Gravitee Warns of ‘Invisible Risk’: Nearly Half of AI Agents Run Without Oversight

While 3M AI agents transform US/UK firms, 47% lack security oversight-leaving 1.5M at risk of going rogue as 88% of businesses report recent security incidents.

NEW YORK, NY, UNITED STATES, February 4, 2026 /EINPresswire.com/ -- The study’s key findings highlight a widening gap between rapid deployment and effective oversight:

- Large firms in the US and UK have rolled out 3 million AI agents, with plans for millions more in 2026.
- Almost half of agents (47%) are not actively monitored and not secured: an estimated 1.5 million at risk of going rogue
- 88% of firms say they have already experienced or suspected an AI agent-related security or data privacy incident in the last twelve months.

Gravitee, the open-source leader in Agentic API and event management, today announced new research that reveals that nearly half of the 3 million AI agents deployed by enterprise firms are ungoverned and at risk of ‘going rogue’.

The new research of 750 CTOs and tech VPs was carried out on behalf of Gravitee, a leading provider of API management and agentic AI solutions.

AI agents, autonomous ‘digital workers’ that execute complex tasks without human interference, are expected to bring productivity gains to firms across the globe. But this new research reveals that they are being deployed faster than security teams can keep up.

Without proper governance, AI agents can ‘go rogue’ - exhibiting unintended or unwanted behaviours such as making incorrect decisions, exposing data, or triggering security breaches.

The new data suggests that there are more than 1.5 million ungoverned AI agents already operating at major firms, presenting a significant risk to consumers and businesses alike.

88% of firms say they have already experienced or suspected an AI agent-related security or data privacy incident in the last twelve months. In some cases, AI agents have exposed confidential data, acted on outdated or incomplete information or deleted databases without permission.

These missteps underscore the risks of deploying autonomous systems without guardrails.

“There are now over 3 million AI agents operating within corporations, a workforce larger than the entire global employee count of Walmart,” said Rory Blundell, CEO of Gravitee “But far too often, these autonomous agents are left ungoverned and unchecked. Every day, I hear stories of catastrophic data leaks and unauthorized deletions. Without governance, these agents will stop being productivity gains and start becoming liabilities: a danger to consumers and businesses alike.”

The research forms part of Gravitee’s State of AI Agent Security 2026 report, released today

Gravitee’s AI Agent Management platform gives organizations the power to secure, manage, and observe interactions between APIs, Events, and Agents - all within the same unified framework. The Denver-based software provider was recognised by Gartner® as a Leader in the 2025 Gartner Magic Quadrant™ for API Management.

In January, Gravitee launched Gravitee 4.10: establishing the non-negotiable foundation for AI Agent Management, controlling identity, access, policies, and trust for every agent interaction. It allows teams to run AI agents in production with the same discipline they already apply to APIs and event streams. Last year, Gravitee hosted the inaugural A2A (Agent-to-Agent) Summit - the world’s first conference for the A2A protocol, bringing together the industry’s brightest minds to shape how this new ecosystem evolves.

ENDS

About Gravitee
Gravitee.io, with a valuation of over $300m, is the open-source leader in Agentic API & Event Management. The Gravitee platform empowers enterprises to design, secure, and govern APIs, event streams, and AI-driven interactions across hybrid, multi-cloud, and edge environments. With a federated, agent-ready approach and native support for real-time traffic and autonomous agents via the Gravitee Agent Mesh, Gravitee enables secure, scalable, and intelligent connectivity in an increasingly complex ecosystem.

Methodology
On behalf of Gravitee, Opinion Matters surveyed 750 (500 US, 250 UK) individuals with the job titles: CIOs & CTOs, VPs of engineering / DevOps, Heads of Platform / API Management working in banks and enterprise firms with 250+ employees, across a range of industries.
Survey conducted in December 2025.

Nicholas Bennett
Gravitee
nicholas.bennett@graviteesource.com
Visit us on social media:

LinkedIn