implementation guide



Hitachi Solutions  
UK



# Disclaimer

Microsoft Copilot Studio (1) is not intended or made available as a medical device for the diagnosis of disease or other conditions, or in the cure, mitigation, treatment or prevention of disease, or otherwise to be used as a component of any clinical offering or product, and no license or right is granted to use Microsoft Copilot Studio for such purposes, (2) is not designed or intended to be a substitute for professional medical advice, diagnosis, treatment, or judgment and should not be used as a substitute for, or to replace, professional medical advice, diagnosis, treatment, or judgment, and (3) should not be used for emergencies and does not support emergency calls.

Any agent you create using Microsoft Copilot Studio is your own product or service, separate and apart from Microsoft Copilot Studio. You are solely responsible for the design, development, and implementation of your agent (including incorporation of it into any product or service intended for medical or clinical use) and for explicitly providing end users with appropriate warnings and disclaimers pertaining to use of your agent.

You are solely responsible for any personal injury or death that may occur as a result of your agent or your use of Microsoft Copilot Studio in connection with your agent, including (without limitation) any such injuries to end users.

