

Ory Agent Security Brings Identity Enforcement Into the Agent Harness

Customers deploy Ory Agent Security because, "extending trust to non-human identity is vital"

SCOTTSDALE, AZ, UNITED STATES,
September 10, 2026 /

EINPresswire.com/ -- [Ory](#), one of the world's most widely adopted platforms for customer, B2B, and agent identity

management, today announced the general availability of Ory Agent Security, the first Agent IAM control plane designed to secure AI agents at the point where they take action.



Existing AI security controls can isolate an agent, monitor its activity or control traffic passing through a gateway, but they generally sit outside the agent itself. That leaves a fundamental gap between knowing what an agent did and controlling what it is allowed to do. Controlling what they are allowed to do is critical as AI agents are moving into enterprise environments faster than organizations can govern them.

“

Partnering with Ory allows us to deliver real, deterministic agent security today, not just future roadmap promises.”

*John Poptsis, Managing
Director at TeleGlobal*

Ory Agent Security closes that gap by enforcing identity and access policies directly inside the agent harness. It evaluates a tool action against policy before execution,

allows or denies the action, records that decision, and binds actions to an accountable owner and delegated agent identity. This creates a chain of accountability from the human who owns an agent through the agent, any sub-agents and the tools they invoke.

“AI agents act with human credentials and leave a record that cannot answer the only question that matters. If an AI agent took a destructive action in your environment tomorrow, what would your audit log say, and could you name the human who set it running?,” said Jeff Kukowski, CEO of Ory. “The security model has to evolve accordingly. Ory Agent Security puts control where the action happens, so organizations can enforce what their agents are allowed to do, and are actually doing, rather than simply observing it afterward. This is the difference between an agent program you can govern and one you are hoping stays contained.”

Ory Agent Security supports 11 leading agent harnesses and 14 agent SDK frameworks, including Claude Code, LangChain/LangGraph, OpenAI Agents SDK and Vercel AI SDK. This allows teams to apply the same identity and authorization model across the different agents and frameworks they use including custom-built agents.

Ory believes the best place to start getting control of agents is to “turn the lights on” so organizations can see and understand what agents are doing. That’s why the platform starts in observe mode by design, giving teams full visibility into the humans, agents, sub-agents and tools operating in their environment without blocking developers or slowing existing workflows. Organizations move into enforcement on their own timeline, applying controls that range from broad guardrails to fine-grained permissions. Policies can be revoked immediately, and every decision is captured through OpenTelemetry to support audit and security workflows.

Ory Agent Security is also designed for organizations that cannot put agent activity into a black-box security service. It can be self-managed in cloud, on-premises or air-gapped environments, or deployed through the Ory Network. The platform is built on standards including OAuth 2.1, OIDC, Zanzibar-style permissions and OpenTelemetry, allowing it to work alongside existing identity, security and infrastructure investments.

This approach builds on Ory’s identity infrastructure, which supports more than 3.25 billion identities, 4.4 billion transactions per day and more than 34,000 production deployments.

“Our clients trust TeleGlobal to manage and secure their critical technology infrastructure securely and with confidence, and as AI agents with non-human identities become embedded across the enterprise, identity, authorization, and governance become fundamental to maintaining that trust. Ory is a critical component of the TeleGlobal Compass™ framework because it provides enterprise-grade identity and access controls required to extend security and governance within the agentic AI environment. By integrating Ory into our managed services, we help clients move from AI experimentation to secure, governed AI adoption at scale, while preserving the flexibility to choose the AI platforms, agent frameworks that best support their business. Partnering with Ory allows us to deliver real, deterministic agent security today, not just future roadmap promises. More importantly, because Ory supports a wide range of agent harnesses and SDK’s, we can give our customers complete flexibility and choice in how they build, without forcing them to compromise on control or governance.” said John Poptsis, Managing Director at TeleGlobal.

Ory Agent Security is generally available today at <https://www.ory.com/agent-security> and can be deployed through the Ory Network or as a self-managed solution.

About TeleGlobal

TeleGlobal Consulting Group Inc. is an established Canadian Managed Services and Managed Security Services Provider (MSP/MSSP) with more than 27 years of experience helping small and

mid-sized public and private organizations manage technology, cybersecurity, governance, compliance and emerging technology risk. Through the TeleGlobal Compass™ framework, TeleGlobal's multidisciplinary team brings together Managed Services, Cybersecurity, Governance/Compliance, and AI Enablement to help organizations manage risk, strengthen resilience, and navigate technology change with confidence. Based in the Greater Toronto Area, TeleGlobal combines strategic advisory with practical implementation to deliver Simple, Scalable, Secure, and Strategic solutions aligned with business priorities, regulatory obligations, and evolving risk helping clients modernize, innovate, and grow responsibly. Visit www.teleglobal.ca.

About Ory

Ory is the modern identity platform for customer identity and access management (CIAM), B2B IAM, and Agent IAM. As one of the world's most widely adopted IAM platforms, 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.

Press

Ory Corp

+1 347-560-5798

[email us here](#)

Visit us on social media:

[LinkedIn](#)

This press release can be viewed online at: <https://www.einpresswire.com/article/941019448>

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.