
ITS 2026
LEAD
INNOVATE
OPTIMIZE
CLOUD WITHOUT THE CHAOS
PRESENTED BY sherweb

Top security and governance concerns about generative AI

Data oversharing and data leaks

80%

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

Identification of risky AI use

41%

of security leaders cited that the identification of risky users based on queries into AI was one of the top AI controls they want to implement[2]

AI governance and risk visibility

84%

Want to feel more confident about managing and discovering data input into AI apps and tools[2]

1. First Annual Generative AI study: Business Rewards vs. Security Risks, Q3 2023, ISMG, N=400
2. Microsoft data security index 2024 report

Tools to secure and govern your AI use

Address oversharing concerns

- Gain visibility into overshared content
- Remediate excessive permissions
- Prevent AI from processing sensitive files

Protect against data loss and insider risks

- Get alerts and reports of risky behavior and AI use
- Protect sensitive files and interactions
- Dynamically apply security policies based on risky actions

Govern AI use to meet regulations & policies

- Inspect interaction content and audit logs
- Investigate for compliance and ethical violations
- Enforce lifecycle policies and legal holds

Secure

Govern

Tools to secure and govern your Copilot use

Address oversharing concerns

- Gain visibility into overshared content
- Remediate excessive permissions
- Prevent AI from processing sensitive files

Protect against data loss and insider risks

- Get alerts and reports of risky behavior and AI use
- Protect sensitive files and interactions
- Dynamically apply security policies based on risky actions

Govern AI use to meet regulations & policies

- Inspect interaction content and audit logs
- Investigate for compliance and ethical violations
- Enforce lifecycle policies and legal holds

Secure

Govern

Prepare data for AI by ensuring correct access to files

What is oversharing?

Copilot + Agents only access data that an individual user is authorized to access

Oversharing happens when an employee has access to information beyond what is necessary to do their job

What causes oversharing?

Accidentally saving a file to a location with broad access permissions

A user sharing content with someone who should not have access

Files do not have access protections

Gain visibility into overshared content

Identify potentially overshared sites and files

Sites and files with sensitive data

Data shared broadly

Frequently accessed data

Prioritize highest impact risks

Risk assessment

- High Risk
- Medium Risk
- Low Risk

Example

A site contains documents with credit card numbers

+

Everyone in the organization can access the site's content

+

575 unique users accessed the site's content last week

=

High Risk: Prioritize remediation

Remediate excessive permissions and apply oversharing protections

Prepare

Fix existing oversharing risks

- Restrict user and/or Copilot + Agent access to risky sites while remediating identified oversharing risks
- Act on policy suggestions to mitigate oversharing risks
- Prevent Copilot + Agents from processing certain sensitive files and from using them in responses if required
- Remove organization-wide site access as needed

Operate

Monitor for new oversharing risks

- Get notifications when new oversharing occurs with options for remediation
- Further secure sensitive data through file level access controls and Data Loss Prevention policies
- Improve Copilot+ Agent responses by archiving or deleting unneeded content

For detailed guidance see: aka.ms/Copilot/OversharingBlueprintLearn

Tools to secure and govern your Copilot use

Address oversharing concerns

- Gain visibility into overshared content
- Remediate excessive permissions
- Prevent Copilot + Agents from processing sensitive files

Protect against data loss and insider risks

- Get alerts and reports of risky behavior and AI use
- Protect sensitive files and interactions
- Dynamically apply security policies based on risky actions

Govern AI use to meet regulations & policies

- Inspect interaction content and audit logs
- Investigate for compliance and ethical violations
- Enforce lifecycle policies and legal holds

Secure | **Govern**

Protect against data loss and insider risks

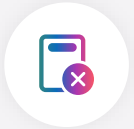
What is data loss and insider risk?

Data loss and insider risks may occur without Copilot + Agent use. The productivity benefits of these tools create opportunities for these risks to happen with less effort

Data loss is when unsafe or inappropriate sharing, transfer, or use of sensitive content occurs

Insider risk involves users misusing their authorized access to cause harm. This misuse may be intentional or unintentional

What causes data loss and insider risks?



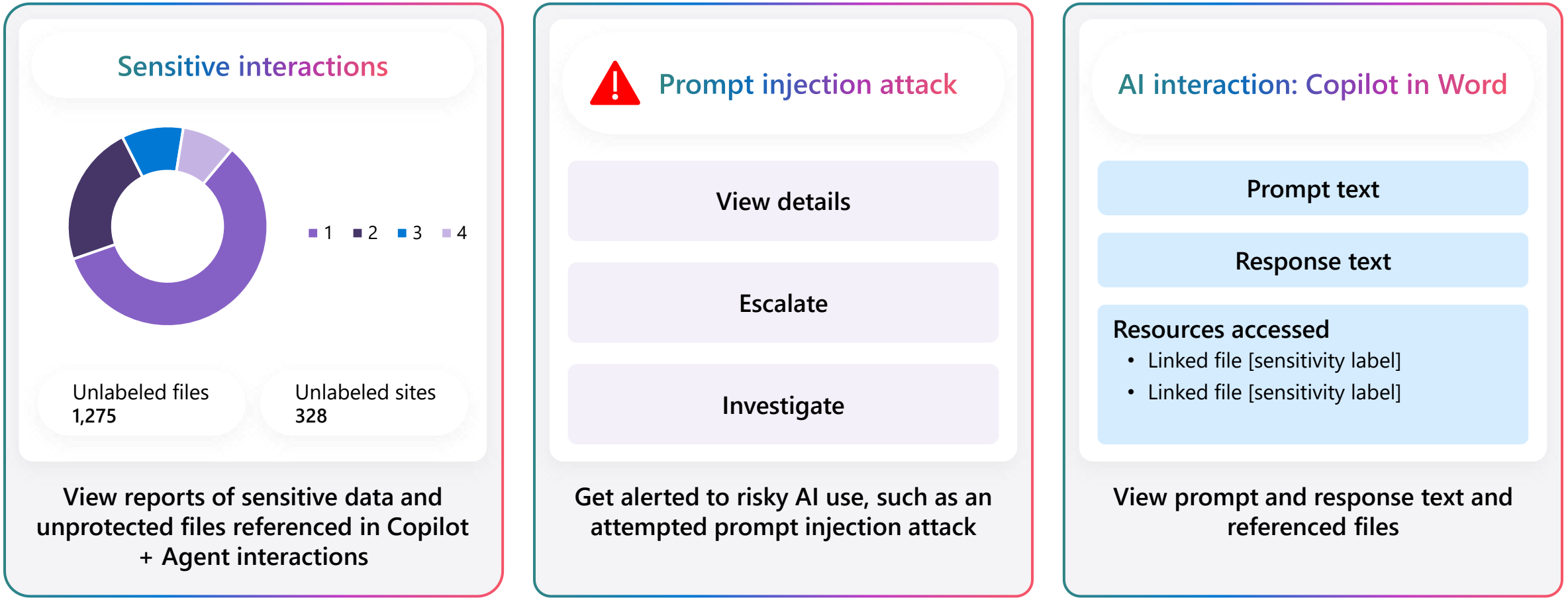
Copilot or an Agent creates documents that aren't protected by default, because the inputs weren't protected

Using Copilot or an Agent to access or summarize sensitive data in a way that violates usage guidelines

A user's credentials are compromised, and the bad actor uses Copilot or an Agent to access sensitive data

An employee has resigned, wants to keep company IP, and uses Copilot or an Agent to quickly find the most relevant content

Get alerts and reports of risky behavior and AI use



View reports of sensitive data and unprotected files referenced in Copilot + Agent interactions

Get alerted to risky AI use, such as an attempted prompt injection attack

View prompt and response text and referenced files

Proactive alerts, real time reports, and visibility to possible risks

Images for illustrative purposes only. Actual user experience may differ.

Protect sensitive files and Copilot interactions

Document contains **sensitive merger information**

Auto-label as **Mergers and acquisitions**

Detect when content contains sensitive data and auto-apply protections

Copilot, please summarize **Merger document.docx**

Here is the summary of your document…

Copilot, create a new document with this summary

Copilot response and Copilot created documents inherit sensitivity labels and protections

Admin creates policy to prevent Copilot access for files labeled as **Mergers and acquisitions**

Copilot, please summarize **Merger document.docx**

This document is currently protected, so I can't provide details about its content

Optionally, block Copilot access to sensitive files

Protect files even if they are moved or downloaded

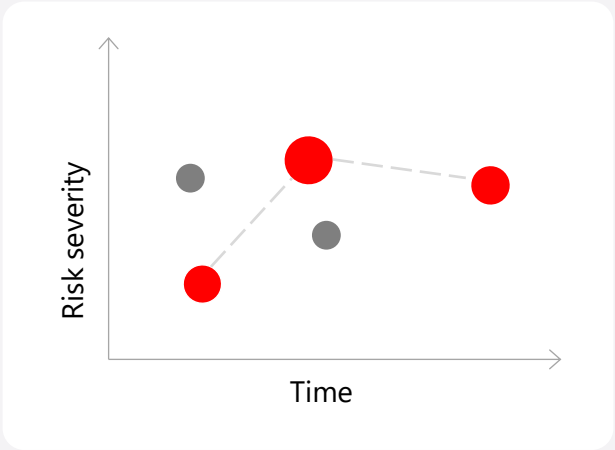
Dynamically apply security policies based on risky actions

A user performs a series of risky actions

Actions deviate from usual pattern of behavior

- Has a series of risky interactions via Copilot or an Agent
- Downloads 100s of files containing sensitive data

Identifies the sequence of events as a risky pattern



Uses AI for risk analysis

Automatically adds the user to more strict security policies

Block actions until investigated

- Can't access content in sensitive sites
- Prevent sharing or downloading content
- Block from deleting content

Balance productivity and risk mitigation

Images for illustrative purposes only. Actual user experience may differ.

Tools to secure and govern your Copilot use

Address oversharing concerns

- Gain visibility into overshared content
- Remediate excessive permissions
- Prevent Copilot + Agents from processing sensitive files

Protect against data loss and insider risks

- Get alerts and reports of risky behavior and AI use
- Protect sensitive files and interactions
- Dynamically apply security policies based on risky actions

Secure

Govern AI use to meet regulations & policies

- Inspect interaction content and audit logs
- Investigate for compliance and ethical violations
- Enforce lifecycle policies and legal holds

Govern

Govern AI use to meet regulations & policies

What is Copilot + Agent governance?

Governance supports Copilot + Agent use in adherence to your organization's policies and regulatory requirements

Governance is enforced by a set of compliance and management controls for the safe and effective use of AI

It includes the option to include interactions in existing compliance, management, and legal processes alongside other types of Microsoft 365 content

Why you need Copilot + Agent governance

Configure admin controls to support compliance with a specific AI regulatory framework, such as EU AI Act, NIST AI Risk Management Framework

Limit exposure from misuse by identifying issues early and mitigating them quickly

Increase Copilot + Agent response quality by limiting its access to outdated information

Keep or delete AI generated content according to your risk management preferences

Audit interactions, enforce lifecycle policies and legal holds

AI interaction: Copilot in Word Audit log entry

- Date/time
- User
- Detailed event data
- And more

Audit Copilot + Agent interactions to access detailed log information

Retain for 6 months then delete

Copilot interaction

Delete after 90 days

Meeting recording and transcript

Enforce retention and deletion policies for interactions and meeting recordings + transcripts

Legal hold

Include a user's Copilot and Agent prompts and responses in a legal hold

Investigate for compliance and ethical violations

Copyright violation

Insider trading

Corporate sabotage

Regulatory collusion

And more

Receive an alert if a possible compliance or ethical violation occurs and start an investigation

Perform an admin search for litigation or an investigation and include Copilot and Agent generated content

EU AI Act

NIST AI Risk Management Framework

ISO standards 42001 and 23894

Assess and track adherence to regulatory frameworks

Shadow AI

Mitigate Shadow AI risks with governance

What is Shadow AI and what are the risks?

Employees are excited to try Generative AI apps due to productivity benefits. Sometimes, they will use apps that are not sanctioned nor managed by IT

Left unchecked, sensitive data (e.g. PII, Intellectual Property) might be shared with "Shadow AI" apps, creating risk of leakage, malicious use, or use to train 3rd party algorithms

Monitoring Shadow AI can help uncover use in the business and manage security, privacy, and compliance risks

How to discover and govern Shadow AI use?

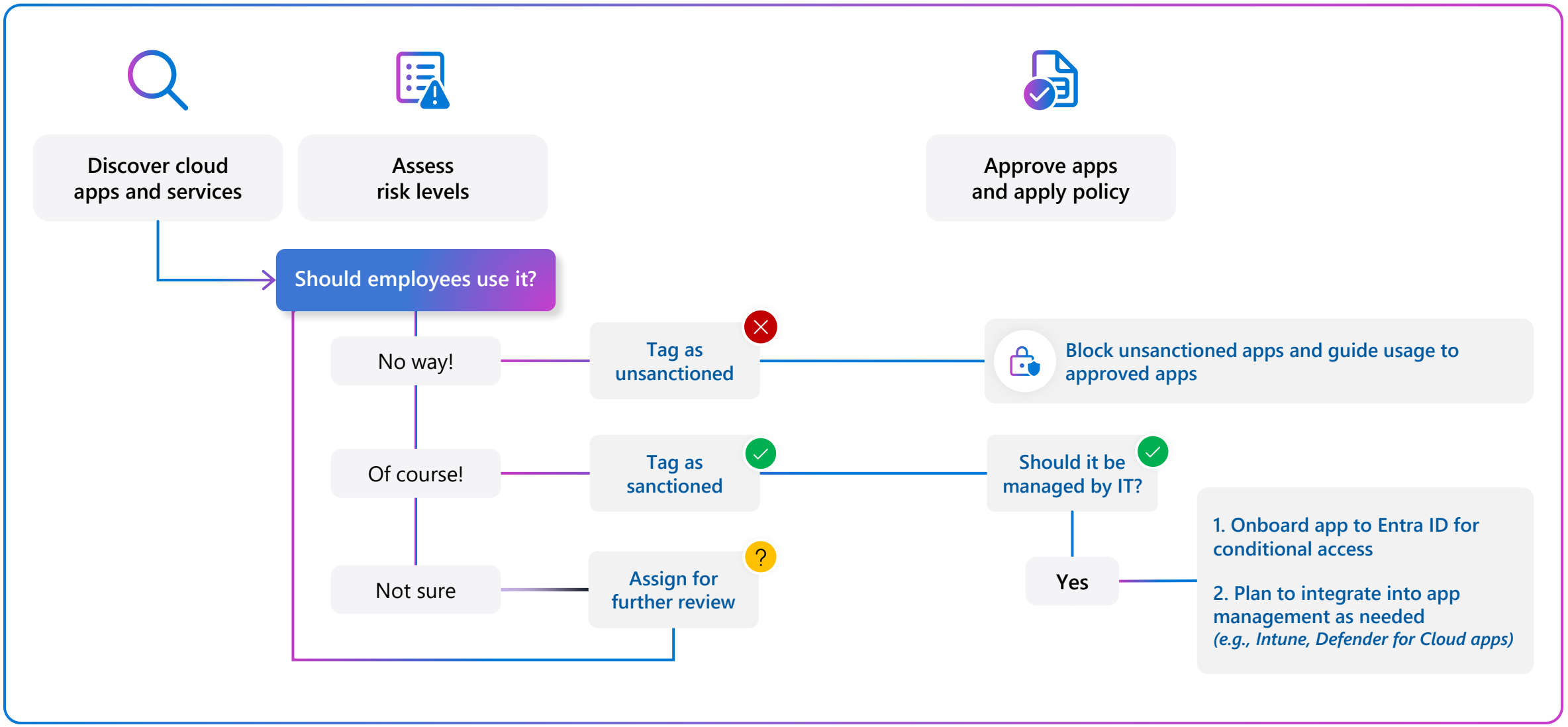
Gaining visibility on Shadow AI apps on the corporate environment (endpoints, network)

Understand the security & compliance risks of the specific cloud AI apps against a common benchmark (GDPR, SOC reports, etc)

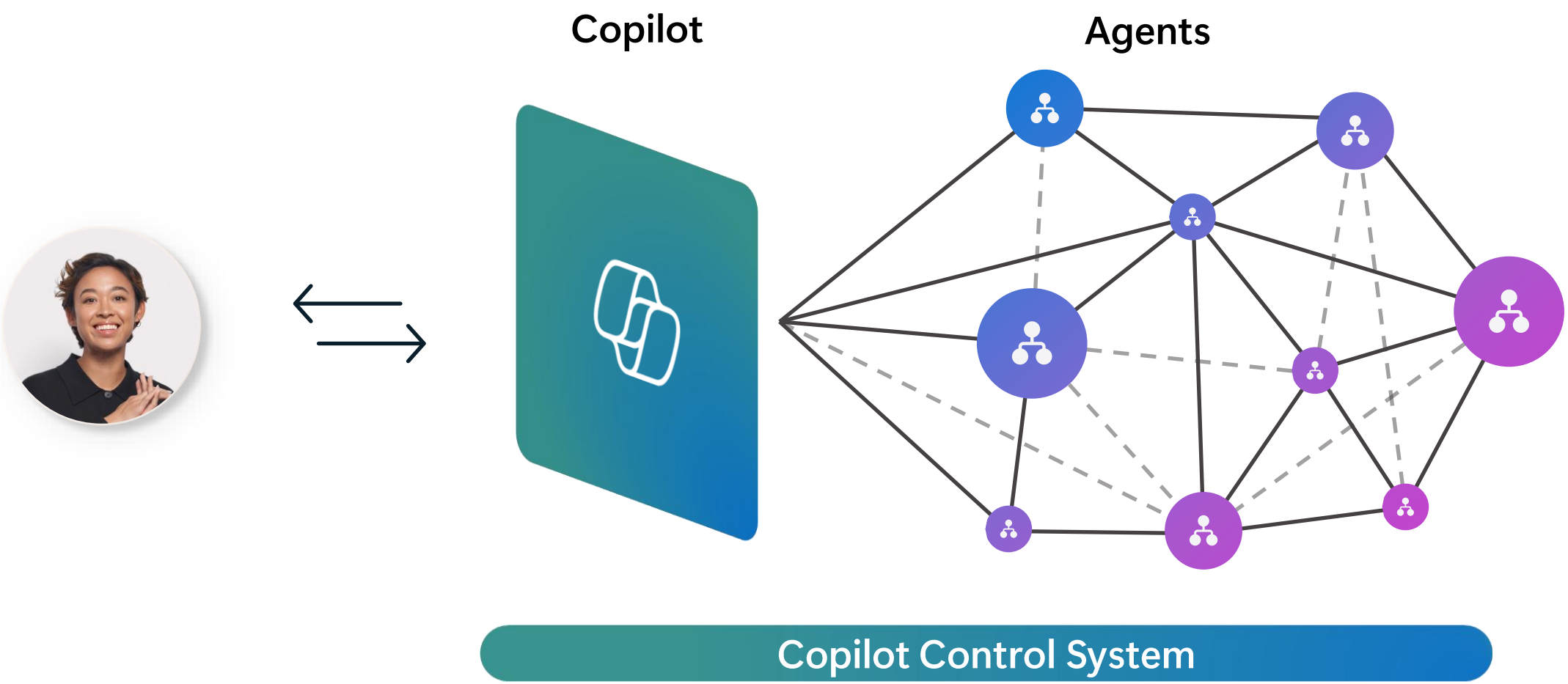
Audit & automatically block unsanctioned apps, while managing relevant apps with IT security

Enhance protection on managed apps by applying data classification best practices

Discover and manage apps in your environment



Copilot is the UI for AI




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

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[1]

Microsoft 365 Copilot is built on trust

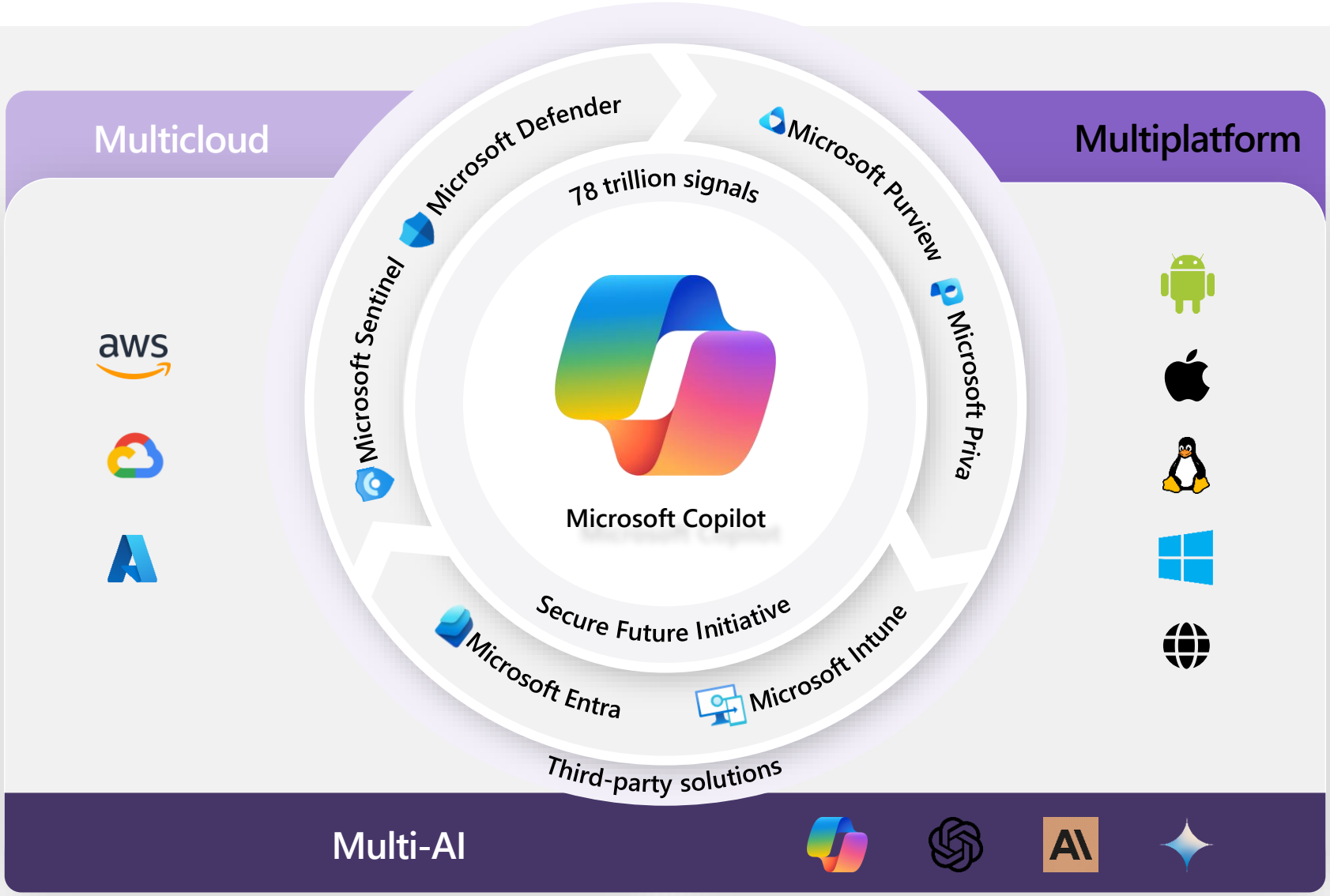
[1] Learn more about the Customer Copyright Commitment

Copilot – Compliance Certifications

● Included	Microsoft 365 Copilot & Chat
SOC2 Type 1	●
SOC2 Type 2	In Progress
ISO 27001	●
ISO 27017	●
ISO 27018	●
ISO 27701	●
ISO 9001	N/A[1]
ISO 42001	●
CSA STAR	●
GDPR	●
CCPA	●
HIPAA	●
FedRAMP High	In Progress[2]
BSI C5	●

1. Our other ISO certifications cover ISO 9001 clauses, as stated in customer-facing footnote. So far, we haven't seen customer demand for ISO 9001 certification, which focuses on quality management systems. If we see demand for ISO 9001, we can then plan and resource accordingly.
2. Microsoft 365 Copilot and Chat in the GCCH environment meet the bar of FedRAMP High controls. Microsoft is working towards FedRAMP High certification.

AI-first end-to-end security for the age of AI



Copilot Control System

Copilot + Agents

Security & Governance	Management Controls	Measurement & Reporting
Data security	Copilot licensing	Readiness and adoption
AI security	Agent lifecycle	Productivity impact
Compliance & privacy	Customization	Business value & ROI

Copilot + Agents

+

Microsoft Purview

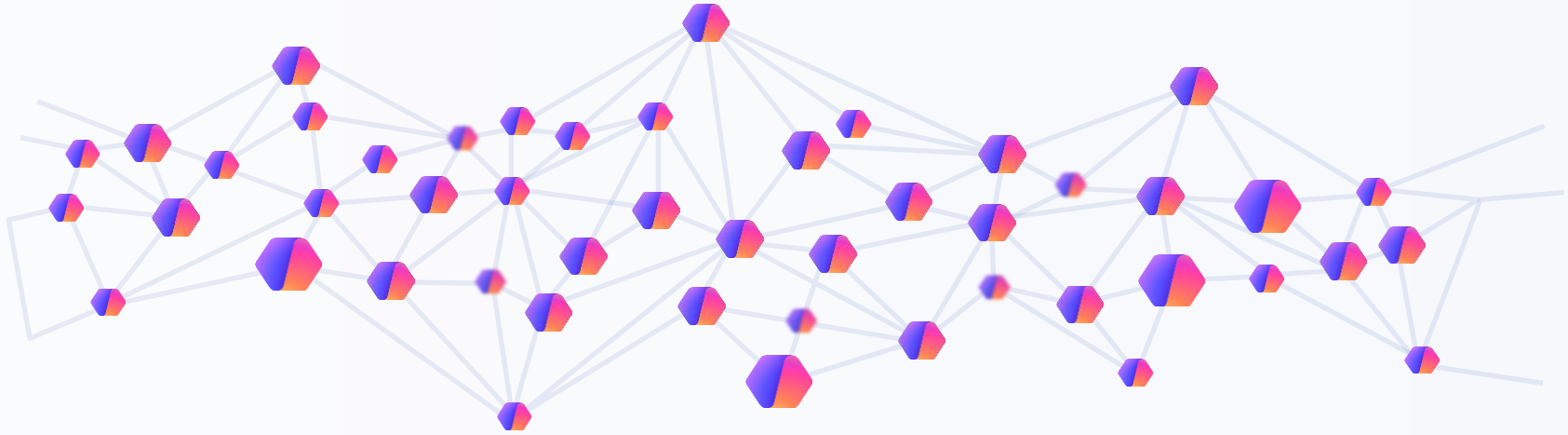
Secure	Govern
Honors your existing permissions	Supports your lifecycle policies and audit requirements
Protects against data loss and insider risk	Detect and investigation non-compliant and unethical usage
Assess oversharing risks and apply recommended corrections	Guided assistance to remain compliant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

A complete solution for enterprise-ready AI


Microsoft Agent 365
The control plane for agents

Microsoft Agent 365

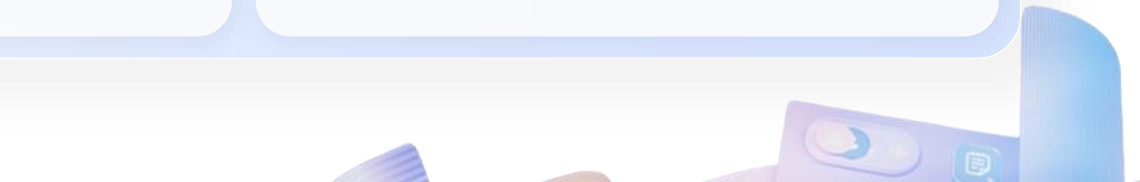
The control plane for agents



Observe

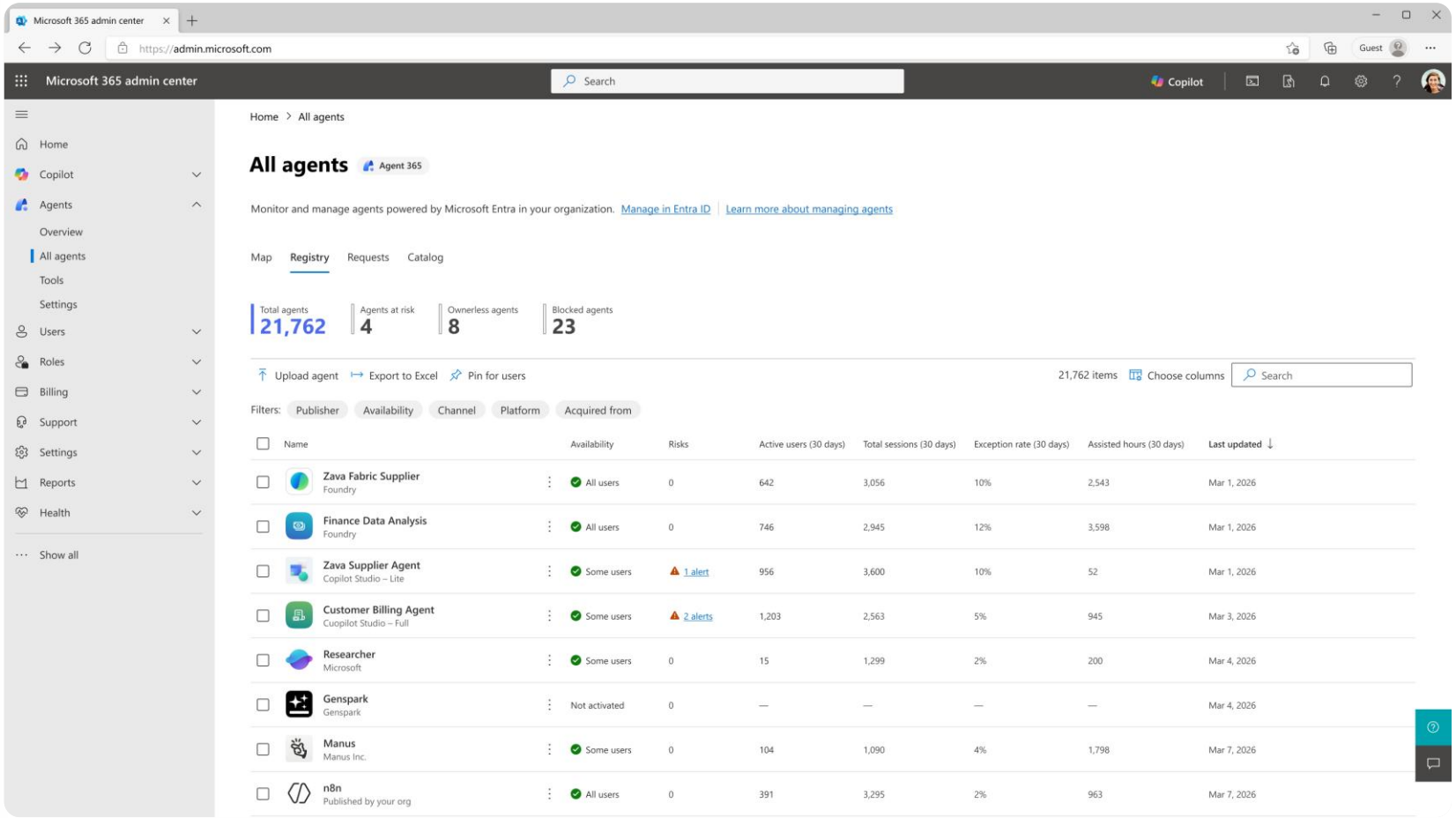
Govern

Secure



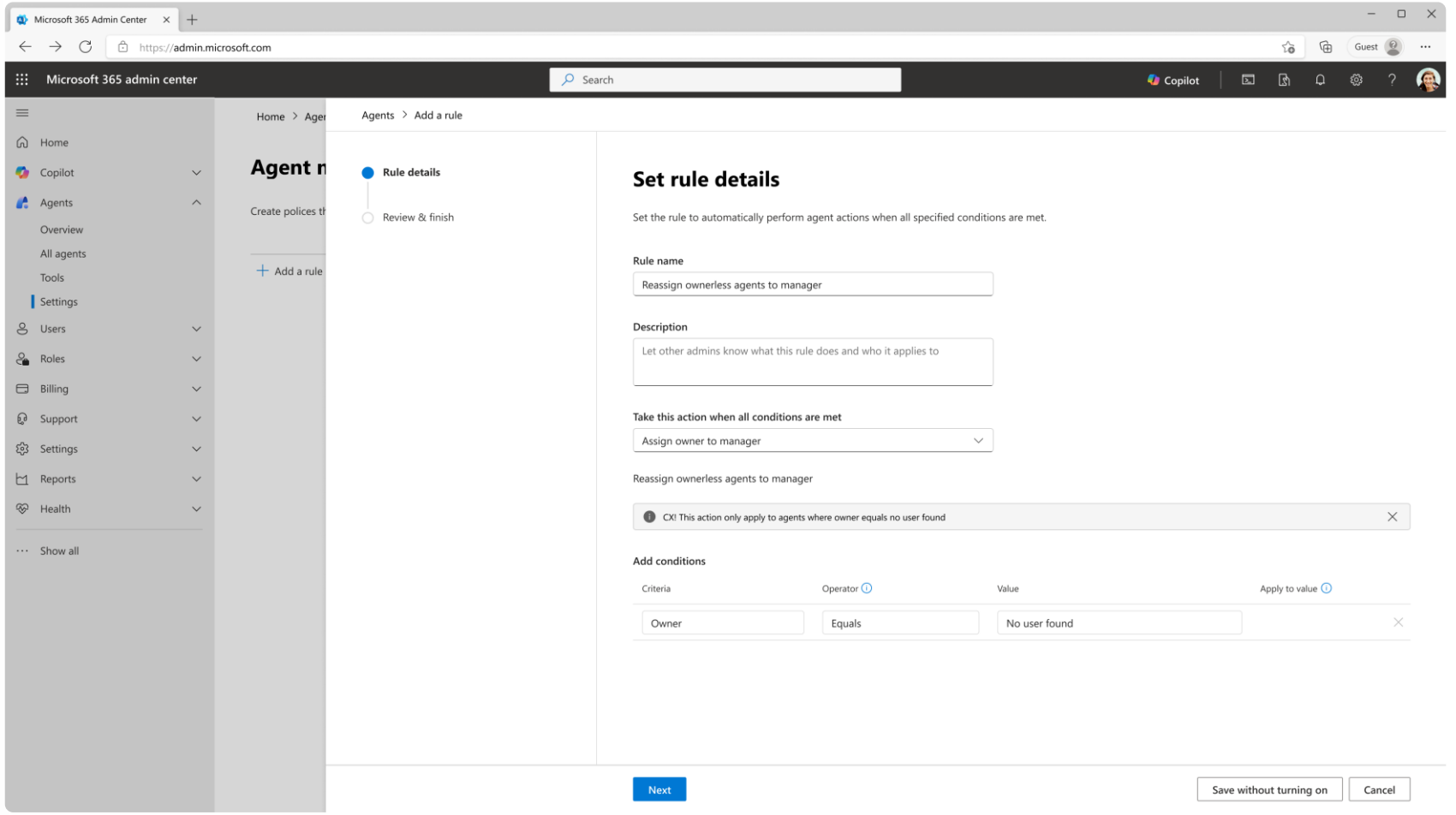
Observe

Gain visibility into agents in your environment, understand how they're used, and act quickly on performance, behavior, and risk signals before they impact the business.



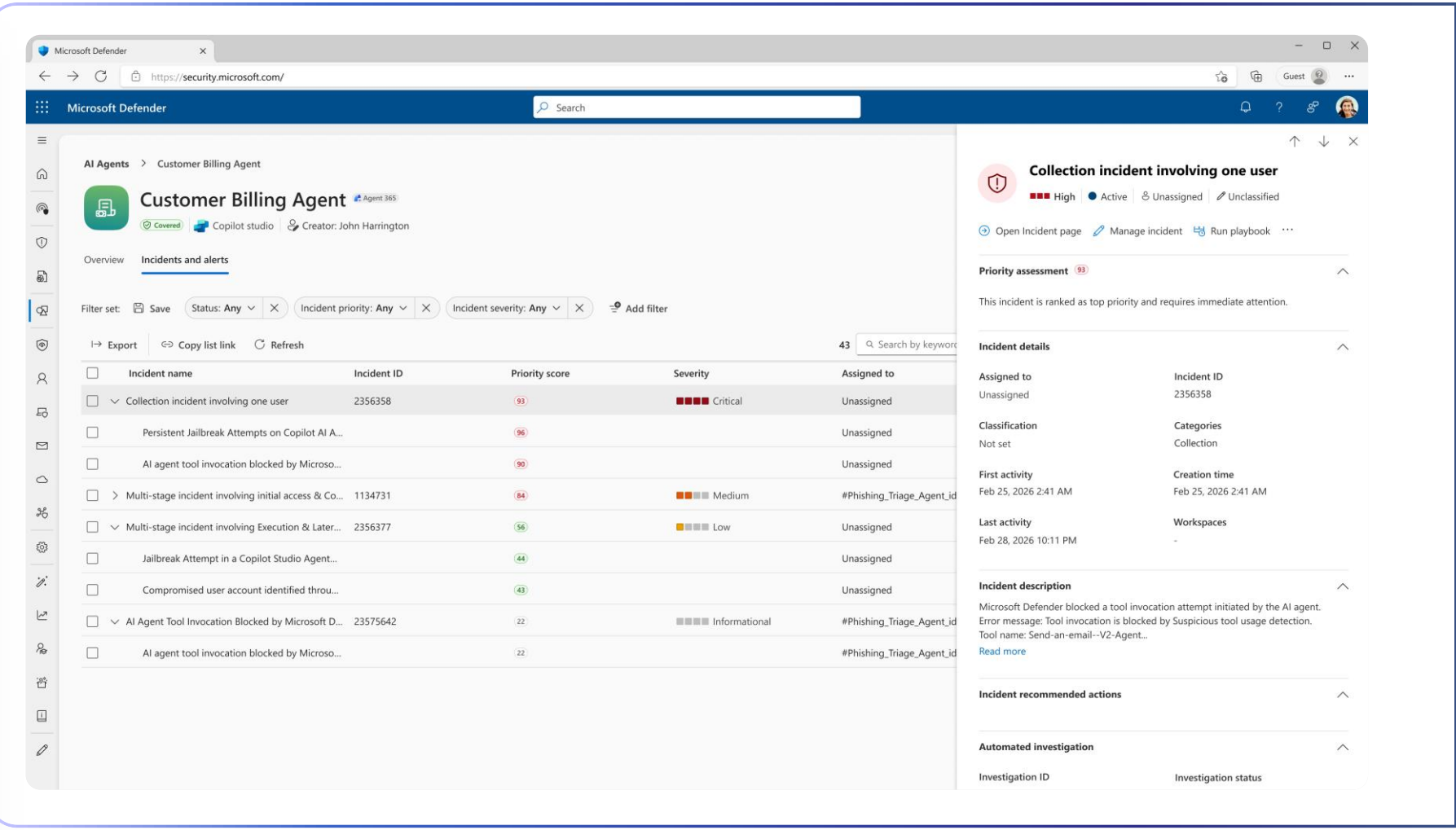
Govern

Establish guardrails for agents and people, onboard agents with IT oversight, and govern agent access to resources and data. Be audit ready with built-in compliance and data retention.



Secure

Secure agent identities, control access to resources, prevent data oversharing and leaks, and defend against threats and vulnerabilities with enterprise-grade security solutions.



Microsoft Agent 365

The control plane for agents

Observe

Monitor and manage agents in real time

- Registry
- Agent maps
- Agent analytics
- Role-specific oversight

Govern

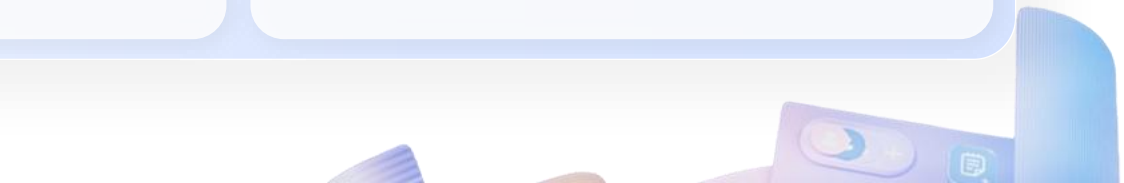
Govern agents throughout their lifecycle

- Agent onboarding
- Access and integration governance
- Lifecycle management
- Audit and logging
- Data compliance

Secure

Protect all agents across your enterprise

- Access control
- Data security
- Threat protection



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

Microsoft 365 Admin Center

Centralized hub to manage users, apps, and settings securely across your Microsoft 365 environment.

Microsoft Defender

Extend comprehensive security posture and advanced threat protection to agents.

Microsoft Entra

Protect agent identities, and secure their access to any app or resource, from anywhere.

Microsoft Purview

Manage, protect and govern data that agents use and create across your entire organization.

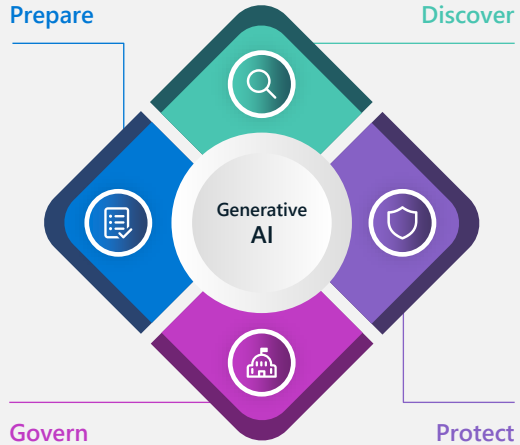
Secure and govern M365 Copilot + Agents with confidence

Prepare your environment and implement Zero Trust strategy for secure M365 Copilot + Agents adoption

Discover security, privacy, and safety risks with comprehensive visibility

Protect against emerging threats and safeguard sensitive data with end-to-end security

Govern M365 Copilot + Agents usage and systems to comply with code-of-conduct and regulatory policies



Take the Security for AI Assessment

Gain Clarity

on how your security posture aligns with your M365 Copilot + Agents initiatives.

Identify Key Gaps

that could impact your M365 Copilot + Agents transformation.

Receive Tailored Recommendations

to strengthen your M365 Copilot + Agents security strategy.

Download Your Full Report

to share findings and align your team.

Keep the Momentum Going

with expert guidance and next steps.

Thank you!

sherweb