

Enterprise Agent Infrastructure: The Missing Layer Between Agent and Production

MANAGEMENT SUMMARY & CORE TAKEAWAY

Enterprise agent infrastructure is the operational layer between a working AI agent and its safe, production-grade operation: identity, policy enforcement, sandbox isolation, observability and a deployment harness. Four major launches within a single week in August 2026 show that most companies still lack this layer – and that is exactly where agent projects fail.

CONTEXT & EXECUTIVE RELEVANCE

Between 11 and 19 August 2026, four major vendors published their version of the same answer within eight days of each other. Red Hat extended OpenShift AI with OpenShell. Google expanded its Gemini Enterprise Agent Platform with a runtime, registry and gateway. BCG introduced the Enterprise AI Control Plane (EACP), a vendor-agnostic governance layer. And IBM rolled out its watsonx Agentic Control Plane across AWS and IBM Cloud. The timing is not a coincidence. All four platforms solve the same problem: the operational gap between a working agent prototype and its safe, controlled operation at enterprise scale.

An agent control plane is not a new AI capability. It is the operating layer underneath it. It answers five questions that no individual agent application can answer on its own:

CORE ACTION ITEMS

- 01 Identity: which agent acts on whose behalf, with which permissions?
- 02 Policy enforcement: which actions is an agent allowed to take, and which not – enforced at the process level, not only in a prompt?
- 03 Sandbox isolation: how do you prevent a malfunctioning agent from reaching systems it was never meant to touch?
- 04 Observability: can you reconstruct, after the fact, exactly what an agent did, when, and why?

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