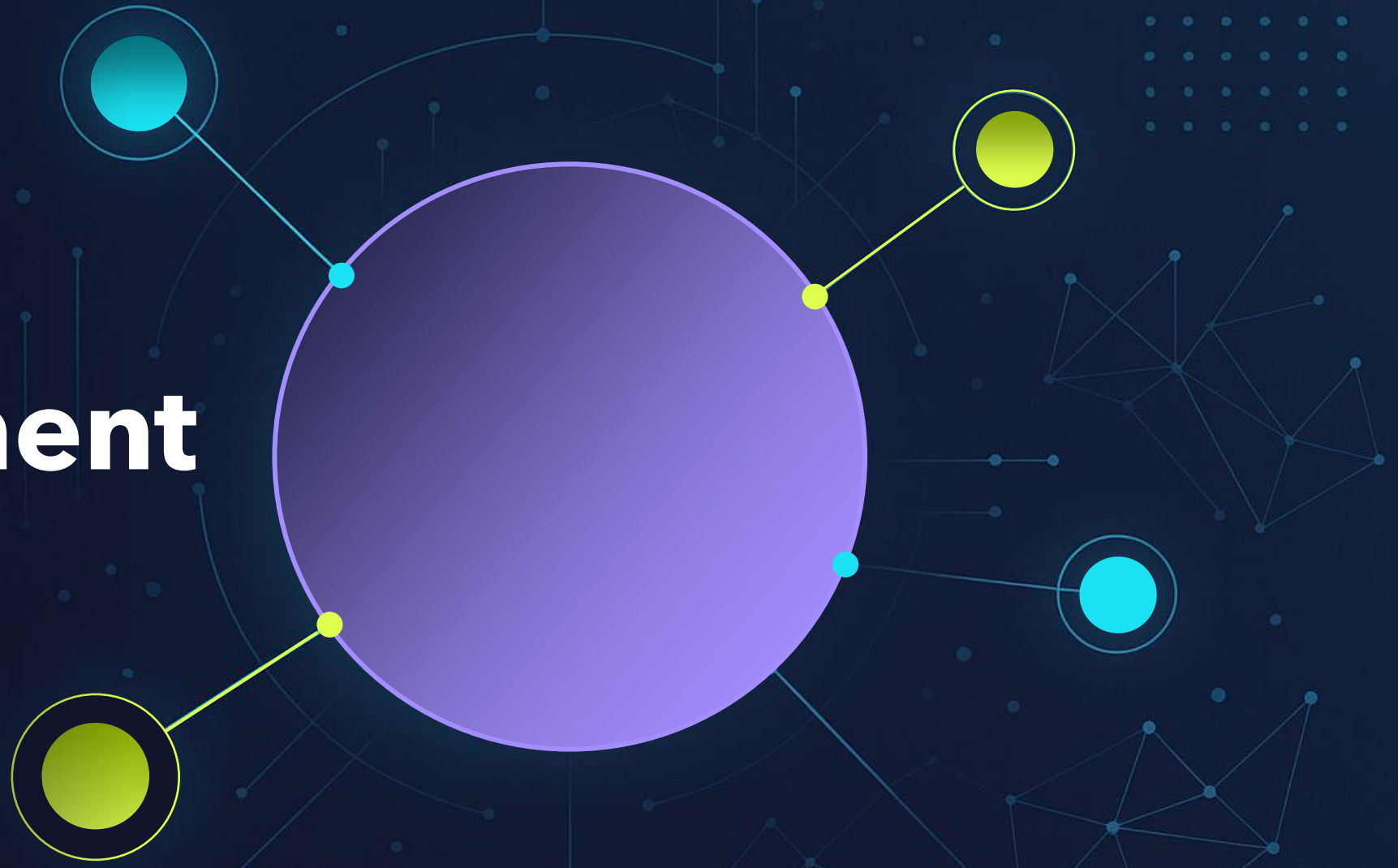
MICROSOFT SECURITY
MARCH 2026

Agent Management and Agent 365

The Control Plane for Agents



Agents introduce new security risks

slalom

Agent sprawl & resource access

82%

Of leader expect to use agents in the next 12-18 months to meet demand for workforce capacity

Data oversharing & leaks

80%

Of leaders cited leakage of sensitive data as their main concern

Shadow AI, new AI threats & vulnerabilities

88%

Of organizations are concerned about indirect prompt injection attacks

Regulatory compliance

55%

Of how AI is and will be regulated are seeking guidance

Is your organization ready?

Can you discover and manage agents?

Are agents behaving within the enterprise?

Who / what are agents sharing sensitive information with?

Are the agents well governed and audited – what are my costs?

Top 5 Adoption hurdles:

Lack of inventory and observability of ALL agents

Trust, governance, and security

Clarity on ROI and business outcomes

Navigating agent security tools and capabilities

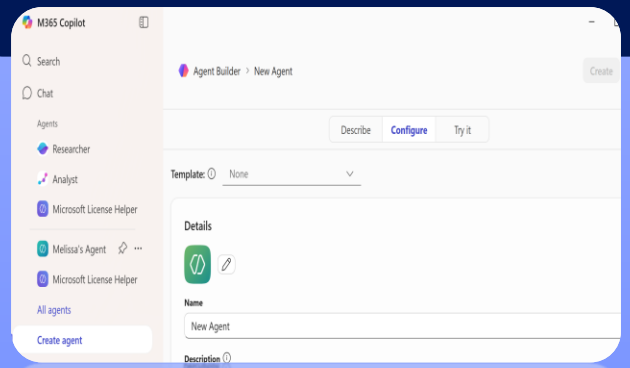
Organizational readiness for new workflows and roles

Agent Building

With agent building tools available comes agent sprawl

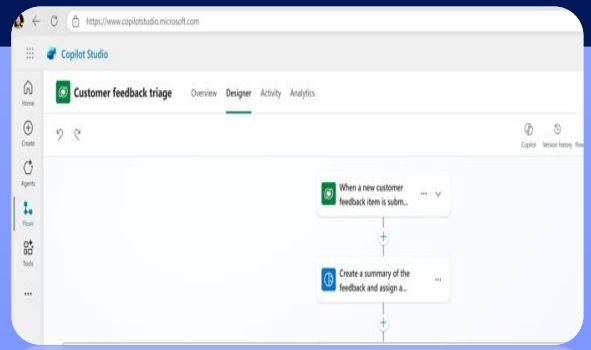
Agent Builder

Build simple, task-focused agents directly in M365 Copilot



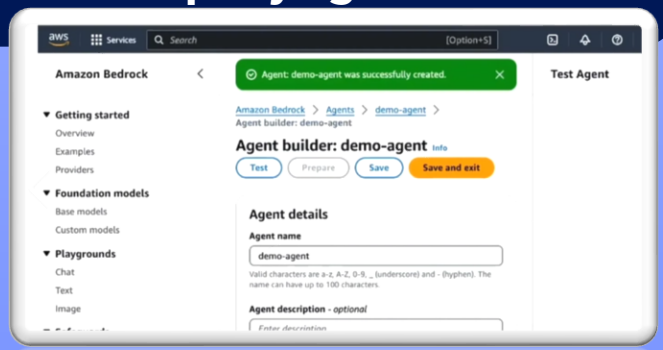
Copilot Studio & AI Foundry

Enable sophisticated custom agent building and workflows

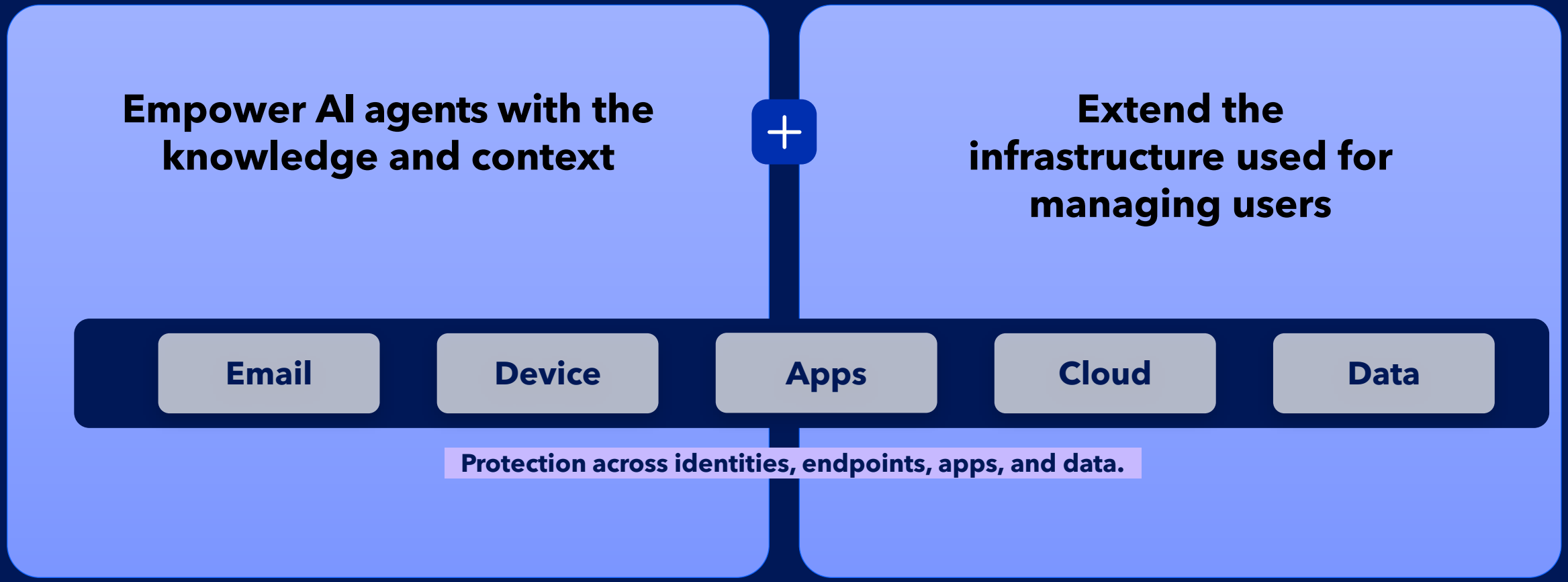


Other AI platform Agents

Use Entra-backed Agent Identity for Agent Registry and management for custom and 3rd party agents



How do you make AI agents as trusted as your best employees?



Security Across the Environment

Building M365 Security foundations into enterprise-grade AI Solutions

M365 Copilot
Harden identity and data controls in M365

Copilot Studio + Azure AI Foundry
Extend M365 protections to app-level governance

Visual Studio/GitHub/ Azure AI Foundry
Secure the platform, data, models, and operations

Securing AI — **AI for Security**

Identity and Agent Access Management

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

Microsoft Purview

Manage, protect and govern data across your entire organization.

Microsoft Defender XDR and Sentinel Graph

Centralize telemetry and advanced threat protection across the enterprise.

Security Copilot

Rapidly analyze threats, investigate incidents, and automate response actions.

Agent365

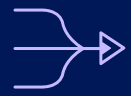
Features of Agent365

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.

slalom

Microsoft 365 E7

The Frontier Worker Suite

Microsoft 365

Microsoft 365 E5 + Entra Suite

Secure productive work

Microsoft 365 Copilot

AI built for work

Microsoft Agent 365

Control plane for agents

General Availability May 1, 2026

slalom

Agent365 Readiness Pilot

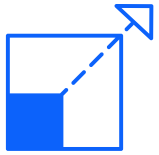
Features of Agent365

Phase 1: Strategy Understand readiness to deploy and manage agents	**Phase 2: Governance** Establish policies for agent creation and use	**Phase 3: Configure** Configure and pilot governance, security, and operational models for agents	**Phase 4: Transition** Iterate and standardize how agents are created, controlled, and deployed
• AI Agent readiness assessment • Risk and security gap analysis • Agent use case prioritization	• Agent Lifecycle Management Process • Secure Agent architecture design • Agent design standards • Reusable agent templates	• Agent testing and validation procedures • Pilot Identity Controls for Agents • Pilot Data Protections for Agents • Pilot Reusable agent templates	• Pilot Results and Insights • Policy Adjustments • Refined Agent deployment model

Ways Slalom Can Help

Agent 365 Use cases

M365 Copilot Rollout and Adoption



Power Apps and Power Platform

Permissions Management

Application Refactoring

Change Management and Adoption

Governance Planning

Custom Policy Replacements

Post-Migration Support

slalom

Agent365 Readiness Pilot

Features of Agent365

	STRATEGY	GOVERNANCE	CONFIGURE	TRANSITION
PHASE	**Phase 1**	**Phase 2**	**Phase 3**	**Phase 4**
• Assess AI agent security readiness across identity, data governance, and platform controls.				
• Evaluate existing controls in Microsoft Entra ID and Microsoft Purview that govern data and access used by agents.				
• Identify sensitive data sources and systems agents may access.				
• Identify high-value agent use cases, data sources available for access				
• Assess governance maturity for Agent Management				
• Define governance structure for oversight of agent development, deployment, registration, and knowledge source usage.				
• Establish lifecycle management processes for agent approval, monitoring, and retirement.				
• Define agent identity controls, permissions, and RBAC for agents (i.e. conditional access)				
• Establish data access policies for agents {i.e. DLP policies and Sensitivity Label incorporation)				
• Configure identity and access controls for agents.				
• Implement pilot data protection policies and monitoring using Purview				
• Pilot reusable agent templates				
• Validate agent security controls through testing and monitoring				
• Evaluate pilot outcomes to identify gaps and improvements				
• Refine policies for agent deployment, monitoring, and lifecycle management operating model				
• Standardize controls for secure agent creation and access management				
• Document operational procedures for ongoing governance and risk monitoring				
• Establish a roadmap to scale agents with consistent security controls.				

slalom

slalom | Microsoft

Solution Areas

Our Global Microsoft Cloud team offers expertise in the following solution areas

AI Business Solutions

Modern Work

M365 Copilot + Agents, M365, Viva, Teams, SharePoint Online, SAM + RIM,SP Embed, Exchange Online, SharePoint Premium

What We Do

- Transition to cloud/consolidate M365 tenants
- App rationalization + roadmap
- Modern Work Governance
- Migrations (platform, apps, legacy)
- Modernize endpoint management
- Enable frontline workers
- Cultivate modern employee experiences
- Copilot Readiness, rollout and AI agents
- AI-powered content processing
- Headless content apps
- Modernize communications
- Knowledge management

2026 Initiative

- Teams Voice
- W365

D365 & Power Platform

Customer Engagement (CE), Customer Insights (CI), Power Apps, Power Automate, Copilot Studio

What We Do

- Personalize customer experience
- Implement all Dynamics CE modules
- Data unification and customer profiling
- Rapidly build apps
- Automate business processes
- Discover business insights
- Low-code development & analytics COEs
- Finance and Operations (F&O) modules

Cloud and AI Platform

Azure Infrastructure

Blueprints, Enterprise Scale, CAF, Azure Migrate, Infra as Code, VMWare on Azure

What We Do

- Extend and Uplift your VMWare estate to Azure
- Deploy cloud adoption framework and enterprise scale architecture
- Establish Infrastructure as Code practices
- Migrate servers to IaaS, PaaS, and/or Containers
- Modernize user compute on Azure Virtual Desktop
- Optimize Azure service consumption / performance

Not Considering

- SAP on Azure migrations
- Azure Stack hardware

Azure Applications

.NET, DevOps, Cloud Development, AKS, Serverless, API Management, GitHub, Azure Functions, Logic Apps

What We Do

- Refactor, rearchitect, rebuild and rehost legacy .NET and Java apps with PaaS, low code and managed databases
- Design and build cloud native applications and integrations
- Drive DevOps excellence with GitHub and Azure DevOps
- Train and assist development teams on best practices for cloud solutions
- GitHub Enterprise Cloud and Advanced Security migrations and adoption

Azure Data & AI Services

Fabric, Power BI, Synapse, Azure OpenAI, Data Lake, Data Factory, Databricks, AI Foundry, Machine Learning, Cosmos DB

What We Do

- Analytics roadmaps
- Intelligent platforms for Data + AI
- Data analytics cloud governance
- Ingestion frameworks
- Data Modernization
- Copilot for Power BI and Fabric
- IoT architecture design patterns

Not Considering

- HoloLens
- Gaming

Security

Microsoft Security

Entra ID, Agent 365, Purview, Intune, Defender Suite, Sentinel, Security Copilot, Microsoft Security Adoption Framework

What We Do

- Assess & Build Zero Trust foundations
- Securing AI and AI for Security
- Modernize security/defend against threats
- Protect and govern sensitive information, files, and structured data sets
- Secure Azure, hybrid & multi-cloud services
- Build entitlements and user/app lifecycles

Not Considering

- Penetration tests
- Audits/certifications