Pressemitteilung

Keeper Security integriert Passkey-Unterstützung für mobile Geräte

Keeper bietet die sichere Verwaltung und plattformübergreifende Funktionalität sowohl für Passkeys als auch für herkömmliche Passwörter

München, 2. April 2024 – Keeper Security, ein führender Anbieter von Zero-Trust- und Zero-Knowledge-Lösungen zum Schutz von Anmeldedaten, privilegiertem Zugang und Remote-Verbindungen, kündigt heute die Unterstützung von Passkey-Management für mobile Geräte mit iOS und Android an. Mit Keeper werden Passkeys im Keeper Vault erstellt, gespeichert und verwaltet und können für die einfache Anmeldung bei Websites und Anwendungen in allen Browsern und Betriebssystemen verwendet werden. Solange der Anwender Zugang zu seinem Keeper Vault hat, kann er auf seine Passkeys zugreifen, egal ob auf dem Desktop oder seinem mobilen Gerät.

„Keeper ist führend auf dem Weg in eine sichere, passwortlose Zukunft, indem wir unsere Unterstützung für Passkeys weiter ausbauen", sagt Craig Lurey, CTO und Mitbegründer von Keeper Security. „Da diese faszinierende neue Authentifizierungsmethode an Popularität gewinnt, benötigen Benutzer eine Plattform, die eine sichere Verwaltung mehrerer Anmeldemethoden bietet - einschließlich Passkeys und herkömmlicher Passwörter. In dieser hybriden Welt bietet Keeper eine nahtlose Benutzererfahrung über alle Betriebssysteme und Geräte hinweg."

Ein Passkey ist ein kryptografischer Schlüssel, mit dem sich Nutzer bei Konten und Apps anmelden können, ohne ein Passwort eingeben zu müssen - ähnlich wie bei einer digitalen Version einer Schlüsselkarte, die auf einem Telefon, Tablet oder Computer gespeichert ist. Der Passkey nutzt biometrische Daten auf dem Gerät, wie beispielsweise den Fingerabdruck oder die Gesichtserkennung. Dies ermöglicht es, sich bei unterstützten Apps und Konten auf die gleiche Weise anzumelden wie ein Nutzer, der sein Telefon oder Tablet mit seinem Fingerabdruck oder mit Gesichtserkennung entsperrt.

Bereits im Juni 2023 kündigte Keeper die Unterstützung für Passkeys in seinen Browsererweiterungen für Chrome, Firefox, Edge, Brave und Safari an. Die Unterstützung für iOS und Android ist für die kommenden Wochen geplant. Keeper speichert und füllt den Passkey automatisch aus, ähnlich wie bei einer passwortbasierten Anmeldung. Der Keeper Vault ermöglicht die Verwaltung der Passkeys, einschließlich der Möglichkeit einer gemeinsamen Nutzung durch Familienmitglieder oder Teams in Unternehmen.

Um einen sicheren Passkeys zu erstellen und zu speichern, ruft der Benutzer die "Sicherheit" oder "Kontoeinstellungen" auf der Website auf. Wenn der Benutzer auf "Passkey erstellen" klickt, wird er gefragt, ob er den Passkey in seinem Keeper Vault speichern möchte. Sobald der Benutzer das nächste Mal diese Website besucht, kann er sich mit dem im Keeper Vault gespeicherten und mit Zero-Knowledge-geschützen Passkey von jedem Gerät aus anmelden.
Dies ist ein entscheidender Vorteil, da Passkeys sonst nur mit dem Gerät verwendet werden können, mit dem sie erstellt wurden. Der Passkey-Datensatz im Keeper Vault des Benutzers enthält das Datum, an dem der Passkey erstellt wurde, den Benutzernamen und die

Website oder App, auf der er erstellt wurde. Passkey-Datensätze können im Tresor wie jeder andere Datensatz verwaltet werden, wie beispielsweise in Ordnern abgelegt oder für andere Benutzer freigegeben.

Passkeys sind einfacher zu verwenden als viele traditionelle Authentifizierungsmethoden. Sie sind zudem resistent gegen Phishing, so dass sich die Benutzer nahtlos und sicher bei unterstützten Websites anmelden können. Die passwortlose Technologie, die erstmals 2022 vorgestellt wurde, basiert auf Industriestandards des World Wide Web Consortium (W3C) und der FIDO Alliance und wird von Apple, Google, Microsoft, Paypal, eBay und anderen unterstützt.

Mehr über die Unterstützung von Keeper für Passkeys, ist hier zu finden.

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