Secure and Govern AI and Agents with Microsoft Agent 365

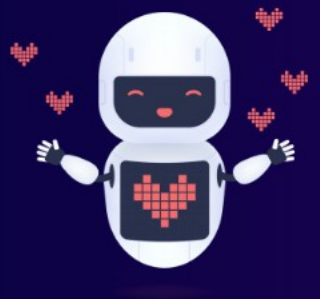
Sophie Ke, Sr. PMM
Craig Jahnke, Principal Solution Engineer

June 15–19, 2026 • McCormick Place, Chicago

TechCon 365

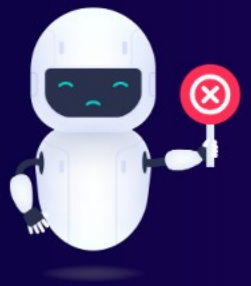
PHOTOGRAPHY DURING THE SESSION

Feel free to capture the moment! Taking pictures of the presentation, during the session is perfectly fine.



SELFIES WITH THE SPEAKER

We encourage interaction! If you'd like to take a selfie with the speaker, don't hesitate to ask. Most speakers will be happy to oblige during appropriate breaks.



RECORDING AND LIVE STREAMING

Recording or live streaming the session, in part or in full, is strictly prohibited. Thank you for respecting our content and Speakers.

About me

Sophie Ke

Sr. Product Marketing Manager
Agent 365 and Copilot Controls
Microsoft

- I am responsible for shaping the Security and Governance narrative for Agent 365 and Microsoft 365 Copilot.
- I have extensive technical expertise in Microsoft Purview and Security for AI, and a career spanning government, public, and non-profit sectors. I am dedicated to making people's lives more efficient and better.
- I am a Yoga teacher, recreational ballet dancer, and lover of cats. I love to travel and try new and exciting food all around the world. My favourite cuisines are Japanese, Korean, and French, although I will always have a soft spot for Swedish meatballs and beans on toast.

About me

Craig Jahnke

Principal Solution Engineer, Microsoft

- I lead AI strategy, adoption, and enablement work — helping organizations Understand where AI actually drives value, building the right workflows, and making sure people know how to use them in their day-to-day work.

- I have 20+ years in Microsoft focused technology roles and the last several years have been centered on AI, automation, and helping teams adopt new capabilities in a practical, sustainable way.

- I have spent more than a decade running Microsoft community groups and conferences, helping new speakers get started and creating spaces for people to learn from each other. Outside of work, I'm usually golfing, grilling, or working on a backyard project

- LinkedIn: https://www.linkedin.com/in/craig-jahnke-0490b02/

Agenda

01 Introduction

02 Secure & Govern Microsoft 365 Copilot

03 Secure & Govern agents

04 Resources to help you get started

AI is transforming how work gets done

46%

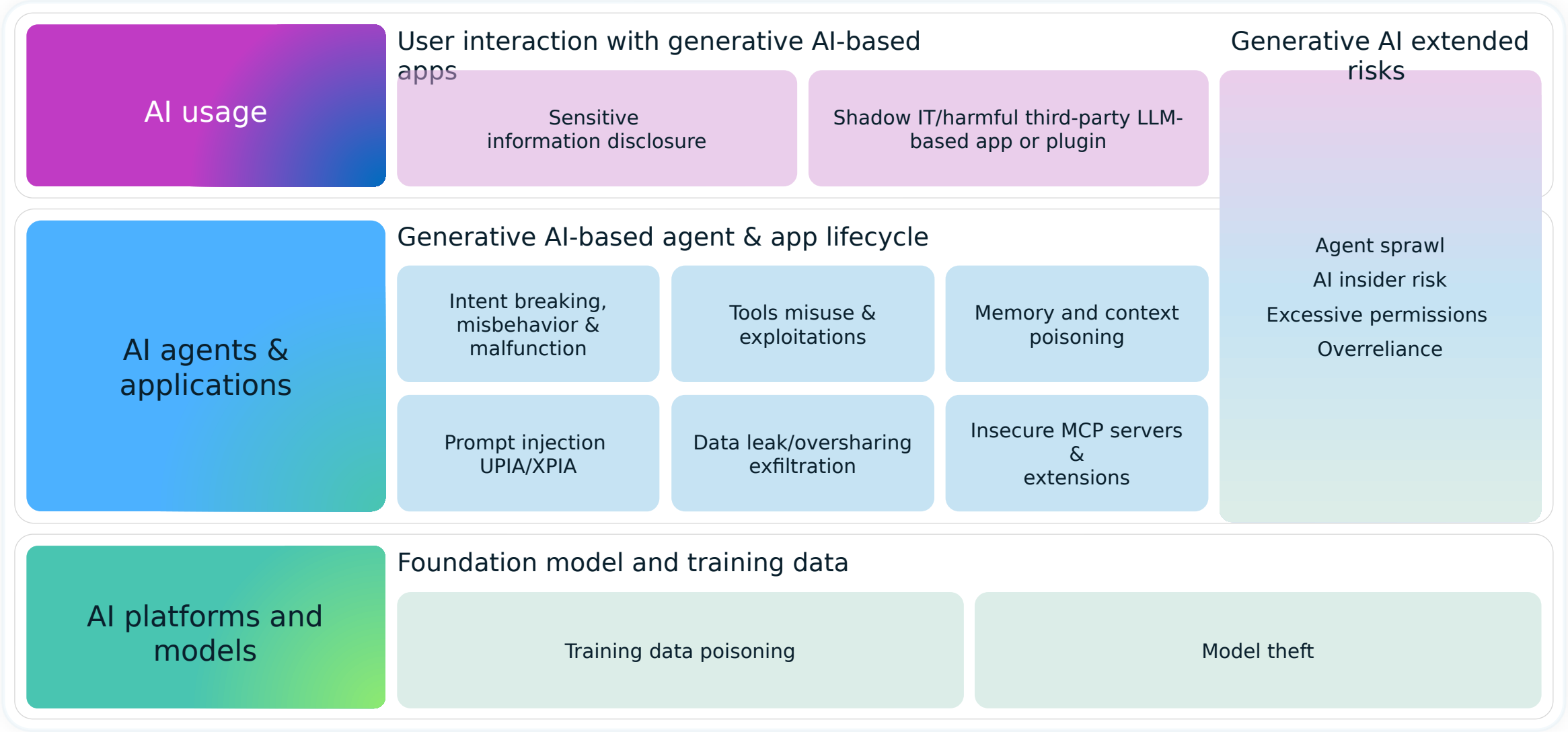
of leaders surveyed report they are using AI & Agents to fully automate workflows or processes[1]

1.3B

AI agents projected to be automating workflows by 2028[2]

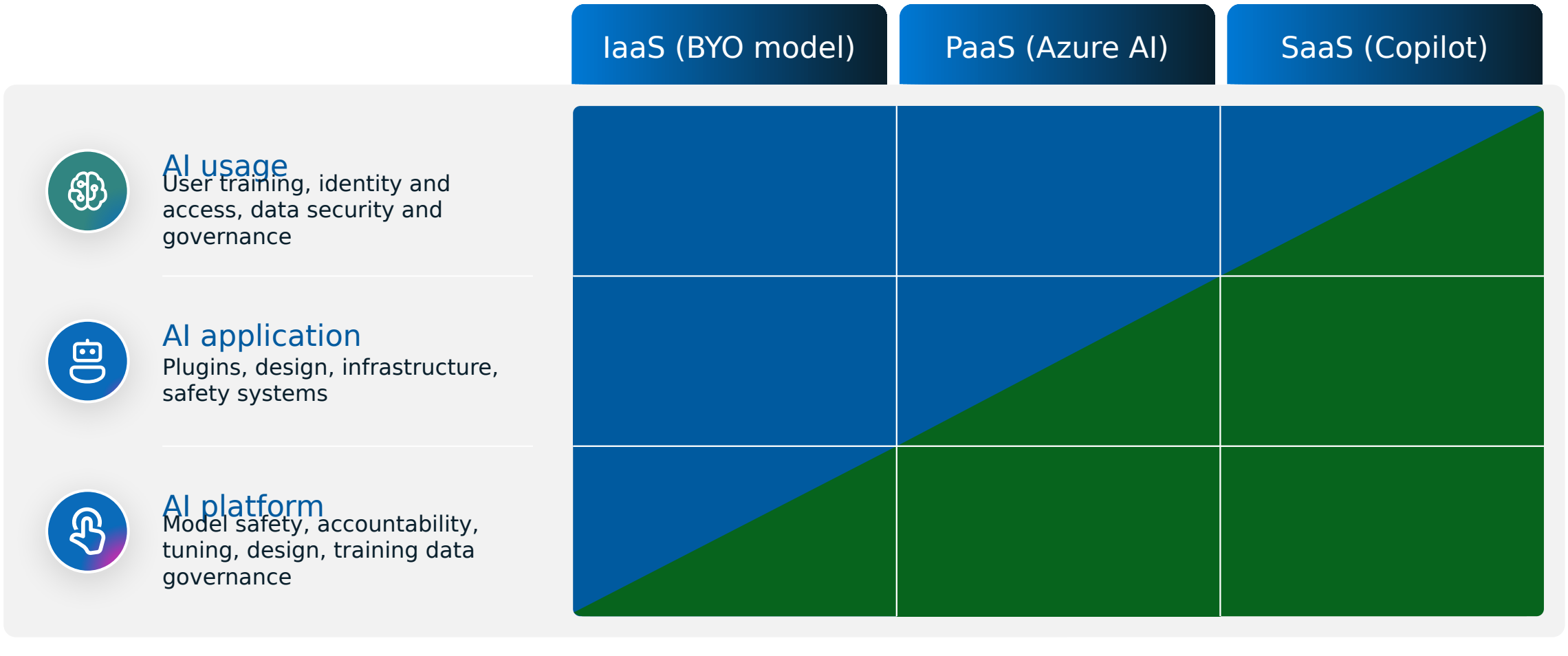
1. Work Trends Index | 2. IDC Info Snapshot, sponsored by Microsoft, 1.3 Billion AI Agents by 2028, May 2025
#US53361825

Gen AI accelerates the threat landscape across layers

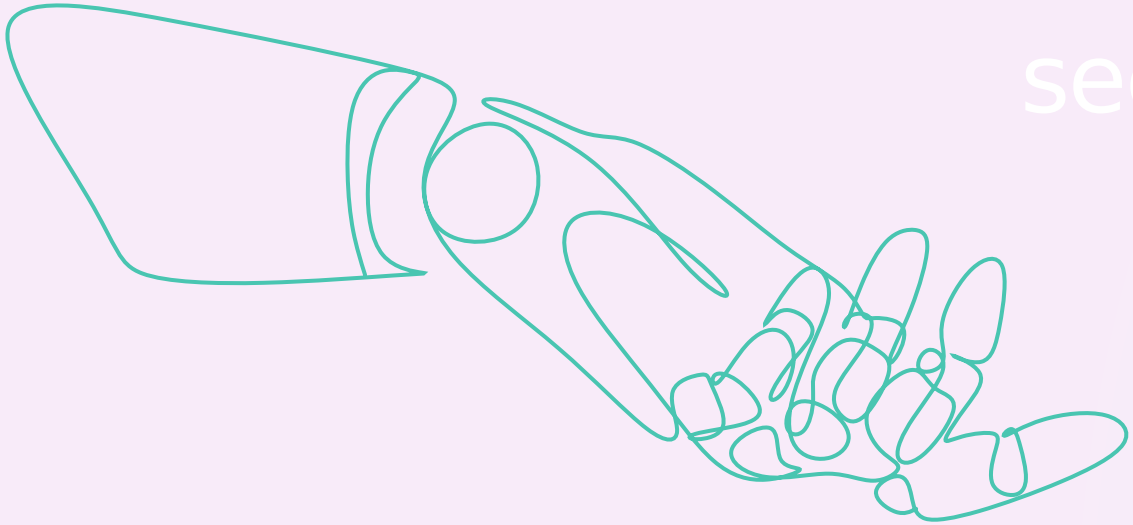


MITRE ATLAS | MSRC AI Bug Bar | OWASP Top 10 for LLM | OWASP Top 10 for ML

Organizations’ responsibilities for managing risks vary based on the types of AI services they use



To unlock the potential of agentic AI, we need to start with trust. And trust starts with security



Secure and Govern

Microsoft 365 Copilot

Agents

Secure and Govern

Microsoft 365 Copilot

Agents


Microsoft commitments and controls
M365
Microsoft 365 Copilot is built on trust
Tools to manage Copilot data

Read more at aka.ms/EDPLearn

Microsoft commitments and controls

We secure your data at rest and in transit

You control your data

Your data is not used to train or enrich foundation models

You're protected against AI security and copyright risks

Microsoft 365 Copilot is built on trust

Microsoft 365 Copilot

Microsoft Purview

Security & Governance

- Honors your existing permissions
- Supports your lifecycle policies and audit requirements
- Protects against data loss and insider risk
- Detect and investigation non-compliant and unethical usage
- Assess Oversharing risks and apply recommended corrections
- Guided assistance to remain compliant with AI Regulations

A complete solution for enterprise-ready AI

Tools to secure and govern Microsoft 365 Copilot

Microsoft Purview

Provides security, compliance, and governance across data and files

SharePoint Advanced Management

Included in Microsoft 365 Copilot

Provides SharePoint site management and content governance capabilities

Problem summary

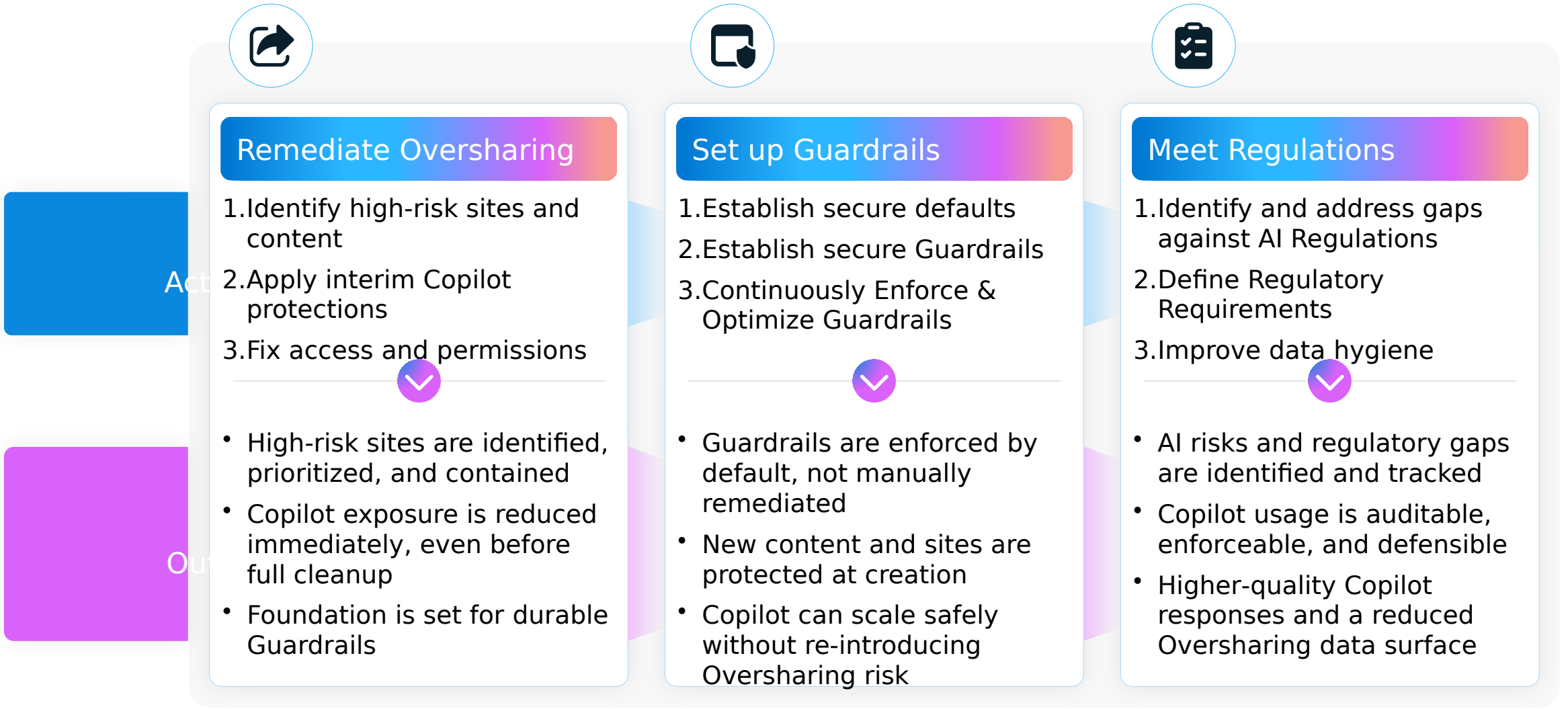
Microsoft 365 Copilot builds on the data already in Microsoft 365, prompting organizations to strengthen oversharing, data loss, and insider risks practices to support safe, confident adoption.

If grounding data and Copilot interactions are not secured, it could lead to

- Access to information beyond what the user needs for their role
- Unauthorized disclosure of confidential information
- Out of date or irrelevant responses

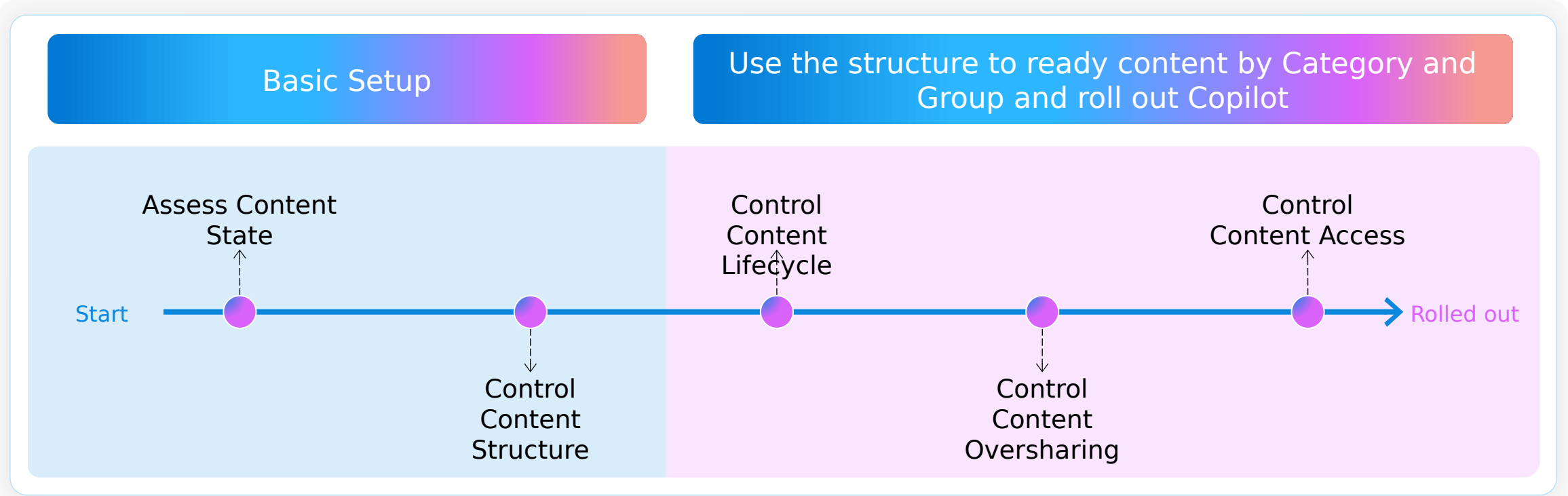
By addressing these risks, organizations can ensure that Microsoft 365 Copilot is secured end to end

Secure and Govern Microsoft 365 Copilot



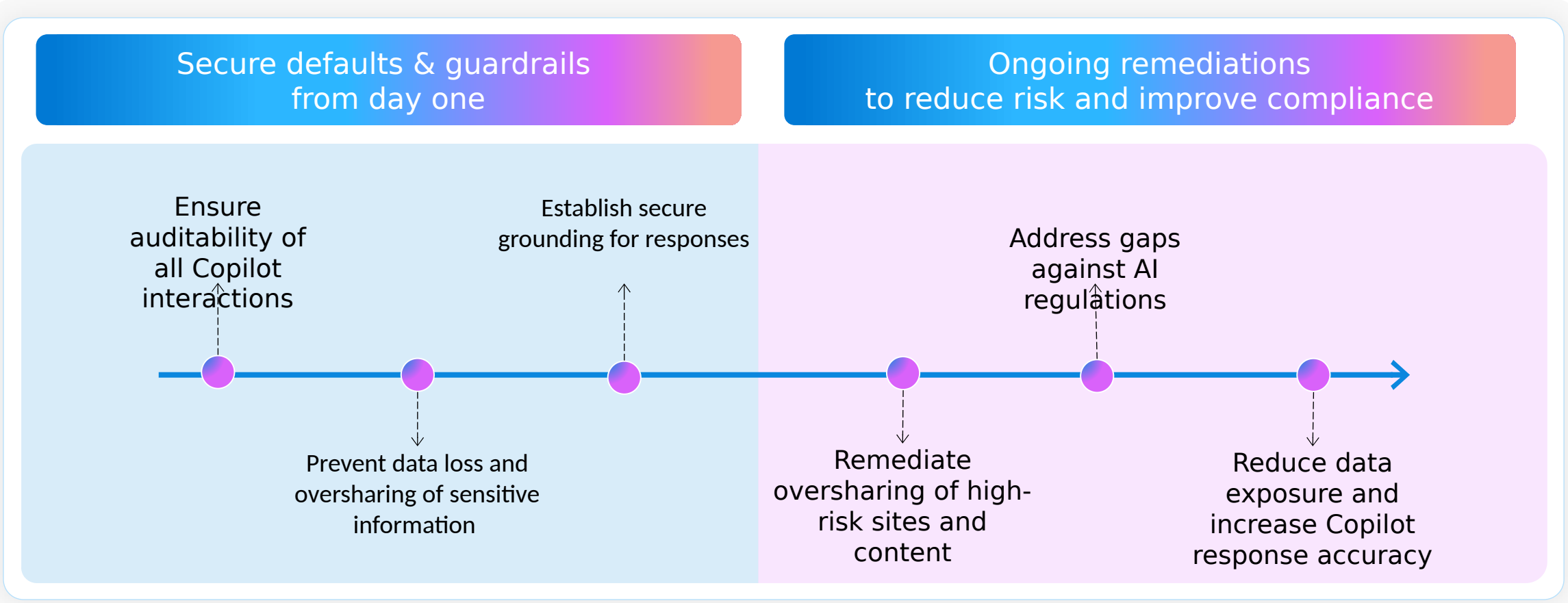
Content Readiness Journey

powered by SharePoint Advanced Management (SAM)



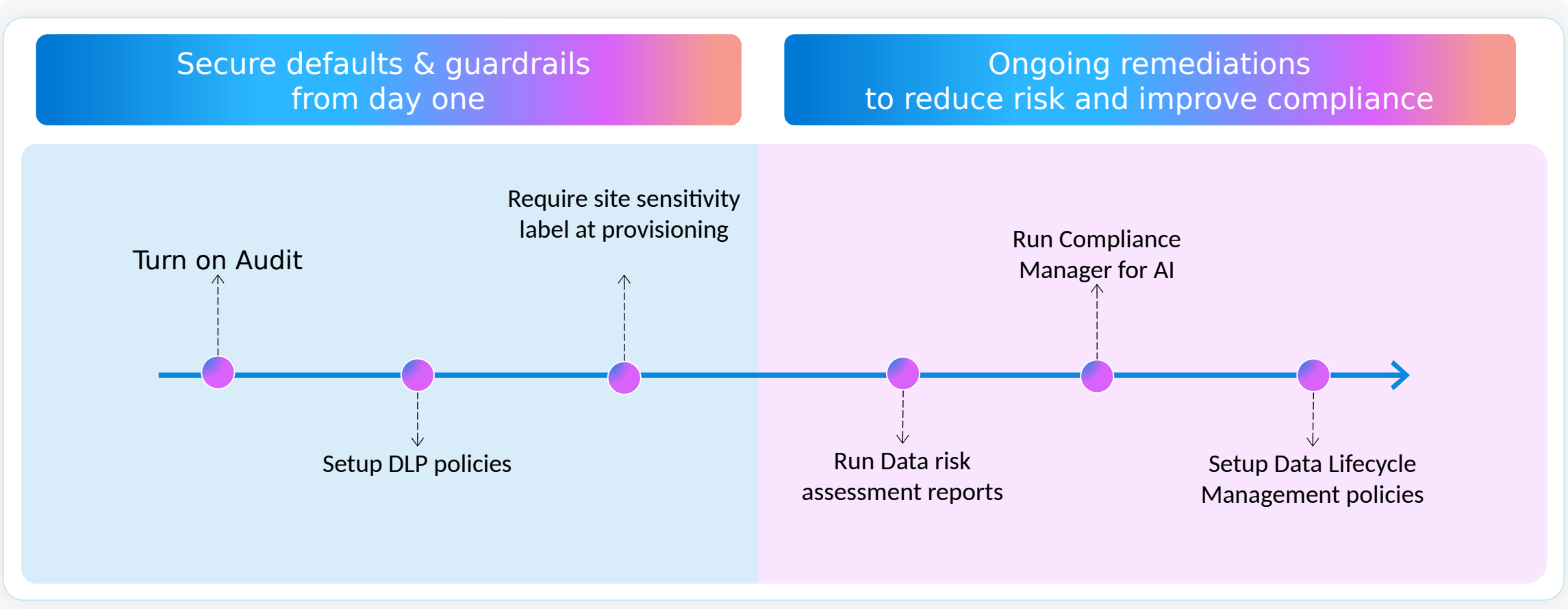
Secure & Govern Microsoft 365 Copilot

With Microsoft Purview



Secure & Govern Microsoft 365 Copilot

With Microsoft Purview



Customers with E5 | Optimized

LEGEND | 1. Copilot and SAM | 2. OE3/ME3 | 3. ME5/Purview suite

Secure & Governed Foundation for Microsoft 365 Copilot

Realize value quickly with Copilot by remediating Oversharing, enforcing Guardrails, and meeting AI Regulations

Select deployment services are included in your FastTrack benefit. Other critical services are available thru Microsoft Unified or our Partner Ecosystem

Deployment checklist

Remediate Oversharing

1.Identify high-risk sites and content

- Run SAM Content Management Assessment to identify sites with oversized audiences, EEEU usage, broken inheritance, inappropriate sharing, as well as sensitive content, identify sites that are inactive or ownerless[1]
- Review Purview Data Security Posture Management (DSPM) Data Risk Assessments to identify sites with sensitive data and risky/sharing links accessible to Copilot[3]
- Prioritize remediation for sites and content that are high risk

2. Apply interim Copilot protections

- Enable SAM Restricted Content Discovery (RCD) to exclude sensitive sites from Copilot discovery[1]
- Configure Purview Data Loss Prevention (DLP) for Copilot to exclude sensitive content from Copilot grounding[3]
- Validate via audit and reports that Copilot no longer surfaces restricted content

3. Fix access and permissions

- Initiate SAM site access reviews for sites flagged as high-risk so site owners can remediate down to the file level[1]
- Review Purview DSPM Data Risk Assessment recommendations for sites flagged as high-risk and take remediation actions such as apply site sensitivity labels to change sites from public to private, enforce allowed sharing links, set default labels, and remediate sharing links that are too permissive[3]
- Remove interim Copilot restrictions once site access and permissions are fully remediated.

Setup Guardrails

1.Establish secure defaults

- Enforce Restricted Access Control (RAC) by default for business-critical sites at provisioning time[1]
- Disable or restrict use of Company-wide sharing groups and Sharing with Anyone link at the tenant level[2]
- Require site sensitivity labels at provisioning to enforce correct site privacy and sharing controls by default[2]

2.Establish secure Guardrails

- Configure auto-label and default sensitivity labels to ensure sensitive files and emails are protected[3]
- Setup Purview DLP for Copilot policy to restrict Copilot processing of labeled sensitive contentc[3]
- Enable Purview DLP for Copilot prompt policy to restrict Copilot from responding to prompts containing sensitive information[1]
- Enable Purview Insider Risk Management (IRM) policies to detect potentially inappropriate or non-compliant AI usage[3]

3.Continuously Enforce & Optimize Guardrails

- Use DSPM Activity Explorer to review Copilot interactions, prompts and responses, web search keywords, and sensitive data activity[3]
- Use DSPM Data Risk Assessments to continuously validate that sensitive data remains protected from Copilot access[3]
- Review Purview IRM and DLP alerts to detect and investigate risky AI usage or potential data loss[3]

Meet Regulations

1.Identify and address gaps against AI Regulations

- Use Purview Compliance Manager to assess your tenant against AI-related regulatory requirements and Microsoft recommended actions[3]
- Review improvement actions related to data protection, auditability, and AI usage controls[3]
- Assign and track remediation actions to close identified compliance gaps[3]
- Validate improvements using Purview DSPM reports[3]

2.Define Regulatory Requirements

- Decide how long to keep audit logs in accordance with regulatory and internal requirements[2,3]
- Decide how to keep or when to delete Copilot interactions based on legal risk or regulatory requirements with Purview Data Lifecycle Management[2,3]
- Use Purview eDiscovery to search, preserve, and produce Copilot-related content for audits or legal requests[2,3]

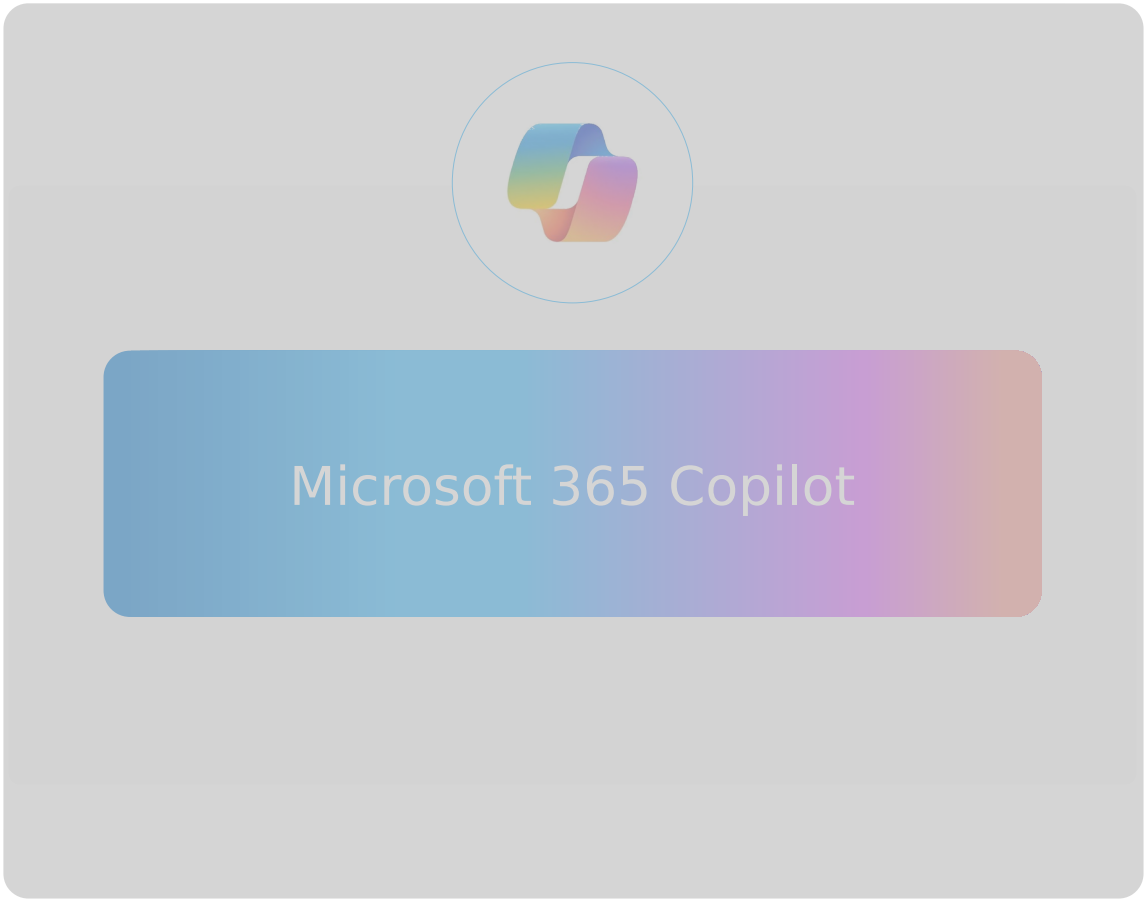
3.Improve data hygiene

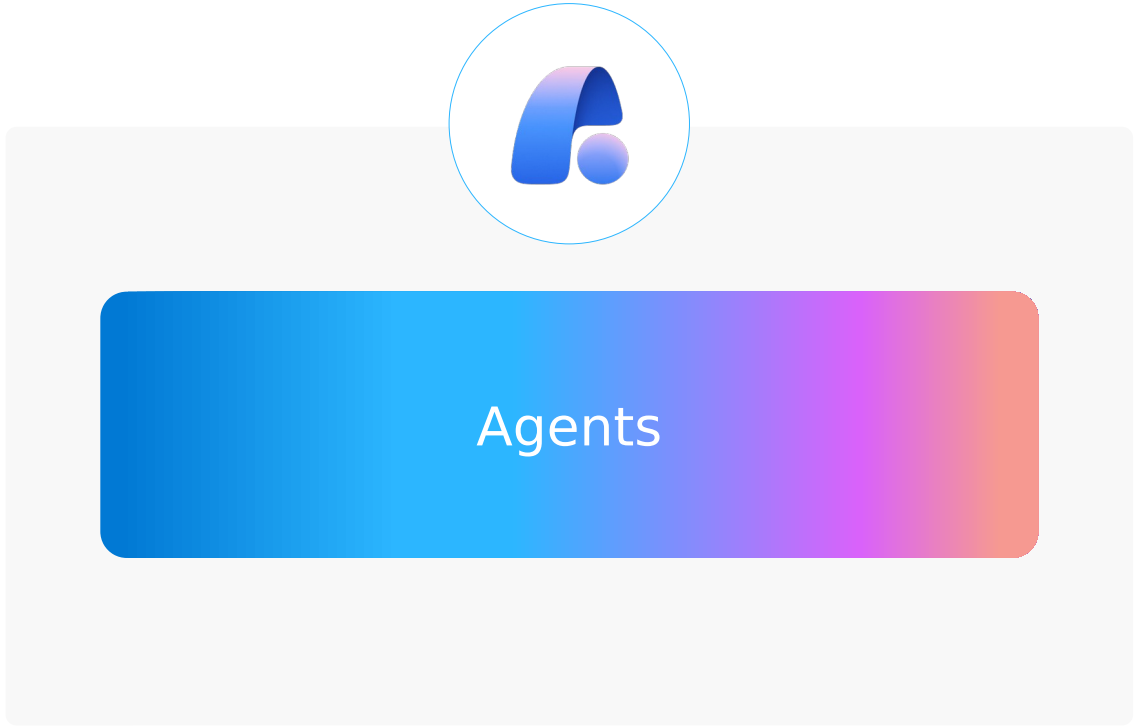
- For Sites
  - Maintain lifecycle hygiene by identifying and addressing inactive or obsolete sites using SAM policies and reports[1]
  - Use Microsoft 365 Archive to store inactive but high-value content at a lower cost while preventing Copilot from processing or reasoning over it consumption
- For Files
  - Apply Purview retention and deletion policies to reduce data exposure while meeting record-keeping obligations[2,3]
  - Use Purview retention labels + Microsoft 365 Archive to exclude files from Copilot use while preserving them for recordkeeping obligations or discovery [2, consumption]

Guidance assumes Copilot technical prerequisites in place: Technical enablement of core services (Teams, SharePoint, Exchange), Office Applications deployed (modern Outlook recommended) and on current or monthly update channel

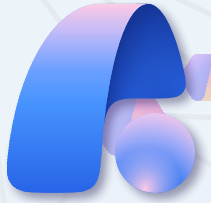
Last updated March 6, 2026

Secure and Govern





Now available



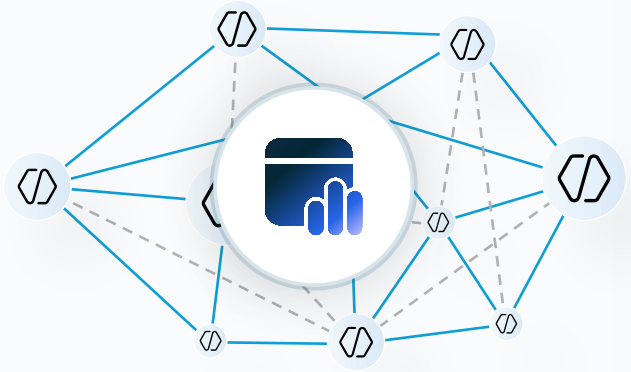
Microsoft Agent 365

The control plane for agents

Microsoft Agent 365

The control plane for agents

Observe

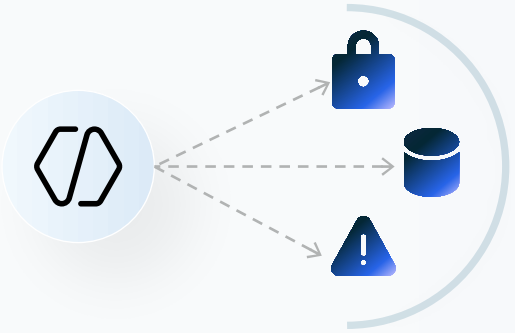


Monitor and manage agents in real time

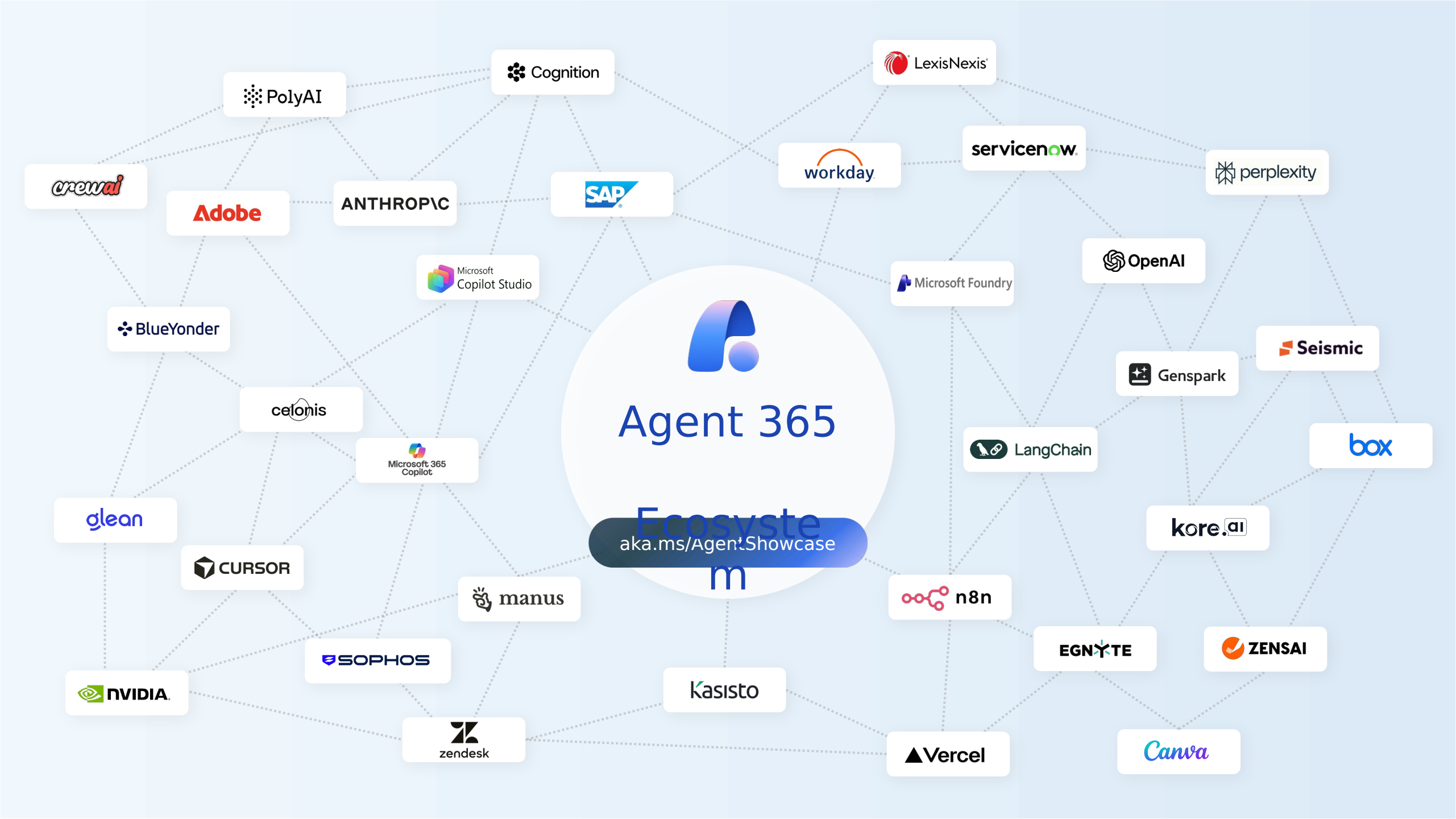
Govern

Establish guardrails for agents and users

Secure



Protect agents comprehensively


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

Gen AI and agents create security challenges

Agent sprawl & resource access

82%

of leaders expect to use agents in the next 12–18 months to meet demand for workforce capacity[3]

Data oversharing & leakage

80%

of leaders cited leakage of sensitive data as their main concern[1]

Shadow AI, new AI threats & vulnerabilities

88%

of organizations are concerned about indirect prompt injection attacks[2]

Regulatory compliance

55%

of leaders lack understanding of how AI is and will be regulated and are seeking guidance[1]

1. First Annual Generative AI study: Business Rewards vs. Security Risks, , Q3 2023, ISMG, N=400
2. How to Secure Custom-Built AI Agents, Gartner, 17 March 2025, Dionisio Zumerle, Jeremy D'Hoinne
3. Microsoft Work Trend Index Survey 2025

Microsoft Security for AI

Control agent sprawl & resource access

Prevent data oversharing & leaks

Defend against AI threats and vulnerabilities

Enable regulatory compliance

Control agent sprawl & resource access

Prevent data oversharing & leaks

Defend against AI threats and vulnerabilities

Enable regulatory compliance

82%

of leaders expect to use agents
in the next 12–18 months to meet demand for workforce capacity

Source: Microsoft Work Trend Index Survey 2025

AI agents introduce new access control challenges

Unseen = Unsecured

- Unknown and unmanaged agents
- No access control and excessive permissions
- No monitoring and high risks of misuse

Identity is the first step to secure agents

- Inventory and assign identities to all AI agents
- Enforce least privilege and protect access
- Enable monitoring and auditing

IT helpdesk agent	9d7287bd-ca05-49ab
Customer support agent	7c7509tf-bn77-82wg
Device refresh agent	3j3488uk-pq41-50od

Public Preview

Microsoft Entra Agent ID

Secure access for AI agents

Register and manage agents

- Agent ID
- Registry

Govern agent identities and lifecycle

- Lifecycle management
- Sponsors and managers
- Access governance

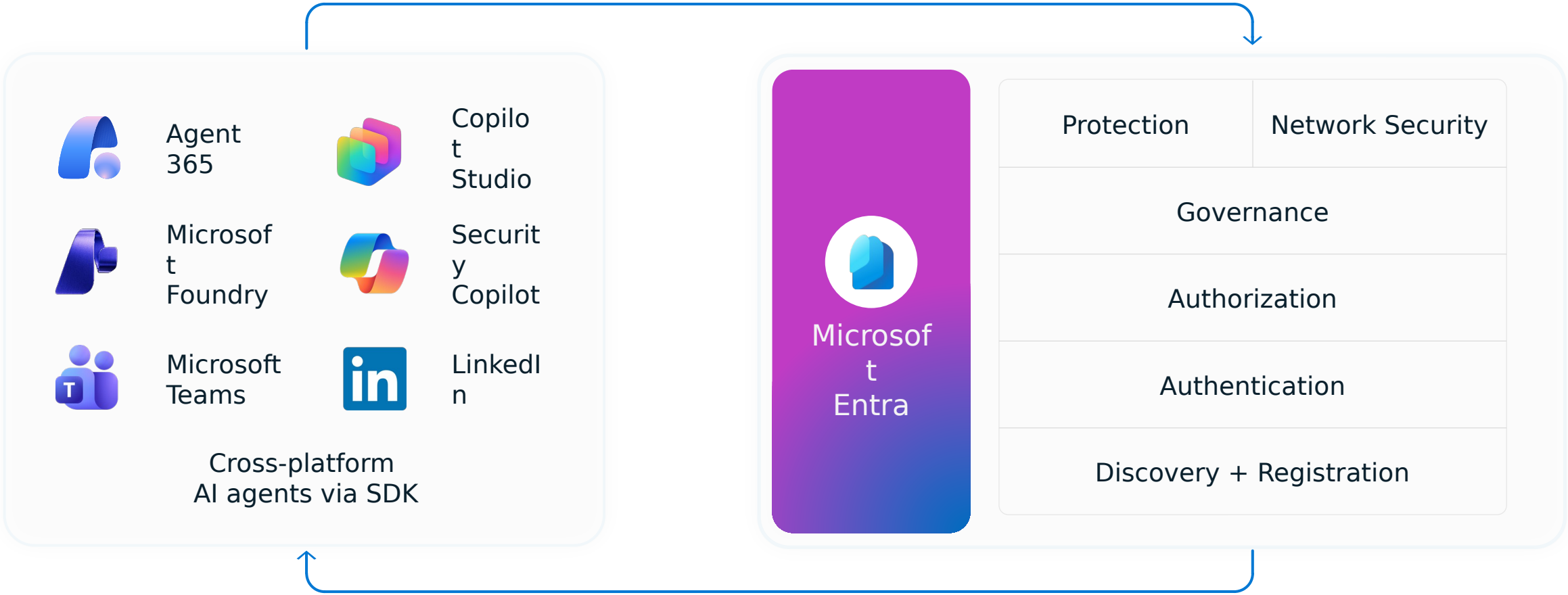
Protect agent access to resources

- Conditional access
- Identity protection
- Traffic filtering

Learn more about EntraAgentID

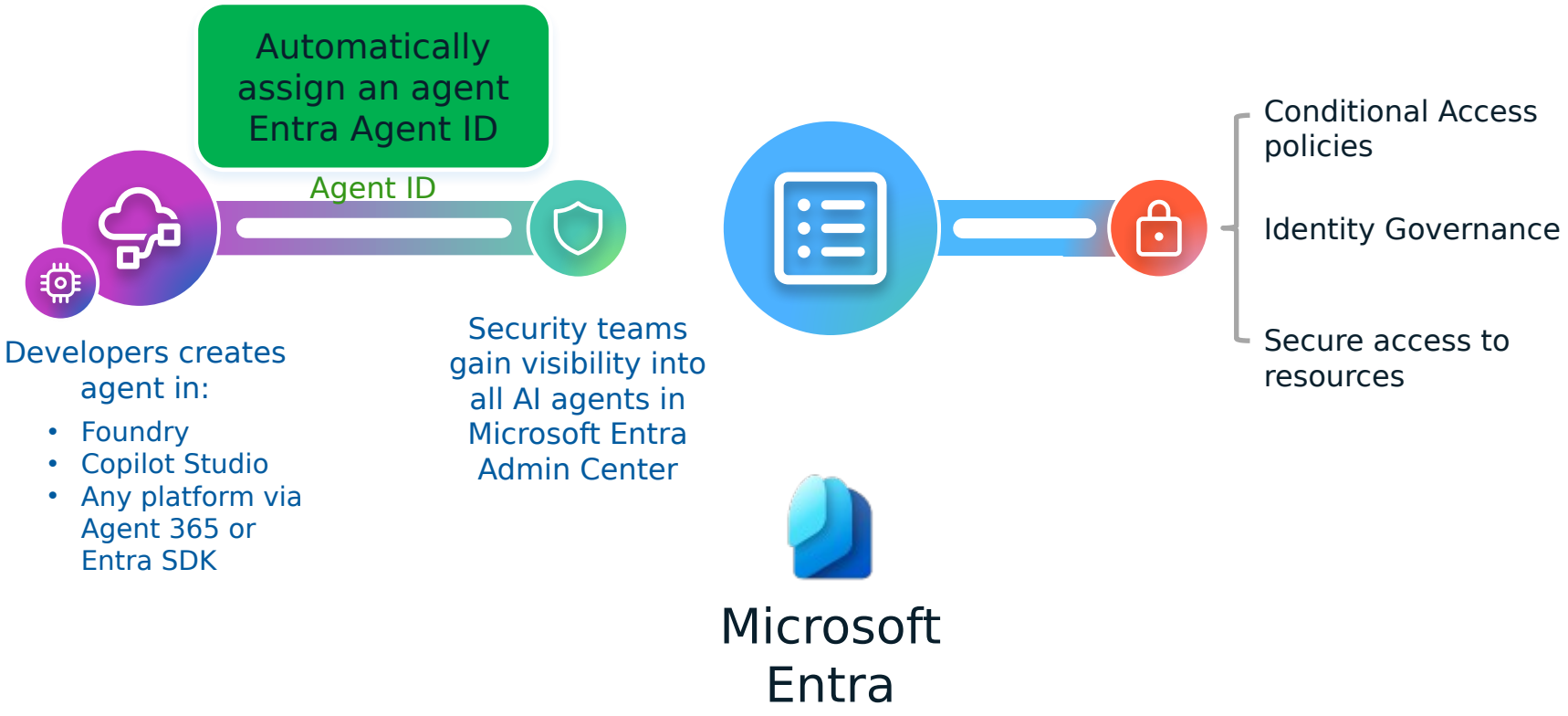
Included with Agent 365

Microsoft Entra Agent ID



Bring the same protections and controls you rely on for users to AI Agents

Manage agent sprawl, risks and behaviour with Microsoft



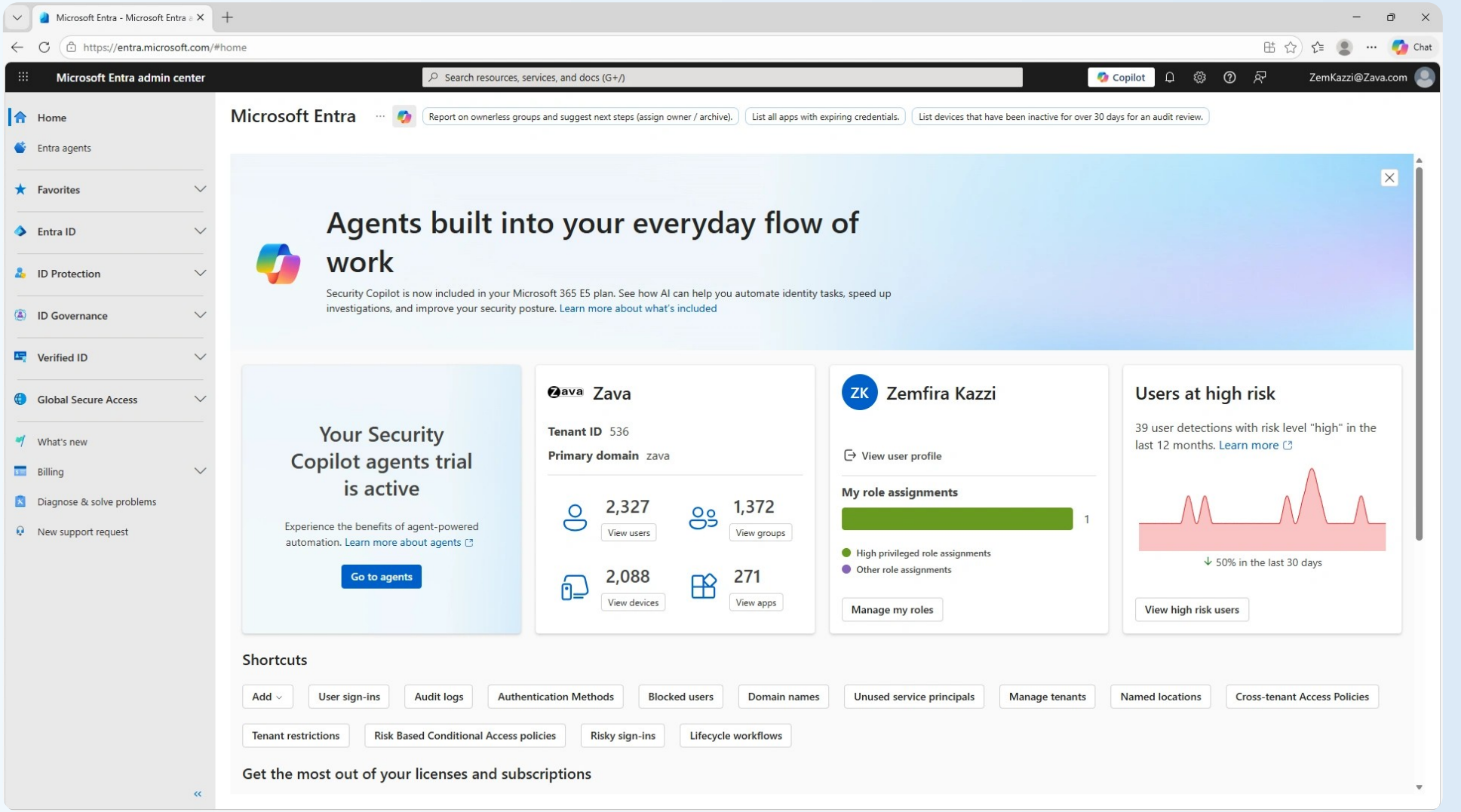
+ Native integration, no developer effort needed

+ Using the same tools to manage non-human identities

+ Industry-leading identity and access management

Start secure › Stay secure

Demo: Onboard agents



Control agent sprawl & resource access

Prevent data oversharing & leaks

Defend against AI threats and vulnerabilities

Enable regulatory compliance

Data risks deepen with the rise of agents

How do you govern agents when tools and compliance processes are fragmented?

How are you preventing unsupervised agent access to sensitive data and ensuring accountability for their actions?

How do you control autonomous agent interactions that could expose sensitive information?

Do you have visibility into what agents are generating, accessing, and sharing across your environment?

Public Preview

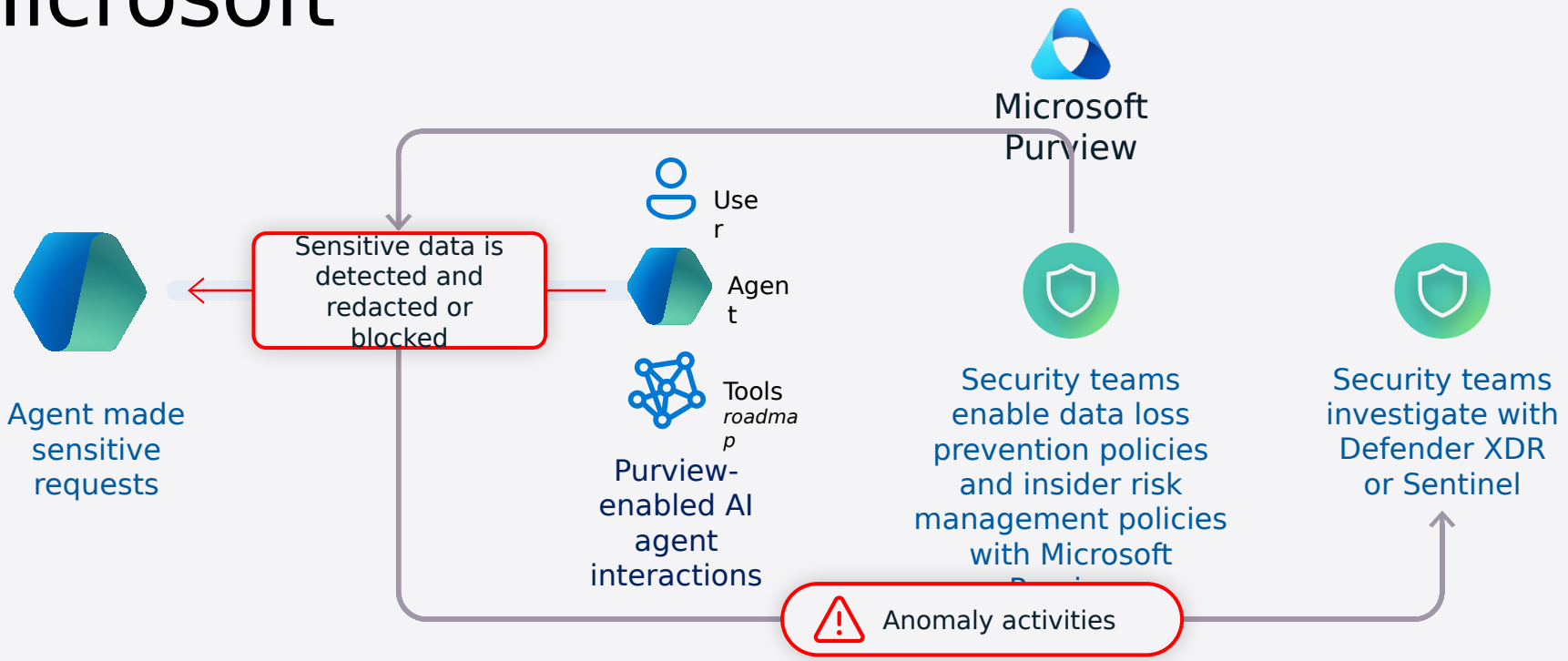
Microsoft Purview

Observe agent risk	Protect sensitive data	Maintain compliance
• Agent visibility & risk in DSPM • Insider Risk Management for Agents	• Purview protections for agent interactions • Support for Agent ID	• Compliance controls extended to agents • Retention, audit, eDiscovery, Comms Compliance

Included with Agent 365

aka.ms/

Prevent data leaks and oversharing with Microsoft



+ Granular data loss prevention controls

+ Native integration for Microsoft AI + support for browser-based AI

+ Industry-leading data security solutions

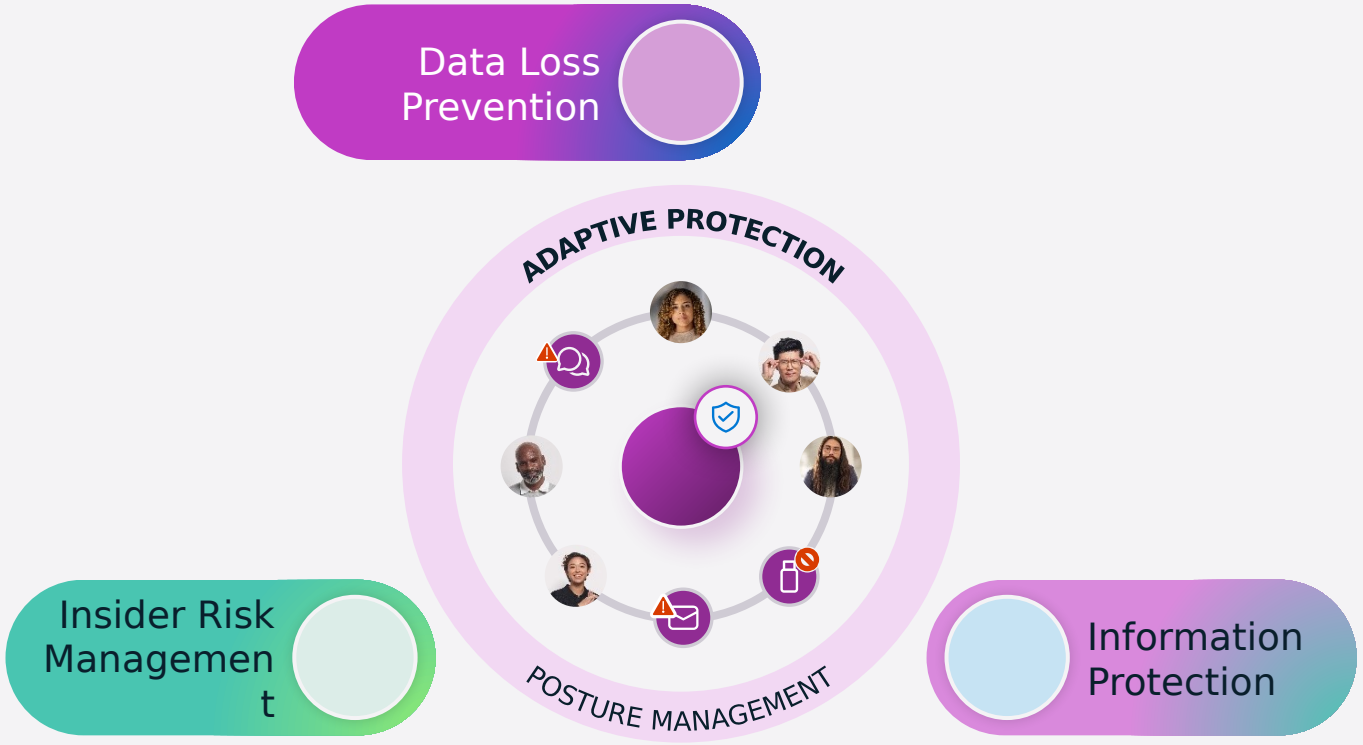
Start secure → Stay secure

Unified data protection for user & agent interactions

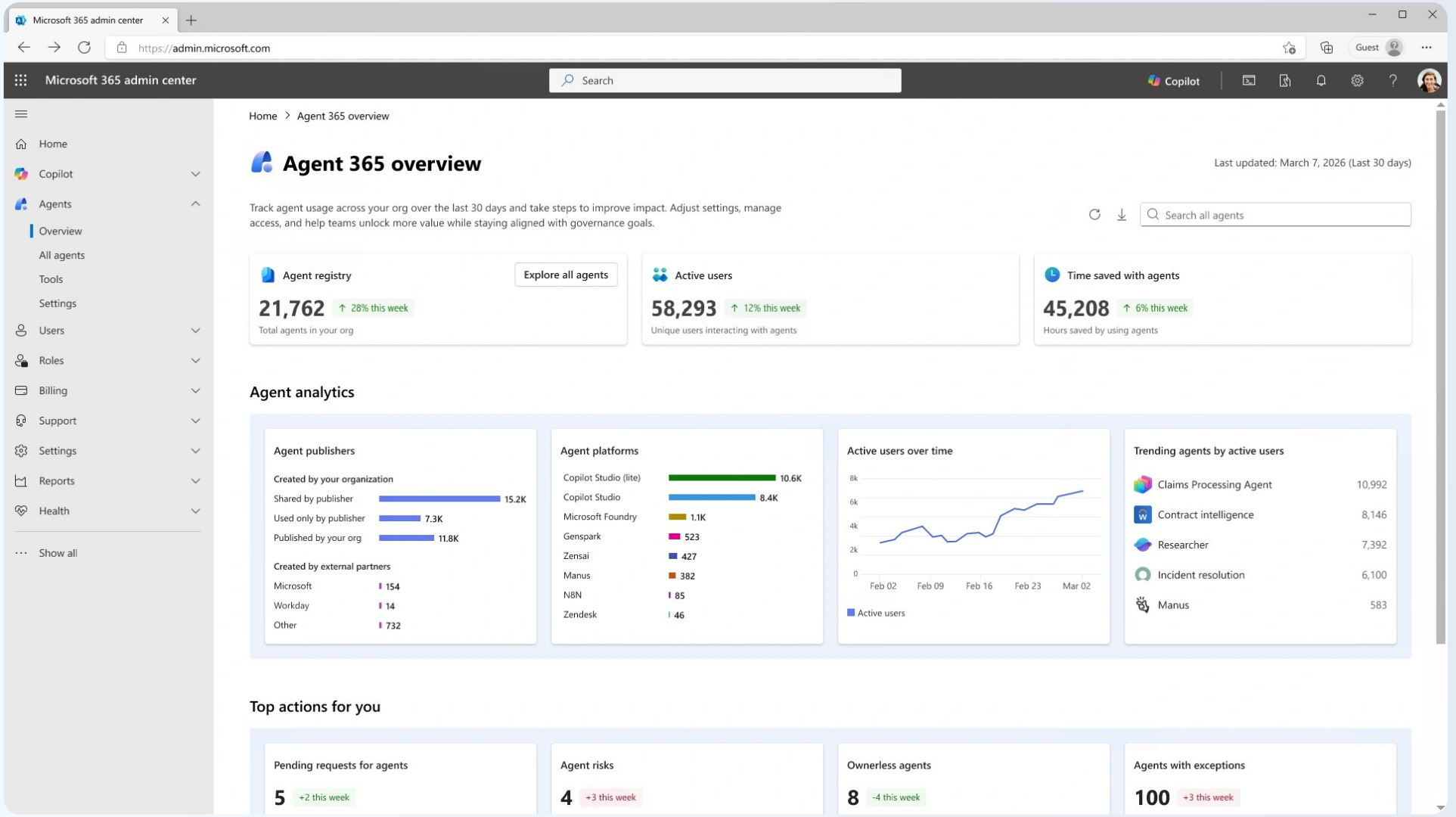
Discover and classify sensitive data in AI interactions and inherit and honor sensitivity labels in AI outputs

Prevent AI from processing certain documents and block runtime **AI interactions** containing sensitive data

Detect and investigate risky user and agent activities with AI apps and agents that may result in data security incidents



Demo: Prevent data oversharing and leaks



Control agent sprawl & resource access

Prevent data oversharing & leaks

Defend against AI threats and vulnerabilities

Enable regulatory compliance

Defend against vulnerabilities and threats

Start secure

Security posture management

Get comprehensive visibility of AI assets

Identify and remediate vulnerabilities among AI assets

Prioritize and reduce risks across cloud and AI

Stay secure

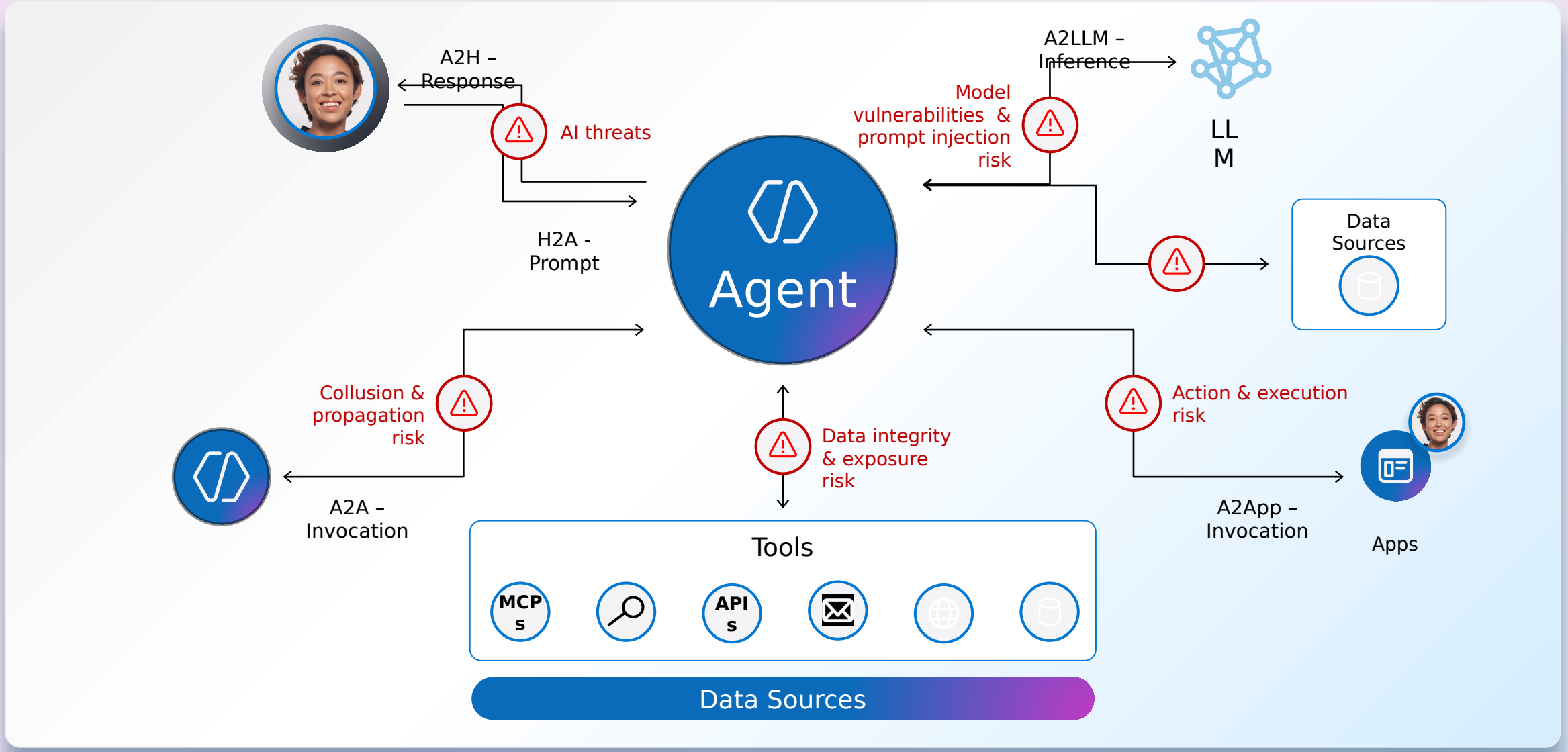
Threat protection

Continuously monitor for malicious AI activities

Detect and respond to AI-specific attacks in real time

Correlate and contextualize threat signals into incidents

Agents introduce additional threats



What’s new

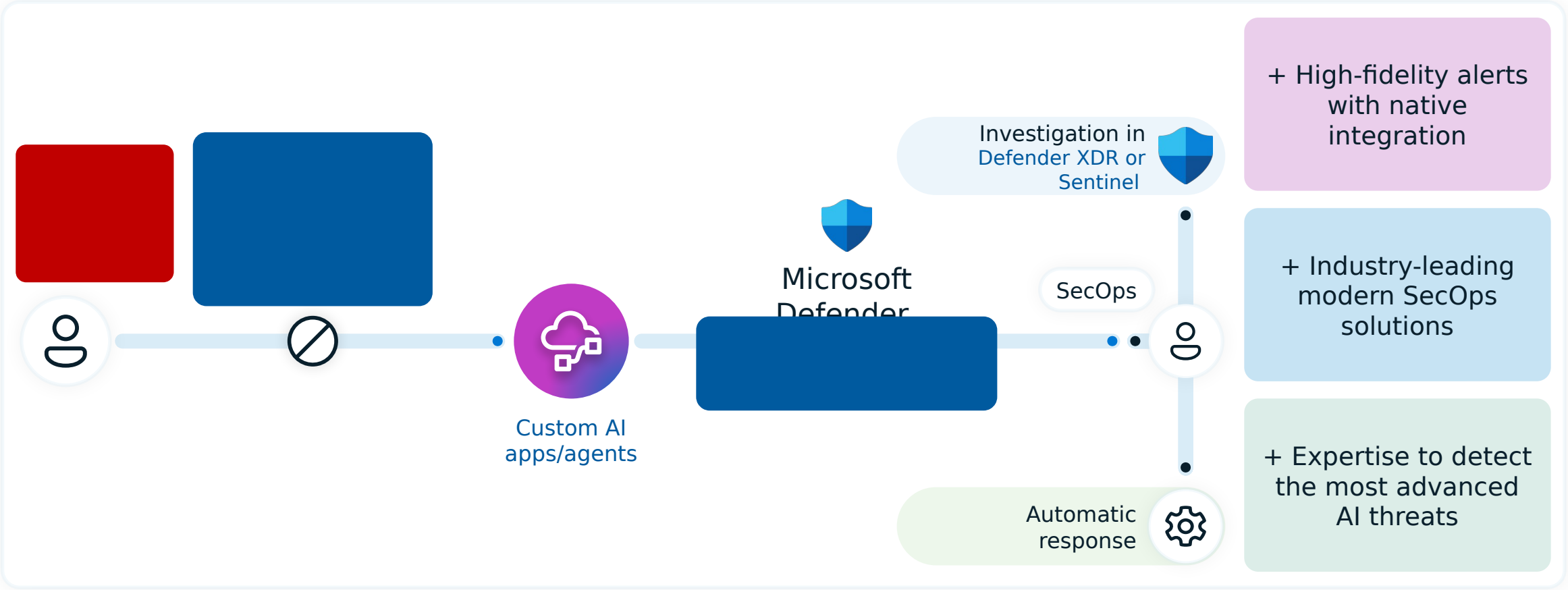
Microsoft Defender

Security posture and threat protection for Agents

Prevent threats	Detect threats	Investigate & respond
• Real-time protection • Security posture management • Attack path analysis	• OOTB threat detections • Ability to create custom detections	• Agent inventory • Advanced hunting

Included with Agent 365

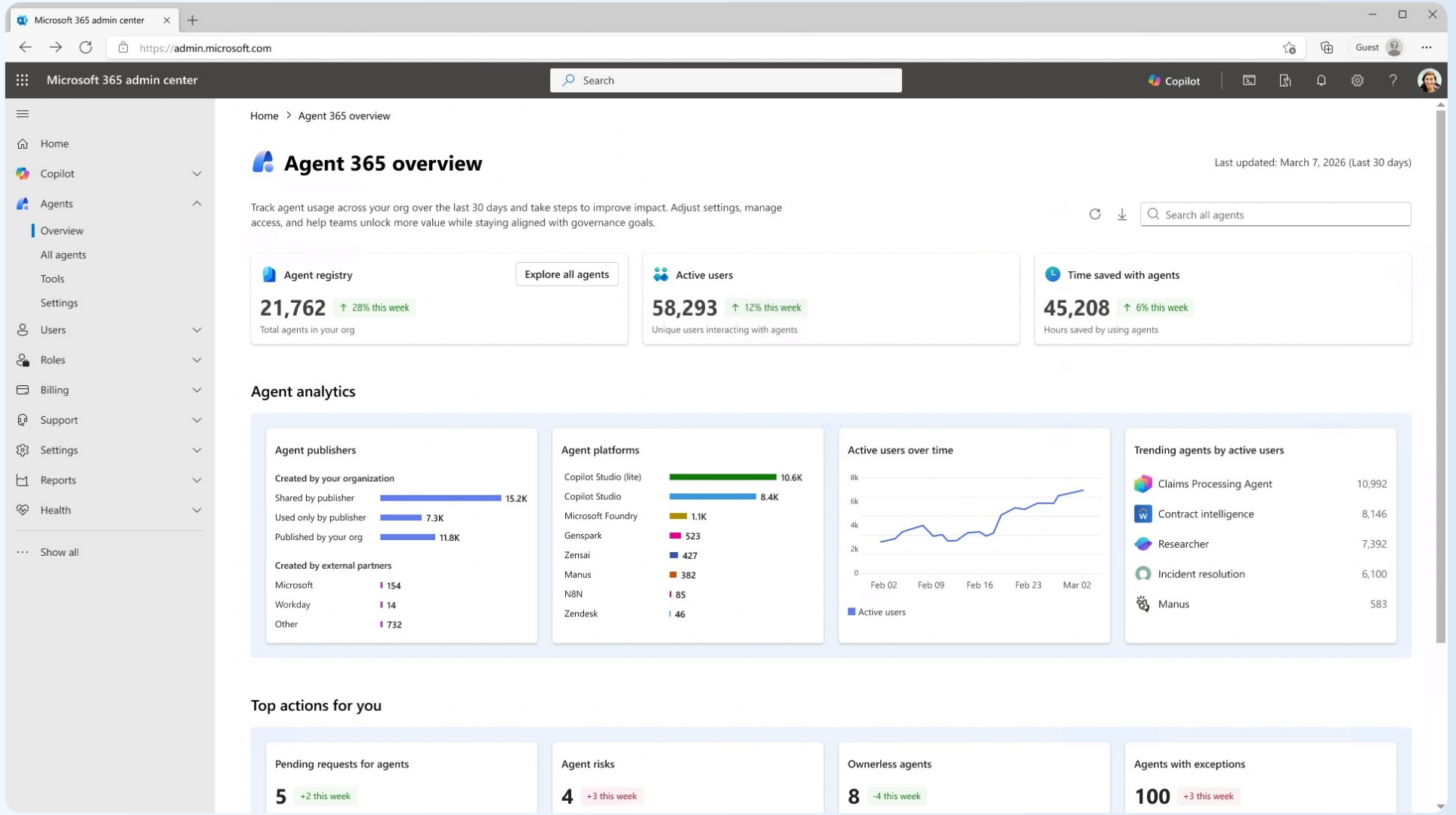
Protect against prompt-based injection attacks



Start secure

Stay secure

Demo: Defend against AI threats and vulnerabilities



AI regulations are emerging across all regions

AI laws expanding across 50+ countries and regions

Organizations must prove AI safety, security, and transparency

Compliance has become the foundation of trust and resilience

Microsoft’s view: AI innovation and regulation aren’t opposites — they must advance together.

Microsoft Purview Compliance Manager

What’s new

AI-powered regulatory templates

- Helps CISOs, Risk, Legal, Compliance, and IT leaders.
- Turns overwhelming regulation into clear, actionable priorities
- Applies across Microsoft Foundry and other services to access agent compliance posture

Home
Solutions
Learn
Settings
Compliance Manager
Compliance Manager
Overview
Improvement actions
Solutions
Assessments
Regulations
Policies
Alerts
Reports
Related Solutions
Data Lifecycle Management
Data Loss Prevention

Regulations

Review the list of regulations available to your organization. you can create assessments for specific regulations to track your compliance against them. Learn more about regulations

Free regulation licenses used 1/3

Purchased regulation licenses used 0/25

Create new template | Customize template | 395 Items | Search | Group by

Service: Any | Role type: Any | Created by: Any | Activation: Any | Availability: Any | Status: Any

Regulations	Status	Availability	Created by	Last updated date	Overarching regulation	Created date
Sub-Service Compliance Readiness (4)						
PCI DSS v4.0	Ready to use	Pre-Deployment	Microsoft	10/7/2023	PCI DSS	27/2/2023
System and Organization Controls (SOC) 2	Ready to use	Pre-Deployment	Microsoft	10/7/2023	System and Organization	27/2/2023
ISO/IEC 27001:2013	Ready to use	Pre-Deployment	Microsoft	10/7/2023	ISO/IEC 27001:2013	27/2/2023
NIST 800-53 rev.4	Ready to use	Pre-Deployment	Microsoft	10/7/2023	NIST 800-53	28/2/2023
Included templates (6)						
Data Protection Baseline	Ready to use	Included	Microsoft	10/7/2023	Data protection baselines	10/2/2023
AI Baseline	Ready to use	Included	Microsoft	29/10/2025	AI baseline	10/10/2025
NIST AI RMF - Custom template	Draft	Included	Cassandra Dunn	5/11/2025	EU Artificial Intelligence Act	5/11/2025
Premium AI templates (4)						
NIST AI Risk Management Framework (RM...	Ready to use	Premium AI	Microsoft	3/10/2025	NIST AI Risk Management Fram...	27/3/2024
ISO/IEC 23894:2023	Ready to use	Premium AI	Microsoft	3/10/2025	ISO/IEC 23894:2023	25/4/2024

Overview | Microsoft Purview

https://purview.microsoft.com/compliancemanager/templatespage?tid=da73347b-6831-4955-9394-095812d69c93

Microsoft Purview

Home
Solutions
Learn
Settings
Compliance Manager

Compliance Manager
Overview
Improvement actions
Solutions
Assessments
Regulations
Policies
Alerts
Reports

Related Solutions
Data Lifecycle Management
Data Loss Prevention

Regulations

Review the list of regulations available to your organization. you can create assessments for specific regulations to track your compliance against them. Learn more about regulations

Create new template | Customize template

Service: Any | Role type: Any | Created by: Any | Activation: Any | Availability: Any | Status: Any

Regulations	Status	Availability	Created by
Sub-Service Compliance Readiness (4)			
PCI DSS v4.0	Ready to use	Pre-Deployment	Microsoft
System and Organization Controls (SOC) 2	Ready to use	Pre-Deployment	Microsoft
ISO/IEC 27001:2013	Ready to use	Pre-Deployment	Microsoft
NIST 800-53 rev.4	Ready to use	Pre-Deployment	Microsoft
Included templates (6)			
Data Protection Baseline	Ready to use	Included	Microsoft
AI Baseline	Ready to use	Included	Microsoft
NIST AI RMF - Custom template	Draft	Included	Cassandra Dunn
Premium AI templates (4)			
NIST AI Risk Management Framework (RM...	Ready to use	Premium AI	Microsoft
ISO/IEC 23894:2023	Ready to use	Premium AI	Microsoft
ISO/IEC 42001:2023	Ready to use	Premium AI	Microsoft
Content	Content	Content	Content

Create custom template

Create editable templates quickly by uploading your own regulation document or by starting fresh with a blank template. Learn more

Use your own document

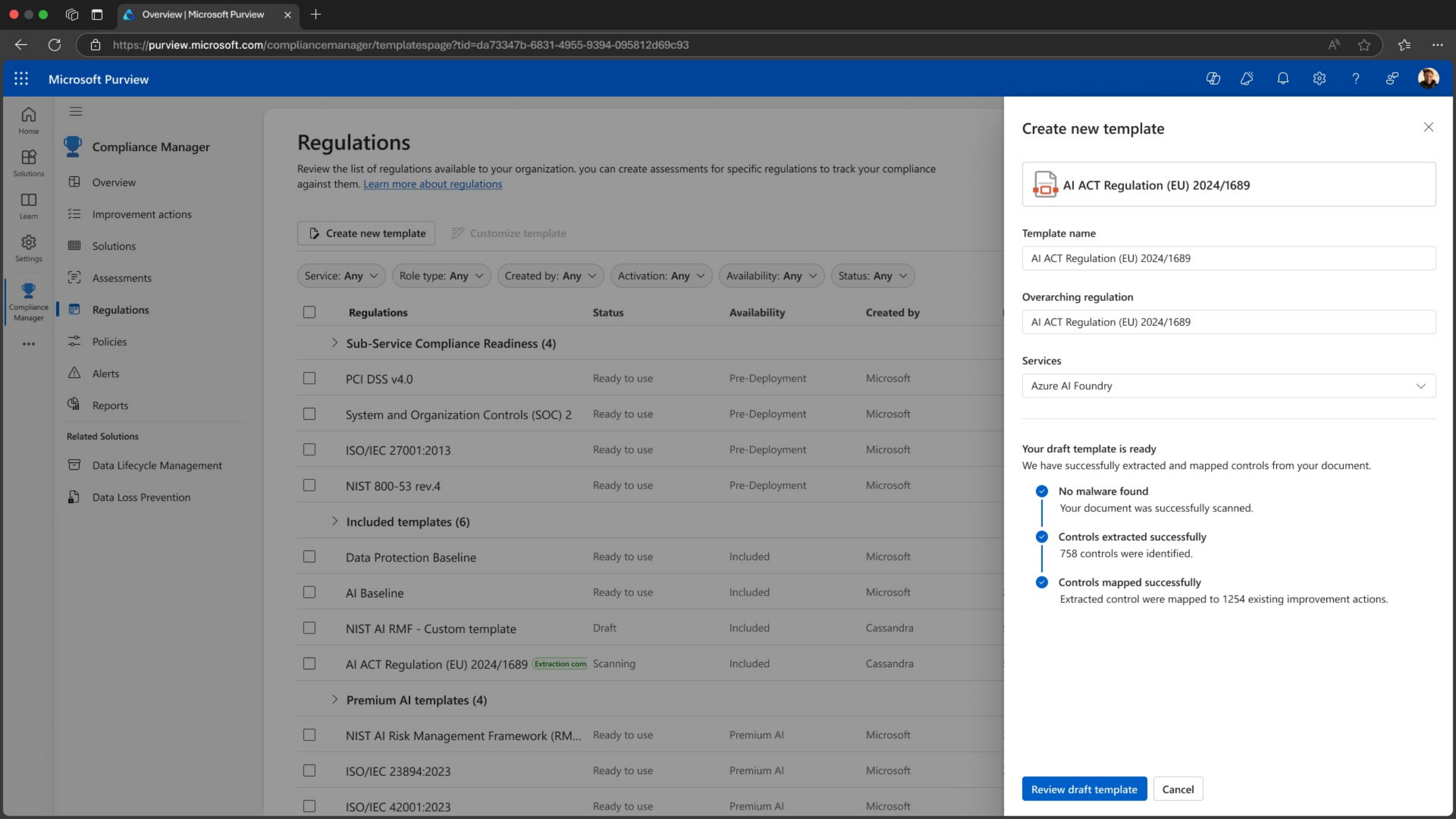
Your file will go through three steps: **Scan for malware > Extract controls > Map controls to existing improvement actions.**
This process may take several minutes depending on file size.

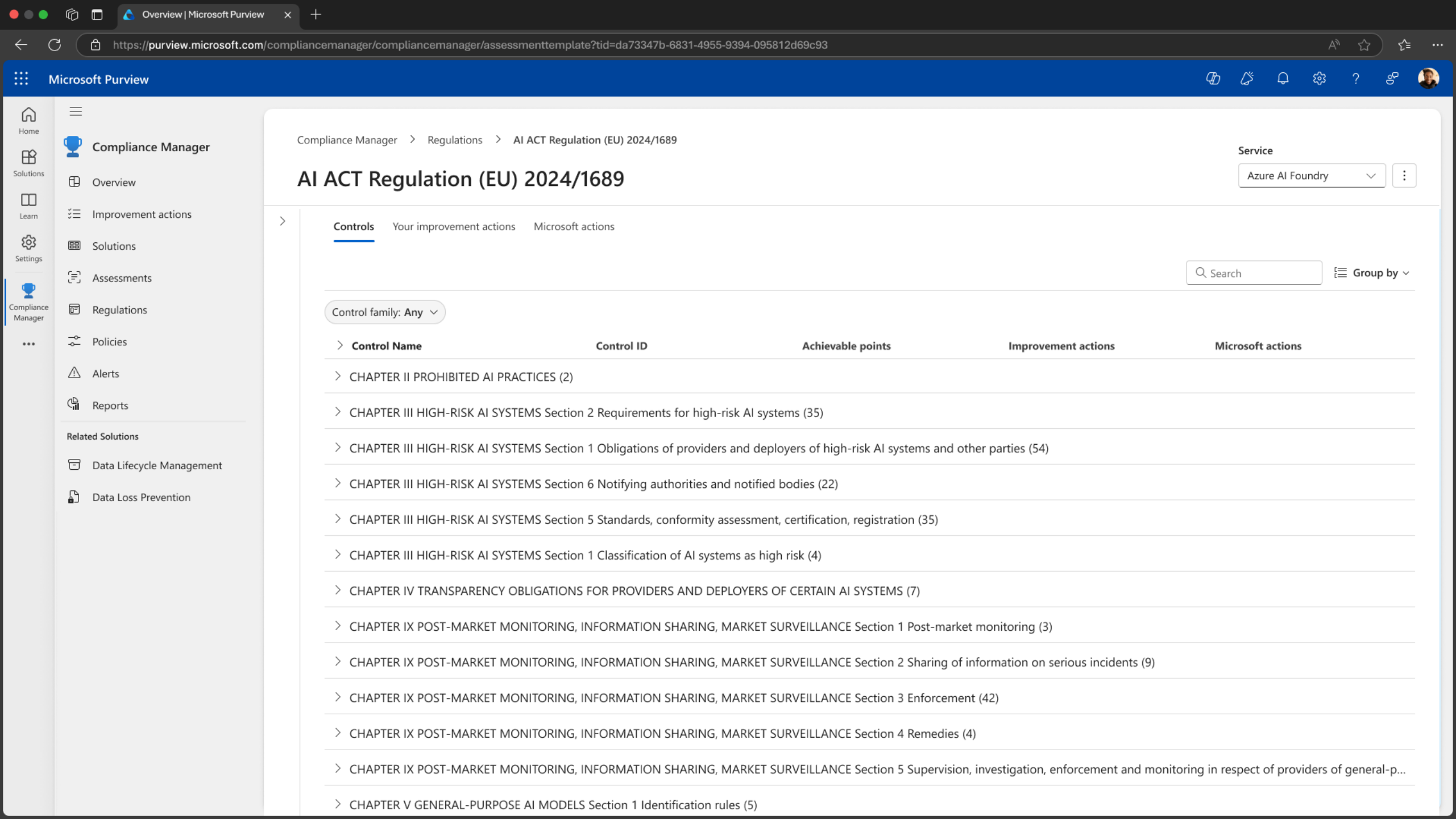
Upload PDF document

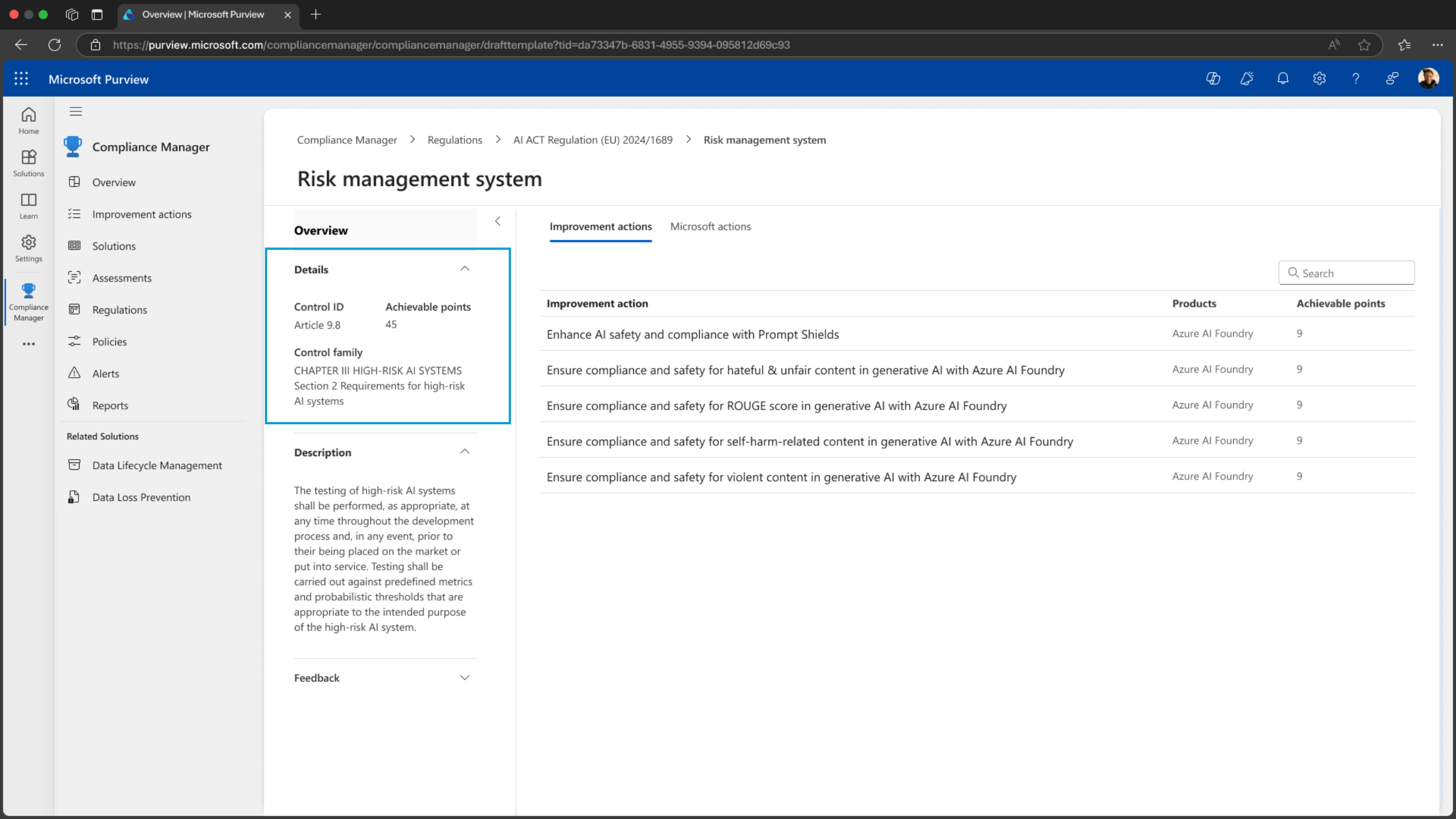
Start from blank template

Begin with a blank template and define your controls manually.

Create blank template


Overview | Microsoft Purview
https://purview.microsoft.com/compliancemanager/templatespage?tid=da73347b-6831-4955-9394-095812d69c93
Microsoft Purview
Home
Solutions
Learn
Settings
Compliance Manager
Compliance Manager
Overview
Improvement actions
Solutions
Assessments
Regulations
Policies
Alerts
Reports
Related Solutions
Data Lifecycle Management
Data Loss Prevention
Regulations
Review the list of regulations available to your organization. you can create assessments for specific regulations to track your compliance against them. Learn more about regulations
Create new template
Customize template
Service: Any
Role type: Any
Created by: Any
Activation: Any
Availability: Any
Status: Any
Regulations
Status
Availability
Created by
Sub-Service Compliance Readiness (4)
PCI DSS v4.0 Ready to use Pre-Deployment Microsoft
System and Organization Controls (SOC) 2 Ready to use Pre-Deployment Microsoft
ISO/IEC 27001:2013 Ready to use Pre-Deployment Microsoft
NIST 800-53 rev.4 Ready to use Pre-Deployment Microsoft
Included templates (6)
Data Protection Baseline Ready to use Included Microsoft
AI Baseline Ready to use Included Microsoft
NIST AI RMF - Custom template Draft Included Cassandra
AI ACT Regulation (EU) 2024/1689 Extraction com Scanning Included Cassandra
Premium AI templates (4)
NIST AI Risk Management Framework (RM... Ready to use Premium AI Microsoft
ISO/IEC 23894:2023 Ready to use Premium AI Microsoft
ISO/IEC 42001:2023 Ready to use Premium AI Microsoft
Create new template
AI ACT Regulation (EU) 2024/1689
Template name
AI ACT Regulation (EU) 2024/1689
Overarching regulation
AI ACT Regulation (EU) 2024/1689
Services
Azure AI Foundry
Your draft template is ready
We have successfully extracted and mapped controls from your document.
No malware found
Your document was successfully scanned.
Controls extracted successfully
758 controls were identified.
Controls mapped successfully
Extracted control were mapped to 1254 existing improvement actions.
Review draft template
Cancel


Overview | Microsoft Purview
https://purview.microsoft.com/compliancemanager/compliancemanager/assessmenttemplate?tid=da73347b-6831-4955-9394-095812d69c93
Microsoft Purview
Home
Solutions
Learn
Settings
Compliance Manager
Compliance Manager
Overview
Improvement actions
Solutions
Assessments
Regulations
Policies
Alerts
Reports
Related Solutions
Data Lifecycle Management
Data Loss Prevention
Compliance Manager > Regulations > AI ACT Regulation (EU) 2024/1689
AI ACT Regulation (EU) 2024/1689
Service
Azure AI Foundry
Controls
Your improvement actions
Microsoft actions
Search
Group by
Control family: Any
Control Name
Control ID
Achievable points
Improvement actions
Microsoft actions
CHAPTER II PROHIBITED AI PRACTICES (2)
CHAPTER III HIGH-RISK AI SYSTEMS Section 2 Requirements for high-risk AI systems (35)
CHAPTER III HIGH-RISK AI SYSTEMS Section 1 Obligations of providers and deployers of high-risk AI systems and other parties (54)
CHAPTER III HIGH-RISK AI SYSTEMS Section 6 Notifying authorities and notified bodies (22)
CHAPTER III HIGH-RISK AI SYSTEMS Section 5 Standards, conformity assessment, certification, registration (35)
CHAPTER III HIGH-RISK AI SYSTEMS Section 1 Classification of AI systems as high risk (4)
CHAPTER IV TRANSPARENCY OBLIGATIONS FOR PROVIDERS AND DEPLOYERS OF CERTAIN AI SYSTEMS (7)
CHAPTER IX POST-MARKET MONITORING, INFORMATION SHARING, MARKET SURVEILLANCE Section 1 Post-market monitoring (3)
CHAPTER IX POST-MARKET MONITORING, INFORMATION SHARING, MARKET SURVEILLANCE Section 2 Sharing of information on serious incidents (9)
CHAPTER IX POST-MARKET MONITORING, INFORMATION SHARING, MARKET SURVEILLANCE Section 3 Enforcement (42)
CHAPTER IX POST-MARKET MONITORING, INFORMATION SHARING, MARKET SURVEILLANCE Section 4 Remedies (4)
CHAPTER IX POST-MARKET MONITORING, INFORMATION SHARING, MARKET SURVEILLANCE Section 5 Supervision, investigation, enforcement and monitoring in respect of providers of general-p...
CHAPTER V GENERAL-PURPOSE AI MODELS Section 1 Identification rules (5)


Overview | Microsoft Purview
https://purview.microsoft.com/compliancemanager/compliancemanager/drafttemplate?tid=da73347b-6831-4955-9394-095812d69c93
Microsoft Purview
Home
Solutions
Learn
Settings
Compliance Manager
Compliance Manager
Overview
Improvement actions
Solutions
Assessments
Regulations
Policies
Alerts
Reports
Related Solutions
Data Lifecycle Management
Data Loss Prevention
Compliance Manager > Regulations > AI ACT Regulation (EU) 2024/1689 > Risk management system
Risk management system
Overview
Details
Control ID
Article 9.8
Achievable points
45
Control family
CHAPTER III HIGH-RISK AI SYSTEMS
Section 2 Requirements for high-risk AI systems
Description
The testing of high-risk AI systems shall be performed, as appropriate, at any time throughout the development process and, in any event, prior to their being placed on the market or put into service. Testing shall be carried out against predefined metrics and probabilistic thresholds that are appropriate to the intended purpose of the high-risk AI system.
Feedback
Improvement actions
Microsoft actions
Search
Improvement action
Products
Achievable points
Enhance AI safety and compliance with Prompt Shields
Azure AI Foundry
9
Ensure compliance and safety for hateful & unfair content in generative AI with Azure AI Foundry
Azure AI Foundry
9
Ensure compliance and safety for ROUGE score in generative AI with Azure AI Foundry
Azure AI Foundry
9
Ensure compliance and safety for self-harm-related content in generative AI with Azure AI Foundry
Azure AI Foundry
9
Ensure compliance and safety for violent content in generative AI with Azure AI Foundry
Azure AI Foundry
9

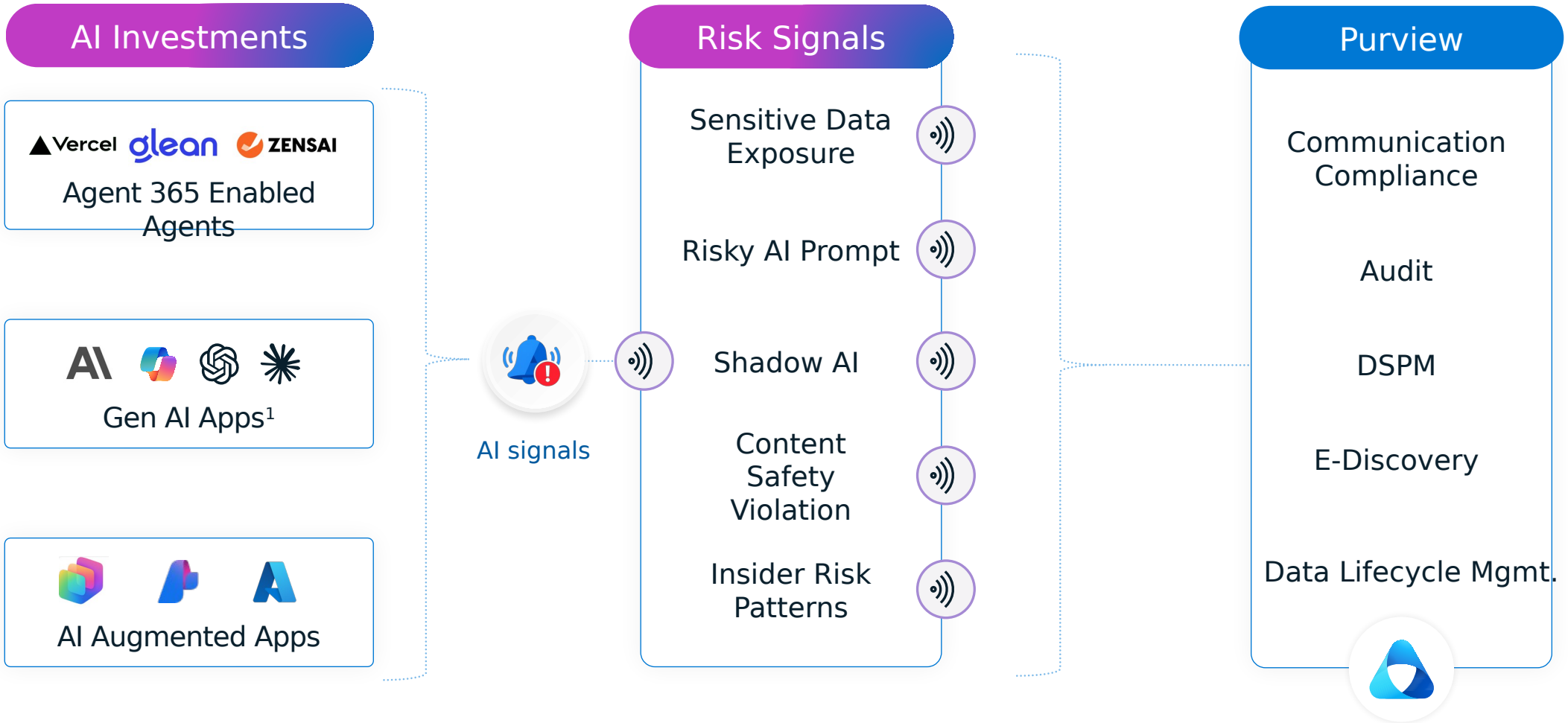
Name
Administrative Units
Type
Locations
Retention settings
Finish

Choose where to apply this policy

The policy will apply to content that's stored in the locations you choose.

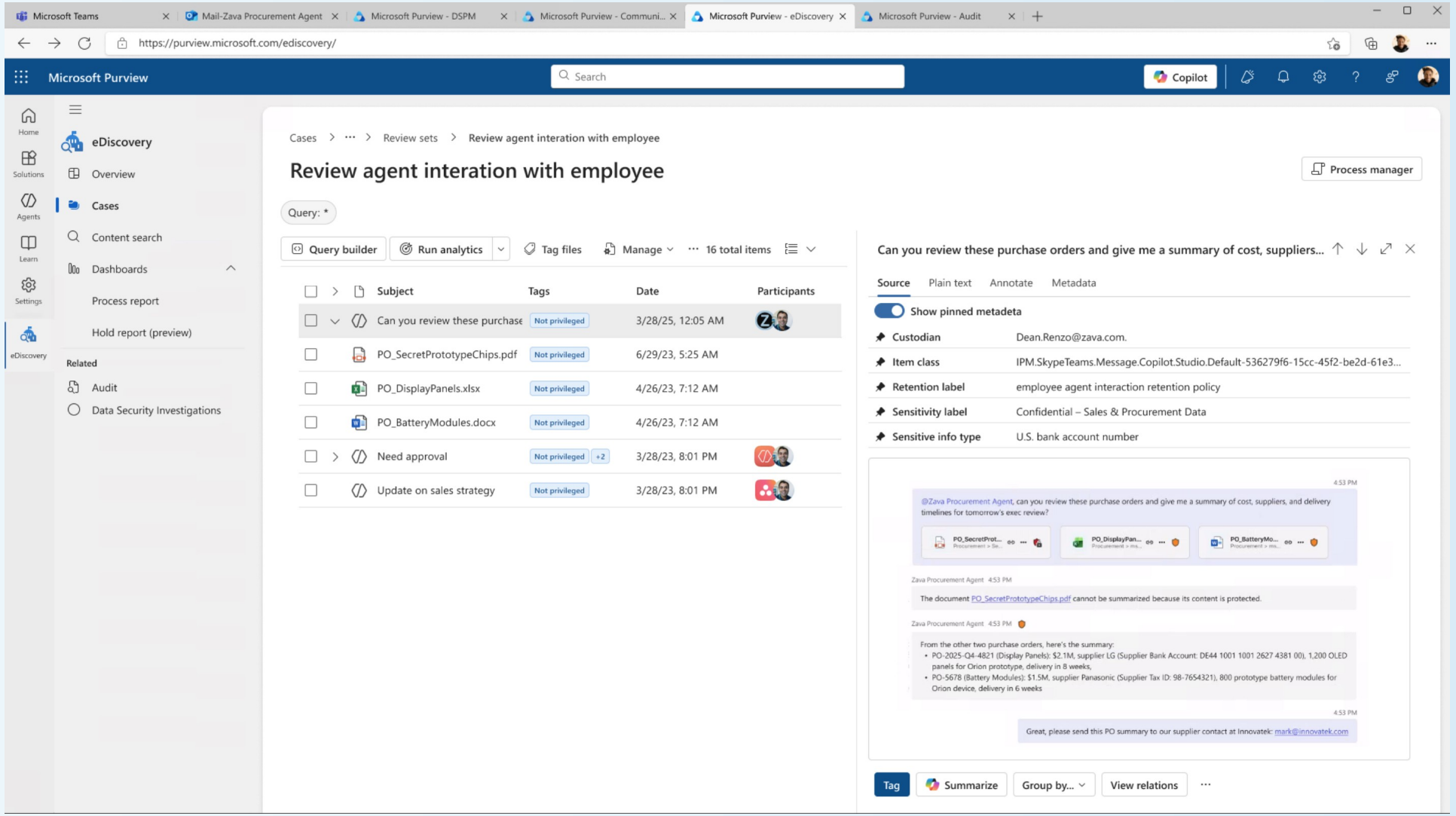
Status	Location	Applicable Content	Included	Excluded
Off	Teams channel messages	Messages from channel conversations and channel meetings. Doesn't apply to Teams private channel messages. More details		
Off	Teams chats	Messages from individual chats, group chats, meeting chats, bot chats. More details		
Off	Teams private channel messages	Messages from Teams private channels. More details		
Off	Yammer community messages	Messages from Yammer community discussions. More details		
Off	Yammer user messages	Private messages and community message notifications. More details		
On	Microsoft Copilot experiences (Preview)	Built-in and custom Copilot experiences. Learn more	All users Edit	None Edit
Off	Enterprise AI apps (Preview)	Non-Copilot AI apps that are onboarded or connected to your org using methods like Entra registration and data connectors. Learn more		
Off	Other AI apps (Preview)	AI Apps users interact with through a browser. These apps are categorized as "Generative AI" in the Defender for Cloud		

Enable GenAI-related compliance signals



[1]Signals dependent on Purview network and browser-based support; scoped to sensitive data exposure, risky AI prompt, shadow AI

Demo: Purview to govern agents

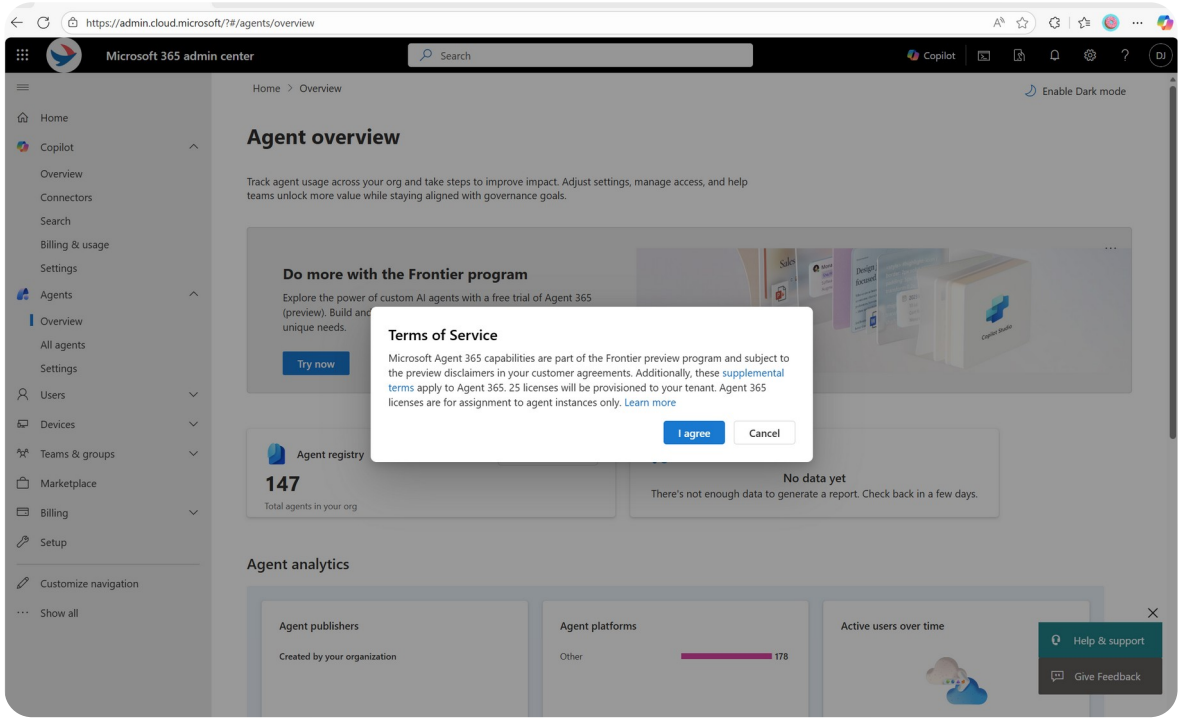


The best way to manage agents is to extend infrastructure you use for managing users.

- Microsoft 365 Admin Center
- Microsoft Defender
- Microsoft Entra
- Microsoft Intune
- Microsoft Purview

Get started with Agent 365

- As an admin, go to admin.microsoft.com
- If you're already enrolled in the Frontier program, click "Try now" on the Agent overview page and accept terms.
- If not already in the Frontier program, select Copilot > select Settings > under User access, select Copilot Frontier > choose the groups to grant access.



Learn more

Overview
aka.ms/agent365

Documentation
aka.ms/agent365docs

Blog
aka.ms/agent365blog

Secure and Govern Microsoft 365 Copilot

A Foundational Deployment Guide

Remediate Oversharing

- Identify high-risk sites and content
- Apply interim Copilot protections
- Fix access and permissions

Set up Guardrails

- Establish secure defaults
- Establish secure guardrails
- Continuously enforce & optimize guardrails

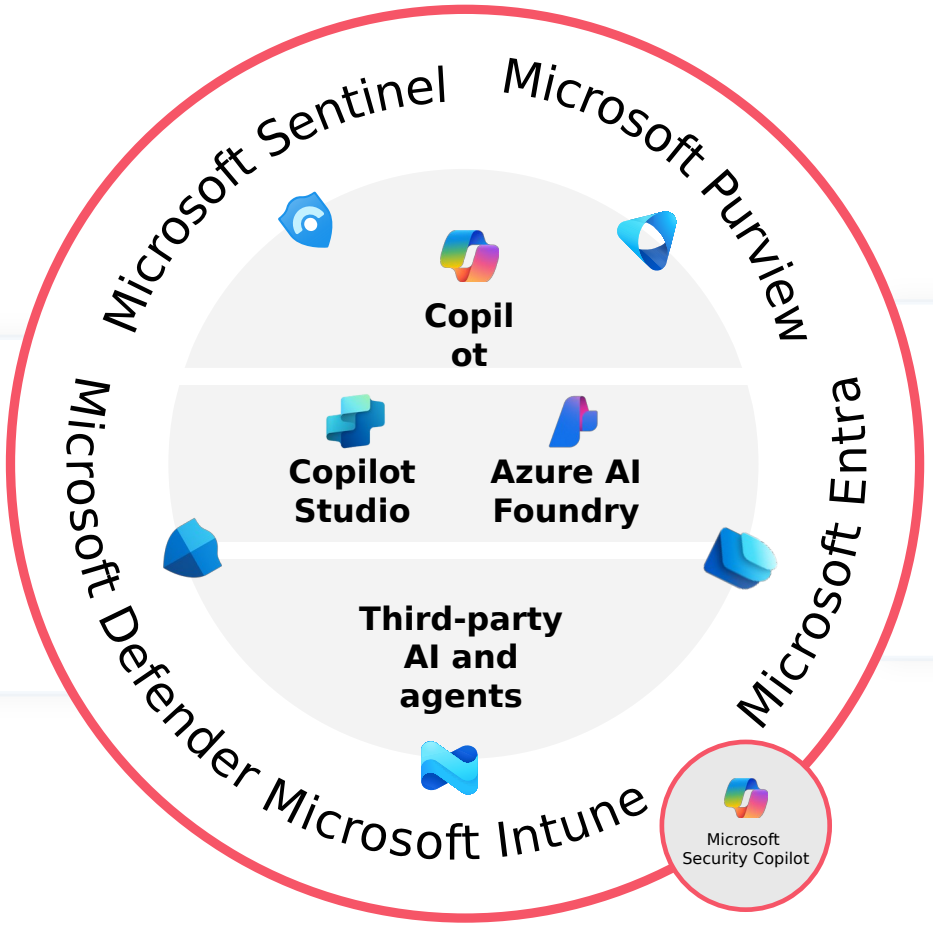
Meet Regulations

- Identify and address gaps against AI Regulations
- Define Regulatory Requirements
- Improve data hygiene

Download the blueprint at
aka.ms/Copilot/SecureGovern

Microsoft Security AI-first end to end platform

100T daily threat signals[1]
Among the largest volume + diversity [2]

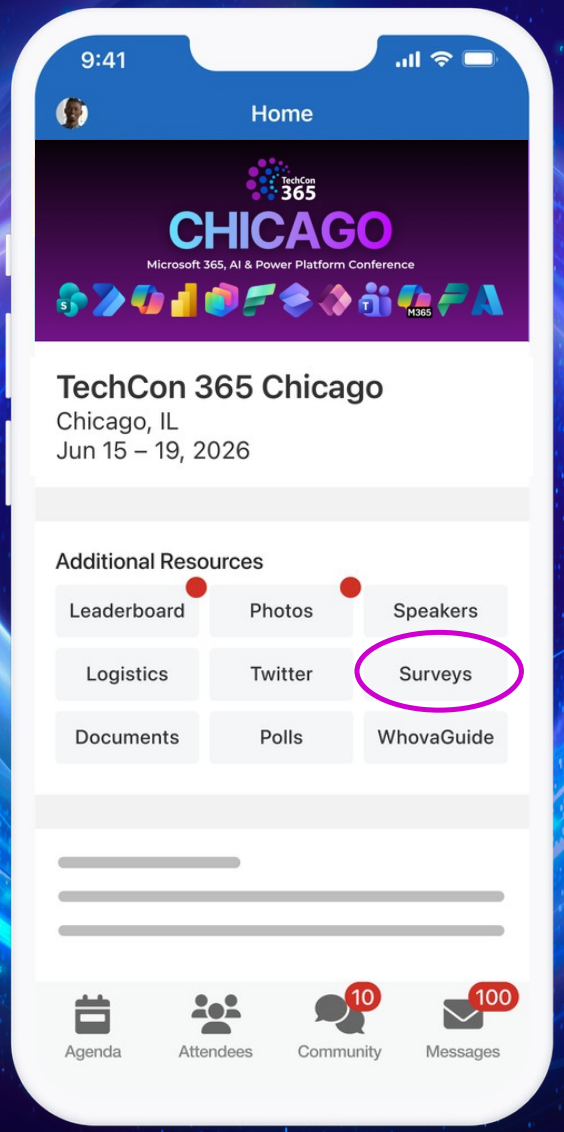


1.5 million customers[3]
Supported through services
Professional | Managed | Technical support

1 Based on Microsoft internal data. Accurate as of July 2025
2 Based on publicly available information as of July 2025
3Microsoft FY25 Fourth Quarter Earnings Conference Call, Jonathan Neilson, Satya Nadella, Amy Hood. July 30, 2025

Together we can empower the future we imagin

How was the session?



Search for Whova in the App Store or Google Play

Fill out the Session Surveys in the TechCon 365 Chicago Event App and be eligible to **WIN PRIZES!**

Thank you

Questions?

#TechCon365 • Chicago 2026

Agent 365 Placemat (1 of 2)

A365 provides enterprises observability, security, and governance for AI agents

Value pillar	Product Surface	Feature Name	Feature Description	Included with Microsoft cloud subscription[1]	Agent 365 $15 pupm
Observability	Entra	Agent Identity	Agent Identity[2]	•	•
		Agent Registry	Visibility into rich agent metadata, permissions and access, security and compliance[4]	•	•
	MAC[3]	Basic agent usage insights	Basic usage insights for agents used in M365 Copilot (active users and response count) in MAC agent usage report	•	•
		Advanced agent usage insights	Advanced agent usage insights for all agents across Agent Registry, Agent Overview page, and Agent card		•
		Agent Map	Visual representation of agent connections, usage, behavior, and relationships across the tenant		•
		Registry sync	Synchronize agents and agent metadata from external platforms that aren't managed by Agent 365 into the Agent 365 registry[6]		•
		Graph API	Graph API provides access to agent registry, basic metadata and governance actions.[6]		•
Governance	Entra	Agent Identity Governance	Access packages for agents to define scope of agent permissions[7]		•
		Lifecycle management for agents	Built-in Entra lifecycle policies automate sponsor-driven workflows to maintain accountability		•
	MAC[3]	Admin agent governance actions	Admin agent governance actions (publish, deploy, block, delete, approve, assign agents to specific user/groups, reassign agent owner, pin, etc.)	•	•
		Automate agent lifecycle actions	Automate agent lifecycle actions using conditions-based rules[8]		•
		Tool controls for agents	Control which tools (including Microsoft MCP servers) agents can access tenant-wide		•
		Policy templates for agents	Policy templates to apply consistent security and compliance controls to agents		•
	Purview	Audit logs and eDiscovery for agent activity	Audit logs of agent activities and eDiscovery (content search)[9] of agent interaction to export and hold for legal, regulatory and investigative needs	•	•
		Data Lifecyle Management for agent data and interactions	Data Lifecyle Management for agent generated data and interactions in line with regulations and org policies		•
		Communication Compliance for agents	Detect and review non-compliant agent interactions, extend compliance manager to agents to assess, manage, and demonstrate AI compliance		•

1. Included with Microsoft 365 and Azure subscription except for where noted, Microsoft 365 E5 required
2. Agent ID is a feature of the Entra platform and is needed for policies, governance, and security protection including ATG configuration
3. Available for agents with delegated access and agents with their own access operating behind the scenes. Please refer to the Microsoft 365 public roadmap for GA timeline for agents with their own access and that participate in team workflows.
4. Unified Agent Registry powers agent inventories in Defender, Purview
5. Dependent on user having Intune as part of Microsoft 365 E5
6. Currently in public preview and will be Included in the existing A365 license. Refer to the Microsoft 365 public roadmap for the GA timeline
7. Dependent on user having Entra P1 or Microsoft 365 E3
8. Bulk reassignment of ownerless agents built in Agent Builder and bulk deployment of Microsoft-built agents will GA on May 1. Additional standard rules and customizable rules coming post GA.
9. Only content search is included with Microsoft Cloud subscription. Post discovery data export and hold is charged to the
11. For delegated access flows, depends on user having Entra P1 or Microsoft 365 E3 to support conditional access for user's agents
12. For delegated access flows, depends on user having Entra P2, Microsoft 365 E5, or Entra Suite to support Identity Protection for user's agents
13. Using network capabilities inclusive of threat intelligence filtering, Web and URL filtering, prompt injection protection, and network file filtering
14. Applicable to agents running on Entra registered devices with a Global Secure Access client installed.
15. Discovery and blocking of unsanctioned local agents on endpoints are included in Microsoft 365 E5 subscription, and for customers that have deployed Microsoft Defender for Endpoint and Intune, it can be managed through the Agent 365 experience in Microsoft 365 Admin Center or through Defender and Intune portals.
16. Endpoint features expected to be in Public Preview in June.
17. Defender features listed here are currently in public preview and will be included in the existing A365 license. Please refer to the Microsoft 365 public roadmap for the GA timeline

Agent 365 Placemat (2 of 2)

A365 provides enterprises observability, security, and governance for AI agents

Value pillar	Product Surface	Feature Name	Feature Description	Included with Microsoft cloud subscription[1]	Agent 365 $15 pupm
Security	Purview	Data Security Posture Management for agents	Data Security Posture Management with AI Observability provides deep interaction visibility for Agents		•
		Insider Risk Management for agents	Extend Insider Risk Management to agents – detect anomalous and risky agent activities		•
		Agents inherit and honor data sensitivity labels	Agents inherit and honor data sensitivity labels[10]		•
		Data loss prevention for agents	Data loss prevention: block agents from accessing and sharing sensitive content		•
	Entra	Conditional access and identity protection for agents	Conditional access[11] and identity protection[12] for agents (for agents with delegated access - extend user policies to agents)		•
		Secure Access Service Edge (SASE) for agents	Monitor and block malicious and non-compliant network traffic[13] for agents, operating on user devices[14] and Copilot Studio agents		•
	Intune	Device compliance for agent conditional access	Policy to require device compliance for agents' Entra Conditional Access protection[5, 11]		•
		Policy controlled environment for agents runtime	Automatic Intune enrollment[5] for Windows 365 for Agent endpoints for continuous policy configuration and enforcement		•
		Block unsanctioned local endpoint agents	Block the most common ways OpenClaw runs on Windows managed devices with Intune policies[5, 15, 16]	ME5 & ME7	ME5 & ME7
	Defender	Discovery of AI on endpoints	Sync shadow AI endpoint agents, discovered by Microsoft Defender (available with MDE P2, ME5, or ME7 only[16]	ME5 & ME7	ME5 & ME7
		Agent Security Posture Management	Identify and remediate agent misconfigurations and exposure risks, relationship mapping for local agents (agent to devices, MCPs, etc.)[17]		•
		Threat Detection and Blocking for agents	Detect suspicious agent activity, receive alerts and allow blocking for tool invocations for agents [17]		•
		Threat Hunting and Investigation for agents	Collect A365 unified agent observability logs and allows Investigation and hunting for threats in for agents[17, 18]		•

1. Included with Microsoft 365 and Azure subscription except for where noted, Microsoft 365 E5 required
2. Agent ID is a feature of the Entra platform and is needed for policies, governance, and security protection including ATG configuration
3. Available for agents with delegated access and agents with their own access operating behind the scenes. Please refer to the Microsoft 365 public roadmap for GA timeline for agents with their own access and that participate in team workflows.
4. Unified Agent Registry powers agent inventories in Defender, Purview
5. Dependent on user having Intune as part of Microsoft 365 E5
6. Currently in public preview and will be Included in the existing A365 license. Refer to the Microsoft 365 public roadmap for the GA timeline
7. Dependent on user having Entra P1 or Microsoft 365 E3
8. Bulk reassignment of ownerless agents built in Agent Builder and bulk deployment of Microsoft-built agents will GA on May 1. Additional standard rules and customizable rules coming post GA.
9. Only content search is included with Microsoft Cloud subscription. Post discovery data export and hold is charged to the
11. For delegated access flows, depends on user having Entra P1 or Microsoft 365 E3 to support conditional access for user's agents
12. For delegated access flows, depends on user having Entra P2, Microsoft 365 E5, or Entra Suite to support Identity Protection for user's agents
13. Using network capabilities inclusive of threat intelligence filtering, Web and URL filtering, prompt injection protection, and network file filtering
14. Applicable to agents running on Entra registered devices with a Global Secure Access client installed.
15. Discovery and blocking of unsanctioned local agents on endpoints are included in Microsoft 365 E5 and E7 subscriptions, and for customers that have deployed Microsoft Defender for Endpoint and Intune, it can be managed through the Agent 365 experience in Microsoft 365 Admin Center or through Defender and Intune portals.
16. Endpoint features expected to be in public preview in June.
17. Defender features listed here are currently in public preview and will be included in the existing A365 license. Please refer to the Microsoft 365 public roadmap for the GA timeline
18. Defender Threat Investigation and Hunting will require a user to be licensed for Microsoft Defender for Cloud Apps

Microsoft 365 E7: The Frontier Suite

		Microsoft 365 E5 (w/Teams)	Microsoft Entra Suite	Microsoft 365 Copilot	Microsoft Agent 365	Microsoft 365 E7 (w/Teams)
		$60[1]	$12	$30	$15	$99[2]
Productivity	**Microsoft 365 apps:** Create and refine work across the apps people know and love	•				•
	OneDrive & SharePoint: Share, manage, and collaborate on content across teams	•				•
	Teams: Meet, chat, and call	•				•
	Windows: Secure, manage, and run work across enterprise devices	•				•
	Teams Phone: Cloud-based phone system built into Teams	•				•
	Power BI Pro: Turn data into shared, actionable insights	•				•
Security & Compliance	**Entra:** Identity and access management	• P2	• Suite			• Suite
	Defender: Endpoint, email, identity, and cloud threat protection	•				•
	Purview: Data security and compliance (ex. information protection, DLP, insider risk)	•				•
	Intune: Endpoint and device management	•				•
AI	**Copilot:** AI built into core productivity apps and Teams	○		•		•
	Copilot Studio & Agent Builder: Build, deploy, and scale custom AI agents	○ Metered		•		•
	Agent flexibility: Choose from pre-built agent library or access 3P marketplace			•		•
	Work IQ: AI grounded in personal and work data (incl. 3P data via connectors)	○		•		•
Agent	**Agent 365:** Observe, monitor and manage agents in real time				•	•

1: $51.45 w/o Teams | 2. $90.45 w/o

Expertise and tools for your journey

Technical expertise via our FastTrack partners

aka.ms/Microsoft/FastTrack

Tools, resources & training on our Adoption Hub

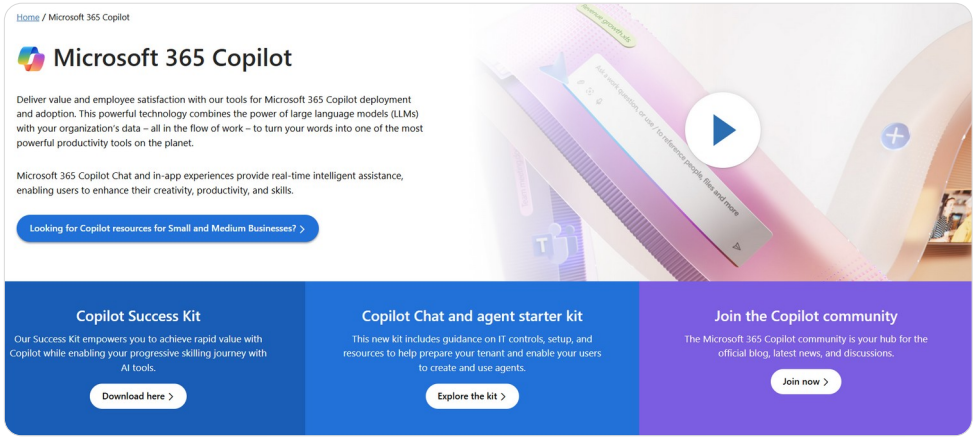
adoption.microsoft.com

Events and real-world knowledge in our **community**

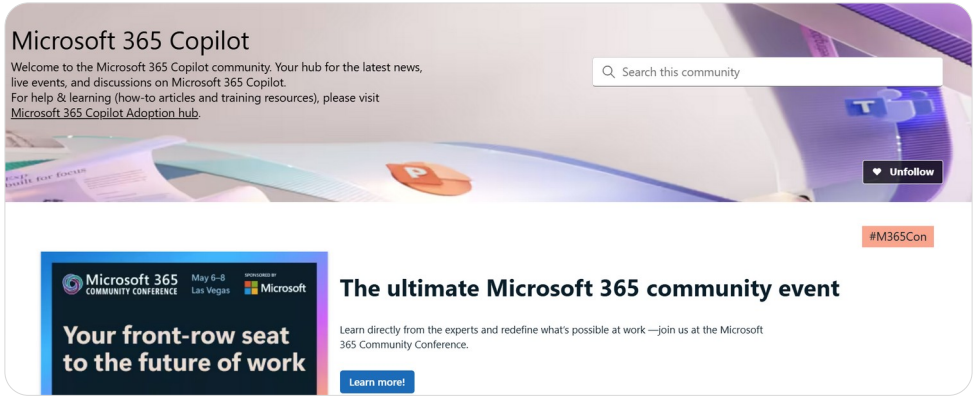
aka.ms/TechCommunity

News & community content

Microsoft Community Learning
aka.ms/Community/LearningChannel
Community led expert content on all your favorite Microsoft services.



Start your week with live news and event updates aka.ms/MondaysatMicrosoft
Watch live or on-demand & share our blog.



Stay Connected!

Engage with the best community in tech... There's something for everyone!

Microsoft Tech Community

The community platform for Microsoft 365 – forums, blogs, and events

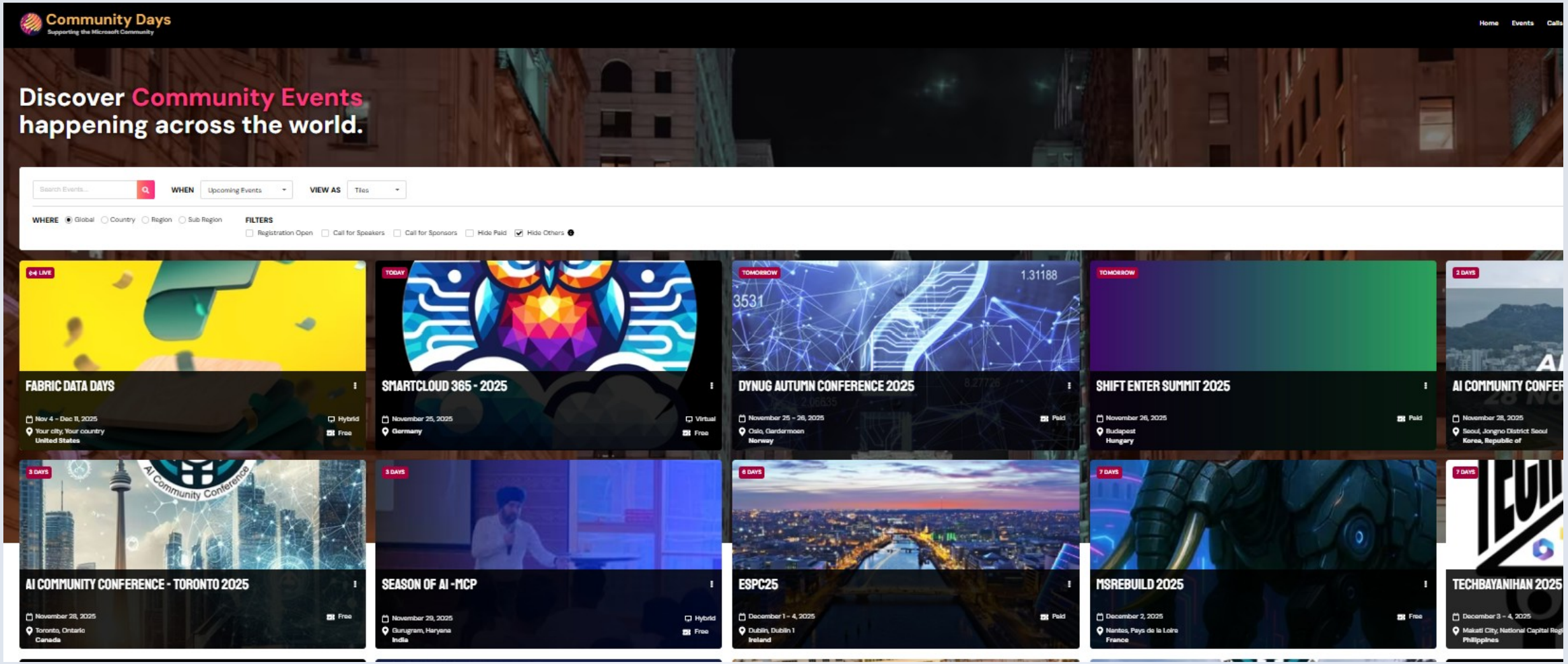
CommunityDays.org

Find or host a local event in your area
or to match your interests www.communitydays.org

Microsoft Community on LinkedIn

News, announcements and training delivered to your news feed https://aka.ms/microsoftcommunitylinkedin

The one stop shop for Microsoft ecosystem community events

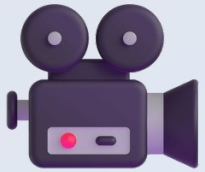


www.communitydays.org

SharePoint at 25 film: *More than Code*

In honor of SharePoint’s 25th birthday, *More Than Code* is a short film that explores the people, passion, and innovation behind one of the most transformative platforms in modern work. This film captures the stories of builders, leaders, and community champions who helped shape SharePoint into the knowledge backbone for collaboration, Copilot, and the next generation of agents.

SharePoint is more than code—it's 25 years of connection, innovation and impact.



Watch the digital premiere

Stream the documentary online globally in late April and celebrate SharePoint’s 25-year journey from anywhere.

Watch the SharePoint at 25 digital event

Prepare for the film with a special digital event featuring insights, stories, and what’s next for SharePoint in the era of AI.

[redacted]

The Microsoft Global Community Initiative (MGCI) - Empowering global Microsoft communities with the tools, training, and resources to create impactful events and amplify diverse voices.

Learn, Share, Grow.

Event producers unite!

Join MGCI today!
https://aka.ms/MGCI

Thank you to our Microsoft Most Valuable Professionals (MVP) and Regional Directors!