

Enterprise-Governance für KI-Agenten: Die Kontroll-Schicht ist da

MANAGEMENT SUMMARY & KERNAUSSAGE

Die Antwort auf Agent Sprawl ist da: Google, UiPath, GitLab und Salesforce haben innerhalb von 72 Stunden konkrete Enterprise-Controls für KI-Agenten ausgerollt – zentrale Lizenz- und Sicherheitsverwaltung, Nutzungslimiten, Sandbox-Beschränkungen. Schweizer Unternehmen können ihre Agenten damit erstmals kontrolliert statt chaotisch skalieren, sofern sie die Kontroll-Schicht aktiv nutzen und nicht nur bereitstellen.

KONTEXT & RELEVANZ FÜR ENTSCHEIDER

In nur drei Tagen haben vier grosse Anbieter unabhängig voneinander das gleiche Signal gesendet: Am 19. August hat UiPath mit Maestro Flow eine Orchestrierungs-Oberfläche für Entwickler lanciert, die Coding-Agenten wie Claude Code, Cursor oder GitHub Copilot mit Enterprise-Tauglichkeit – also Persistenz und Governance – ausstattet. Am selben Tag hat Salesforce Zahlen veröffentlicht, die zeigen, wie schnell das Problem gewachsen ist: Die «Agenten-Belegschaft» der Kunden hat sich zwischen Februar 2025 und April 2026 verdreifacht. Am 20. August hat GitLab mit Version 19.3 Nutzungslimiten für GitLab Credits, eingeschränkte Sichtbarkeit für Custom Agents auf Gruppenebene und einen produktiven Secrets Manager eingeführt. Und am 21. August hat Google Antigravity in die Gemini-Enterprise-Abonnements integriert – mit Admin-Kontrollen für Lizenzen, Sicherheit und Ausgaben, Sandbox-Beschränkungen und Freigabe-Gates für Terminal-Befehle.

Das Muster ist eindeutig: Nachdem Unternehmen im letzten Jahr primär mit dem Agent Sprawl beschäftigt waren – also mit unkontrolliert wachsenden Agenten-Flotten ohne zentrale Übersicht – liefern die grossen Plattformen jetzt die technische Antwort darauf. Nicht mehr «wie baue ich einen Agenten», sondern «wie behalte ich hundert davon unter Kontrolle».

KERN-HANDLUNGSEMPFEHLUNGEN

- 01 Google Antigravity (21. Aug.): Admin-Kontrollen für Lizenzen, Sicherheit und Spend, Sandbox-Restriktionen, Freigabe-Pflicht für Terminal-Kommandos – integriert in Gemini Enterprise.
- 02 UiPath Maestro Flow (19. Aug.): Orchestrierungs-Canvas für Entwickler, verbindet Coding-Agenten mit Enterprise-Grade-Persistenz und -Governance.
- 03 GitLab 19.3 (20. Aug.): Nutzungslimiten für Credits, gruppenweite Sichtbarkeitsbeschränkung für Custom Agents, GA für den Flow Creator Agent, Secrets-Manager-Unterstützung.
- 04 Salesforce-Daten (19. Aug.): Agenten-«Headcount» hat sich in 15 Monaten verdreifacht, Aktivierungszeit sank um 53%, durchschnittliche Aktionen pro Konto wachsen mit 31% CAGR pro Monat.

SCHWEIZER UMSETZUNGSKRITERIEN (REVD SG & IT-ARCHITEKTUR)

- ☑ Vollständige Konformität mit dem neuen Schweizer Datenschutzgesetz (revDSG).
- ☑ Keine Abhängigkeiten: Zero Lock-In auf proprietäre geschlossene Modelle.
- ☑ Schnittstellen zu Schweizer ERPs (Abacus, Bexio, M365) im operativen Betrieb.

Unverbindliche Prozess-Analyse

Lass uns in 20 Minuten prüfen, wo KI-Agenten in deinem Unternehmen sofort messbare Entlastung schaffen.

ki-outsourcing.ch