

ÉTUDE DE CAS

L'entreprise informatique mondiale améliore la sécurité et la conformité grâce à Keeper



Contexte

Cette organisation est une société de services technologiques qui a des clients dans divers secteurs, y compris la finance, les télécommunications, les médias, le commerce de détail et la santé.

Industrie

Services technologiques

Employés

Plus de 11 000

Solutions

Gestionnaire de mots de passe entreprise

- Assistance Platinum



Le défi

En tant qu'entreprise en croissance rapide avec un personnel mondial, l'organisation avait le sentiment de vouloir renforcer la sécurité des mots de passe. Les employés utilisaient diverses solutions de gestion des mots de passe, ce qui entraînait une fragmentation, une incohérence et un manque de visibilité en matière de gestion des identifiants.

En outre, les administrateurs informatiques voulaient transmettre les meilleures pratiques de sécurité dans l'ensemble des services. À mesure que l'organisation a amélioré les normes ISO et d'autres normes de cybersécurité, le manque de solution unifiée de gestion des mots de passe a créé des lacunes de conformité et des inefficacités administratives.

Les défis clés incluaient :

Visibilité et contrôle d'accès limités: les employés ont utilisé différents outils, tels que [les gestionnaires de mots de passe basés sur un navigateur](#), ce qui complique l'application de la sécurité et le maintien de la qualité des données.

Exigences de conformité et risques de sécurité : le respect de l'amélioration continue des normes ISO et de certification de cybersécurité nécessitait une solution structurée et de niveau entreprise. L'organisation avait besoin d'une visibilité supplémentaire sur l'hygiène des identifiants et d'un moyen transparent d'appliquer les meilleures pratiques en matière de sécurité des données.

Nous voulions unifier notre gestion des mots de passe dans le cadre d'une solution unique et sécurisée que notre équipe de cybersécurité pourrait examiner et gérer.

- Responsable de la gestion des projets



La solution Keeper

L'organisation a évalué plusieurs solutions de gestion des mots de passe avant de choisir Keeper Security. Keeper s'est démarqué comme l'une des options les plus sécurisées et les plus riches en fonctionnalités, offrant une protection des mots de passe de niveau entreprise, un partage sécurisé des identifiants et une sécurité de premier ordre. La solution de Keeper offre de nombreux avantages, notamment :

Gestion centralisée des mots de passe – Keeper a fourni à l'organisation une plateforme unique et sécurisée pour le stockage et la gestion des mots de passe de l'organisation. Cela garantissait que tous les identifiants étaient protégés par l'architecture [Zero-Trust et Zero-Knowledge](#) de Keeper.

Adoption et formation des utilisateurs – Keeper est reconnu comme le premier gestionnaire de mots de passe pour les organisations de toutes tailles et est conçu pour être facile à utiliser et rapide à déployer. Le vaste [portail de documentation](#) de Keeper fournit des instructions détaillées et les meilleures pratiques du système pour aider les administrateurs à tirer le meilleur parti de leur déploiement. Pour les utilisateurs finaux, des [guides détaillés sur les produits](#) et des [vidéos de formation](#) favorisent l'adoption par les utilisateurs.

Nous avons offert à notre équipe une formation pour les utilisateurs finaux et une formation pour les administrateurs. C'est une interface assez intuitive, et nous avons eu une expérience de mise en œuvre très fluide.

– Responsable de la gestion des projets

Fonctionnalités de sécurité avancées – les mesures de sécurité robustes de Keeper, y compris l'authentification multifactor (MFA) et le chiffrement de bout en bout, garantissent que les communications internes sensibles et les données sont protégées. La capacité de partager les identifiants en toute sécurité et de manière transparente au sein des membres de l'équipe sans exposer les données sensibles ajoute une couche de protection supplémentaire.

Rentable – quelle que soit la taille ou le type d'organisation, Keeper dispose d'un abonnement rentable qui s'adapte aux besoins de l'organisation. Le modèle de tarification transparent de Keeper, jumelé à un service client de classe mondiale, classé n°1 dans le service client d'entreprise sur [G2](#), permet aux organisations de maximiser leur investissement.

La meilleure sécurité – l'architecture de sécurité Zero-Trust et Zero-Knowledge de Keeper est inégalée dans la protection de l'information et l'atténuation du risque de violation de données. Keeper combine la cryptographie à courbe elliptique (ECC) au niveau de l'appareil avec [plusieurs couches de chiffrement](#) (aux niveaux du coffre-fort, du dossier et de l'enregistrement), l'authentification multifactor et biométrique, ainsi que le chiffrement AES 256 bits validé par la norme FIPS 140-3 et PBKDF2. Keeper est [conforme aux normes SOC 2 et ISO 27001](#), la conformité la plus ancienne du secteur, ainsi qu'aux normes FedRAMP et StateRAMP.



Impact sur l'organisation

En implémentant Keeper dans l'ensemble de l'organisation, un personnel réparti dans le monde entier de plus de 11 000 employés, l'organisation a obtenu un contrôle centralisé sur la sécurité des mots de passe et des clés d'accès. Cela a permis à l'équipe informatique d'appliquer des politiques de mots de passe fortes, de surveiller l'hygiène des identifiants et de faciliter la gestion des accès sécurisés. Les principaux impacts comprennent :

Sécurité et conformité plus fortes – Keeper a amélioré la posture de sécurité de l'organisation et garanti la conformité avec de nombreuses certifications standard de l'industrie, telles que les exigences de certification ISO. Les administrateurs informatiques peuvent désormais utiliser le tableau de bord centralisé de Keeper pour surveiller la sécurité des identifiants en temps réel.

Intégration et départs rationalisés – grâce à Keeper, l'accès aux identifiants des comptes peut être provisionné ou désactivé de manière transparente pendant le processus d'intégration ou de départ de l'entreprise. Ce qui a rationalisé la collaboration et l'efficacité opérationnelle de Keeper au niveau de l'organisation.

Adoption par les utilisateurs et collaboration transparente – l'interface intuitive et la facilité d'utilisation de Keeper ont entraîné des taux d'adoption élevés, en particulier parmi le personnel non technique. Keeper offre également un [forfait famille gratuit à tous les utilisateurs professionnels](#), ce qui accélère l'adoption. L'extension de navigateur conviviale simplifie la gestion des mots de passe et des clés d'accès, ce qui améliore la collaboration entre les services et réduit les frictions lors de l'accès aux enregistrements partagés.

L'équipe a vraiment apprécié la manière dont Keeper a proposé un forfait familial gratuit. C'était un avantage supplémentaire qui a accéléré l'adoption par les utilisateurs.

– Responsable de la gestion des projets

Sécurité et visibilité – l'organisation a intégré de manière transparente Keeper à son [fournisseur SSO](#), ce qui permet aux employés de s'authentifier auprès de Keeper avec leurs identifiants SSO et d'accéder en toute sécurité au cloud de l'organisation et aux applications natives qui ne prennent pas en charge le SSO. [KeeperFill®](#), une fonctionnalité de l'extension de navigateur, de l'application mobile et de l'application de bureau Keeper, permet aux utilisateurs d'utiliser le remplissage automatique des identifiants sur les sites Web et les applications.

Ces capacités d'intégration et cette facilité d'utilisation, ainsi que la sécurité de premier ordre et l'architecture de sécurité Zero-Knowledge de Keeper, ont fourni à l'organisation une solution de gestion des mots de passe sécurisée pour se protéger contre les cybermenaces.



Keeper Password Manager

La plupart des entreprises ont une visibilité limitée sur les pratiques de leurs employés en matière de mots de passe, ce qui peut augmenter considérablement le risque cybernétique. L'hygiène des mots de passe ne peut être améliorée sans informations critiques concernant l'utilisation et la conformité des mots de passe. La solution de Keeper est d'offrir une sécurité, une visibilité et un contrôle ultimes.

Les données sont protégées avec l'architecture Zero-Knowledge security de Keeper, et un chiffrement de classe mondiale. Le Zero-knowledge signifie que seul l'utilisateur a connaissance et accès à son mot de passe principal et à la clé de chiffrement utilisée pour chiffrer et déchiffrer ses informations.

Keeper est intuitif et facile à déployer, quelle que soit la taille de l'entreprise. Keeper s'intègre à Active Directory et aux serveurs LDAP, ce qui simplifie le provisionnement et l'intégration. [Keeper SSO Connect®](#) s'intègre dans les solutions SSO existantes et est autorisé par FedRAMP et StateRAMP.

Keeper est conçu pour s'adapter aux organisations de toute taille. Des fonctionnalités telles que les autorisations basées sur les rôles, le partage d'équipe, l'audit départemental et l'administration déléguée soutiennent les organisations au fur et à mesure de leur croissance. [Keeper Commander](#) fournit des API robustes pour s'intégrer aux systèmes actuels et futurs.

Cas d'usage professionnel : Keeper Password Manager

- Prévenir les violations de données liées aux mots de passe et les cyberattaques
- Prise en charge des clés d'accès pour une authentification sans effort
- Renforcer la conformité
- Stimuler la productivité des employés
- Mettre en œuvre des politiques et des procédures en rapport avec le mot de passe
- Réduire les coûts du service d'assistance
- Réduire la formation grâce à une mise en œuvre rapide des mesures de sécurité
- Sensibiliser les employés à la sécurité et améliorer leur comportement

À PROPOS DE KEEPER

Keeper Security transforme la cybersécurité pour des millions d'individus et des milliers d'organisations dans le monde. Construite avec un chiffrement de bout en bout, la plateforme de cybersécurité intuitive de Keeper est approuvée par les entreprises du Fortune 100 pour protéger 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 d'entreprise, des secrets et des connexions avec l'accès au réseau Zero-Trust et l'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](https://keepersecurity.com).

Des milliers d'entreprises et des millions de personnes dans le monde entier font confiance à Keeper et l'apprécient.



G2
Leader d'entreprise



PCMag
Choix de l'éditeur



App Store
Productivité la mieux
évaluée



Google Play
Plus de 10 millions
d'installations