

Enterprise Governance for AI Agents: The Control Layer Has Arrived

MANAGEMENT SUMMARY & CORE TAKEAWAY

The answer to agent sprawl has arrived: Google, UiPath, GitLab and Salesforce rolled out concrete enterprise controls for AI agents within 72 hours — centralized license and security management, usage caps, sandbox restrictions. Enterprises can now scale agents in a controlled way, provided they actively govern the control layer rather than merely installing it.

CONTEXT & EXECUTIVE RELEVANCE

In just three days, four major vendors independently sent the same signal. On August 19, UiPath launched Maestro Flow, a developer-first orchestration canvas that gives coding agents such as Claude Code, Cursor and GitHub Copilot enterprise-grade durability and governance. The same day, Salesforce published data showing how fast the underlying problem has grown: customers' AI agent 'headcount' tripled between February 2025 and April 2026. On August 20, GitLab shipped version 19.3, introducing usage caps for GitLab Credits, group-level visibility restrictions for custom agents, and a production-ready Secrets Manager. And on August 21, Google folded Antigravity into Gemini Enterprise subscriptions, adding admin controls for licenses, security and spend, sandbox restrictions, and approval gates for terminal commands.

The pattern is unmistakable. After a year in which enterprises were largely occupied with agent sprawl — fleets of agents multiplying without central oversight — the major platforms are now delivering the technical answer. The question has shifted from 'how do we build an agent' to 'how do we keep a hundred of them under control.'

CORE ACTION ITEMS

- 01 Google Antigravity (Aug 21): admin controls for licenses, security and spend, sandbox restrictions, mandatory approval for terminal commands — now part of Gemini Enterprise.
- 02 UiPath Maestro Flow (Aug 19): a developer orchestration canvas connecting coding agents to enterprise-grade durability and governance.
- 03 GitLab 19.3 (Aug 20): usage caps for Credits, group-level visibility restrictions for custom agents, general availability for the Flow Creator Agent, Secrets Manager support.
- 04 Salesforce data (Aug 19): agent 'headcount' tripled in 15 months, time to activation down 53%, average actions per account growing at a 31% CAGR per month.

SWISS COMPLIANCE & ARCHITECTURE GUIDELINES

- ☑ Full compliance with revised Swiss Data Protection Act (revDSG).
- ☑ Zero vendor lock-in on closed proprietary models.
- ☑ Seamless integration into Abacus, Bexio and M365 ecosystems.

Non-Binding Process Analysis

Let us review in 20 minutes where AI agents create immediate measurable efficiency in your workflows.

ki-outsourcing.ch