Keeper Security Debuts Secure Model Context Protocol AI Agent Integration for Secrets Management

New Keeper Secrets Manager integration capabilities enable automated workflows through AI agents while protecting critical stored data

LONDON, UNITED KINGDOM, July 10, 2025 /EINPresswire.com/ -- Keeper Security, the leading cybersecurity provider of zero-trust and zero-knowledge Privileged Access Management (PAM) software protecting passwords, passkeys, privileged accounts, secrets and remote connections, today announced the launch of Model Context Protocol (MCP) AI Agent Integration for Keeper Secrets Manager. The new capability enables organisations to automate workflows through AI agents while enforcing strict security, access and compliance controls.

> “AI agents are becoming powerful tools for operational efficiency, but their access to sensitive data must be governed by strong controls.”
>
> *Craig Lurey, CTO and Co-founder of Keeper Security*

The integration enables customers to securely connect and authorize their own third-party AI tools, such as local or cloud-based assistants, to interact with Keeper Secrets Manager under controlled conditions. With Keeper’s MCP, these tools can retrieve or manage secrets stored in the Keeper Vault, without compromising Keeper’s zero-trust and zero-knowledge architecture.

As businesses increasingly adopt AI assistants to improve work productivity, secure integration with sensitive systems remains a top concern. Recent research by Salesforce found that 78% of UK companies are already using agentic AI tools, demonstrating a clear appetite among British businesses to embrace automation and AI-driven efficiency. While third-party tools may operate outside of zero-knowledge boundaries from the customer side, Keeper maintains zero knowledge of all stored data. MCP acts as a secure, auditable bridge for this interaction.

“AI agents are becoming powerful tools for operational efficiency, but their access to sensitive data must be governed by strong controls,” said Craig Lurey, CTO and Co-founder of Keeper Security. “With our Model Context Protocol integration, organisations can adopt AI responsibly while ensuring their digital assets remain protected.”

Key benefits include:

- Zero-Trust Design: AI agents only receive explicit access to designated folders, supporting least-privilege access models.

- Human-in-the-Loop Oversight: Sensitive operations require real-time user confirmation to prevent unintended actions.

- Streamlined Data Retrieval: Users no longer have to copy and paste information, which increases efficiency and reduces memory-based risks.

- Enterprise-Grade Logging and Compliance: All AI activity is monitored and auditable to meet regulatory and security requirements.

- Cross-Platform Support: Keeper's MCP integration for Secrets Manager runs on Linux, macOS, Windows and Docker.

- Admin-Controlled Enablement: The integration is disabled by default and must be explicitly enabled by an administrator in the Keeper Admin Console using the existing Keeper Secrets Manager enforcement settings.

With this integration, Keeper Secrets Manager users can allow AI assistants to perform tasks such as generating secure passwords, retrieving and updating secrets, managing file attachments and running system health checks – all within a secure, policy-driven environment.

"Model Context Protocol provides the secure framework enterprises need to confidently deploy AI agents with their secrets management infrastructure," said Jeremy London, Director of Engineering, AI and Threat Analytics for Keeper Security. "By implementing MCP in Keeper Secrets Manager, we're giving organisations the ability to automate workflows while maintaining our zero-trust security model and full audit capabilities."

Part of Keeper's broader KeeperPAM® platform, Keeper Secrets Manager helps organisations eliminate hard-coded credentials, automate password rotation and protect infrastructure secrets. The platform is SOC-2, SOC-3 and ISO 27001, 27017 and 27018-certified, FIPS 140-3 validated and FedRAMP and GovRAMP Authorized (™).

To learn more about Keeper's secure AI agent integration capabilities, visit docs.keeper.io.

###

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 zero-knowledge privileged access management solution unifies enterprise password, secrets and connections management with zero-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 KeeperSecurity.com.

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