Keeper Security Closes the Standing Privilege Gap in Cloud Identity with Keeper Privileged Cloud

New just-in-time access capability within KeeperPAM ensures privileged credentials are granted only when needed and revoked automatically when a session expires

LONDON, UNITED KINGDOM, July 16, 2026 /EINPresswire.com/ -- Keeper Security, the leading zero-trust and zero-knowledge identity security and Privileged Access Management (PAM) platform, today announces Keeper Privileged Cloud, which launched within KeeperPAM® earlier this year. The capability delivers Just-In-Time (JIT) access and zero standing privilege across cloud identity providers including AWS IAM, Azure Entra ID, Google Cloud Platform, Okta and Active Directory, ensuring privileged credentials exist only for the duration of an approved session and are revoked automatically when the session ends. By eliminating the window in which unused privileged credentials linger in cloud identity platforms, Keeper Privileged Cloud shrinks the attack surface to the exact moments that access is actually in use, eliminating any dormant permissions adversaries could exploit in between.

> “Because Keeper Privileged Cloud was built into KeeperPAM from the ground up, access governance, credential protection and audit all live in the same zero-knowledge architecture.”
>
> *Craig Lurey, CTO and Co-founder of Keeper Security*

According to Keeper research, 64% of organisations lack fully consolidated privileged access governance, and 43% still allow direct application logins that bypass their identity provider entirely. These gaps leave privileged credentials sitting in cloud identity platforms long after the work that required them is finished, creating the standing footholds attackers look for.

How It Works

When a user submits a request for elevated access and it’s approved, Keeper Privileged Cloud applies the access level an administrator has pre-configured for that request type – for example a specific role or group scoped to a defined set of permissions – and adds temporary group

membership or role assignment in the target identity platform, time-bound to the approved window. Once access is approved, the user launches the target console or application directly from the Keeper Vault through Remote Browser Isolation, with every action in the session recorded and analysed in real time by KeeperAI. When the approved window expires, KeeperPAM removes the elevated access automatically. No standing accounts are created, no privileged credentials are shared with end users and no manual cleanup is required.

One Platform, One Audit Trail

Most organisations try to close the standing privilege gap by piecing together JIT access from their identity provider, their PAM tool and their cloud provider. The result is three systems, three audit trails and no single point of enforcement. Keeper Privileged Cloud consolidates that into one platform spanning password management, secrets management, session management and endpoint privilege management. Because the capability is native to KeeperPAM rather than bolted on through a third-party connector, access governance, credential protection and audit operate within the same zero-knowledge architecture from the start.

That governance model also extends to non-human identities and AI agents. Every identity, human or machine, receives only the access the task requires, for the duration of that task, with a complete audit record. Organisations need no separate tools, no separate vendors and no separate integration projects.

"The challenge with standing privileges is that removing them requires coordination across multiple systems that were never designed to work together," said Craig Lurey, CTO and Co-founder of Keeper Security. "Most JIT access tools are added after the fact, as a layer on top of systems that were never built to revoke access automatically. Because Keeper Privileged Cloud was built into KeeperPAM from the ground up, rather than layered on afterward, access governance, credential protection and audit all live in the same zero-knowledge architecture. That is the only way zero standing privilege holds up at scale, instead of becoming one more system to maintain."

Availability

Keeper Privileged Cloud is available as part of the KeeperPAM platform and is included in existing KeeperPAM licences. Existing customers can contact their Keeper customer success team to enable the 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