Keeper Security Research Finds Over Half of European Orgs Have Experienced an NHI Security Incident in the Past Year

Survey of Infosecurity Europe 2026 attendees reveals adoption of AI agents and NHI has outpaced the governance structures required to secure them

LONDON, UNITED KINGDOM, June 10, 2026 /EINPresswire.com/ -- Keeper Security, the leading zero-trust and zero-knowledge identity security and Privileged Access Management (PAM) platform, today highlights a significant governance gap as organisations expand AI-driven and non-human access without the controls required to secure it. Insights gathered from an in-person survey of cybersecurity professionals at Infosecurity Europe 2026 in London show that AI agents and Non-Human Identities (NHIs) are now deeply embedded in enterprise environments, yet the governance structures designed to manage them are lagging behind.

> “What European organisations are contending with is not a future threat, but rather, a governance deficit that attackers are exploiting right now. ”
>
> *Darren Guccione, CEO and Co-founder, Keeper Security*

Infosecurity Europe is one of the most influential information security conferences globally, drawing thousands of practitioners, CISOs and security professionals to London each year. Keeper's on-site survey captured responses from 86 attendees directly on the conference floor, providing a practitioner-level view into how European security organisations are approaching NHI governance and agentic AI security.

More than two-thirds of respondents (68%) report that AI agents or AI-powered tools exist as privileged identities within their organisations. But only 15% of those respondents said they have full visibility into NHIs across cloud, on-premises and SaaS environments. Nearly two-thirds (65%) identified the lack of visibility into AI, automation and machine access as their top risk.

Meanwhile, governance structures are not keeping pace with the scale of AI adoption. Only 14% of organisations manage NHIs through a single, centralised platform. The majority operate across multiple tools – 39% with unclear or shared ownership and 33% with clear ownership –

resulting in inconsistent policies and fragmented control. When asked whether AI agents are actively managed as privileged identities, only 21% said they do so consistently. More than half (55%) manage AI tools only in some cases or for limited use cases, while 18% do not treat them as privileged identities at all.

These gaps carry measurable consequences. More than half of respondents (55%) report experiencing a security incident involving NHIs or credentials in the past 12 months; 8% with significant business impact. Only 18% of respondents have continuous, automated detection and response in place for NHI behaviour. A further 35% operate limited monitoring of selected systems and 13% do not monitor NHI activity at all. Excessive or standing privileges were flagged as a major risk by 55% of respondents, indicating a specific and addressable exposure in environments where access is not continuously reviewed.

“AI agents are now a mainstream concern of enterprise infrastructure across Europe,” said Darren Guccione, CEO and Co-founder, Keeper Security. “What European organisations are contending with is not a future threat, but rather, a governance deficit that attackers are exploiting right now. The question is no longer whether to invest in securing non-human identities, but whether organisations can close the gap before it causes financial, operational and reputational harm.”

Despite the gaps in current practice, investment intent is clear. Nearly two-thirds of respondents (64%) plan to increase investment in securing NHIs and AI-driven access over the next 12 to 24 months, with 22% anticipating significant strategic investment and 41% expecting targeted, incremental improvements.

The findings point to three specific gaps European organisations need to close: centralised visibility across cloud, on-premises and SaaS environments; consistent policy enforcement for both human and non-human identities; and continuous, automated monitoring that leveraged AI threat detection to reduce manual review. KeeperPAM addresses each risk directly, unifying password management, secrets management and privileged access controls in a single zero-trust, zero-knowledge architecture that governs all identities, both human and non-human, from a single control plane.

Visit keepersecurity.com to learn more about securing AI agents and non-human identities.

###

About Keeper Security
Keeper Security is the leading zero-trust and zero-knowledge identity security solution, trusted by millions of people and thousands of organisations globally. KeeperPAM® is Keeper's privileged access management platform that unifies password and passkey management, secrets management, privileged session management and endpoint privilege management in a single cloud-native platform, protected with quantum-resistant encryption. KeeperAI delivers real-time,

AI-native threat detection across every privileged session. As AI agents proliferate and identity becomes the defining attack surface, Keeper governs access for humans, machines, non-human identities and AI agents, serving as the unified control plane for access, compliance and visibility across the enterprise. For more information, visit KeeperSecurity.com.

Charley Nash
Eskenzi PR
email us here
