

Microsoft Agent 365

Agent 365 - The Control Plane for Agents



Registry

Get the complete view of all agents.



Access Control

Bring agents under management.



Visualization

Explore and monitor connections between agents, people and data



Interop

Equip agents with the same apps to simplify human-agent workflows.



Security

Protect agents from threat, detect and remediate attacks that target agents.

Microsoft Agent 365 helps organizations deploy, govern, and manage AI agents at scale. Slalom helps you turn that promise into a practical operating model: clear strategies, strong guardrails, and day-to-day visibility so teams can innovate without creating new risk.

Agent Governance Challenges:

- 1. Agent sprawl & blind spots:** Agents multiply across teams and tools, making it hard to know what exists, what it connects to, and who owns it.
- 2. Over-permissioned agents:** Without “right-sized” access, agents can reach too much data or take actions outside intended boundaries.
- 3. Limited auditability:** Leaders need logs, reporting, and eDiscovery-ready oversight to stay compliant and investigate issues.
- 4. Value without control:** Business teams want speed; security teams need guardrails. Without shared visibility, adoption stalls or goes rogue.

Slalom’s Modern Approach to Agent Management

We help you move from experimentation to enterprise-grade agent operations—so AI agents are onboarded, secured, monitored, and improved with the same rigor you apply to people, apps, and data.

ACTIVITIES

Strategy, Alignment, & Readiness:

- Executive AI vision alignment workshops
- Identify and prioritize agent scenarios

Foundation & Environment Setup

- Review Agent Registry for optimization
- Review Tool registry for availability considerations

Agent Governance Design

- Security and team agent governance workshops to determine and configure:
 - Allowed Agent Types
 - Establish security templates
 - Define agent sharing user access capabilities
- Define intake, governance, and lifecycle management

Deployment and Change Enablement

- Develop Agent playbooks and usage guidance
- Recommend expansion to additional agent use cases and departments

Duration: 2 hour workshop
6-10 week delivery

Cost: TBD - MSFT funding may be available

Who it’s for: Security Leaders, Architects, Administrators

How to get started: Reach out to your Slalom contact for more information

Why Choose Slalom for your Microsoft Security Journey?

With over 20 years of experience partnering with Microsoft, Slalom’s experts are ready to work with you to develop a customized roadmap to help you achieve your goals and set priorities on which initiatives should take precedence.

Slalom will work with your security and business leaders to bring a hands-on approach to helping your enterprise implement Microsoft Agent 365 in a way that actually works for how your teams operate. We don’t just turn on features – we help you rethink how AI agents should be governed, secured, and embedded across your business.

