KEEPER | Pressemitteilung

Keeper Security erweitert seine Password-Management-Plattform mit einer bidirektionalen One-Time-Sharing-Funktion

Neue verschlüsselte Sharing-Technologie ermöglicht sicheren Datenaustausch zwischen Teams, die den Keeper Password Manager einsetzen, und ihren Kunden.

MÜNCHEN – 28. Mai 2025 – Keeper Security, ein führender Cybersecurity-Anbieter für Zero-Trust- und Zero-Knowledge Privileged Access Management (PAM)-Software zum Schutz von Passwörtern, Passkeys, privilegierten Konten, Geheimnissen und Remote-Verbindungen, kündigt heute ein Update seiner Passwortmanagement-Plattform an. Die aktualisierte One-Time-Share-Funktion von Keeper ermöglicht das bidirektionale, verschlüsselte Sharing zwischen Keeper-Anwendern und Nicht-Anwendern. Dies bietet Unternehmen, die Keeper im Einsatz haben, eine sichere Möglichkeit, vertrauliche Informationen mit ihren Kunden, Lieferanten und Partnern auszutauschen.

Die neue bidirektionale Sharing-Funktion baut auf der bestehenden Funktionalität von Keeper's One-Time Share (OTS) auf. OTS dient der sicheren Freigabe von Anmeldedaten und Dateien an einen ausgewählten Empfänger zur einmaligen Verwendung. Diese Freigaben sind während der Übertragung durch die Keeper ‘Elliptic-Curve‘ sowie durch eine AES-256-Kryptografie geschützt und können nur lokal auf dem Gerät des Empfängers entschlüsselt werden. Nach dem Empfang laufen die Freigaben automatisch nach der vom Absender festgelegten Zeit ab. Außerdem ist jede Freigabe auf ein einziges Gerät beschränkt. Der Empfänger kann mehrfach auf die freigegebenen Daten zugreifen, bis die Freigabe abläuft oder vom Absender beendet wird - je nachdem, was zuerst eintritt.

„Das bidirektionale One-Time Share ist der jüngste Schritt in unserem Bestreben, allen Kunden einen einfachen und sicheren Austausch vertraulicher Informationen mit Ende-zu-Ende-Verschlüsselung zu ermöglichen“, sagt Craig Lurey, CTO und Mitbegründer von Keeper Security. "Indem wir die bidirektionale Bearbeitung unterstützen, fügen wir eine weitere Sicherheitsebene für die Cyberabwehr unserer Nutzer hinzu. Wir sind stolz darauf, dass wir branchenweit die Ersten sind, die diese Funktion hinzufügen, und dass wir weiterhin in erster Linie unsere Kunden unterstützen."

Das Update für die bidirektionale Funktionalität ermöglicht einen einfacheren Austausch zwischen Anwendern und Nicht-Nutzern der Keeper-Plattform. Zuvor konnten Nutzer externe Freigaben nur zur Ansicht versenden. Jetzt können auch Nicht-Nutzer Daten mit Keeper-Kunden für beide Parteien Ende-zu-Ende-verschlüsselt austauschen. Das bietet die sichere Erfassung und den Austausch von vertraulichen Informationen wie Dokumenten und Anmeldedaten, ohne dass unsichere E-Mail-, Textnachrichten- oder Instant-Messaging-Kanäle verwendet werden müssen.

Anwender geben Datensätze frei, indem sie den gewünschten Datensatz aus ihrem Keeper Vault auswählen und eine einmalige Freigabe initiieren. Der Nutzer kann die Zugriffseinstellungen anpassen und einen sicheren, zeitlich begrenzten Link erstellen. Der Empfänger klickt auf den Link, um den Inhalt zu sehen und um Inhalte hochzuladen, zu ändern oder zu kommentieren. Sobald das Zeitlimit erreicht ist oder der Zugriff widerrufen wird, endet die Sitzung endgültig und der Datensatz ist nicht mehr zugänglich.

Organisationen können die bidirektionale einmalige Freigabe nutzen, um beispielsweise folgende Vorgänge zu erleichtern:

- **Kollaboration:** Sicheres Sammeln von signierten Dokumenten, Feedback oder sensiblen Dateien von Kunden, Auftragnehmern und Partnern, ohne dass diese ein Konto erstellen müssen.
- **Lieferantenanfragen:** Sicheres Anfordern von Compliance-Dokumenten oder privaten Anmeldeinformationen von Dritten.
- **Interne Audits:** Vorübergehende Freigabe und Empfang von Informationen für Prüfer oder juristische Teams.

Um mehr über die neue One-Time-Share-Funktion von Keeper zu erfahren, besuchen Sie bitte unser Dokumentationsportal.

###

Über Keeper Security:
Keeper Security verändert die Cybersicherheit für Millionen von Einzelpersonen und Tausende von Unternehmen weltweit. Die intuitive Cybersicherheitsplattform von Keeper ist mit einer End-to-End-Verschlüsselung ausgestattet und genießt das Vertrauen von Fortune-100-Unternehmen, um jeden Benutzer auf jedem Gerät und an jedem Standort zu schützen. Unsere patentierte Zero-Trust- und Zero-Knowledge-Lösung für das Privileged Access Management vereint die Verwaltung von Unternehmenspasswörtern, Geheimnissen und Verbindungen mit Zero-Trust-Netzwerkzugriffen und Remote-Browser-Isolation. Durch die Kombination dieser wichtigen Identitäts- und Zugriffsverwaltungskomponenten in einer einzigen cloudbasierten Lösung bietet Keeper beispiellose Transparenz, Sicherheit und Kontrolle und gewährleistet gleichzeitig die Einhaltung von Compliance- und Audit-Anforderungen. Erfahren Sie unter KeeperSecurity.com, wie Keeper Ihr Unternehmen vor den heutigen Cyberbedrohungen schützen kann.

Folgen Sie Keeper auf 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