Keeper Security Introduces KeeperDB™, Integrating Zero-Trust Database Access into KeeperPAM®

LONDON, UNITED KINGDOM, March 19, 2026 /EINPresswire.com/ -- New capability embeds a secure, zero-trust database interface directly into the Keeper Vault, eliminating exposed credentials, unmanaged tools and insecure access paths

Keeper Security, the leading zero-trust and zero-knowledge identity security and Privileged Access Management (PAM) platform, today announces KeeperDB, a new vault-embedded database access capability that enables secure, policy-controlled database interactions directly from the Keeper Vault. KeeperDB enables developers, database administrators and security teams to work with sensitive data through a unified interface that simplifies workflows while maintaining strict access governance. KeeperDB will be officially launched at RSA Conference 2026.

Enterprise databases are among the most sensitive assets in any organisation, yet access is often managed through a mix of desktop tools, shared credentials and network tunnels, which provide limited visibility and control. Databases are frequent targets of cyber attacks and insider misuse, and fragmented tools substantially increase risk of credential exposure, data exfiltration and audit gaps while inhibiting least-privilege access.

KeeperDB broadens KeeperPAM with a beautiful, vault-native interface that unifies database session management within the zero-trust and zero-knowledge platform. Access is governed by centralised policies and fully recorded for audit and compliance purposes. By embedding database access directly into the Vault, KeeperDB helps reduce credential sprawl, standardise database access workflows and strengthen audit readiness across cloud and on-prem environments.

“Database access has historically been one of the most used yet least-governed areas of enterprise security,” said Darren Guccione, CEO and Co-founder of Keeper Security. “KeeperDB brings database management into the vault – allowing organisations to apply the same zero-trust controls, visibility and auditing they rely on for privileged access – without introducing new tools, credentials or attack paths.

KeeperDB enables users to launch database sessions directly from a database record in the Keeper Vault, with the option to connect through either a Graphical User Interface (GUI) or

Command-Line Interface (CLI). Initial support includes MySQL, PostgreSQL, Oracle and Microsoft SQL Server.

Key benefits include:

- Eliminating credential exposure by ensuring database credentials are never revealed to users or stored on endpoints.
- Reducing data exfiltration risk through granular controls such as read-only access and governed data transfer policies.
- Strengthening audit readiness with full visual session recording of database activity,
- Standardising and centralising database access within the Keeper Vault, replacing fragmented tools and unmanaged workflows.
- Improving usability for technical teams by providing a modern, browser-based interface without sacrificing zero-trust controls.

For organisations that continue to rely on existing database clients, KeeperDB will be complemented by KeeperDB Proxy (https://docs.keeper.io/en/keeperpam/privileged-access-manager/tunnels/keeperdb-proxy), which enables secure connections through Keeper while maintaining centralised policy enforcement, credential protection and session visibility. Additional details on availability will be provided alongside upcoming Keeper Gateway and Keeper Vault releases.

“Most database access today happens through disparate tools that sit outside security controls,” said Craig Lurey, CTO and Co-founder of Keeper Security. “We built KeeperDB so teams can work the way they’re used to, but inside a zero-trust environment. It’s a simpler, safer way to manage database access that enhances productivity.”

To learn more about Keeper’s product suite, visit KeeperSecurity.com (http://keepersecurity.com/).

###

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 (http://keepersecurity.com/)

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