FIOR launches AI Gateway 26.2 to help enterprises find and control AI agents

New release adds features in discovery of tools as well as agents, threat intelligence, NVIDIA OpenShell integration and ANS integration

LONDON, UNITED KINGDOM, November 12, 2026 /EINPresswire.com/ -- • AI Gateway 26.2 discovers the AI models, agents and tools operating across an organisation's systems, identifies each one with a cryptographically secure passport, and enforces what it is permitted to do before it acts
• Deploys across public and private cloud, customer data centres, edge locations and disconnected environments, so organisations avoid lock-in to a single cloud, AI provider or hosted service
• Feeds strengthened threat intelligence directly into policy and enforcement decisions, so observed threats and unsafe behaviour shape what each agent is permitted to do

FIOR Group today launched AI Gateway 26.2, the latest version of its core product, giving organisations a single point of control to discover, identify and govern the AI models, agents and tools operating across their systems, wherever those systems are hosted.

As AI adoption spreads across enterprise estates, organisations increasingly face a discovery problem before they face a governance problem. AI models, agents, development assistants, tools and machine-to-machine services can appear across workloads and networks without becoming part of a centrally managed security architecture. Many organisations still rely on inventories, policy documents and post-event analysis to manage that risk, none of which can identify or stop an agent's action in real time.

AI Gateway 26.1 closes that gap by sitting directly between an organisation's systems and the AI they use, where it can see and act on AI activity as it happens.

The new release combines Sensor, Tool Catalogue, Model Catalogue, Threat Intelligence and Agent Identity upgrades within a single architecture that can be deployed in public or private clouds, in customer data centres, at edge locations or in environments with restricted or no external connectivity, with the same controls applied whichever AI models and tools are in use.

FIOR Sensor discovers that activity across hosts, applications and networks, and each model, agent or tool it uncovers can be linked to an identity. The Gateway then evaluates each

requested action against organisational policy and the approved models and tools held in FIOR's Tool and Model Catalogues, blocking anything that falls outside permissions deterministically before the action is executed.

The release also strengthens FIOR's Threat Intelligence capability, which feeds security evidence directly into the Gateway's policy and enforcement decisions. Observed threats and unsafe agent behaviour can shape each decision as it is made, taking threat intelligence beyond standalone monitoring tools and into live enforcement. For security teams, this shortens the distance between identifying a threat and acting on it.

AI Gateway 26.2 is an infrastructure-neutral platform, so security-sensitive AI traffic can remain within an organisation's own security boundary, with no requirement to route it through a FIOR-hosted service. That independence allows organisations to change or add cloud and AI providers without rebuilding their security controls or becoming locked into a single vendor.

AI Gateway 26.2 is also ready to integrate with NVIDIA OpenShell, an open-source runtime that executes autonomous AI agents in policy-controlled sandboxes. In a combined deployment, OpenShell isolates and supervises each agent as it runs, while FIOR's AI Gateway verifies which agent is acting, governs which models and tools it may use, applies organisational policy and threat intelligence, and records each decision as security evidence.

Finally, in line with The Linux Foundation launch of the Agent Name Service (ANS), an open standard that gives AI agents an identity issued as P-256 agent certificates, AI Gateway 26.2 includes ANS integration in the FIOR AI Gateway, so customers can use ANS identities for their AI agents from day one.

The FIOR AI Gateway takes an agent's ANS identity and strengthens its cryptographic security, giving customers superior identity security for every agent. It brings ANS together with FIOR's advanced authority controls: the customer decides what each agent may do, under their own sovereign control. FIOR believes that most customers want sovereign AI identity where no data on the existence or activities of their AI agents are shared with an identity provider, which is how FIOR AI Gateway is built. But customers now have a choice to include ANS amongst the many possible factors used to create a cryptographically secure agent identity.

James Patrick, Chief Technology Officer at FIOR, said:
"Enterprise AI security starts with being able to see what exists, identify what is acting and control what it can reach. AI Gateway 26.2 is a significant leap forward in each of those areas. Many organisations cannot yet say which AI models and agents are running across their systems, and no policy can govern what it cannot see. And because the Gateway runs wherever our customers' AI runs, they can secure it without handing control to any single vendor, including us."

ENDS

NOTES TO EDITORS

About FIOR
FIOR is the identity and enforcement layer for AI.

FIOR's AI Gateway enables organisations to identify all AI agents, issue unique cryptographically secure passports to each agent, determine what each agent is authorised to do and enforce those permissions before actions are executed.
Designed to operate across organisational and technology boundaries, FIOR provides cryptographic identity, deterministic policy enforcement, rapid revocation and tamper-evident audit capabilities for autonomous AI systems.
FIOR works with enterprises, governments, technology companies and infrastructure providers seeking to deploy AI agents securely and at scale.
www.fior.group

Media contacts
Henry Lerwill & Francesca Eaton, Hawthorn Advisors
fior@hawthornadvisors.com

David Williams
Fior Group Limited
Visit us on social media:
LinkedIn

This press release can be viewed online at: https://www.einpresswire.com/article/956092349

EIN Presswire's priority is source transparency. We do not allow opaque clients, and our editors try to be careful about weeding out false and misleading content. As a user, if you see something we have missed, please do bring it to our attention. Your help is welcome. EIN Presswire, Everyone's Internet News Presswire™, tries to define some of the boundaries that are reasonable in today's world. Please see our Editorial Guidelines for more information.
© 1995-2026 Newsmatics Inc. All Right Reserved.