Keeper Security Introduces Universal Secrets Sync to Eliminate Credential Drift Across Cloud Environments

New KeeperPAM capability automatically distributes rotated secrets to AWS, Azure and Google Cloud in a single rotation event with no manual steps or drift

LONDON, UNITED KINGDOM, June 15, 2026 /EINPresswire.com/ -- Keeper Security, the leading zero-trust and zero-knowledge identity security and Privileged Access Management (PAM) platform, is announcing the availability of Keeper Universal Secrets Sync, which launched on June 4th. The new capability within KeeperPAM® automatically distributes credentials and secrets to external secrets managers and cloud platforms the moment they rotate, closing the gap between stored secrets and what's actually running in production.

> “Universal Secrets Sync makes distribution automatic and auditable.”
>
> *Craig Lurey, CTO and Co-founder, Keeper Security*

For organisations managing secrets across multi-cloud environments, the risk is not only exposure – it's drift. When credentials stored in a PAM platform fall out of sync with what is running in production pipelines, the consequences range from access failures and delayed incident response to shadow secrets that carry active privileges no security team can see, govern or revoke. Global research has found that 86% of IT and security leaders agree their organisation would benefit from a PAM solution, yet even among organisations with PAM in place, 46% still struggle to manage privileged access consistently across cloud and hybrid environments. Universal Secrets Sync closes that gap.

Automatic Distribution Across Every Cloud Target

Keeper Universal Secrets Sync monitors one or more Keeper Secrets Manager shared folders and automatically distributes the contents to configured cloud targets, including AWS Secrets Manager, Azure Key Vault and Google Cloud Secret Manager. When a secret rotates in KeeperPAM, every cloud environment receives the updated credential automatically, with no manual exports, no custom integration scripts and no reconfiguration after rotation required.

Additional capabilities include:

- Automatic sync – Any change to a secret in a linked shared folder triggers an automatic push to all connected cloud targets. No manual action is required; the Gateway processes and distributes the update in the background.
- Dry Run mode – Security teams preview exactly what will change before any secret is distributed, making Universal Secrets Sync compatible with change control requirements and environments that require additional oversight.
- Multi-folder sync – Secrets from multiple Keeper shared folders can be synchronised in a single configuration.
- Sync Identity – Administrators can specify a dedicated IAM role, managed identity or service account, with least-privilege access to the secrets store, for the Keeper Gateway to assume during sync operations.
- Error recovery – Missing secrets and permission errors are surfaced automatically, reducing the risk of sync failures going undetected.

"Secrets drift is one of the most underappreciated risks in enterprise security programmes," said Craig Lurey, CTO and Co-founder of Keeper Security. "organisations unknowingly leave stale credentials active in downstream cloud environments when distribution is manual. Universal Secrets Sync makes distribution automatic and auditable. Every secret rotation updates to all connected targets simultaneously, with Dry Run mode giving teams full visibility into what will change before anything is written."

Flexible Retrieval for Every Workload

Universal Secrets Sync gives developers the right access path for each use case. Cloud-native applications that demand high throughput and low latency continue reading directly from AWS Secrets Manager, Azure Key Vault or Google Cloud Secret Manager using familiar native SDKs and IAM controls – ideal for services performing hundreds of thousands or millions of retrievals per day. For CI/CD pipelines, scripts, internal tools and services running outside the cloud, developers retrieve secrets directly from Keeper Secrets Manager via the KSM SDK or CLI, with full zero-knowledge protection end-to-end. The result is a single source of truth with two complementary access patterns – fast, native retrieval where scale matters, and direct KSM access where reach and zero-knowledge control matter most.

Keeper Universal Secrets Sync is available now as part of KeeperPAM and is included in existing KeeperPAM licenses. Existing customers should contact their Keeper customer success manager to enable this feature. New customers can request a demo at keepersecurity.com.

###

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/919782801

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.