Ory Launches Agent Security, the First Agent IAM Control Plane for Enterprise AI

Patent-pending architecture embeds identity and access controls at the point where AI agents invoke tools, execute commands, and take action

SCOTTSDALE, AZ, UNITED STATES, June 9, 2026 /EINPresswire.com/ -- Ory, one of the world's most widely adopted platforms for customer, workforce, and agent identity management, today announced the availability of Ory Agent Security, the first Agent IAM control plane designed to secure AI agents at the point where they take action.

As organizations rapidly deploy AI-powered coding assistants and autonomous agents across development environments, security teams face a growing challenge. Most security approaches focus on the perimeter, governing credentials, network access, or protocol boundaries. Yet the most important security decision occurs before, at the moment an agent decides to execute a command, invoke a tool, access data, or interact with a business system.

> Ory's plugin-based approach provides a flexible foundation for securing and governing agent-driven workflows.""
>
> *Simon Moffatt, Founder and Analyst, The Cyber Hut*

Most AI security products secure the perimeter. Ory secures the action.

Ory Agent Security takes a fundamentally different approach. Its patent-pending architecture embeds identity, authorization, and governance controls directly into the agent harness, the software layer that connects AI agents to tools, APIs, files, and enterprise systems. This enables organizations to evaluate and enforce policy before actions are executed rather than after the fact.

"The enforcement point that matters is not where an agent connects to infrastructure. It's where the agent decides to act," said Jeff Kukowski, CEO of Ory. "Most AI security products secure the perimeter. Ory secures the action. By embedding a control plane directly into the agent harness, organizations can apply identity, authorization, and governance controls exactly where they

matter most. As AI agents become part of critical workflows, Agent IAM is emerging as a foundational layer of enterprise security."

Unlike approaches that focus primarily on gateways, credentials, proxies, or protocol-level controls, Ory Agent Security evaluates authorization decisions within the agent harness itself, at the point where actions are dispatched. At the moment an action is requested, the platform evaluates the agent identity, delegated user identity, requested tool, command parameters, and applicable policy before allowing the action to proceed.

Built for enterprise AI adoption, Ory Agent Security enables organizations to:
• Authenticate AI agents before they access enterprise systems, data, and services.
• Apply fine-grained authorization policies that govern what agents are permitted to do.
• Control and monitor agent access to tools, APIs, and downstream resources.
• Enforce security policies throughout the agent lifecycle using an event-driven architecture.
• Capture comprehensive audit trails of agent actions, decisions, and security-relevant events.
• Extend security controls through a flexible plugin framework that allows organizations to implement governance controls tailored to their risk requirements.

As AI agents become increasingly capable of executing tasks, invoking tools, accessing sensitive information, and interacting with business systems, organizations require more than traditional access management. Ory Agent Security provides a framework for governing not only agent identity, but also how agents interact with tools and systems, helping organizations establish trust, accountability, and control over agent-driven workflows.

By enforcing policy at the point where actions originate, Ory helps organizations address emerging AI security risks that traditional controls often struggle to govern, including prompt-injection-driven actions, unauthorized tool usage, excessive permissions, and agent behavior that occurs outside conventional protocol boundaries. The result is a consistent security layer that operates independently of the underlying model, framework, or transport mechanism.

"Agentic AI is exposing identity and governance gaps that traditional access control models were never designed to address," said Simon Moffatt, founder and analyst at The Cyber Hut. "Organizations need visibility into who is acting, what tools agents can access, and how decisions are made. Ory's plugin-based approach provides a flexible foundation for securing and governing agent-driven workflows."

Ory Agent Security is available immediately. For pricing, deployment information, and product details, visit https://www.ory.com/agent-security.

About Ory
Ory is the modern identity platform for customer identity and access management (CIAM), B2B IAM, and Agent IAM. Ory is one of the world's most widely adopted IAM platforms and manages more than 2.5 billion identities across open source and commercial deployments. Ory's

infrastructure powers 10 percent of the top 40 websites and serves leading enterprises in financial services, technology, media, and other sectors requiring flexible, high performance identity solutions. With over 45,000 GitHub stars and 700 million downloads, Ory delivers enterprise grade security with developer friendly flexibility. Ory is backed by investments from Insight Partners, Balderton Capital, PHX Ventures, and IQT. For more information, visit www.ory.com.

Press
Ory Corp
+1 347-560-5798
email us here
Visit us on social media:
LinkedIn
