



KEEPER®

Communiqué de presse

Keeper Security annonce la prise en charge des Passkey sur les appareils mobiles

Keeper® offre une gestion sécurisée et une fonctionnalité multiplateforme de pointe pour les passkeys et les mots de passe traditionnels.

CHICAGO, 2 avril 2024 - [Keeper Security](#), le principal fournisseur de logiciels de cybersécurité Zero Trust et Zero Knowledge basés sur le cloud qui protègent les mots de passe, les secrets, les connexions et les accès privilégiés, annonce aujourd'hui une nouvelle mise à jour pour iOS et Android qui inclut la prise en charge de la gestion des passkeys. Avec Keeper, les passkeys sont créés, stockés et gérés dans le coffre-fort de Keeper, et peuvent être utilisés pour se connecter à des sites web et des applications à travers tous les navigateurs et systèmes d'exploitation avec facilité. Tant que vous avez accès à votre coffre-fort Keeper, vous avez accès à vos passkeys, que ce soit sur votre ordinateur ou sur votre appareil mobile.

« Keeper ouvre la voie à un avenir sûr, sans mot de passe, en élargissant notre support pour les passkeys », a déclaré Craig Lurey, CTO et cofondateur de Keeper Security. « Alors que cette nouvelle méthode d'authentification gagne en popularité, nous comprenons que les utilisateurs ont besoin d'une plateforme qui offre une gestion sécuritaire de plusieurs méthodes d'ouverture de session, y compris les clés d'accès et les mots de passe traditionnels. Dans ce monde hybride, Keeper offre une expérience transparente à travers les systèmes d'exploitation et les appareils ».

Un passkey est une clé cryptographique qui permet aux utilisateurs de se connecter à des comptes et à des applications sans saisir de mot de passe, un peu comme la version numérique d'une carte magnétique stockée sur un téléphone, une tablette ou un ordinateur. Le passkey exploite les données biométriques de votre appareil, telles que votre empreinte digitale ou la reconnaissance faciale, ce qui vous permet de vous connecter aux applications et comptes pris en charge de la même manière que vous déverrouillez votre téléphone ou votre tablette avec votre empreinte digitale ou votre visage.

En juin 2023, Keeper a annoncé la prise en charge des passkeys dans ses extensions de navigateur pour Chrome, Firefox, Edge, Brave et Safari, la prise en charge pour Android étant prévue plus tard cette année. Keeper enregistre et remplit automatiquement le mot de passe, de la même manière qu'une connexion par mot de passe. Le coffre-fort de Keeper permet de gérer les clés, y compris la possibilité de les partager entre les membres de la famille et les équipes de travail.

Les principaux navigateurs et plateformes ont commencé à intégrer le support des passkeys dans leurs systèmes d'exploitation, laissant aux développeurs de sites web et d'applications la responsabilité d'intégrer le support des passkeys dans leurs flux d'ouverture de session. Étant donné que les passkeys ne fonctionnent que sur les sites web et les plateformes qui les prennent en charge, Keeper a créé un [annuaire des passkeys](#) pour fournir aux utilisateurs une liste actualisée des endroits où ils peuvent être utilisés.

Pour créer et sauvegarder un passe-partout, les utilisateurs visiteront l'écran « Sécurité » ou « Paramètres du compte » du site web. En cliquant sur « Créer un mot de passe », l'utilisateur

devra indiquer s'il souhaite sauvegarder le mot de passe dans son Coffre-fort Keeper. La prochaine fois que l'utilisateur visitera un site web qui supporte la connexion par clé, il pourra utiliser la clé sauvegardée dans son Coffre-fort pour se connecter. L'enregistrement de la clé dans le coffre-fort de l'utilisateur contient la date de création de la clé, le nom d'utilisateur et le site web ou l'application sur lequel elle a été créée. Les enregistrements de clés peuvent être gérés dans le coffre-fort comme n'importe quel autre enregistrement, y compris être placés dans des dossiers ou partagés avec d'autres utilisateurs.

Les Passkeys sont à la fois plus faciles à utiliser que de nombreuses méthodes d'authentification traditionnelles et plus résistantes au phishing, ce qui permet aux utilisateurs de se connecter aux sites web pris en charge de manière transparente et plus sûre. La technologie sans mot de passe, introduite pour la première fois en 2022, repose sur les normes industrielles du World Wide Web Consortium (W3C) et de l'alliance FIDO, et est soutenue par Apple, Google, Microsoft, Paypal, eBay et bien d'autres encore.

###

A propos de Keeper Security:

Keeper Security transforme la cybersécurité pour les personnes et les organisations du monde entier. Les solutions de Keeper, abordables et faciles à utiliser, sont construites sur la base d'une sécurité Zero Trust et Zero Knowledge pour protéger chaque utilisateur sur chaque appareil. La solution de gestion des accès privilégiés de nouvelle génération Keeper se déploie en quelques minutes et s'intègre de manière transparente à n'importe quelle stack technologique pour prévenir les violations, réduire les coûts du service d'assistance et garantir la conformité. Des millions de personnes et des milliers d'organisations font confiance à Keeper, le leader en matière de gestion de mots de passe et de passkeys, de gestion des secrets, d'accès privilégié, d'accès à distance sécurisé et de messagerie chiffrée.

Pour en savoir plus, visitez le site KeeperSecurity.com

Suivre Keeper: [Facebook](#) [Instagram](#) [LinkedIn](#) [X](#) [YouTube](#)

Contact Presse :

Christelle Klein :

06 63 97 01 67

cklein@hl-com.com