KEEPER® + St. Anna Kinderkrebsforschung

ÉTUDE DE CAS

L'Institut de recherche sur le cancer des enfants St. Anna active la gestion sécurisée des mots de passe

CONTEXTE

L'Institut de recherche sur le cancer des enfants St. Anna, basé à Vienne, en Autriche, œuvre depuis 1988 à l'amélioration du taux de guérison des enfants et des adolescents atteints de cancer.

L'Institut de recherche sur le cancer des enfants St. Anna coordonne des études multicentriques et participe de ce fait activement aux avancées internationales dans le domaine de l'oncologie pédiatrique.

Industrie
Soins de santé

Employés
250+

Solutions
Keeper Password Manager

- Enterprise
- BreachWatch®
- Module de rapports et d'alertes avancés

LE DÉFI

L'Institut de recherche sur le cancer des enfants de St. Anna (St. Anna CCRI), une organisation de renom dédiée à la recherche sur le cancer pédiatrique, a été confronté à des défis majeurs en matière de gestion et de protection de ses identifiants numériques. Véritable pôle de recherche scientifique et de collaboration, le personnel de cette organisation, composé essentiellement de chercheurs et de personnel administratif, avait besoin d'un système de gestion des mots de passe pour traiter les données sensibles de manière sûre et efficace.

Avant d'implémenter Keeper, St. Anna CCRI utilisait un ancien gestionnaire de mots de passe qui avait plusieurs défauts majeurs. Les principaux défauts étaient le faible taux d'adoption par le personnel non technique, ainsi que la visibilité et les rapports limités offerts aux administrateurs. De plus, la violation de données du système existant, qui a défrayé la chronique en 2022, a encore freiné l'adoption et l'utilisation du produit par les utilisateurs. St. Anna CCRI avait besoin d'un gestionnaire de mots de passe complet, sécurisé et convivial, pouvant s'intégrer à sa pile technologique existante, favoriser l'environnement de travail collaboratif au sein de l'organisation et rétablir la confiance entre le personnel.

Faible adoption par les utilisateurs - Les utilisateurs finaux ont trouvé l'ancien système encombrant et peu intuitif. Par conséquent, plusieurs ont continué d'utiliser des méthodes de gestion des mots de passe risquées et obsolètes, telles que les notes autocollantes ou les feuilles de calcul partagées. Ces pratiques ne présentaient pas seulement un risque important de sécurité, mais entravaient également la productivité et la collaboration au sein de l'organisation.

Visibilité et contrôles administratifs limités - Les administrateurs du système étaient confrontés à des capacités de contrôle d'accès limitées, notamment en ce qui concerne le déclassement et le transfert des identifiants stockés des employés qui étaient des contractuels à court terme de l'entreprise. Le manque de contrôle d'accès critique et de visibilité était une cause d'inquiétude majeure.

Problèmes de sécurité - Lorsque l'ancien gestionnaire de mots de passe a connu une violation de sécurité publique en 2022, le personnel de St. Anna CCRI a commencé à abandonner la solution en interne. Cet incident a non seulement exposé l'institut aux risques de piratage des données et aux cybermenaces, mais il a également entraîné chez le personnel une perte de confiance envers le système existant. La violation a révélé la nécessité d'une solution plus sûre et plus fiable pour protéger les informations hautement sensibles de l'organisation.

LA SOLUTION KEEPER

Anna CCRI a trouvé sa solution avec Keeper, un système de gestion des mots de passe robuste et convivial qui permet de répondre àleurs besoins fondamentaux. La plateforme Keeper offre un mélange unique de capacités d'intégration transparentes, de facilité d'utilisation et de sécurité optimale, ce qui en fait le choix idéal pour l'environnement collaboratif de l'organisation.

Adoption par les utilisateurs et formation - Keeper offre une extension intuitive pour navigateur web qui permet le remplissage automatique des mots de passe et des informations de connexion, supprimant ainsi la nécessité pour les employés de se souvenir des identifiants ou de les saisir manuellement. Cette fonctionnalité est particulièrement avantageuse pour le personnel non technique, dont elle simplifie les opérations quotidiennes. De plus, le portail de documentation de Keeper fournit des ressources complètes et conviviales pour les administrateurs. Pour les utilisateurs finaux, les manuels et les vidéos de formation intuitifs de Keeper garantissent une adoption élevée par les employés, peu importe leur niveau de compétence technique.

Contrôles d'accès basés sur les rôles (RBAC) - La plateforme Keeper offre de formidables fonctionnalités de collaboration et d'organisation telles que le partage sécurisé des mots de passe et les-contrôles d'accès basés sur les rôles. Grâce à ces fonctionnalités prêtes à l'emploi, les administrateurs peuvent mettre en place des contrôles spécifiques sur le partage des enregistrements et des mots de passe, garantissant ainsi le respect des politiques de sécurité à l'échelle de l'organisation.

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 possède les certifications SOC 2 et ISO 27001 les plus anciennes de l'industrie. Keeper est conforme au GDPR, au CCPA et à l'HIPAA, ainsi qu'autorisé par FedRAMP et StateRAMP, certifié PCI DSS et certifié par TrustArc pour la protection de la vie privée.

La solution Keeper combine la cryptographie à courbe elliptique au niveau de l'appareil avec plusieurs couches de cryptage (au niveau du coffre-fort, du dossier et de l'enregistrement), une authentification multifactorielle et biométrique, et un cryptage AES 256 bits plus PBKDF2 validé par la norme FIPS-140-2.

> **« Du point de vue de la sécurité informatique, la principale préoccupation était l'utilisation des notes sur le bureau et le stockage non sécurisé des mots de passe et des identifiants. Concernant l'acceptation par les utilisateurs finaux, la fonctionnalité de collaboration pour le partage des dossiers et des fichiers a été la clé. Keeper a été accepté plus facilement parce que la collaboration est beaucoup plus facile par rapport à tout ce qu'ils ont utilisé avant. »**
>
> **Ingomar Schmickl | Responsable informatique Institut de recherche sur le cancer des enfants St. Anna**

IMPACT SUR L'ORGANISATION

L'implémentation de Keeper à St. Anna CCRI a marqué un véritable changement dans l'approche de l'organisation en matière de sécurité des données et d'efficacité opérationnelle. La migration de l'ancien système de gestion des mots de passe vers Keeper n'a pas seulement amélioré leur posture de sécurité, mais a également eu un impact profond sur le flux de travail global et la productivité au sein de l'organisation.

Implémentation - St. Anna CCRI avait prévu une période de trois mois pour la migration de leurs archives et de leurs identifiants de leur ancien système vers Keeper. Cependant, grâce aux outils d'importation automatisés de Keeper, ce processus a été considérablement accéléré et terminé des mois avant le délai prévu, avec une perturbation des opérations quotidiennes très réduite. Cette efficacité témoigne de la conception conviviale de Keeper et de ses capacités d'intégration transparentes. En effet, Keeper s'intègre au fournisseur d'identité (IdP) existant de St. Anna CCRI, ce qui simplifie davantage les fonctionnalités administratives et la gestion des utilisateurs, tout en renforçant la sécurité.

Adoption par les utilisateurs - St. Anna CCRI exploite la fonctionnalité de dossiers partagés de Keeper – une fonctionnalité qui permet aux utilisateurs de gérer l'accès aux systèmes sensibles, tels que les bases de données de recherche, de manière efficace et sécurisée. La fonctionnalité One-Time Share de Keeper permet le partage sécurisé de fichiers et d'identifiants dans une capacité limitée dans le temps et verrouillée sur l'appareil. En utilisant les dossiers partagés et la fonctionnalité One-Time Share, les équipes de St. Anna CCRI peuvent aisément collaborer et partager les identifiants nécessaires sans nuire à la sécurité, ce qui permet de protéger leurs recherches.

Sécurité et visibilité - Pour s'assurer que leurs employés ne stockent ou ne partagent plus leurs identifiants par des méthodes obsolètes, St. Anna CCRI a utilisé la console d'administration de Keeper pour obtenir une visibilité et un contrôle sur l'utilisation des mots de passe par les employés. Cette fonctionnalité permet aux administrateurs de comprendre rapidement et facilement l'état de sécurité des mots de passe et des identifiants de leur organisation. En utilisant Keeper pour la gestion des mots de passe, le stockage des mots de passe et le partage des dossiers sont maintenant harmonisés dans tout l'institut.

L'adoption de Keeper par toute l'organisation a positionné St. Anna CCRI à la pointe de la sécurité des données. La migration réussie vers Keeper, ainsi que les niveaux de sécurité supplémentaires, servent de modèle pour d'autres organisations confrontées à des défis similaires dans la sécurisation de leurs données sensibles et le respect des protocoles de sécurité.

GESTIONNAIRE DE MOTS DE PASSE KEEPER

La plupart des entreprises n'ont qu'une visibilité limitée sur les pratiques de leurs employés en matière de mots de passe, ce qui accroît 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 maître 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 l'approvisionnement et l'intégration. Keeper SSO Connect® s'intègre à toutes les solutions SSO existantes à l'aide de SAML 2.0.

Keeper est conçu pour s'adapter à toutes les tailles d'organisations. 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 : Gestionnaire de mots de passe Keeper

- Prévenir les violations de données liées aux mots de passe et les cyberattaques
- 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 DU KEEPER

Keeper Security est l'une des entreprises de logiciels de cybersécurité à la croissance la plus rapide, protégeant plus de 100 000 organisations et des millions de personnes dans plus de 150 pays. Keeper est pionnier de la sécurité zero knowledge et zero trust, conçu pour tout environnement informatique. Son offre principale, KeeperPAM®, est une plateforme conçue sur le cloud et basée sur l'IA qui protège tous les utilisateurs, appareils et infrastructures contre les cyberattaques. Reconnu pour son innovation dans le Magic Quadrant de Gartner pour la gestion des accès privilégiés (PAM), Keeper sécurise les mots de passe et les clés d'accès, l'infrastructure de secrets, les connexions à distance et les terminaux avec des politiques d'application basées sur le rôle, le moindre privilège et l'accès juste-à-temps. Découvrez pourquoi des organisations de premier plan font confiance à Keeper pour se défendre contre les adversaires modernes en visitant le site **KeeperSecurity.com**.

Keeper est une solution de confiance, appréciée par des milliers d'entreprises et des millions d'utilisateurs dans le monde.

G2
Leader d'entreprise

PCMag
Choix de le rédaction

App Store
Productivité la mieux notée

Google Play
Plus de 10 millions d'installations