Concurrency

Governing & Securing AI at Scale

Concurrency AI Summit 2026

Joe Steiner

Solutions Architect

Complex Human Relationship with AI

Through fiction and opinion, society has expressed a spectrum of points of view concerning Artificial Intelligence since the 1950's

Doomsday

Detrimental

Neutral

Improvement

Utopia

Concurrency

Complex Human Relationship with AI

Through fiction and opinion, society has expressed a spectrum of points of view concerning Artificial Intelligence since the 1950's

Doomsday | Detrimental | Neutral | Improvement | Utopia

Doomsday & Utopia scenarios make for good movies & storytelling but not likely to be realized. Whether AI is Detrimental, Neutral or an Improvement is up to all of us.

Concurrency

New Tech Usage Models

Concurrency

AVOID USE

- No Benefits
- Ban → Shadow IT Mutiny
- Employee Dissatisfaction
- New Risks

New Tech Usage Models

Concurrency

AVOID USE

- No Benefits
- Ban → Shadow IT Mutiny
- Employee Dissatisfaction
- New Risks

FREE RANGE USE

- Max Benefits
- Unmanaged Usage
- Employee Distrust
- Maximum Risk

New Tech Usage Models

Concurrency

AVOID USE

- No Benefits
- Ban → Shadow IT Mutiny
- Employee Dissatisfaction
- New Risks

RESPONSIBLE USE

- Most Benefits
- Managed Usage
- Employee Satisfaction
- Minimum Risk

WIDE OPEN USE

- Max Benefits
- Unmanaged Usage
- Employee Distrust
- Maximum Risk

Responsible Use requires Governance

AI Governance

Enable Responsible AI Use & Development by Focusing on:

- Minimizing Risks – Security, Operational, Financial, etc.
- Maximizing Business Value Realization
- Ensuring Usability
- Maintaining Trust

Key Areas:

- Policy & Strategy
- Education & Enablement
- Protection & Monitoring
- Ongoing Testing & Development

Concurrency

Responsible AI Usage Progression

Concurrency

01

Not Using AI Yet

02

Using Free Public AI

03

Investing in AI Assistants (Copilot)

04

Building AI Offerings

Not Using AI Directly?

No avoiding AI.
Create your AI Policy.
Educate yourself and your organization about AI.
Restrict AI Use & Access until ready.

Concurrency


TEMPLE
Surfside

Policy & Strategy

1. **Embrace a Zero Trust Security Policy: Never trust, always verify**
   - Zero Trust Assessment and/or Workshop
   - Make progress towards adoption (don't need to solve all at once)
   - Zero Trust is about enabling not disabling
2. **Create an Acceptable AI Usage Policy**
   - Cross-functional team to develop – IT, Security, HR, Legal, etc.
   - Align with existing corporate governance & policy standards
   - Consider industry standard frameworks as guides such as the MSFT Responsible AI & NIST AI Risk Management Frameworks
   - Define what Acceptable AI usage will be as you move forward

Education & Enablement

1. **Educate the organization on the following using self-service content or hosting an educational session:**

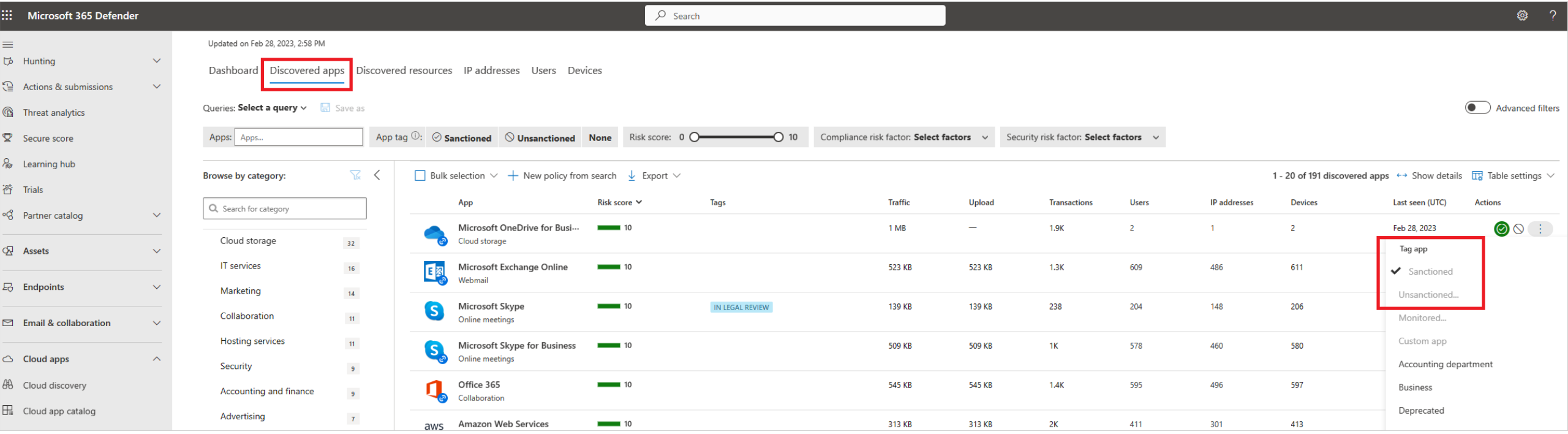
Understanding What AI Can Do

Identifying AI Generated Content

- Text
- Audio
- Video
- Interactive

Protection & Monitoring

1. **Restrict AI tool usage - Defender for Cloud Apps (E5)**
   - Cloud App catalog for AI app discovery (incl risk scoring)
   - Monitor Generative AI apps
   - Alert or Block using Defender for Endpoint or other tooling



Using Public AI?

Be aware of what you share.

Continue to refine you Policy & Educate.

Protect yourself and your organization against untrusted AI tooling and Monitor AI Usage.

Concurrency


TEMPLE
T
Surf-Site

Policy & Strategy

1. **Identify Trusted Public AI tools: Not All Created Equal**
   - Be mindful of what happens with the data shared in a session
   - Only use AI tools from trusted providers
   - Treat Public AI as you would someone outside your organization
   - Trusted AI tools like Microsoft Copilot Chat do not share nor use your data outside of your session
2. **Update AI Policy**
   - Define what is acceptable to share and what is not
   - Define acceptable tools or where to find the current authoritative list
   - Continue to evaluate over time

Education & Enablement

1. **Educate the organization on the following using self-service content or hosting an educational session:**

Appropriate AI Use

- Trusted AI tools & Appropriate Use Cases
- Risks of data sharing
- Risks of using untrusted AI tooling
- Ethical issues
- Verifying AI responses

Protection & Monitoring

1. **Allow Trusted AI tool usage - Defender for Cloud Apps (E5)**
   - Continue to Monitor & Alert and/or Block others
2. **Mark Sensitive Data – Purview**
   - Develop basic Sensitivity Labeling scheme
   - Ensure labeling (manual at least) of highly sensitive data/documents
3. **Manage Browser & Devices – Purview/Intune**
   - Onboard device in Purview and deploy Purview browser extension & Edge DLP to limit data copying and collect AI activity
4. **Monitor AI tool usage – DSPM for AI & Insider Risk (Purview, E5)**
   - Using Insider Risk & DSPM policies to monitor AI activity

Using AI Assistants (Copilot)?

Be aware of what you expose.

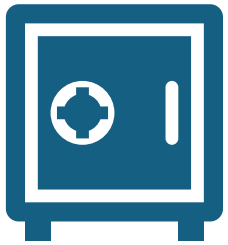
Protect your organization against unexpected information sharing.

Concurrency


TEMPLE
Surfside

Data Governance & Protection

Understand Your Data



Protect Your Data

**Keep the Data You Need,
Remove the Data You Should**

Understand, classify and safeguard your data to ensure responsible access, reduce risk and enable secure use of your information by both people & AI.

Policy & Strategy

1. **Define Data Governance and Protection Policies**
   - Sensitive data definitions & protection policies
   - Retention policies to manage data lifecycle
2. **Create AI Enablement Plan**
   - Training & Ongoing Assistance
   - Basic Copilot Agent creation handling
   - Data sources to be made available for Copilot
   - Encourage creative, responsible use
3. **Update AI Policy**
   - Continue to evaluate over time

Education & Enablement

1. **Educate the organization on the following using self-service content or hosting educational sessions on:**

   Data Protection & Retention

   Copilot Use

   - How to Use
   - Prompt ideas
   - Copilot settings & personalization
   - Agent creation
   - Appropriate Use
   - Verifying AI responses

2. **Consider creating Center of Excellence community led by AI champions**

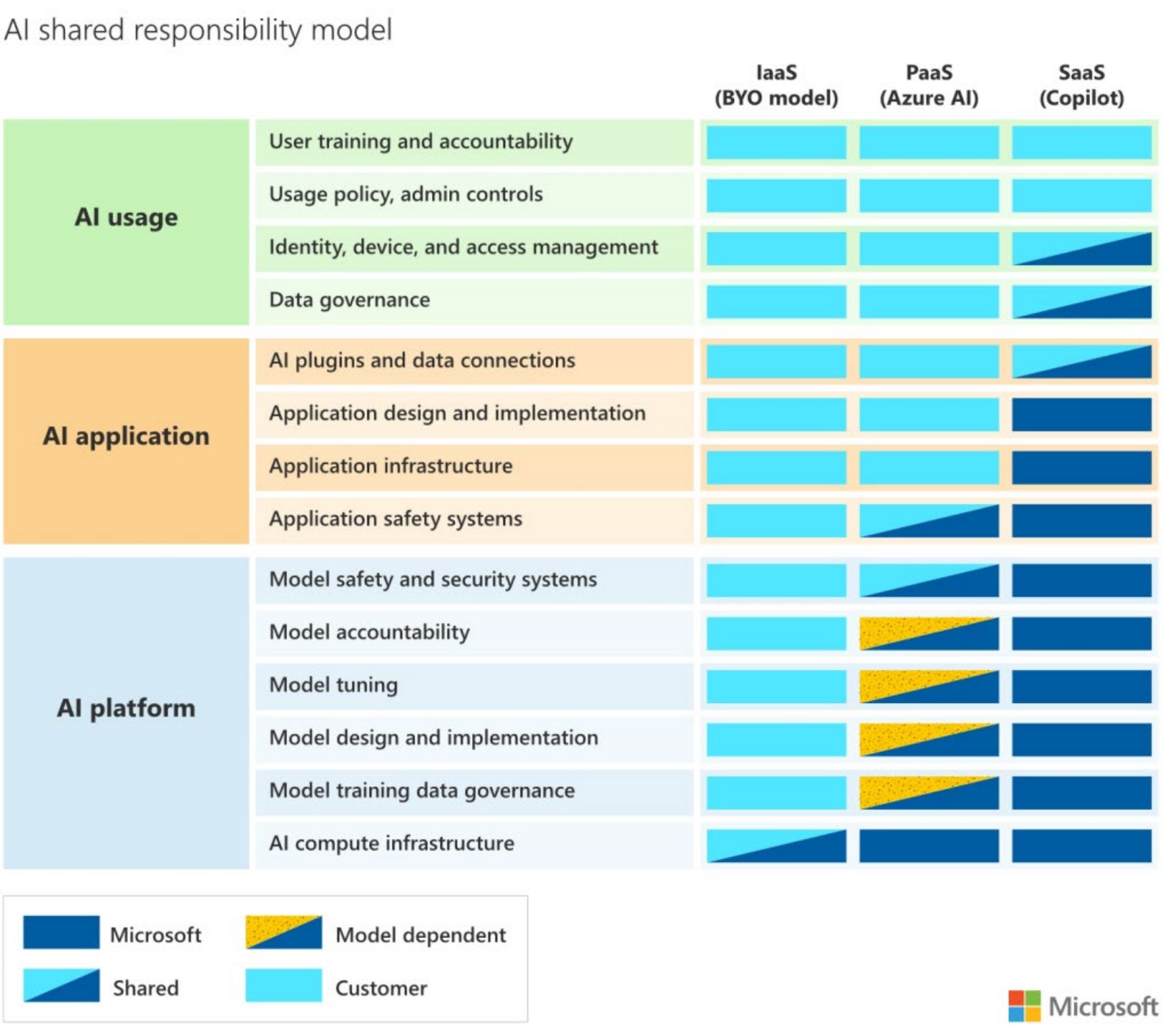
Protection & Monitoring

1. **Review Permissions & Content – SharePoint Advanced Mgmt**
   - Fix permission issues and restrict content discovery & access as needed
2. **Mark Sensitive Data – Purview**
   - Develop next level Sensitivity Labeling scheme
   - Enable automated labeling of all M365 data/documents
3. **Apply Retention Policies - Purview**
4. **Refine Access Policies for Copilot Access – Entra/Intune**
5. **Monitor Copilot Prompts – Purview (E5)**
   - Communication Compliance, Insider Risk, Auditing, DSPM, eDiscovery

Testing & Development

1. **Test Prompts & M365 Search**
   - Check for unexpected/undesirable results
   - Consider data cleanup and/or additional data sources
   - NOTE: M365 Graph & Search data is available within Copilot

AI Shared Responsibility Model



Microsoft

Building AI Offerings?

Assume responsibility for what your AI agent/app provides.

Protect your organization against unexpected or misleading information sharing.

Concurrency


TEMPLE
Surfside

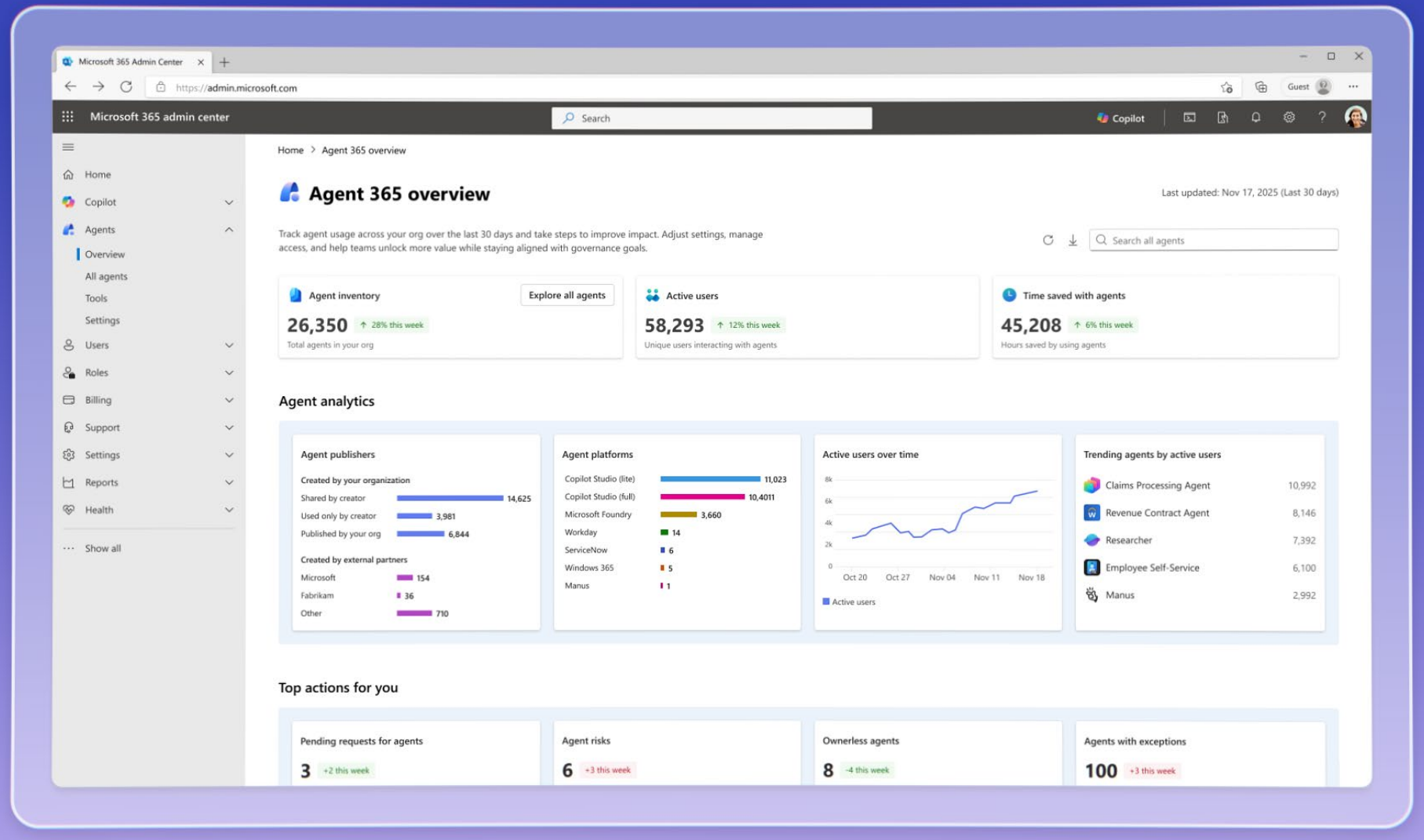
Policy & Strategy

1. **Create AI Strategy**
   - Vision & Objectives including Priorities
   - AI Use Case evaluation model & Portfolio management
   - Approved Technology & Data
   - Governance plan & requirements
   - Organization & process design to support
2. **Plan AI Framework Policies**
   - Lifecycle management
   - Security & Organizational Policies to be considered
   - Cost management
   - Models & tooling to use
   - Drive responsible use
3. **Update AI Policy**

Education & Enablement

1. **Establish a Framework for Publishing AI agents & apps to the organization or for public use via:**
   - **Copilot Control System**
   - **AI Foundry Control Plane**
   - **Agent 365**
2. **Consider creating AI Product group to lead and manage AI app & agent development**

Agent 365


Microsoft 365 Admin Center
https://admin.microsoft.com
Microsoft 365 admin center
Search
Copilot
Home
Copilot
Agents
Overview
All agents
Tools
Settings
Users
Roles
Billing
Support
Settings
Reports
Health
Show all
Home > Agent 365 overview
Agent 365 overview
Last updated: Nov 17, 2025 (Last 30 days)
Track agent usage across your org over the last 30 days and take steps to improve impact. Adjust settings, manage access, and help teams unlock more value while staying aligned with governance goals.
Search all agents
Agent inventory
Explore all agents
26,350
↑ 28% this week
Total agents in your org
Active users
58,293
↑ 12% this week
Unique users interacting with agents
Time saved with agents
45,208
↑ 6% this week
Hours saved by using agents
Agent analytics
Agent publishers
Created by your organization
Shared by creator 14,625
Used only by creator 3,981
Published by your org 6,844
Created by external partners
Microsoft 154
Fabrikam 36
Other 710
Agent platforms
Copilot Studio (lite) 11,023
Copilot Studio (full) 10,4011
Microsoft Foundry 3,660
Workday 14
ServiceNow 6
Windows 365 5
Manus 1
Active users over time
8k
6k
4k
2k
0
Oct 20
Oct 27
Nov 04
Nov 11
Nov 18
Active users
Trending agents by active users
Claims Processing Agent 10,992
Revenue Contract Agent 8,146
Researcher 7,392
Employee Self-Service 6,100
Manus 2,992
Top actions for you
Pending requests for agents
3
+2 this week
Agent risks
6
+3 this week
Ownerless agents
8
-4 this week
Agents with exceptions
100
+3 this week

Protection & Monitoring

Concurrency

1. **Assign Identity to each Agent – Entra**
   - Use Entra Agent identities
2. **Manage Structured Data Estate – Purview**
   - Purview Data Catalog, Endorsements, Permissions
3. **Apply Management Control System – Agent 365/Copilot Control System/Foundry Control Plane**
4. **Define Access Policies for Agents – Entra/Intune**
5. **Manage Agent Compliance – Purview (E5) & Azure Policy**
   - Azure Policy, Purview Compliance Manager, DSPM, eDiscovery
6. **Secure AI Agents/Apps – Defender for Cloud & Foundry**
   - App Governance, AI Agent inventory, CSPM-AI Security Posture Mgmt
   - Foundry Security Baseline, AI Red Teaming Agent & PyRIT, Counterfit

Testing & Development

Concurrency

1. **Monitor Audit Logs**
2. **Establish Incident Management & Support Processes**
3. **Establish DevOps Lifecycle for AI Apps/Agents**
4. **Ongoing Testing & Monitoring**
    - General testing
    - Foundry and/or Copilot Studio tools
    - MSFT Responsible AI Toolkit
    - FairLearn
    - InterpretML & EconML
    - Etc.

AI Governance Progression

Anticipate rather than Oppose.
Enable through Governance Evolution.

	Not Using AI	Using Public AI	AI Assistants	Building AI
Policy & Strategy	Initial AI Usage Policy	Updated AI Policy incl Trusted AI tools	AI Enablement & Data Governance	AI Strategy & Framework
Education & Enablement	AI Awareness	Responsible AI Use	Enablement & Responsible Data Usage	Responsible AI Agent Creation
Protection	Restrict AI Use & Access	Modify Restrictions	Data Governance & Protection	Entra ID & Permissions, Extend Data Protection
Monitoring		Monitor AI Use	Monitor Prompts & Data Sharing	Agent 365, Purview, Defender for Cloud
Testing & Development			Prompt & search testing	DevOps Ongoing Testing/Refining

Concurrency

AI Summit Agenda

March 3, 2026

Timezone: CST

Now Playing 01:00 PM - 02:00 PM

Executive Panel

Unfiltered insights from leaders making real AI decisions inside their organizations today.

Panelists: Brian Atkinson (Atlas Energy), Michael Barrett (Potawatomi Ventures), Hao Jin (Clarios).

Moderator

Joe Steiner, Solutions Architect

Full Schedule

08:30 AM – 09:00 AM	Registration & Coffee
09:00 AM – 09:15 AM	Welcome & Opening Remarks Kate Weiland-Moores
09:15 AM – 10:15 AM	Keynote: The Agent Portfolio Brian Haydin
10:15 AM – 10:30 AM	Networking Break
10:30 AM – 11:30 AM	Data & AI: From Information to Impact Suneer Mehmood
11:30 AM – 12:00 PM	Networking Lunch Provided
12:00 PM – 01:00 PM	Governing & Securing AI at Scale Joe Steiner
01:00 PM – 02:00 PM	**Executive Panel** Moderator: Joe Steiner

Concurrency

Executive Panel

Brian Atkinson
Senior Manager, Data & Applications
Atlas Energy Solutions

Michael Barrett
Chief Information Officer
Potawatomi Ventures

Hao Jin
Senior Manager,
Analytics Solution Delivery
Clarios

Concurrency