Agent 365 Partner Playcard

What is it?

Agent 365 provides one place for IT and security leaders with a unified admin experience to **observe, secure, and govern ALL agents** across the organization. It does that by extending the management, security, and governance processes organizations already use for employees to agents.

It provides centralized visibility, lifecycle management, and policy-driven governance through the Microsoft Admin Center, while leveraging Microsoft security solutions - including Microsoft Defender, Entra, and Purview— to protect and govern agents.

What problems does it solve?

Capability	Problem	Solution
Observability	Organizations lose visibility as agents rapidly proliferate across teams, tools, and platforms, leading to unmanaged shadow agents, unclear ownership, and reactive fire drills when issues arise,	Agent 365 provides a unified control plane that gives IT and security leaders full visibility into all agents in the environment: › Who's using them - registry › How they're used - analytics › How they behave - relationship mapping With this, organizations can proactively identify agent sprawl, usage trends, and emerging risks before they impact the business, shifting from reactive cleanup to proactive management.
Governance	Without consistent governance, agent adoption becomes chaotic. Some agents are reviewed and compliant, others are not. Ownership and lifecycle management break down and IT loses confidence in scaling agents safely.	Agent 365 applies the same policy-driven governance model used for users and apps to agents. It enables: › IT-led onboarding › Least-privilege access › Lifecycle controls › Audit logging › Built-in compliance This ensures every agent starts governed and compliant from day one, allowing IT and Security teams to confidently innovate while maintaining accountability, audit readiness, and regulatory alignment.
Security	Agents behave like users but scale like applications, dramatically expanding the attack surface and introducing new risks such as excessive access, data leakage, prompt injection, and AI-specific threats, often without obvious warning signs.	Agent 365 extends enterprise-grade security controls to agents, including: › Identity protection › Conditional access › Data loss prevention › AI-specific threat protection Security teams gain visibility into agent threats, vulnerabilities, and attack paths, with the ability to detect, investigate, and block risky behaviour in real time.

Key capabilities

Observability

Registry:
Get a complete view of all agents in your organization, including agents built with Microsoft AI platforms, agents from our ecosystem partners, and any agents you register yourself.

Analytics:
Track agent performance, speed, quality, business impact and ROI to make informed decisions.

Mapping:
Visualize how agents fit into the broader ecosystem, connect with other agents, and perform over time to simplify monitoring and accelerate issue identification.

Role-specific oversight:
Extend oversight to security leaders to manage agent risks and business leaders to monitor business metrics and ROI.

Governance

Onboarding:
Onboard agents through IT-controlled workflow, applying security policy templates so every agents starts secure, governed and compliant.

Integration management:
Enforce least-privilege access by controlling which users, data, and tools or MCP servers agents can use. Limit access to only the resources and other agents they need.

Lifecycle management:
Leverage rules-based agent management to automatically enforce lifecycle policies, such as sharing agents with specific users and groups, expiring inactive agents, or flagging and reassigning ownerless agents.

Audit and logging:
Strengthen visibility and traceability of agent actions and interactions with logging, reporting, and audit capabilities.

Data compliance:
Establish content safety controls to detect, retain, and investigate unethical agent interactions.

Security

Access control:
Protect agent identities and prevent breaches by extending conditional access and internet traffic filtering policies from users to agents.

Data security:
Gain visibility into AI-related data exposure, protect the data agents create and access from oversharing, leaks and risky behavior.

Threat protection:
Protect agents from threats and vulnerabilities, and adversarial attacks. Detect, investigate and remediate incidents quickly, with visibility into attack paths.

Agent 365 placemat

View pillar	Product Surface	Features	Included with Microsoft cloud subscription	Agent 365 $15 pupm
Observability	Entra	Agent Identity	✓	✓
	MAC	Agent Registry – Visibility into rich agent metadata, permissions and access, security and compliance	✓	✓
		Basic usage insights for agents used in M365 Copilot (active users and response count) in MAC agent usage report	✓	✓
		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		✓
		Synchronize agents and agent metadata from external platforms that aren't managed by Agent 365 into the Agent 365 registry		✓
Security	Purview	Data Security Posture Management with AI Observability provides deep interaction visibility for Agents		✓
		Extend Insider Risk Management to agents – detect anomalous and risky agent activities		✓
		Agents inherit and honor data sensitivity labels		✓
		Data loss prevention: block agents from accessing and sharing sensitive content		✓
	Entra	Extend user conditional access , and identity protection to agents		✓
	Defender	Security Posture Management - Identify and remediate agent misconfigurations and exposure risks		✓
		Threat Detection and Blocking - Detect suspicious agent activity, receive alerts and allow blocking for tool invocations		✓
		Threat Investigation and Hunting - Collect A365 unified agent observability logs and allow Investigate and hunt for threats in agents		✓
Governance	Entra	Agent Identity Governance - Access packages for agents to give them reduced scope of permissions in comparison to users		✓
	MAC	Admin agent governance actions (publish, deploy, block, delete, approve, assign agents to specific user/groups, reassign agent owner, pin, etc.)	✓	✓
		Automate agent lifecycle actions using conditions-based rules		✓
		Control which tools (including Microsoft MCP servers) agents can access tenant-wide		✓
		Policy templates to apply consistent security and compliance controls to agents		✓
	Purview	Audit logs of agent activities and eDiscovery (content search)10 of agent interaction to export and hold for legal, regulatory and investigative needs	✓	✓
		Data Lifecyle Management for agent generated data and interactions in line with regulations and org policies		✓
		Detect and review non-compliant agent interactions, extend compliance manager to agents to assess, manage, and demonstrate AI compliance		✓

Sales guidance

Pre-requisites for using Agent 365

Agent 365 access is available to tenants with a Microsoft 365 Copilot license

Ideal customers

Agent 365 is built for IT and Security leaders such as CIOs, CTOs, and CISOs who are responsible for enabling AI adoption without losing control, security, or compliance.

The organizations would be:

- Actively adopting **AI agents** or planning to
- Concerned about **shadow agents,** unclear ownership, or lack of visibility
- Looking for a way to **govern and secure agents at scale**
- Already invested in Microsoft 365 and want an integrated control plane instead of another siloed tool

Conversation starters

Visibility	"Many organizations are moving into agent adoption faster than their governance model can keep up. How are you currently tracking which agents exist, who owns them, and what data they can access?"
Governance	"As agents start acting on behalf of users, the challenge shifts from building them to governing them. What guardrails do you have today for onboarding, access, lifecycle, and auditability?"
Security	"Agents behave like users but scale like apps, which creates a new attack surface. How are your security teams thinking about agent identity, data leakage, and threat protection?"
Operational maturity	"Where are you today: experimenting with a few agents, or trying to operationalize AI agents across departments? Agent 365 becomes especially valuable when AI moves from pilot to scale."

Objection handling

Objection	Response
"We already have M365 Copilot. Why do we need Agent 365?"	Copilot helps end users work with AI. Agent 365 is different. It is the control plane for agents and is designed to help organizations observe, govern, and secure agents across the enterprise. The FAQ is clear that Agent 365 complements Copilot rather than replacing it.
"We do not want another standalone security tool."	Agent 365 is positioned as an extension of Microsoft 365 and Microsoft Security, not a bolt-on silo. It brings agent oversight into the Microsoft Admin Center and connects with Entra for identity, Purview for data security and compliance, and Defender for threat protection.
"Do we need Microsoft 365 E7 to buy this?"	No. Microsoft 365 E7 is not required. Agent 365 can be purchased as a standalone per-user subscription, while E7 simply offers the most complete bundled experience.
"Do we need E3 or E5 first?"	No, there is no licensing prerequisite for Agent 365 itself. However, some underlying security and compliance capabilities depend on the customer's broader Microsoft licensing. In other words, Agent 365 works without E3 or E5, but some advanced protections depend on what the customer already owns.

Objection	Response
"Will Agent 365 give us E5-level Purview or Defender if we do not already have it?"	No. Agent 365 license does not grant E5-level security entitlements or upgrade the user's existing Purview or Defender rights.
"We are only in early experimentation. This feels premature."	That is exactly when many organizations should start the conversation. Agent 365 addresses the problems that show up early: shadow agents, unclear ownership, inconsistent governance, and reactive security cleanup. It helps put the model in place before adoption becomes chaotic.
"We use third-party or custom agents too."	Agent 365 is meant to help govern all agents across the organization, including Microsoft-built, partner-built, and custom agents, provided they are integrated correctly.
"Our security team already uses Entra, Purview, and Defender. Why add Agent 365?"	Because those tools each handle important parts of the problem, while Agent 365 acts as the unifying control plane for agents. It uses the registry as a single source of truth and connects identity, threat protection, data security, audit, and governance into one operating model for agentic workloads.

Services opportunity

Registry + Access Control	Data Security + Compliance	Threat Protection	Interoperability + Performance
• Create agent registry & enable employee discovery • Create policies for creation, onboarding & management • Access governance to enforce least privilege access • Define conditional access based on agent context and risk	• Create agent registry & enable employee discovery • Create policies for creation, onboarding & management • Access governance to enforce least privilege access • Define conditional access based on agent context and risk	• Create agent registry & enable employee discovery • Create policies for creation, onboarding & management • Access governance to enforce least privilege access • Define conditional access based on agent context and risk	• Work IQ – supercharge agents with company data • Digital workers – equip agents to use M365 Apps like Outlooks, Teams, etc. • Analyze agent performance to assess ROI & make development enhancements

Key available resources

Download all the resources