Communiqé de presse

Keeper Security lance l'isolation de la navigation à distance Zero Knowledge dans le gestionnaire de connexion de Keeper

La sécurité de la navigation sur le Web passe au niveau supérieur sans la complexité et la latence des VPN traditionnels.

PARIS, le 26 juin 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 aujourd'hui Remote Browser Isolation, un nouveau module de Keeper Connection Manager. Remote Browser Isolation permet aux utilisateurs d'accéder en toute sécurité à des ressources web telles que des applications web internes et des applications cloud - en utilisant n'importe quel navigateur web standard.

Keeper Connection Manager offre aux équipes DevOps et IT un accès instantané à RDP, SSH, aux bases de données, aux web apps et aux endpoints Kubernetes via un navigateur web sécurisé. Construit par l'équipe qui a créé Apache Guacamole, Keeper est déployé en tant que conteneur dans n'importe quel environnement pour un accès transparent et sécurisé sans avoir besoin d'un VPN.

Avec sa dernière mise à jour, Keeper Connection Manager supporte maintenant le lancement de sessions web directement dans l'interface du gestionnaire de connexion grâce à l'utilisation de la technologie Remote Browser Isolation. Comme pour tout autre type de connexion de Keeper Connection Manager, ces sessions peuvent être partagées en temps réel, enregistrées et auditées.

Le protocole de Keeper Remote Browser Isolation, permet d'injecter automatiquement et en toute sécurité des informations d'identification, de soumettre des formulaires et de contrôler l'application web cible sans jamais envoyer les informations d'identification à l'appareil de l'utilisateur. Keeper est compatible avec tous les navigateurs web de bureau et mobiles, y compris Chrome, Edge, Safari, Opera, Firefox et Brave.

« Généralement, les organisations doivent utiliser des VPN ou des produits Zero Trust Network Access (ZTNA) basés sur le cloud pour fournir un accès aux applications web internes ou aux apps basées sur le cloud », a déclaré Craig Lurey, CTO et cofondateur de Keeper Security. « Avec cette dernière fonctionnalité, les organisations peuvent désormais déployer un simple conteneur Keeper Connection Manager dans n'importe quel environnement sur site ou dans le cloud et fournir à leurs utilisateurs et contractants un accès distant sécurisé aux ressources web. L'expérience utilisateur est si transparente que les utilisateurs ne se rendent même pas compte qu'ils sont dans un navigateur virtuel. »

Puisque Keeper Connection Manager est déployé comme un conteneur dans n'importe quel environnement, l'utilisateur a un contrôle total sur le trafic réseau et sur l'environnement d'exécution de l'isolation du navigateur distant. L'ensemble du processus est Zero Knowledge, et ne transige jamais sur un réseau tiers.

En plus de sécuriser l'accès aux applications web, la fonction d'isolation à distance du navigateur de Keeper fournit également une couche supplémentaire de protection contre les cyber-menaces associées aux sites web malveillants. Le site web ne s'exécute jamais localement sur l'appareil de l'utilisateur, ce qui le met à l'abri de nombreux vecteurs d'attaque, telles que les vulnérabilités de scripts intersites répercutées, les falsifications de requêtes intersites et les abus d'API.

Les administrateurs peuvent contrôler les applications web auxquelles il est possible d'accéder par le biais du gestionnaire de connexion, avec la possibilité d'autoriser ou de refuser des sites web et des domaines spécifiques. Keeper integrates with OIDC and SAML 2.0 to securely authenticate users and control access to the target web session, even if the application doesn't support SSO. Plusieurs méthodes d'authentification multi-facteurs (MFA) sont disponibles, et pour les utilisateurs gouvernementaux, CAC/PIV peut être utilisé pour l'authentification.

L'isolation du navigateur à distance est la dernière amélioration de KeeperPAM, la solution PAM facile à utiliser et évolutive de Keeper qui transforme la façon dont les organisations de toutes tailles peuvent se protéger contre les cyberattaques dans un monde de main-d'œuvre distribuée et d'informatique multi-cloud. Le gestionnaire de mots de passe et d'accès privilégiés de Keeper Security Government Cloud est autorisé par FedRAMP et StateRAMP, et maintient le cadre de sécurité Zero Trust de Keeper Security aux côtés d'une architecture de sécurité Zero Knowledge, de sorte que les utilisateurs ont une connaissance, une gestion et un contrôle complets de leurs informations d'identification et de leurs clés de chiffrement.

Découvrez comment la solution d'isolation du navigateur à distance de Keeper est prête à révolutionner la façon dont les entreprises protègent les données sensibles tout en assurant une productivité ininterrompue.

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 Zéro Trust et Zéro 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.

Contact Presse :
Christelle Klein :
06 63 97 01 67
cklein@hl-com.com