KEEPER | Pressemitteilung

Keeper rationalisiert Compliance-Prozesse mit granularen Freigabe-Vorgaben

Keeper hilft Unternehmen bei der Einhaltung strenger Sicherheitsrichtlinien, indem Administratoren volle Transparenz und Kontrolle über die Nutzung und Freigabe von Anmeldedaten und Datensätzen durch Mitarbeiter sowie über einen rollenbasierten Zugriff haben.

München, 10. Januar 2024 – Keeper Security, ein führender Anbieter von Zero-Trust- und Zero-Knowledge-Lösungen zum Schutz von Anmeldedaten, privilegiertem Zugang und Remote-Verbindungen, kündigt die Erweiterung für alle Produkte der Keeper-Plattform mit den „Granular Sharing Enforcements“ (granularen Freigabe-Vorgaben) an. Diese ermöglichen es Administratoren, detaillierte Freigabeberechtigungen auf Benutzerebene vorzugeben. Durch die Implementierung dieser Berechtigungen können Unternehmen sicherstellen, dass Mitarbeiter nur auf die Ressourcen zugreifen können, die sie für ihre Aufgaben benötigen, und so das Risiko eines unbefugten Zugriffs, von Datenverstößen und Seitwärtsbewegungen innerhalb eines Netzwerks minimieren.

„Für Unternehmen sind Sicherheitslösungen, die sie bei der Einhaltung der zunehmenden Vorschriften und Compliance-Anforderungen unterstützen, von entscheidender Bedeutung", sagt Craig Lurey, CTO und Mitbegründer von Keeper Security. „Die granulare Berechtigungskontrolle hilft die Sicherheitslage zu verbessern, indem sie den Zugriff auf sensible Informationen und Systeme einschränkt. Mit „Granular Sharing Enforcements“ ist es für IT-Administratoren einfacher denn je, das Prinzip der geringsten Privilegien zu kontrollieren und die Abläufe im Unternehmen zu optimieren."

Die neuen Granular Sharing Enforcement-Richtlinien von Keeper bieten detailliertere Beschränkungen, die Administratoren auf Benutzer für die Erstellung und Freigabe von Datensätzen anwenden können. Die meisten Mitarbeiter benötigen keinen Zugriff auf alle Daten oder Funktionen innerhalb eines Unternehmens, und viele Branchen und geografische Regionen haben spezifische Vorschriften und Compliance-Anforderungen in Bezug auf Datenschutz und Privatsphäre, einschließlich HIPAA, GDPR, PCI DSS und SOX. Granulare Berechtigungskontrollen ermöglichen es Unternehmen, lokale und branchenspezifische Vorschriften einzuhalten, indem sie Zugriffsrichtlinien definieren und durchsetzen können. Dadurch wird sichergestellt, dass das Unternehmen die Branchenstandards und rechtlichen Anforderungen einhält.

Zu den wichtigsten Funktionen der Keeper „Granular Sharing Enforcements“ gehören:

- **Auditing**: Keeper bietet klare Warnmeldungen und Berichte zu über 100 verschiedenen Ereignistypen.
- **Versionskontrolle**: Nur eine kleine Gruppe von Anwendern kann Datensätze aktualisieren oder freigeben, so dass die Teams sicherstellen können, dass die Informationen konsistent und korrekt sind.
- **Nahtloser Zugriff von jedem Gerät aus**: Keeper bietet plattformübergreifend die gleiche Benutzererfahrung und gewährleistet so eine einfache Nutzung, egal ob im Web, auf dem Desktop oder auf dem Mobilgerät.

- **Verschlüsselung**: Keeper bietet eine sichere Freigabe mit Elliptic-Curve-Verschlüsselung. Diese sorgt dafür, dass Cyberkriminelle keine Passwörter oder andere freigegebene Datensätze während der Übertragung abfangen und nutzen können.

Keeper-Administratoren können die Berechtigungen leicht anpassen, um die Compliance-Anforderungen ihrer Organisation zu erfüllen. Administratoren ändern die Berechtigungen im Abschnitt „Durchsetzungsrichtlinien“ der Verwaltungskonsole für die gewählte Rolle, indem sie „Erstellen“ und „Freigeben“ auswählen. Die meisten Berechtigungen sind für maximale Sicherheit standardmäßig aktiviert. Die Durchsetzungsrichtlinien wurden so konzipiert, dass sie einfach und leistungsfähig sind und es Administratoren ermöglichen, die passenden Einstellungen für ihre individuellen Anforderungen zu wählen.

Granular Sharing Enforcements sind für alle Freigabeanforderungen in Keeper's Enterprise Password Manager, Keeper Secrets Manager und KeeperPAM verfügbar. Mit der Zero-Knowledge-Passwortmanagement- und Sicherheitsplattform von Keeper haben IT-Administratoren einen vollständigen Einblick in die Passwortpraxis ihrer Mitarbeiter und können so die Passwortnutzung überwachen und Passwortsicherheitsrichtlinien durchsetzen, einschließlich starker, eindeutiger Passwörter, Multi-Faktor-Authentifizierung (MFA), rollenbasierter Zugriffskontrolle (RBAC) und anderer Sicherheitsrichtlinien. Keeper Secrets Manager® ist eine vollständig verwaltete, Cloud-basierte Zero-Knowledge-Plattform zur Sicherung von Infrastrukturgeheimnissen wie API-Schlüsseln, Datenbankpasswörtern, Zugangsschlüsseln, Zertifikaten und jeder Art von vertraulichen Daten.

Das neueste Angebot, KeeperPAM™, bietet ein Privileged Access Management (PAM) der nächsten Generation, das den traditionellen PAM-Markt neu definiert. KeeperPAM bietet eine unternehmensgerechte Verwaltung von Passwörtern, Geheimnissen und privilegierten Verbindungen auf einer einheitlichen SaaS-Plattform, die kostengünstig, benutzerfreundlich und einfach zu implementieren ist. KeeperPAM ermöglicht den Zugriff mit geringsten Rechten und bietet Zero-Trust- und Zero-Knowledge-Sicherheit. Unternehmen entscheiden sich für Keeper aufgrund seiner starken Sicherheitsarchitektur, der Fähigkeit, föderierte und passwortlose Authentifizierung mit jedem Identitätsanbieter zu unterstützen, der nahtlosen Integration in lokale, Cloud- oder hybride Umgebungen und der einfachen Nutzung über Desktop- und Mobilgeräte.

###

Über Keeper Security:
Keeper Security verändert weltweit die Cybersicherheit für Menschen und Organisationen. Die erschwinglichen und benutzerfreundlichen Lösungen von Keeper basieren auf der Grundlage von Zero-Trust- und Zero-Knowledge-Sicherheit, um jeden Benutzer auf jedem Gerät zu schützen. Unsere Privileged-Access-Management-Lösung der nächsten Generation ist in wenigen Minuten einsatzbereit und lässt sich nahtlos in jede Technologieumgebung integrieren, um Sicherheitsverletzungen zu verhindern, Helpdesk-Kosten zu senken und die Compliance zu gewährleisten. Keeper genießt das Vertrauen von Millionen von Einzelnutzern sowie Tausenden von Unternehmen und ist der führende Anbieter von erstklassigem Passwort- und Passkey-Management, Geheimnisverwaltung, privilegiertem Zugriff, sicherem Fernzugriff und verschlüsseltem Messaging.

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

###

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