Keeper Security Launches KeeperAI to Deliver Real-Time Detection and Defense Against Cyber Threats

Keeper's agentic AI solution monitors and analyses privileged sessions to instantly identify and terminate attacks

LONDON, UNITED KINGDOM, August 27, 2025 /EINPresswire.com/ -- As cyber attacks become quicker, more pervasive and increasingly automated using artificial intelligence, organisations are struggling to keep pace with the onslaught on modern threats. Privileged accounts, which give access to the most sensitive systems within an organisation, remain top targets, yet traditional security tools often fail to detect sophisticated insider threats and session-level anomalies until after a breach has occurred.

Today, Keeper Security, the leading cybersecurity provider of zero-trust and zero-knowledge Privileged Access Management (PAM) software protecting passwords and passkeys, privileged accounts, secrets and remote connections, announces KeeperAI, a new agentic AI feature for its KeeperPAM® platform. KeeperAI enables real-time session monitoring and analysis, automated threat classification and instant response to combat cyber attacks and suspicious behaviour - customisable to meet an organisation's exact specifications.

"The reality is that cyber threats are no longer just a question of if, but when and how quickly you respond," said Craig Lurey, CTO and Co-founder of Keeper Security. "KeeperAI's agentic capabilities allow you to automatically monitor, identify and mitigate threats in real time, shutting down high-risk sessions, unauthorised access or improper account elevations."

Meeting Today's Security Challenges

Insider threats, privilege misuse and advanced persistent threats have long challenged security teams. In the era of pervasive, AI-powered cyber attacks, traditional manual session reviews and rule-based alerts leave organisations falling woefully behind today's fast-moving threats. KeeperAI addresses this challenge with continuous monitoring of privileged sessions, automatic risk classification and session summaries, and configurable responses that can terminate sessions or trigger alerts when suspicious and malicious behaviour is detected - without the need for human intervention. As a sovereign AI product, each organisation using KeeperAI has full ownership and control over the data it uses and generates.

KeeperAI's key features include:

- Automated Session Analysis: Analyse session metadata, keystroke logs, and command execution logs to detect unusual behaviour.
- Threat Classification: Automatically categorise detected threats and assign risk levels.
- Session Termination: Trigger automatic session termination based on designated threat classification.
- Customisable Configuration: Adjust risk parameters and detection rules to your environment.
- Session Search: Search across sessions to locate specific keywords or activity.
- Flexible Deployment: Support for both third-party, cloud-based and on-premises LLM inference.

KeeperAI will categorise commands into threat risk levels from Critical to High, Medium and Low. Once KeeperAI is enabled, administrators can customise the risk level classification and policy on detection, giving admins the ability to define rule-based policies for specific command patterns - with the choice to automatically terminate risky sessions or simply monitor them when threats are detected. The solution allows customers to integrate with major LLM providers such as AWS Bedrock, Anthropic, Google Gemini and OpenAI. It supports compatible cloud and on-premises deployments without vendor lock-in.

"Security teams shouldn't have to waste hours reviewing logs or manually shutting down risky sessions," said Jeremy London, Director of Engineering, AI and Threat Analytics at Keeper Security." That's why we built KeeperAI as an agentic AI system - it doesn't just detect anomalies, it actively monitors and takes action on them in real time. With controls and parameters configured by humans, KeeperAI independently terminates high-risk sessions and enforces security policies instantly. This eliminates alert fatigue, accelerates response times to seconds and allows teams to focus on strategy instead of firefighting."

Designed for Real-World Impact

KeeperAI currently supports SSH-based sessions, with plans to extend support to RDP, VNC, RBI and database protocols. All risk assessments and incident data feed directly into the Keeper Vault UI, allowing teams to investigate incidents, maintain compliance and integrate with Security Information and Event Management (SIEM) and Security Operations Center (SOC) tools through Keeper's Advanced Reporting and Alerts Module (ARAM).

The solution combines agentic AI with a zero-knowledge architecture so all sensitive data remains encrypted and under customer control. Organisations gain scalable security operations while meeting compliance requirements.

Availability

KeeperAI is available now to all KeeperPAM customers running PAM Gateway version 1.7.0 or

higher and can be deployed in both cloud and Docker-based environments. For more information or to activate KeeperAI, visit Keeper docs.

###

About Keeper Security

Keeper Security is transforming cybersecurity for millions of individuals and thousands of organisations globally. Built with end-to-end encryption, Keeper's intuitive cybersecurity platform is trusted by Fortune 100 companies to protect every user, on every device, in every location. Our patented zero-trust and sero-knowledge privileged access management solution unifies enterprise password, secrets and connections management with sero-trust network access and remote browser isolation. By combining these critical identity and access management components into a single cloud-based solution, Keeper delivers unparalleled visibility, security and control while ensuring compliance and audit requirements are met. Learn how Keeper can defend your organisation against today’s cyber threats at https://www.keepersecurity.com/.

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