KEEPER® | Communiqé de presse

Keeper Security révolutionne le partage sécurisé avec un accès éphémère et une autodestruction des données pour les justificatifs d'identité.

Les nouvelles fonctionnalités sophistiquées d'accès et de partage de Keeper aident à se protéger contre les violations et à garantir la conformité.

CHICAGO, le 9 avril 2024 - Keeper Security, le principal fournisseur de logiciels de cybersécurité Zero Trust et Zero Knowledge protégeant les mots de passe, les passkeys, les accès privilégiés et les connexions à distance, présente deux nouvelles fonctionnalités majeures d'accès privilégié désormais disponibles dans la plateforme Keeper : l'accès limité dans le temps et les archives autodestructrices. Conçues pour l'accès et le partage d'archives chiffrées, ces fonctionnalités offrent de nouvelles méthodes pour élever rapidement et en toute sécurité l'accès et révoquer les droits d'accès une fois qu'ils ont été accordés - réduisant considérablement l'accumulation progressive de privilèges inutiles et réduisant la surface d'attaque potentielle pour les organisations.

Le contexte actuel des entreprises, qui évolue à vitesse fulgurante, exige des solutions toujours plus sécurisées, car les organisations sont soumises à une pression croissante pour protéger les données et les systèmes sensibles. Une gestion efficace des accès privilégiés est cruciale pour la conformité aux réglementations telles que SOX, PCI DSS et HIPAA, afin de garantir la sécurité, la responsabilité et l'intégrité des données sensibles conformément aux exigences spécifiques de leur secteur. L'accès éphémère et les archives autodétruites garantissent que les utilisateurs ont l'accès nécessaire aux informations d'identification et aux fichiers lorsqu'ils en ont besoin, mais que les autorisations sont automatiquement révoquées ou ajustées une fois que le délai ou le projet est terminé. Le contrôle précis des autorisations et de la gestion des accès facilite le respect des exigences de conformité.

« La mise en œuvre de l'accès limité dans le temps et des archives autodestructrices constitue une avancée significative dans le partage sécurisé des informations d'identification et dans la gestion des risques posés par l'escalade des privilèges », a déclaré Craig Lurey, CTO et cofondateur de Keeper Security. « Ces fonctionnalités permettent aux individus et aux organisations de partager des informations en toute sécurité, offrant ainsi un niveau de contrôle plus élevé sur l'accès aux données ».

Avec l'accès limité dans le temps, les utilisateurs peuvent partager en toute sécurité des archives pendant une durée prédéterminée. Il peut s'agir de n'importe quel archive dans le coffre-fort d'un utilisateur, y compris des informations d'identification, des fichiers ou des informations de paiement. À l'issue de cette période, l'accès est automatiquement révoqué, sans qu'aucune des parties n'ait à intervenir. Associé à Keeper Secrets Manager (KSM), les utilisateurs peuvent programmer la rotation automatique d'un identifiant partagé à l'expiration de l'accès, ce qui réduit le risque d'accès non autorisé et minimise l'abus de privilèges. Cette fonctionnalité est très utile lorsque l'on travaille avec des sous-traitants ou des tiers.

Les archives autodestructrices s'appuient sur ce principe avec des archives qui s'effacent automatiquement après que le destinataire a ouvert l'archive partagé. La destruction a lieu après une période déterminée ou lorsque le destinataire a consulté le document pendant cinq minutes, selon ce qui se produit en premier. Un scénario typique est celui de l'intégration d'un employé, lorsque le service informatique doit partager les identifiants de connexion avec un nouveau membre du personnel. Le service informatique peut partager l'archive contenant ces identifiants et, dès réception, l'archive original s'autodétruira, éliminant ainsi le risque associé au fait qu'un trop grand nombre de personnes aient accès aux informations de connexion de l'employé. Cela permet non seulement de renforcer la sécurité en réduisant la fenêtre d'exposition, mais aussi de maintenir un environnement de données propre et organisé, ce qui facilite l'identification et la gestion des informations pertinentes.

À une époque où les cybermenaces sont en constante évolution, Keeper s'engage à demeurer à l'avant-garde des progrès technologiques afin d'assurer le plus haut niveau de protection à ses utilisateurs. L'ajout du partage chiffré des dossiers à la plateforme Keeper fournit une défense solide contre de nombreuses menaces potentielles dans les environnements en ligne et hors ligne. En limitant les privilèges d'accès, les organisations peuvent réduire de manière significative leur surface d'attaque et minimiser l'impact potentiel des incidents de sécurité. Pour en savoir plus sur l'accès limité dans le temps et les archives autodestructrices, cliquez ici.

###

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 TikTok

Contact Presse :