KEEPER
Cybersecurity Starts Here

FICHE PRODUIT

Keeper Enterprise

Votre plus grosse faille de sécurité se cache sous vos yeux.

Chaque jour, vos collaborateurs utilisent des mots de passe faibles, les utilisent pour tous leurs comptes et les oublient.

des violations de données sont dues à un mot de passe faible ou volé[1]

des individus utilisent le même mot de passe pour tous leurs comptes[2]

des appels à l'assistance sont liés aux mots de passe[3]

Sécurité

La sécurité réseau la plus avancée peut être facilement contournée par l'usage de mots de passe faibles. Les habitudes des collaborateurs en matière de mots de passe ne peuvent être améliorées qu'à l'aide d'une bonne visibilité sur leur utilisation et le respect des règles de sécurité.
Keeper résout ce problème en fournissant des notifications, des rapports et audits complets.

Conformité

Chaque norme et réglementation en vigueur en matière de cybersécurité, du NIST à l'ISO et du PCI à l'HIPAA, requiert le suivi et contrôle des accès, ainsi que la mise à disposition d'un journal d'audit. Keeper permet l'attribution de rôles et le suivi des accès partagés. Les journaux d'accès au coffre-fort Keeper peuvent être contrôlés dans le cadre d'un audit de conformité ou d'analyses.

Synchronisation avec Microsoft Active Directory

Keeper® AD Bridge se synchronise avec Microsoft Active Directory et Open LDAP. Cela permet l'intégration rapide des utilisateurs et la création automatique de Nœuds (unités organisationnelles), Utilisateurs, Rôles et Équipes. Keeper permet le contrôle d'accès basé sur les rôles et rend possible l'évolution des rôles au fur et à mesure des promotions internes des employés dans l'entreprise. Cette fonctionnalité inclut le verrouillage des coffres-forts des employés qui quittent la société.

Coûts d'assistance

Keeper réduit les coûts d'assistance liés aux problèmes de mots de passe. Selon Forrester, plusieurs grosses structures ont attribué plus d'un million de dollars par an en coûts d'assistance liés aux mots de passe.

Productivité

Keeper réduit les coûts d'assistance, fait gagner du temps à vos collaborateurs et leur permet de ne plus jamais avoir à se souvenir ou à réutiliser un mot de passe. Keeper génère des mots de passe complexes et aléatoires, et les saisit automatiquement à la place de l'utilisateur.
Les collaborateurs peuvent accéder au coffre-fort Keeper et à son interface intuitive sur n'importe quel appareil où qu'ils se trouvent. Keeper est disponible en 21 langues pour une utilisation mondiale.

Automatisation du changement des mots de passe

Keeper® Commander SDK fournit aux administrateurs et aux développeurs informatiques des outils de commande en ligne et donne accès au code source Python pour la gestion et la rotation des mots de passe et les fonctionnalités du coffre-fort.
Keeper supprime les mots de passe codés en dur ou en texte clair dans le backend. Les connecteurs comprennent les connexions Unix Windows et AD, les bases de données Oracle, Microsoft SQL, MySQL, Postgres et Dynamo, les mots de passe AWS et les clés d'accès API.

> **« Les gestionnaires de mots de passe peuvent aider à mieux gérer les coûts liés aux mots de passe et générer un retour sur investissement probant . »**
>
> - Forrester[4]

Ils nous font confiance

THOMSON REUTERS®

grand river Health

Quest Federal Credit Union

Oregon State University

Authentification à deux facteurs

Keeper prend en charge l'authentification à deux facteurs (2FA) dont SMS, Keeper DNA® (montre intelligente), TOTP (Google Authenticator et Authy par exemple), FIDO U2F (Yubikey par exemple), Duo et RSA SecuriD.
L'authentification à deux facteurs peut être appliquée par le biais de contrôle basé sur les rôles.

Architecture Zero-Knowledge

Tous les chiffrements et déchiffrements sont réalisés sur l'appareil de l'utilisateur. La norme PBKDF2 avec 100 000 itérations est utilisée pour générer une clé à partir du mot de passe principal de l'utilisateur.
Chaque enregistrement est chiffré AES-256 à l'aide d'une clé différente et unique qui est générée de façon aléatoire côté client. Le chiffrement RSA est utilisé pour le partage sécurisé des enregistrements entre les utilisateurs et les équipes. L'infrastructure de Keeper synchronise le chiffrement du texte entre les appareils. L'affectation des clés est imposée entre le client et le serveur. Toutes les données en transit et au repos sont toujours chiffrées - elles ne peuvent être vues par les employés de Keeper Security ou par des tiers.

Déploiement à grande échelle

Un déploiement à grande échelle est possible à l'aide d'un portail ou d'une messagerie existante. Par exemple, pour une université, le système de messagerie en place pour les élèves permet de mettre en place des coffres-forts pour chaque élève.

Prise en charge des filiales, services, bureaux et succursales

Keeper a été créé pour prendre en charge les différents types d'unités organisationnelles afin de répondre aux besoins des entreprises de toutes tailles et tous secteurs. L'administrateur de Keeper peut définir les politiques de gestion des mots de passe par rôle, équipe et type de structure. Ainsi, les différentes divisions, succursales, filiales et bureaux d'une organisation peuvent tous être protégés par Keeper, tout en ayant des droits d'accès, des permissions et des politiques différentes pour appliquer la gestion sécurisée des mots de passe au sein d'un groupe d'entreprises. Chaque structure peut utiliser plusieurs administrateurs Keeper avec des permissions bien définies sur leurs utilisateurs, rôles et équipes.

Intégration avec les principales solutions SSO

Keeper® SSO Connect s'intègre à votre IdP et est la solution parfaite pour les applications qui ne prennent pas en charge les protocoles SAML. Keeper fournit également aux utilisateurs un accès privilégié et un coffre-fort sécurisé pour stocker tous leurs mots de passe non-SSO, certificats numériques, clés de chiffrement et clés d'accès API.

ADFS · Microsoft Azure · okta · G Suite
JumpCloud · amazon web services · CAS · IBM Security
Ping Identity · onelogin · Centrify · f5

Attestations et certifications Keeper

GSA Schedule 70 Contract 47QTCA18D00C9 · AICPA SOC · PCI DSS Compliant · TRUSTe Certified Privacy

Adopté par des millions d'utilisateurs et des milliers d'entreprises

PCMag	G2 Crowd	Gartner peer Insights	Trustpilot	GetApp
Choix de l'équipe	**Leader entreprise printemps 2019**			
4,5 étoiles sur 5	4,7 étoiles sur 5	4,7 étoiles sur 5	9,3 sur 10 sur TrustScore	4,8 étoiles sur 5

[1] Verizon 2017 Data Breach Incident Report [2] Keeper Survey of 1000 Internet Users in 2017 [3] Gartner Group [4] Forrester Report: Best Practices: Selecting, Deploying and Managing Enterprise Password Managers