

Keeper Security Launches Integration With Wiz to Remediate Critical Cloud Vulnerabilities

With integration, Keeper's identity security platform remediates vulnerabilities discovered by Wiz, enabling closed-loop protection across cloud environments.



LONDON, UNITED KINGDOM, June 16, 2026 /EINPresswire.com/ -- Keeper Security, the leading zero-trust and zero-knowledge identity security and Privileged Access Management (PAM) platform, today announces a new integration with Wiz, a leading cloud and AI security platform that is now part of Google Cloud. Joining the [Wiz Integration Network](#) establishes Keeper as a

“

By bringing cloud visibility and access management into a unified workflow, teams can better secure both human and machine identities at scale.”

Oron Noah, VP of Product, Extensibility & Partnerships at Wiz

remediation engine for identity security vulnerabilities discovered by Wiz, closing the loop between cloud security detection and active risk resolution. When Wiz identifies an identity-related vulnerability, spanning human users, machine identities, AI agents and database accounts, it automatically surfaces the finding in Keeper's Cloud Security dashboard, where security teams can review and remediate each issue directly within KeeperPAM®.

As cloud environments grow more complex, organisations face an expanding attack surface driven by the rapid proliferation of Non-Human Identities (NHIs), autonomous

AI agents and over-privileged service accounts. Wiz surfaces these risks with unmatched cloud visibility, and Keeper provides joint customers with an automated, trusted path from discovery to remediation.

“Finding a vulnerability is the first half of the battle,” said Craig Lurey, CTO and Co-founder of Keeper Security. “By integrating with Wiz, Keeper helps customers rotate compromised credentials, enforce privileged access management and reduce over-permissioned identities, turning Wiz's detection power into faster, more decisive risk reduction. This is the future of cloud security – detection and remediation working as one, giving security teams a clear path from vulnerability discovery to resolution across the identities and workloads that matter most.”

“We're happy to welcome Keeper to the Wiz Integration Network,” said Oron Noah, VP of

Product, Extensibility & Partnerships at Wiz. “Together, we’re helping customers connect cloud risk findings with privileged access controls, making it easier to move from discovery to remediation. By bringing cloud visibility and access management into a unified workflow, teams can better secure both human and machine identities at scale.”

At the heart of the integration is a real-time workflow that transforms Wiz’s Issues into Keeper-driven remediation actions. When a Wiz customer enables the Keeper integration, Wiz scans the cloud environment for identity security vulnerabilities within Keeper’s remediation scope. Security teams can then select a finding and execute the appropriate remediation action through KeeperPAM:

- Rotate compromised credentials and vault updated secrets
- Bring unmanaged accounts under PAM governance
- Reduce excessive privileges for users, service accounts and IAM roles
- Map Wiz Issues to existing PAM records or onboard new resources
- Submit resolutions back to Wiz to close the loop on each finding

This tight integration bridges the gap between cloud security detection and identity security remediation, giving security teams a single, closed-loop workflow. Rather than manually triaging Wiz Issues and separately executing remediation steps in Keeper, KeeperPAM works alongside Wiz by automatically receiving identity-related Issues and streamlining the remediation steps. For teams, this results in accelerated Mean Time To Remediation (MTTR) and a dramatically reduced window of exposure before a vulnerability can be exploited.

The integration is especially powerful in AI-native environments, where autonomous agents and service accounts can rapidly accumulate excessive permissions across cloud infrastructure. Wiz’s AI Application Protection Platform (AI-APP) detects over-privileged AI agents, insecure service configurations and other AI-native risks. Keeper serves as a designated remediation engine, enforcing least privilege policies and enabling just-in-time access controls for AI agents in response. Together, they secure the full AI lifecycle from code to runtime, without requiring manual intervention from security teams.

Key benefits include:

Streamlined Identity Remediation: When Wiz discovers an identity security vulnerability, Keeper takes action – rotating compromised credentials, enforcing PAM controls and reducing excess privileges – streamlining the steps between detection and resolution.

Closed-Loop Security Workflow: Connect Wiz’s industry-leading cloud and AI vulnerability detection directly to Keeper’s privileged access management platform for a complete detect-to-remediate pipeline that operates at cloud scale.

Accelerated Mean Time to Remediation: By accelerating response to identity vulnerabilities at the moment of discovery, organisations dramatically shrink the window of exposure and reduce the risk of breach escalation.

Comprehensive Identity Coverage: Remediation scope covers the full range of identity types, including human users, machine identities, AI agents and database accounts, ensuring no privileged entity goes unmanaged across cloud environments.

KeeperPAM, Keeper's cloud-native privileged access management platform, unifies password, secrets and connections management with zero-trust network access, endpoint privilege management and remote browser isolation in a single solution. Built on a zero-trust and zero-knowledge architecture, KeeperPAM provides real-time visibility, automated credential security and AI-powered session monitoring to help organisations prevent breaches and maintain compliance across hybrid and multi-cloud environments.

By connecting detection directly to remediation, Keeper and Wiz give security teams the confidence that cloud risks are not just visible, but actively resolved. KeeperPAM's zero-trust architecture ensures every remediation action maintains a verifiable chain of custody – from Wiz's initial finding through to Keeper's corrective action – supporting both continuous compliance and audit readiness.

Keeper's integration with Wiz is available now. Review the full release notes in the [Keeper documentation](#).

###

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](#)

This press release can be viewed online at: <https://www.einpresswire.com/article/919909015>

EIN Presswire's priority is source transparency. We do not allow opaque clients, and our editors try to be careful about weeding out false and misleading content. As a user, if you see something we have missed, please do bring it to our attention. Your help is welcome. EIN Presswire, Everyone's Internet News Presswire™, tries to define some of the boundaries that are reasonable

in today's world. Please see our Editorial Guidelines for more information.

© 1995-2026 Newsmatics Inc. All Right Reserved.