Microsoft Agent 365 Launch Deck

April 2026

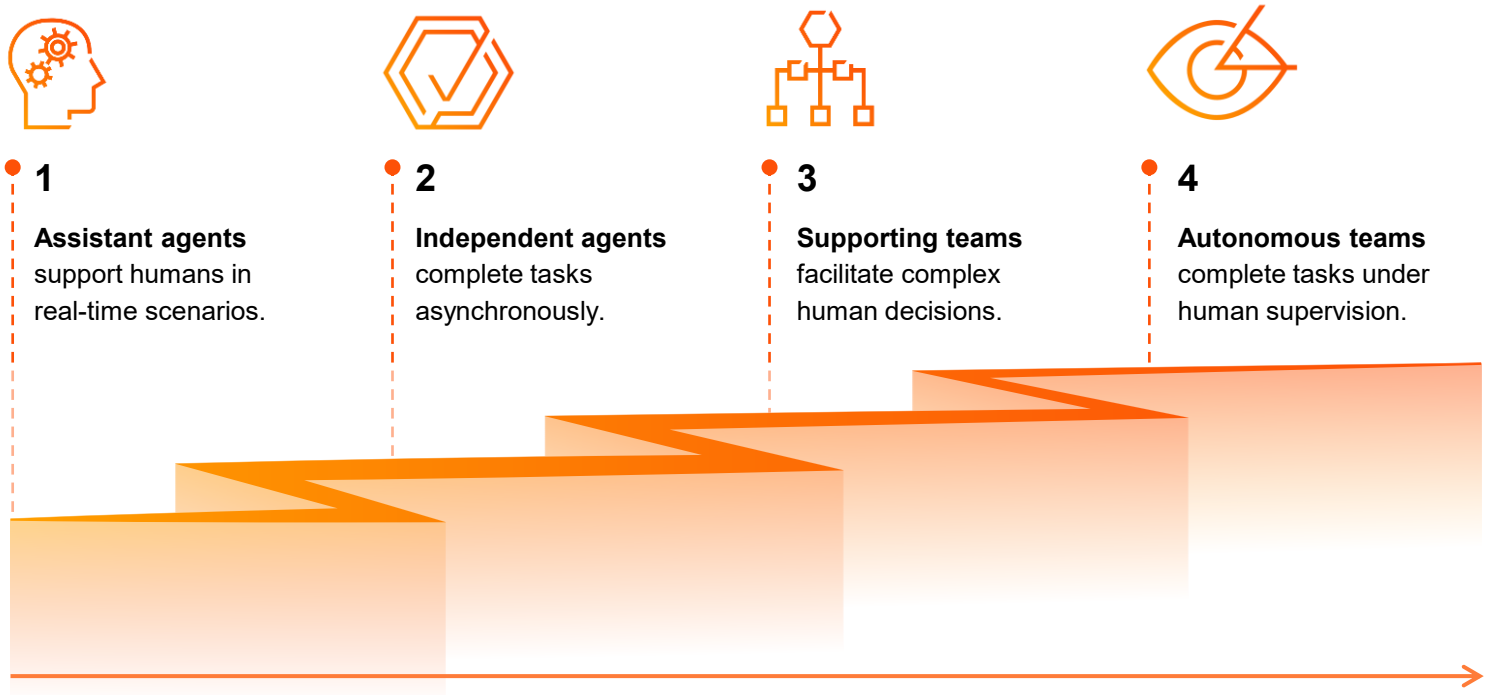
Why Microsoft Agent 365?

The current problem

- Organizations are deploying AI agents at increasing speed, with rapidly-expanding use cases across customer service, support, sales, marketing, IT, cybersecurity, and more.
- Agent capability and autonomy is also evolving at record pace.
- Many kinds of agents are being built—Microsoft, custom, and third-party.
- Organizations are trying to balance day-to-day agent management with time spent on strategic initiatives.

79% **of senior executives say their companies are already adopting agents***

Evolution of agent maturity



Key security challenges

1. Ineffective agent lifecycle governance
2. Shadow agents and incomplete inventory
3. Inadequate access controls
4. Over-permissioned content
5. Insufficient monitoring and auditing
6. Insider threat and data leakage
7. Insufficient agent observability
8. Sensitive data exposure
9. Insufficient retention management

*AI agents: Your next insider threat?

Gain safer AI adoption at enterprise scale with Microsoft Agent 365

Microsoft Agent 365 gives you a centralized control pane for governing AI agents across Microsoft 365 so you can scale **safer AI adoption** with centralized governance, observability, and security.

The benefits of adopting Microsoft Agent 365

Enable policy adherence and audit readiness through centralized agent governance across Microsoft, third-party, and employee-created agents.

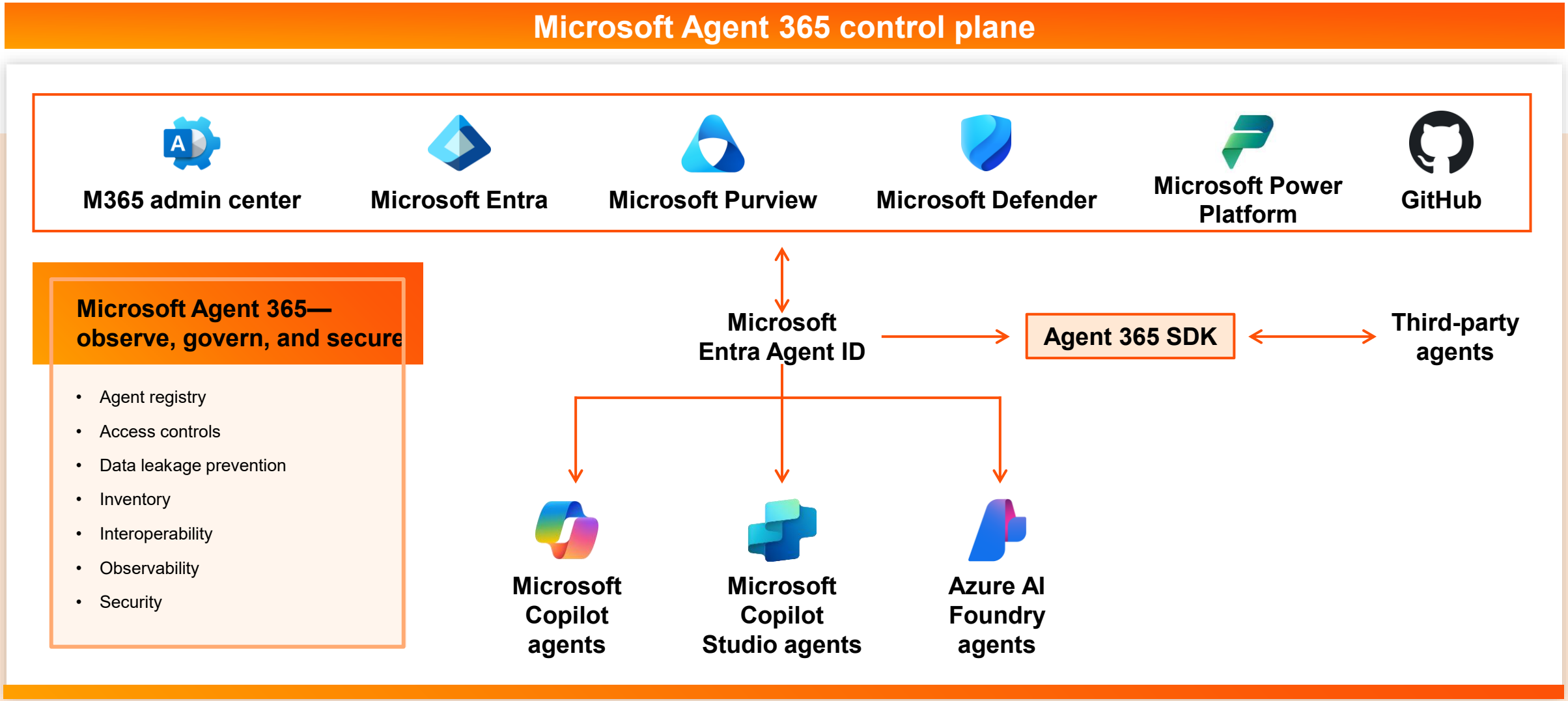
Prevent inadvertent or malicious exposure of sensitive data by enforcing enterprise identity controls on agent access, data usage, and sharing.

Accelerate secure innovation with confidence by leveraging the familiar security and compliance capabilities of the Microsoft Security stack.

Enable IT teams to focus on strategic initiatives by simplifying agent oversight and improving visibility through the Microsoft 365 admin experience.

Increase automation by scaling the use of governed agents capable of handling complex requests.

What is Microsoft Agent 365?



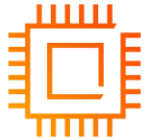
Combine Microsoft Agent 365 and security tools to get secure agent adoption

Works with **Microsoft Purview to enforce data govern-ance** (e.g. classification, DLP, or insider risk) on data that Microsoft Agent 365 agents access or generate.

Works with **Microsoft Defender to detect and safeguard** against threats (e.g., prompt injection, data exfiltration, or malicious plugins and agents) across Microsoft Agent 365 workloads.

Works with **Microsoft Entra ID to provide identity, authentication**, and conditional access so agents act securely on behalf of users and services.

Leverages **Microsoft's M365 admin center as the central place** to configure, govern, and monitor Microsoft Copilot and Microsoft Agent 365 usage, policies, and tenant-level settings.



Microsoft Agent 365 **integrates Microsoft agents** built across Copilot, Copilot Studio, Azure AI Foundry, and Power Platform **while onboarding third-party agents through connectors and APIs** secured with Microsoft Entra ID.

Implementing agent security and governance with Microsoft Agent 365

In four to six weeks, we can help baseline your Microsoft Agent 365 deployment, define core controls, and prioritize the actions required to scale securely.

Discovery and strategic alignment workshop

- Understand the organization's approach to and progress on building AI agents
- Discuss priority use cases and strategic objectives
- Align on risk, compliance, and governance expectations
- Educate stakeholders on Microsoft Agent 365 capabilities and value

Agent governance current state

- Understand the current sprawl of agents across Microsoft and third parties
- Understand agent governance across the agent development life-cycle and associated security controls
- Review existing ownership, access models, and usage standards
- Assess current admin settings, policies, and telemetry gaps

Define security and governance baseline

- Define minimum controls for Agent ID, access, and approvals
- Establish baseline governance lifecycle flows for agents
- Align Microsoft Purview, Microsoft Defender, and admin center monitoring controls

Build roadmap and prioritize actions

- Sequence quick wins, 90-day actions, and a 6- to 12-month roadmap for Microsoft Agent 365 utilization
- Define a scope and approach for proof of concept or pilot
- Prioritize by risk, value, effort, and dependency
- Define target governance model, RACI, and KPIs

Pilot and change management

- Work with in-scope teams to perform a pilot of Microsoft Agent 365
- Perform integration and configuration with other Microsoft security capabilities (e.g., Microsoft Purview, Microsoft Defender, and Microsoft Entra ID)
- Leverage lessons learned to refine security controls baseline and develop a playbook to be used for change management and communication

Deliverables

An actionable set of deliverables that help accelerate your journey when securely adopting AI agents

Workshop: See Microsoft Agent 365 in Action

- Aligns Microsoft Agent 365 capabilities to priority use cases, risk management objectives, and enterprise readiness for scaled adoption
- Workshop readout summarizes key decisions, strategic priorities, and success factors to inform the assessment, controls, roadmap, and pilot Microsoft Agent 365

Baseline control matrix

- Structured control matrix mapping Microsoft Agent 365 risks to recommended controls aligned to Microsoft capabilities (e.g., Microsoft Purview, Microsoft Defender, etc.)
- Defined control requirements outlining minimum and enhanced control expectations across identity, access, data protection, monitoring, and lifecycle governance

Pilot and change management

- Completes pilot for Microsoft Agent 365
- Offers lessons learned
- Refines a set of security controls documentation
- Produces a playbook for change management and broader consumption

Current state and gap assessment

- Produces a structured assessment report that details agent inventory, ownership, access models, and usage patterns
- Configuration review of existing controls, highlighting effectiveness relative to leading practices
- Risk-based gap analysis that identifies potential exposure areas across agent governance, data protection, and monitoring

Prioritized roadmap

- Phased roadmap across near-, mid-, and long-term horizons
- Prioritization framework with initiatives ranked by risk, business value, effort, and Microsoft ecosystem dependencies
- Target operating model with key metrics and indicators to support Microsoft Agent 365 oversight, scalability, executive reporting, and audit readiness

Let's get started

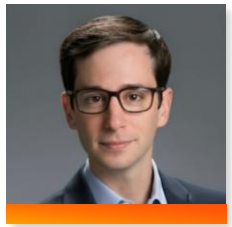
Rapid start and evolve

We can help you unlock the true potential of your workforce by empowering employees to use Microsoft Agent 365 to create and deploy agents securely.

Together, we can enable your organization to observe, govern, and secure agents at scale—positioning your teams to build with confidence and accelerate your AI agent journey.

Contacts

Scott Sikorski
PwC US | Principal
scott.g.sikorski@pwc.com



David Ames
PwC US | Principal
david.m.ames@pwc.com

Joe Ponder
PwC US | Managing Director
joe.ponder@pwc.com

Workshop

Discovery workshop

1-2 hours

Learn how to get started with Microsoft Agent 365 and see it in action while we ideate current and future states.

Current state

Agent governance current state

1-2 weeks

Discover agents across your organization while we assess your current agent governance and control capabilities.

Framework

Security and governance baseline

1-2 weeks

Define minimum controls and establish baseline governance for your agents.

Future state

Roadmap and action prioritization

1-2 weeks

Identify near- and long-term wins prioritized by risk, value, effort, and dependency to get you to your target governance model.

Pilot

Pilot and change management

3-4 weeks

Perform a pilot of the capabilities, including security integration, and enable change management.

Why PwC?

Industry expertise

PwC brings deep industry expertise—together with our technical skills—to provide the most relevant point of view for our clients, based on their business.

Leaders in AI

PwC has established AI leadership and deep, hands-on experience delivering AI strategy, engineering, and adoption programs.

Thought leadership

1. Agentic AI: The next frontier of cyber defence
2. AI agents: Your next insider threat?
3. Who's in control: Managing the cyber risks of AI agents
4. Unlocking value with AI agents: A responsible approach
5. PwC: Responsible AI

Risk and regulatory

PwC has decades of experience helping organizations manage risk and meet complex regulatory requirements through established governance, controls, and compliance frameworks.

Breadth of services and support

PwC assists with end-to-end transformation—from upfront strategy and planning, solution design, and build through to implementation, operating model setup, and adoption.

PwC sector expertise

Financial services

Industrial products

Consumer markets and retail

Energy, utilities, and resources

Technology, media, and telecommunications

Health and life sciences

Deals and private equity

Thank you