Pressemitteilung

Keeper Security führt innovative biometrische Anmeldung mit Passkeys ein

Das neue Update ermöglicht den nativen passwortlosen Zugriff auf den Tresor über die Browser-Erweiterung und die Commander-CLI.

MÜNCHEN, 20. August 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, gibt die Einführung der biometrischen Anmeldung mit FIDO2/WebAuthn-Passkeys in der Chrome/Edge-Browsererweiterung und der Keeper Commander CLI bekannt.
Dieses Update ist das erste seiner Art in der Branche. Es ermöglicht Nutzern, sicher auf ihren Keeper-Tresor mit Passkeys zuzugreifen, die durch biometrische Daten oder PINs geschützt sind – plattformübergreifend, einschließlich Windows-Geräten über Windows Hello und Mac-Geräten mit Touch ID – und ersetzt damit die Notwendigkeit, Passwörter einzugeben.
Die biometrischen Daten verlassen niemals das Gerät des Nutzers und werden niemals an Keeper übertragen oder sind für Keeper zugänglich, wodurch vollständige Privatsphäre gewährleistet ist. Kunden müssen keine Begleit-Anwendung installieren, was die Benutzererfahrung vereinfacht und die Zero-Knowledge-End-to-End-Verschlüsselung beibehält.

Ein Passkey ist eine FIDO-Authentifizierungsnachweis, die auf den FIDO-Standards basiert und es Benutzern ermöglicht, sich bei Apps und Webseiten mit dem gleichen Verfahren anzumelden, das sie zum Entsperren ihres Geräts verwenden, wie zum Beispiel biometrische Daten. Die kryptografisch einzigartigen, gerätegebundenen Anmeldedaten sollen herkömmliche Passwörter durch eine phishing-resistente, passwortlose Authentifizierung ersetzen. Passkeys sind sowohl sicherer als auch benutzerfreundlicher, da der Benutzer keinen Benutzernamen, kein Passwort oder keine zusätzlichen Faktoren mehr eingeben muss. Durch die Unterstützung der weit verbreiteten FIDO2/WebAuthn-Protokolle bietet Keeper eine sichere und bequeme Anmeldeerfahrung für seine Browser-Erweiterung sowie für Keeper Commander, seine Befehlszeilen- und SDK-Schnittstelle, auf allen kompatiblen Geräten und Browsern.

„Die Sicherheit verlagert sich von Passwörtern hin zu stärkeren, zuverlässigeren Methoden“, sagt Craig Lurey, CTO und Co-Gründer von Keeper Security. „Mit diesem branchenführenden Update können Nutzer ihre Tresore mit vertrauenswürdigen, gerätebasierten Anmeldedaten wie biometrischen Daten oder PINs entsperren, wodurch die Abhängigkeit von Passwörtern, die gestohlen oder durch Phishing erlangt werden können, verkleinert wird. Keeper ist stolz darauf, als erstes Unternehmen diese Funktion für Privatpersonen und Organisationen anzubieten.“

Windows Hello bietet native biometrische und PIN-Authentifizierung auf Windows 11-Geräten, während Apples Touch ID ähnliche Funktionen auf macOS ermöglicht. Die Implementierung von FIDO2/WebAuthn durch Keeper unterstützt die passkey-basierte

Anmeldung in Chromium-basierten Browsern und bietet eine sichere und nahtlose Erfahrung auf einer Vielzahl von unterstützten Plattformen und Geräten.

Keeper ist Mitglied der FIDO Alliance und unterstützt deren Mission, die Branche über Passwörter hinaus zu entwickeln. Durch ihre Arbeit an der Entwicklung offener Standards wie FIDO2 und WebAuthn hilft die Alliance Unternehmen dabei, sichere, phishing-resistente Authentifizierungsverfahren zu adaptieren, die in bereits verwendeten Geräten integriert sind. Dieses Update spiegelt diesen Wandel wider – es vereinfacht die Anmeldung, stärkt gleichzeitig den Schutz und erleichtert es IT-Teams, den passwortlosen Zugriff in großem Maßstab zu unterstützen.

Neben der Aktivierung der Passkey-Anmeldung unterstützt Keeper die Erstellung, sichere Speicherung und das automatische Ausfüllen von Passkeys auf allen Geräten, Browsern und Betriebssystemen. Die plattformübergreifende Passkey-Verwaltung von Keeper ist über die Browser-Erweiterung, mobile Apps, den Web- und Desktop-Tresor sowie die Keeper Commander CLI verfügbar, sodass Nutzer Passkeys verwenden können, ohne Kompromisse bei der Benutzerfreundlichkeit oder Sicherheit eingehen zu müssen. Unabhängig davon, ob sie auf ihren Keeper-Tresor zugreifen oder sich bei unterstützten Webseiten und Anwendungen anmelden, können die Nutzer Passkeys nahtlos speichern und automatisch ausfüllen – ohne Passwort oder zweiten Faktor.

Die Passkey-Anmeldefunktion von Keeper entspricht dem zunehmenden Einsatz von Passkeys in Unternehmen. Laut dem Insight-Bericht von Keeper „Navigating a Hybrid Authentication Landscape“ verwenden derzeit 80 Prozent der Unternehmen Passkeys oder planen deren Einführung, um das Risiko von Bedrohungen wie Phishing und automatisches Passwort-Ausfüllen zu verringern. Viele stehen jedoch vor Herausforderungen bei der Verwaltung hybrider Systeme, die Passwörter mit passwortlosen Methoden kombinieren. Keeper erleichtert die Einführung von Passkeys in großem Maßstab, indem es FIDO2-Standards auf allen Geräten, Plattformen und Browsern unterstützt und so die Komplexität für Nutzer und IT-Teams gleichermaßen beseitigt.

Die Keeper-Browsererweiterung steht ab sofort auf der Webseite von Keeper, im Chrome Web Store und im Microsoft Edge Add-ons Store zum Download bereit. Die Keeper Commander CLI ist im Open-Source-Github-Repository von Keeper verfügbar. Weitere Informationen gibt es im Dokumentationsportal von Keeper.

###

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