Ory Launches ‘Ory Talos’ to Lock Down AI Agents and Non-Human Identities Running Unchecked Across Enterprise Networks

New solution replaces static, permanent API keys with dynamic, revocable, least-privilege credentials designed to govern AI agents at scale

SCOTTSDALE, AZ, UNITED STATES, June 4, 2026 /EINPresswire.com/ -- Ory, one of the world’s most widely adopted platforms for customer, workforce, and agent identity management, today launched ‘Ory Talos’, a solution for securing API keys and generating dynamic tokens for non-human identities, including AI agents. The announcement comes as enterprises continue to deploy AI agents in production at a pace that has far outrun the security controls in place to govern them.

> Organizations are asking the right questions about their AI agents: who are you, what are you doing, where can you go, and what do we do if you go rogue”
>
> *Jeff Kukowski, CEO, Ory Corp.*

AI Agents Are in Production. Security Isn't.

Non-human identities (NHIs) now outnumber human ones 144 to 1, according to Entro Labs research. A recent EMA survey commissioned by Ory found that more than 80 percent of organizations have already deployed AI agents in production. Only 21 percent have documented policies for governing them.

The results are predictable. Eighty percent of those organizations report agents exhibiting unplanned behavior(1). Thirty-nine percent have experienced unauthorized(2) access incidents. And roughly 60 percent of security and identity leaders(3) say their existing IAM stack is not ready for agentic AI.

Standard API keys make it worse. A static key never expires. Developers routinely grant admin-level access because it is easier than scoping permissions precisely. Keys get hardcoded into source code and uploaded to public repositories. Once a key has been distributed it needs human intervention for revocation which creates the problem of knowing if a key has been distributed in vulnerable places such as public repos or embedded in the code of an application.

As software-to-software traffic comes to dominate enterprise networks, the blast radius of any single compromised credential grows exponentially, and AI agents accelerate the vulnerability.

What ‘Ory Talos’ Does

Ory Talos transforms traditional API keys into programmable, hardened identities. It combines Macaroon-based delegation with token derivation to give organizations precise control over what agents can access, for how long, and from where. When something goes wrong, access can be revoked instantly.
The platform is built on the same high concurrency Go architecture as Ory Hydra, which powers OpenAI’s more than 900 million weekly active users. It is designed to handle the authentication throughput that large-scale agentic workflows demand without the performance degradation that strains legacy IAM platforms.

Talos’s key capabilities include:
• Macaroon-Based Delegation: Tokens support chained delegation, letting agents wrap keys with additional caveats as tasks move down the chain. A broad "use credit card" permission, for example, can be narrowed to "payments under $5.00" before being passed to a sub-agent. Permissions can only narrow, never expand.
• Token Derivation and Dynamic Secrets: Long-lived parent keys are exchanged on demand for short-lived child tokens. If a token is stolen, it expires in 15 minutes, not 15 months. Invalidating a parent credential kills all downstream child tokens instantly.
• Fine-Grained Scoping: Avoid over-permissioning by ensuring credentials are limited to only the access they require, in line with the principle of least privilege. For example, a key that needs read-only access should never be granted admin privileges, reducing risk if credentials are exposed or misused.
• IP Whitelists and Time to Live (TTL) Expiration: Keys can be restricted to specific server IPs and given hard expiration dates. Even a compromised credential has a strictly limited window.
• Token Prefixes: Short, human-readable strings attached to the front of API keys make credentials identifiable at a glance and scannable in public repositories to catch leaked keys early.
• Composable and Deployment-Flexible: Ory Talos runs as a standalone service and does not require adoption of the broader Ory platform. Organizations will be able to run it as Ory-managed SaaS or self-host on-premises or in a private cloud. Same code either way, no lock-in.

“Organizations are asking the right questions about their AI agents: who are you, what are you doing, where can you go, and what do we do if you go rogue,” said Jeff Kukowski, CEO, Ory. “But the problem is most have no infrastructure to answer any of them. Ory and Ory Talos change that.”

“A really interesting journey for Lumin with Ory is that we’ve gone from that B2B SaaS, pretty

standard kind of setup in the browser to a full AI-enabled platform," said Max Ferguson, Founder and CEO of Lumin. "Given the complexity of those flows alone, we wouldn't have been able to build that without Ory."

Availability
Ory Talos is generally available beginning June 4, 2025. For more information, visit http://www.ory.com/talos.

Ory provides multiple solutions designed specifically for securing AI agents. From fine-grained permissions and certified OAuth 2.1 authorization to securing API keys and developer plugins that enforce security best practices, Ory ensures your agentic workflows are hardened by design.

About Ory
Ory, the modern choice 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 http://www.ory.com/

(1) https://www.osohq.com/learn/why-your-authorization-model-wont-survive-agentic-ai
(2) https://www.sailpoint.com/identity-library/ai-agents-attack-surface
(3) https://www.ory.com/resources/whitepapers/agentic-ai-identity-security-readiness

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