KEEPER
Cybersecurity Starts Here

FICHE PRODUIT

Mémo sur le secteur de la santé

Le secteur de la santé se fait attaquer

des entreprises du secteur médical ont subi des violations de données au cours des 5 dernières années[1]

par fichier est le coût moyen d'une violation de données en 2019[2]

d'augmentation des attaques par e-mail médical frauduleux au cours des 2 dernières années[3]

Cybersécurité pour le secteur médical

Tandis que le secteur médical redouble d'efforts pour gérer les vagues de cas de COVID-19, les changements organisationnels et de réseau peuvent affaiblir la résistance des entreprises face aux cyberattaques. Les pirates ciblent déjà le secteur médical en lançant des campagnes d'hameçonnage et des attaques par ransomware qui peuvent avoir un impact négatif sur les technologies de données médicales, les dossiers médicaux et la sécurité des patients.[4]

Plus de 93 % des entreprises du secteur ont subi des piratages au cours des 2 dernières années[5] et plus de 80 % des violations de données ont pour origine des mots de passe compromis.[6] Keeper limite le risque d'attaque par ransomware et de violations de données associées à des mots de passe en offrant aux administrateurs une visibilité totale sur les pratiques d'utilisation des mots de passe de leurs collaborateurs à l'aide de rapports et audits complets. Les administrateurs peuvent également contrôler les habitudes de mots de passe de leurs collaborateurs et faire appliquer des politiques de sécurité, telles que l'utilisation de mots de passe complexes uniques et l'authentification multifacteur (MFA).

Plus de productivité

Keeper est l'application idéale de cybersécurité et de productivité. Elle protège tous les collaborateurs, sur site ou en télétravail, contre les cybermenaces et violations de données associées à des mots de passe. Keeper est facile à prendre en main et permet aux collaborateurs de respecter facilement les politiques de protection des mots de passe de l'entreprise.

Keeper génère automatiquement des mots de passe complexes et uniques pour chaque compte, les stocke dans un coffre-fort sécurisé auquel les utilisateurs ont accès où qu'ils soient et sur n'importe quel appareil mobile ou de bureau et saisit automatiquement les identifiants de connexion des collaborateurs sur tous les sites et applis qu'ils utilisent. L'application enregistre même les codes d'authentification à deux facteurs ! Les collaborateurs ne perdent et n'oublient jamais leurs mots de passe : ils gagnent ainsi en productivité et n'ont plus besoin de faire appel à l'assistance pour réinitialiser des mots de passe.

Authentification à deux facteurs

Keeper prend en charge de nombreuses méthodes d'authentification à deux facteurs (2FA), notamment les SMS, Keeper DNA® (avec smartwatch), les solutions TOTP (Google Authenticator et Authy par exemple), FIDO U2F (YubiKey par exemple), Duo et RSA SecurID. L'authentification à deux facteurs peut aussi être appliquée à l'aide de contrôles basés sur les rôles.

Approvisionnement automatique avec adresse e-mail

Approvisionnez facilement et rapidement des milliers d'utilisateurs sur leur compte Keeper au moyen d'une correspondance de domaine d'adresses e-mail. Avec un minimum d'administration, un déploiement à grande échelle peut être réalisé à l'aide d'un canal ou portail e-mail existant.

Approvisionnement flexible

Keeper peut approvisionner facilement des utilisateurs et équipes à partir de Microsoft Azure AD ou d'autres plateformes d'identité à l'aide du protocole SCIM. Keeper prend également en charge l'approvisionnement par ligne de commande basé sur API avec Keeper® Commander SDK. Keeper Commander SDK est disponible sous la forme de code Python open source téléchargeable sur le répertoire GitHub de Keeper.

Respect de la loi HIPAA

La Section 164.308(a)(5) exige des procédures de création, de modification et de protection des mots de passe et la Section 164.312(a)(1) exige un identifiant utilisateur unique, un accès en cas d'urgence et une déconnexion automatique. La Section 164.312(b) traite des contrôles par audit et notamment des journaux d'activité. Keeper fournit à tous les collaborateurs un coffre-fort numérique sécurisé. Keeper génère des mots de passe complexes aléatoires et les saisit automatiquement pour les utilisateurs. Keeper propose des contrôles d'accès en fonction du rôle (RBAC) pour faire appliquer des politiques de moindre privilège. Les dossiers et archives peuvent être partagés en toute sécurité et des autorisations peuvent être facilement ajoutées et retirées. Quand un collaborateur quitte l'entreprise, son coffre-fort Keeper est automatiquement verrouillé et transféré en toute sécurité. Les journaux d'accès à Keeper peuvent être contrôlés pour vérifier le respect des règles ou procéder à des analyses. L'architecture zero-knowledge de Keeper garantit que seuls les utilisateurs finaux ont accès à leur coffre-fort Keeper. Étant donné que Keeper Security n'a jamais accès aux données utilisateur, un contrat d'associé commercial (Business Associate Agreement, BAA) n'est pas requis pour respecter la loi HIPAA.

Architecture zero-knowledge

Tous les chiffrements et déchiffrements de données sont effectués sur l'appareil de l'utilisateur. PBKDF2 avec 100 000 tours est utilisé pour dériver une clé à partir du mot de passe principal de l'utilisateur. Chaque archive est chiffrée avec AES-256, avec une clé différente et unique générée aléatoirement côté client. Le chiffrement RSA est utilisé pour protéger le partage d'archives entre les utilisateurs et les équipes. L'infrastructure de Keeper synchronise du ciphertext chiffré entre les appareils. Une fonction de key pinning est appliquée entre le client et le serveur. Toutes les données stockées et en transit sont toujours chiffrées. Elles ne peuvent pas être consultées par les collaborateurs de Keeper Security ni par un tiers.

Synchronisation avec Microsoft Active Directory

Keeper® AD Bridge est synchronisé avec Microsoft Active Directory ou Open LDAP. Cette synchronisation permet d'approvisionner rapidement les utilisateurs et d'ajouter automatiquement des nœuds (unités organisationnelles), utilisateurs, rôles et équipes. Keeper propose des contrôles d'accès en fonction du rôle (RBAC) et la possibilité d'effectuer un suivi des rôles quand les utilisateurs changent de poste ou de responsabilité. Le verrouillage de coffre-fort est automatique lorsqu'un collaborateur quitte l'entreprise.

À propos de Keeper Security, Inc.

Keeper Security, Inc. (Keeper) est la plateforme de cybersécurité leader du marché pour la prévention des cybermenaces et violations de données associées à des mots de passe. Le logiciel de sécurité et de chiffrement zero-knowledge de Keeper a été choisi par des millions de particuliers et des milliers d'entreprises du monde entier pour limiter le risque de piratage, améliorer la productivité des collaborateurs et respecter des normes de sécurité. Keeper a été nommé « Meilleur gestionnaire de mots de passe de l'année » et « Choix de l'équipe » par PC Magazine et a été également nommé « Choix de l'équipe » par PCWorld. Keeper a remporté quatre récompenses G2 dans la catégorie « Meilleur logiciel » et la récompense « Meilleur produit de gestion de mots de passe pour la cybersécurité des PME » aux InfoSec Awards. Keeper est certifié SOC-2 et ISO 27001 et est homologué par le gouvernement fédéral des États-Unis via le système SAM (System for Award Management). Pour en savoir plus, consultez https://keepersecurity.com.

Compatibilité avec les solutions SSO leaders du marché

Keeper® SSO Connect est compatible avec votre fournisseur d'identité et est une solution idéale pour les applications qui ne prennent pas en charge les protocoles SAML. Keeper fournit aux utilisateurs avec accès privilégié un coffre-fort sécurisé où 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 tierces de Keeper

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

Récompenses et reconnaissances reçues par Keeper

Leader entreprise 2021
4,7 étoiles sur 5

Choix de l'équipe
4,5 étoiles sur 5

Gartner Peer Insights
4,6 étoiles sur 5

Spiceworks
4,9 étoiles sur 5

[1] Industry Analysts [2] Cision PR Newswire [3] HIPAA Journal [4] NJCCIC [5] Herjavec Group Healthcare Cybersecurity Report 2020 [6] ZDNet