Keeper Security Research Reveals 89% of IT Leaders Struggle to Manage Growing Identity Footprint Amid AI Expansion

LONDON, UNITED KINGDOM, May 6, 2026 /EINPresswire.com/ -- New global study of 3,200 cybersecurity decision-makers finds AI adoption is accelerating identity sprawl, with more than half of UK IT leaders citing AI-driven attacks as a primary source of increased security pressure

Keeper Security, the leading zero-trust and zero-knowledge identity security and Privileged Access Management (PAM) platform, today releases its latest global insight report, "Identity Security at Machine Speed." The study examines the challenges cybersecurity decision-makers face as identity ecosystems expand to include humans and a growing number of Non-Human Identities (NHIs), and finds that legacy tools and unchecked Artificial Intelligence (AI) adoption are widening security gaps that attackers exploit.

Conducted with 3,200 cybersecurity decision-makers and senior IT leaders across Europe, the United States, Asia-Pacific and the Middle East, the research explores how the rapidly expanding identity ecosystem, spanning employees, contractors, third parties and machine accounts, is reshaping enterprise security strategy.

Among the key findings:

- Identity sprawl is a near-universal challenge: Nearly nine out of ten (89%) senior UK IT leaders report that managing the growing identity footprint is challenging, which falls in line with the global figure, and reflects the scale and complexity of modern security environments. This consensus masks a specific UK pressure point: more than half (52%) of UK respondents cite AI-driven attacks as a key driver of increased security pressure, the highest figure among European markets surveyed.
- Control is fragmented, not consolidated: Identity authority is often distributed across systems, with no single cybersecurity control plane. Globally, 96% cited disconnected or poorly integrated security tools as creating exploitable gaps. In the UK, 67% of respondents identify this to a moderate or great extent, above the global figure of 63%, which points to integration complexity as a persistent challenge for UK security teams.
- Detection is improving, but exposure windows remain: UK organisations lead European peers on real-time detection, with 33% identifying credential misuse within minutes – above the global average of 28%. A further 51% detect within hours. However, 14% still take days or longer to identify unauthorised privileged access, representing a meaningful residual risk.

As AI adoption accelerates, new governance gaps emerge:

• AI usage is multiplying NHIs: 43% of respondents globally identify AI-related NHI management and security as a top identity governance gap, a figure matched closely by UK respondents at 40%. As AI agents and machine accounts proliferate within UK enterprise environments, the absence of unified governance over non-human identities is creating an expanding attack surface.
• Employee AI use is a top concern: Over half (56%) of respondents are concerned about employees inadvertently exposing sensitive information to AI systems, with 55% of UK respondents identifying this as a leading AI security gap. UK organisations also register the highest concern among European markets about AI-driven social engineering and impersonation at 40%, well above the global average of 35%, reflecting heightened awareness of AI-assisted deception as a threat vector.
• Shadow AI creates blind spots: A lack of visibility into the AI tools employees use was identified as a significant governance gap by 42% of organisations. This sits alongside a broader picture of third-party risk: 34% of UK respondents identify incidents involving third-party vendors or suppliers as a source of increased security pressure, above both the global average of 28% and the figures recorded in Germany and France, highlighting the supply chain dimension of identity risk for UK enterprises.

UK respondents present a picture of above-average threat awareness combined with growing but uneven defensive capability. Over a quarter (27%) report attacks occurring at least weekly. Investment intent is ahead of many markets: 50% of UK respondents are prioritising AI security tools over the next 12 months and 38% plan investment in passwordless or passkey authentication, the highest figure among European markets in the study.

“AI agents, service accounts and machine identities radically outnumber human users in many environments. Most organisations lack the capabilities in their current identity security stack to govern them. Every unmanaged identity is a prime target for attackers,” said Darren Guccione, CEO and Co-founder of Keeper Security. “Given the accelerated proliferation of AI and machine identities within enterprise infrastructure, the implementation of pervasive identity governance with real-time detection and least-privilege enforcement is essential.”

Keeper delivers a zero-trust, zero-knowledge identity security and PAM platform designed for modern enterprise environments where AI adoption is accelerating and machine identities are proliferating at scale. KeeperPAM integrates enterprise password management, secrets management, privileged session management and endpoint privilege management with agentic AI-driven threat detection and response. The platform enables organisations ranging from Fortune 100 enterprises to federal agencies to protect sensitive data, streamline compliance and reduce the risk of damaging breaches.

Read the full Keeper insight report, “Identity Security at Machine Speed,”

(https://www.keepersecurity.com/en_GB/resources/insight-report-identity-security-at-machine-speed/) or learn more about Keeper's suite of products at KeeperSecurity.com (http://keepersecurity.com/).

###

About Keeper Security
Keeper Security is one of the fastest-growing cybersecurity software companies that protects thousands of organisations and millions of people in over 150 countries. Keeper is a pioneer of zero-knowledge and zero-trust security built for any IT environment. Its core offering, KeeperPAM®, is an AI-enabled, cloud-native platform that protects all users, devices and infrastructure from cyber attacks. Recognised for its innovation in the Gartner Magic Quadrant for Privileged Access Management (PAM), Keeper secures passwords and passkeys, infrastructure secrets, remote connections and endpoints with role-based enforcement policies, least privilege and just-in-time access. Learn why Keeper is trusted by leading organizations to defend against modern adversaries at KeeperSecurity.com (http://keepersecurity.com/).

Learn more: KeeperSecurity.com
(https://www.keepersecurity.com/?&utm_medium=press_release&utm_campaign=Communications)

Charley Nash
Account Manager
charley@eskenzipr.com
Visit us on social media:
LinkedIn
Instagram
Facebook
YouTube
TikTok
X
