Keeper Security lance une connexion biométrique innovante avec des clés d'accès

La nouvelle mise à jour permet un accès natif sans mot de passe au coffre-fort via l'extension de navigateur et l'interface CLI Commander

Paris, France – 20 août 2025 – Keeper Security, le principal fournisseur de solutions de cybersécurité pour la gestion des accès privilégiés (PAM) de type « zero trust » et « zero knowledge » qui protège les mots de passe et les clés d'accès, les comptes privilégiés, les secrets et les connexions à distance, annonce la sortie d'une fonctionnalité de connexion biométrique utilisant les clés d'accès FIDO2/WebAuthn sur l'extension de navigateur Chrome/Edge et l'interface CLI Keeper Commander. Cette mise à jour, la première du genre dans le secteur, permet aux utilisateurs d'accéder en toute sécurité à leur coffre-fort Keeper à l'aide de clés d'accès protégées par des données biométriques ou des codes PIN sur plusieurs plateformes, y compris les appareils Windows via Windows Hello et les appareils Mac à l'aide de Touch ID, sans avoir à saisir de mot de passe. Les informations biométriques ne quittent jamais l'appareil de l'utilisateur et ne sont jamais transmises à Keeper ni accessibles par celui-ci, ce qui garantit une confidentialité totale. Les clients n'ont pas besoin d'installer une application compagnon, ce qui simplifie l'expérience utilisateur et garantit un chiffrement de bout en bout sans connaissance.

Une clé d'accès est un identifiant d'authentification FIDO, basé sur les normes FIDO, qui permet à un utilisateur de se connecter à des applications et à des sites web en utilisant le même processus que celui utilisé pour déverrouiller son appareil, par exemple la biométrie. Les identifiants cryptographiques uniques et liés à l'appareil sont conçus pour remplacer les mots de passe traditionnels par une authentification sans mot de passe et résistante au phishing. Les clés d'accès sont à la fois plus sûres et plus faciles à utiliser, car l'utilisateur n'a plus besoin de saisir son nom d'utilisateur, son mot de passe ou des facteurs supplémentaires. En prenant en charge les protocoles FIDO2/WebAuthn largement adoptés, Keeper offre une expérience de connexion sécurisée et pratique pour son extension de navigateur ainsi que pour Keeper Commander, son interface de ligne de commande et son SDK, sur tous les appareils et navigateurs compatibles.

« La sécurité évolue et passe des mots de passe seuls à des méthodes plus robustes et plus fiables », a déclaré Craig Lurey, directeur technique et

cofondateur de Keeper Security. « Cette mise à jour de pointe permet aux utilisateurs de déverrouiller leurs coffres-forts à l'aide d'identifiants fiables et liés à leur appareil, tels que des données biométriques ou des codes PIN, réduisant ainsi leur dépendance aux mots de passe qui peuvent être volés ou piratés. Keeper est fier d'être le premier à offrir cette fonctionnalité aux particuliers et aux entreprises. »

Windows Hello offre une authentification biométrique et par code PIN native sur les appareils Windows 11, tandis que Touch ID d'Apple offre des fonctionnalités similaires sur macOS. La mise en œuvre de FIDO2/WebAuthn par Keeper prend en charge la connexion par clé d'accès sur les navigateurs basés sur Chromium, offrant une expérience sécurisée et transparente sur une large gamme de plateformes et d'appareils pris en charge.

Keeper est fier d'être membre de la FIDO Alliance et de soutenir sa mission qui consiste à faire évoluer le secteur au-delà des mots de passe. Grâce à son travail de développement de normes ouvertes telles que FIDO2 et WebAuthn, l'Alliance aide les organisations à adopter une authentification sécurisée et résistante au phishing, intégrée aux appareils que les utilisateurs utilisent déjà. Cette mise à jour reflète cette évolution : elle simplifie la connexion tout en renforçant la protection et en facilitant la prise en charge à grande échelle de l'accès sans mot de passe par les équipes informatiques.

En plus de permettre la connexion par clé d'accès, Keeper prend en charge la création, le stockage sécurisé et le remplissage automatique des clés d'accès sur tous les appareils, navigateurs et systèmes d'exploitation. La gestion multiplateforme des clés d'accès de Keeper est disponible via son extension de navigateur, ses applications mobiles, son coffre-fort web et de bureau, ainsi que via Keeper Commander CLI, permettant aux utilisateurs de tirer parti des clés d'accès sans compromettre la convivialité ou la sécurité. Qu'ils accèdent à leur coffre-fort Keeper ou se connectent à des sites web et applications pris en charge, les utilisateurs peuvent stocker et remplir automatiquement leurs passkeys en toute transparence, sans mot de passe ni deuxième facteur d'authentification.

La fonctionnalité de connexion par passkey de Keeper s'inscrit dans la tendance croissante à l'adoption des passkeys au sein des entreprises. Selon le rapport Insight de Keeper intitulé « Navigating a Hybrid Authentication Landscape » (Naviguer dans un paysage d'authentification hybride), 80 % des entreprises utilisent actuellement ou prévoient d'adopter des clés d'accès pour réduire les risques liés aux menaces telles que le phishing et le credential

stuffing. Cependant, beaucoup d'entre elles sont confrontées à des difficultés pour gérer des systèmes hybrides qui combinent des mots de passe et des méthodes sans mot de passe. Keeper facilite l'adoption à grande échelle des clés d'accès en prenant en charge les normes FIDO2 sur tous les appareils, plateformes et navigateurs, ce qui élimine la complexité pour les utilisateurs et les équipes informatiques.

L'extension de navigateur Keeper est désormais disponible au téléchargement sur le site web de Keeper, le Chrome Web Store et le Microsoft Edge Add-ons Store. L'interface CLI Keeper Commander est disponible dans le référentiel Github open source de Keeper. Pour plus d'informations, consultez le portail de documentation de Keeper.

A propos de Keeper Security :

Keeper Security transforme la cybersécurité pour des millions d'individus et des milliers d'organisations dans le monde. Construite avec un cryptage de bout en bout, la plateforme de cybersécurité intuitive de Keeper protège chaque utilisateur, sur chaque appareil, en chaque lieu. Notre solution brevetée de gestion des accès à privilèges Zero-Trust et Zero-Knowledge unifie la gestion des mots de passe, des secrets et des connexions avec isolation du navigateur à distance. En combinant ces composants de gestion essentiels de l'identité et des accès en une seule solution cloud-based, Keeper offre une visibilité, une sécurité et un contrôle inégalés tout en veillant à ce que les exigences en matière de conformité et d'audit soient respectées. Découvrez comment Keeper peut défendre votre organisation face aux cybermenaces sur KeeperSecurity.com.