Pressemitteilung

Keeper Security stellt KeeperDB™ vor: Integration von Zero-Trust-Datenbankzugriff in KeeperPAM®

Neue Funktion integriert eine sichere, Zero-Trust-Datenbankschnittstelle direkt in den Keeper Vault und eliminiert offengelegte Anmeldedaten, unkontrollierte Tools und unsichere Zugriffspfade

MÜNCHEN, 19. März 2026 – Keeper Security, eine führende Zero-Trust- und Zero-Knowledge-Plattform für Identitätssicherheit und Privileged Access Management (PAM), stellt heute KeeperDB vor. KeeperDB ist eine neue, in den Keeper Vault integrierte Funktion für den Datenbankzugriff, die sichere, richtliniengesteuerte Datenbankinteraktionen direkt aus dem Keeper Vault heraus ermöglicht. Es erlaubt Entwicklern, Datenbankadministratoren und Sicherheitsteams, mit sensiblen Daten über eine einheitliche Schnittstelle zu arbeiten, die Workflows vereinfacht und gleichzeitig strenge Zugriffskontrollen gewährleistet. Die offizielle Vorstellung von KeeperDB erfolgt auf der RSA Conference 2026.

Datenbanken in Unternehmen gehören zu den sensibelsten Ressourcen einer Organisation, doch der Zugriff darauf wird häufig über eine Mischung aus Desktop-Tools, gemeinsam genutzten Anmeldedaten und Netzwerktunneln verwaltet, was nur begrenzte Transparenz und Kontrolle bietet. Datenbanken sind häufig Ziel von Cyberangriffen und Missbrauch durch Insider. Darüber hinaus erhöhen uneinheitliche Tools zusätzlich das Risiko von Zugangsdatenlecks, Datenexfiltration und Lücken bei Audits erheblich, während sie gleichzeitig den Zugriff nach dem Prinzip der geringsten Berechtigungen behindern.

KeeperDB erweitert KeeperPAM um eine benutzerfreundliche, Vault-native Schnittstelle, die die Sitzungsverwaltung von Datenbanken in der Zero-Trust- und Zero-Knowledge-Plattform zentralisiert. Der Zugriff wird durch zentrale Richtlinien gesteuert und vollständig für Audit- und Compliance-Zwecke protokolliert. Durch die direkte Einbettung des Datenbankzugriffs in den Vault hilft KeeperDB, die Verbreitung von Anmeldedaten zu reduzieren, Datenbankzugriffs-Workflows zu standardisieren und die Audit-Bereitschaft in Cloud- und On-Premises-Umgebungen zu stärken.

„Der Datenbankzugriff war historisch gesehen einer der am häufigsten genutzten, aber am wenigsten kontrollierten Bereiche der Unternehmenssicherheit“, sagt Darren Guccione, CEO und Mitgründer von Keeper Security. „KeeperDB bringt das Datenbankmanagement in den Vault. Damit können Unternehmen für Datenbanken dieselben Zero-Trust-Kontrollen, Transparenz- und Audit-Funktionen anwenden, auf die sie sich beim privilegierten Zugriff verlassen – ohne neue Tools, Anmeldedaten oder Angriffsvektoren einzuführen.“

Mit KeeperDB können Benutzer Datenbanksitzungen direkt aus einem Datenbankdatensatz im Keeper Vault starten – wahlweise über eine grafische Benutzeroberfläche (GUI) oder eine Befehlszeilenschnittstelle (CLI). Die initiale Unterstützung umfasst MySQL, PostgreSQL, Oracle und Microsoft SQL Server.

Zu den wichtigsten Vorteilen von KeeperDB gehören:

- Vermeidung der Offenlegung von Anmeldeinformationen, indem Datenbank-Anmeldedaten nie für Benutzer sichtbar oder auf Endgeräten gespeichert werden.
- Reduzierung des Risikos von Datenabfluss durch granulare Kontrollen wie schreibgeschützten Zugriff und gesteuerte Datenübertragungsrichtlinien.
- Stärkung der Audit-Bereitschaft durch vollständige visuelle Aufzeichnung aller Datenbankaktivitäten.
- Standardisierung und Zentralisierung des Datenbankzugriffs im Keeper Vault, wodurch fragmentierte Tools und unkontrollierte Workflows ersetzt werden.
- Verbesserte Benutzerfreundlichkeit für technische Teams durch eine moderne, browserbasierte Oberfläche – ohne Kompromisse bei Zero-Trust-Kontrollen.

Für Unternehmen, die weiterhin auf bestehende Datenbank-Clients setzen, wird KeeperDB durch KeeperDB Proxy ergänzt. Dieser ermöglicht sichere Verbindungen über Keeper, während zentrale Richtlinien, Anmeldedatenschutz und Sitzungstransparenz gewahrt bleiben. Weitere Details zur Verfügbarkeit werden im Rahmen der bevorstehenden Veröffentlichungen von Keeper Gateway und Keeper Vault bekannt gegeben.

„Der Großteil des Datenbankzugriffs erfolgt heute über verteilte Tools, die außerhalb der Sicherheitskontrollen liegen“, sagt Craig Lurey, CTO und Mitgründer von Keeper Security. „Wir haben KeeperDB entwickelt, damit Teams wie gewohnt, jedoch in einer Zero-Trust-Umgebung, arbeiten können. Dies ist ein einfacherer und sichererer Weg, den Datenbankzugriff zu verwalten, der gleichzeitig die Produktivität steigert.“

Keeper Security stellt KeeperDB live auf der RSA Conference 2026 (Stand S-1535, South Exhibition Hall) vor. Weitere Informationen zum Produktportfolio von Keeper finden Sie unter KeeperSecurity.com.

###

Über Keeper Security:
Keeper Security ist eines der am schnellsten wachsenden Unternehmen für Cybersicherheitssoftware, das Tausende von Organisationen und Millionen von Menschen in über 150 Ländern schützt. Keeper ist ein Pionier der Zero-Knowledge- und Zero-Trust-Sicherheit für jede IT-Umgebung. Das Herzstück, KeeperPAM®, ist eine KI-unterstützte, Cloud-native Plattform, die alle Benutzer, Geräte und Infrastrukturen vor Cyberangriffen schützt. Keeper wurde für seine Innovationen im Gartner Magic Quadrant für Privileged Access Management (PAM) ausgezeichnet und sichert Passwörter und Passkeys, Infrastrukturgeheimnisse, Remote-Verbindungen und Endpunkte mit rollenbasierten Durchsetzungsrichtlinien, Least-Privilege und Just-in-Time-Zugriff. Erfahren Sie auf KeeperSecurity.com, wie Keeper Ihr Unternehmen vor den heutigen Cyberbedrohungen schützen kann.

Erfahren Sie mehr unter KeeperSecurity.com
Folgen Keeper: Facebook Instagram LinkedIn X YouTube TikTok

Pressekontakt für Keeper in DACH:
Alexandra Schmidt, +49 170 387 10 64
Thilo Christ, +49 171 622 06 10
keeper@tc-communications.de