



Agentic Control and Management

Govern, operate,
and secure your
digital workforce

Accelerate and de-risk enterprise-wide AI agent adoption with Agentic Control and Management from Capgemini.

Your agentic workforce needs a HR department

AI agents have the potential to revolutionize productivity and business agility. But without full visibility and control, enterprises face a growing risk of shadow AI, identity sprawl, unmanaged permissions, audit gaps, and compliance exposure.

When agents become your digital workforce, you need a digital workforce department to manage them. That's what Agentic Control and Management delivers: a unified framework to deploy, secure, and manage AI agents at enterprise scale, powered by Microsoft Agent 365.

Scale AI agents safely and responsibly with Capgemini

Unified control plane

We make Agent 365 your command center for AI agents, so every agent is registered, owned, permissioned, monitored, and managed. You stay in control of every agent in your organization through a single console, each with an ownership and sponsorship model, and defined access boundaries and least-privilege permissions.



Embedded security and compliance

We build enterprise-grade security and responsible AI guardrails into every layer, while discovering shadow agents and either onboarding or retiring them.

To keep your agents operating reliably, safely, and within defined boundaries, we secure your digital workforce with:

- **Purview** for data governance, data loss prevention(DLP) enforcement, auto labeling, and auditing
- **Defender** for agent behavior analytics and threat detection
- **Sentinel** for security operations center (SOC)-level monitoring and incident correlation
- **Agent 365 Runtime Shield** for runtime guardrails mapped to open worldwide application security project (OWASP) large language models (LLM) and agentic risks
- **Microsoft Foundry Control Plane** for evaluations, safety testing, and continuous improvement

Continuous monitoring and lifecycle management

To ensure agents meet expectations and continuously improve, we define success criteria and establish regular reviews and structured improvement cycles, so agent owners can monitor performance, gather user feedback, and trigger refinements. And when an agent falls short, alerts go out and a structured refinement process is introduced.

The Capgemini difference

- Official Microsoft launch partner for Agent 365, with proven governance frameworks and accelerators
- Proven delivery of agentic workforce management using Agent 365 and Microsoft 365 Copilot
- Structured approach to agent design, deployment, and lifecycle management
- Role-based enablement, AI Centers of Excellence, and change management
- End-to-end delivery from strategy to operation – we build it, run it, and continuously improve it
- Support for enterprise-wide agentic transformation from the Agentic Industry Studio

Five steps to a well-managed digital workforce

Assess

- Inventory all agent – including Microsoft agents, in-house and third-party agents, and shadow AI – across departments and hyperscalers, and identify unauthorized tools and unmanaged deployments
- Evaluate current identity management, DLP policies, threat detection, and observability capabilities against governance requirements
- Clarify the business objectives and pain points driving, and identify high-priority use cases
- Score maturity across the three governance pillars using the Capgemini Maturity Model
- Identify regulatory and compliance gaps, security risks, and priority use cases for governed agents



Plan

- Configure a single console across Agent 365, Copilot Studio, and Microsoft Foundry for managing all agents
- Create agent blueprints, including Entra ID identities, ownership, permissions, and access boundaries for every agent
- Define security templates, with predefined policies for DLP, logging, monitoring, conditional access, and acceptable use
- Determine the managed agentic lifecycle, including governance gates, release readiness criteria, and structured feedback and review processes

Deploy

- Launch the Agent 365 Control Plane, with centralized agent registry and integration with Entra ID, Purview, Defender, and Sentinel
- Onboard 1–3 pilot agents through the governance gate, with validated blueprints, assigned ownership, identities provisioned, and security templates applied
- Activate the observability layer, including real-time telemetry, identity-tagged audit logs, and DLP enforcement
- Enable threat detection and runtime defense with Defender and Sentinel monitoring agent behavior

Operate

- Monitor agent compliance, performance, and security in real time through the observability layer
- Run continuous threat detection and shadow agent scanning to catch unauthorized tools and emerging risks
- Conduct regular reviews of technical KPIs (uptime, error rate) and business KPIs (queries resolved, time saved, user satisfaction)
- Manage incident-handling by defining escalation tiers and fallback procedures, and equipping teams with best practices and knowledge articles

Scale

- Onboard agents under full governance and apply standardized blueprints and security templates across all departments
- Formalize an AI Center of Excellence for long-term governance and AI agent management
- Embed structured feedback loops, with user feedback channels, performance-triggered retraining, and agent retirement processes for underperformers
- Ensure agent management drives value, not just compliance, by tracking ROI per agent, including incidents prevented, time saved, cost savings, NPS, and revenue impact

Learn more

To find out more about how you can control, manage, and secure your digital workforce with Capgemini, get in touch at infra.global@capgemini.com

For more details, contact:

infra.global@capgemini.com

About Capgemini

Capgemini is the business transformation partner for enterprises in the age of AI. We help organizations imagine and build an intelligent, sustainable future, combining AI, technology and human ingenuity to transform how they operate, innovate and grow. With unique end-to-end capabilities spanning strategy, technology, engineering and intelligent operations, we bring together deep industry expertise and market-leading capabilities in AI, cloud and data to turn ambition into measurable business outcomes at scale. Supported by a robust ecosystem of partners and nearly 60 years of expertise, Capgemini is a responsible and diverse global organization of over 410,000 team members in more than 50 countries. The Group reported 2025 revenues of €22.5 billion.

Make it real.

www.capgemini.com

