Keeper Security Launches Agent Kit to Secure AI-Driven Developer Workflows

New integration enables AI coding agents to securely retrieve secrets and manage infrastructure without exposing credentials in chat history or source control

LONDON, UNITED KINGDOM, April 30, 2026 /EINPresswire.com/ -- Keeper Security, the leading zero-trust and zero-knowledge identity security and Privileged Access Management (PAM) platform, today announces the launch of its Keeper Agent Kit. This new suite of specialised AI skills integrates Keeper Secrets Manager and Keeper Commander directly with industry-leading AI coding agents, including Claude Code, Cursor, Codex and GitHub Copilot, to safely automate complex security and administrative workflows.

As organisations rapidly embed Agentic AI into their development lifecycles, they face a critical security gap: the exposure of privileged credentials within AI prompt history. Traditionally, for an AI agent to interact with protected infrastructure, developers have had to manually provide API keys or database credentials within the chat interface, inadvertently storing sensitive data in third-party logs and training sets. The Keeper Agent Kit eliminates this risk by enabling AI agents to interact directly with Keeper's hardened Command Line Interface (CLI) tools, Keeper Commander (https://docs.keeper.io/en/enterprise-guide/commander-cli) and Keeper Secrets Manager CLI (https://docs.keeper.io/en/keeperpam/secrets-manager/secrets-manager-command-line-interface).

"The Keeper Agent Kit provides a definitive framework for how AI agents interact with sensitive enterprise data," said Craig Lurey, CTO and Co-founder of Keeper Security. "By equipping these agents with instructions to use our encrypted CLI tools locally, we ensure the agent runs commands within the developer's own authenticated session. This architecture maintains our zero-knowledge standard while allowing developers to leverage the full speed of AI without leaving the vault door open."

The Keeper Agent Kit is optimised for the modern developer workflow, offering:

• Secure Secret Retrieval: Agents use the keeper-secrets skill to inject credentials into local runtimes, ensuring the raw secret never appears in the chat UI.
• Automated Vault Administration: Through the keeper-admin skill, agents manage users, teams and audit resources via Keeper Commander.
• Streamlined Configuration: The keeper-setup skill automates the configuration of Keeper's

security tools, establishing a secure environment for new projects from the first command.

For teams operating in hosted or orchestrated AI environments, Keeper also offers a Model Context Protocol (MCP) server integration (available in Docker and Node configurations), that enables agent platforms to retrieve secrets via a running MCP server process rather than local CLI tools. When an AI agent uses Keeper's CLI tools, every action taken by the agent is governed by the same rigorous role-based access controls and audit logging as a human user accessing systems through Keeper.

"Security teams should not have to trade velocity for operational safety," said Jeremy London, Director of Engineering, AI and Threat Analytics for Keeper Security. "With the Agent Kit, we are transforming AI from a conversational assistant into a secure partner that respects the organisational security perimeter. By allowing agents to resolve secrets at runtime without ever seeing the raw credential, we help close one of the most dangerous exposure points in the modern developer stack."

The Keeper Agent Kit (https://docs.keeper.io/en/keeperpam/secrets-manager/integrations/ai-agents?&utm_medium=press_release&utm_campaign=Communications) is now available as an open-source repository under the Apache 2.0 license. Developers can access the kit via the official Keeper Security GitHub.

###

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 organisations 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)

Beth Smith
Eskenzi PR Ltd
beth@eskenzipr.com
Visit us on social media:
LinkedIn

Instagram
Facebook
YouTube
TikTok
X
