Ory Expands AI Agent Security From Development Through Production With New Build and Deploy Capabilities

Embedding identity and security guardrails during agent development extend controls into production, completing Ory's four-stage Agent Security Lifecycle.

SCOTTSDALE, AZ, UNITED STATES, October 22, 2026 /EINPresswire.com/ -- Ory, one of the world's most widely adopted platforms for customer, B2B, and agent identity management, today announced new Build and Deploy capabilities for Ory Agent Security. Build lets developers write identity-aware guardrails directly into custom AI agents and Deploy carries those controls into production consistently and at scale. Combined with Ory's existing Observe and Enforce capabilities, the launch completes Ory's four-stage Agent Security Lifecycle. Ory is the first identity vendor with generally available products at every stage, on a single platform.

> Every agent needs a verifiable identity, clearly defined authority, and accountability for the actions it takes, precisely where the action occurs."
>
> *Jeff Kukowski, CEO, Ory*

Building an AI agent has never been easier, but securing one has not kept pace. Traditional identity controls can verify the person or service account behind an agent, but they reveal far less about what a delegated agent attempts, on whose behalf, and with what authority. An AI agent may have legitimate access to a production environment without legitimate authority to delete a database, export customer records, or modify sensitive configurations. The distinction between possessing valid credentials and being authorized to perform a particular action is where traditional identity models can fall short.

With Build, developers establish an agent's identity, instrumentation, and guardrails while the agent is being written. With Deploy, the same identity, policy and credentials go with the agent into every environment where it runs. Observe and Enforce then act on that identity at runtime. The result is one identity and policy foundation for the agent's entire life.

"The industry has applied considerable focus to how to make AI agents more capable. Now we have to make them accountable," said Greg Vesper, Chief Product Officer at Ory. "To operate at scale, that starts long before an agent reaches production. With Build and Deploy, we're bringing identity, permissions, and security directly into the development process, then carrying those controls into the environments where agents actually operate. Developers can move fast, while security teams retain visibility and control over what those agents are authorized to do."



Ory Agent Security connects the four complementary capabilities of Build-Deploy-Observe-Enforce.



Ory works with the agents, frameworks and deployment methods you already use.

What's new: Build and Deploy

- Build integrates agent identity, policy, instrumentation, and security guardrails directly into custom AI agents using supported developer SDKs and frameworks.
- Deploy brings agent identities, permissions, and security configurations into production through deployment-ready integrations and automated credential management.

Existing capabilities: Observe and Enforce

- Observe enables organizations to see which agents are operating, who or what they're acting on behalf of what actions they attempt, and how policies evaluate those actions.
- Enforce authorizes or denies agent actions at runtime, including individual tool calls and commands, using fine-grained policies applied at the point of execution, from the project level down to sub-agents.

The Agent Security Lifecycle

Ory Agent Security connects the four complementary capabilities of Build-Deploy-Observe-Enforce. Organizations can jump in at any point in the lifecycle, even if they already have agents running in production, expanding their visibility and control progressively over time.

Teams developing new agents can embed identity and security controls from the start. Organizations with agents already operating in production can begin by observing their behavior, then introducing policy enforcement without having to rebuild those agents.

Because all four stages share a common identity and policy foundation, organizations can continuously refine as requirements evolve.

“Partnering with Ory allows us to deliver real, deterministic agent security today, not just future roadmap promises,” said John Poptsis, Managing Director at TeleGlobal.

Identity: the vital ingredient for defense in depth

Endpoint, network, silicon, gateway and agent-harness controls each address different risks; layered defenses make sense, yet all are individually incomplete. Ory provides the underlying identity and policy layer, giving every agent a verifiable identity, defined permissions, and policies that govern what it can do and for how long.

“Defense in depth for agent security is no longer a nice-to-have – it’s now vital. And identity has emerged as the core foundation,” said Jeff Kukowski, CEO of Ory. “Every agent needs a verifiable identity, clearly defined authority, and accountability for the actions it takes, precisely where the action occurs. With new capabilities that address all stages of the Agent Security Lifecycle, Ory is establishing the identity fabric enterprises need to innovate confidently and safely in the Agentic Era.”

Availability

Build and Deploy, as well as Observe and Enforce capabilities are available today as part of Ory Agent Security. Learn more at www.ory.com/agent-security.

###

About Ory
Ory is identity security for the Agentic Era. Built on open standards and trusted at global scale, Ory delivers customer identity and access management (CIAM), B2B IAM, and Agent IAM and security through a unified platform. As one of the world’s most widely adopted IAM solutions, Ory manages more than 3.25 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.

Media contact: Ory Corp · press@ory.com

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

This press release can be viewed online at: https://www.einpresswire.com/article/951372075

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.