Fiche technique

Keeper Secrets Manager (KSM)

Protégez-vous contre les attaques de la chaîne d'approvisionnement grâce à une plateforme moderne cloud-based pour sécuriser les secrets de l'infrastructure tels que les clés API, les mots de passe de bases de données, les clés d'accès et les certificats.

Défis

Les secrets DevOps volés ou faibles sont l'une des principales causes des attaques contre la chaîne d'approvisionnement. Les secrets sont disséminés dans le code source, les fichiers de configuration et les systèmes CI/CD, ce qui expose les organisations aux pirates. Cette surface d'attaque élargie crée plusieurs défis pour les professionnels du DevOps, de la sécurité et de l'informatique :

1. Les équipes de développement privilégient souvent la productivité au détriment de la sécurité et les employés bien intentionnés finissent par coder en dur les identifiants dans l'environnement.
2. Les équipes de travail distribuées et à distance collaborent entre les régions, les systèmes et les environnements, ce qui entraîne un stockage hétérogène des secrets.
3. En l'absence de contrôles d'accès gérés de manière centralisée, les employés risquent d'obtenir des privilèges excessifs.
4. Pour de nombreuses organisations, les politiques internes et de conformité imposent une rotation régulière des identifiants, ce qui n'est possible qu'avec un système de coffre-fort complet.

Les entreprises ont besoin d'un moyen sécurisé, facile à utiliser et rentable pour maîtriser la prolifération des secrets et mettre en œuvre l'accès au moindre privilège. En coordonnant les accès, en appliquant une rotation automatisée des identifiants et en garantissant un chiffrement de bout en bout, les équipes DevOps, informatiques et de sécurité peuvent réduire considérablement le risque d'une violation dévastatrice.

Solution

Keeper Secrets Manager fournit à vos équipes DevOps, informatiques, sécurité et de développement logiciel une plateforme de sécurité Zero-Trust, Zero-Knowledge et cloud-based, pour gérer les secrets d'infrastructure et protéger les données les plus sensibles de votre organisation.

Keeper Secrets Manager centralise vos secrets pour éliminer la prolifération, empêcher les accès non autorisés et fournir un audit et une journalisation. Les capacités étendues du kit de développement logiciel (SDK) et de l'interface de programmation d'application (API) permettent d'injecter des identifiants juste à temps dans n'importe quel langage de programmation, ce qui couvre l'accès des machine aux secrets, en plus de l'accès humain.

À propos de Keeper Security

Keeper Security transforme la cybersécurité pour les personnes et les organisations du monde entier.

Les solutions de cybersécurité de Keeper, abordables et faciles à utiliser, reposent sur une base de sécurité Zero-Trust et Zero-Knowledge pour protéger chaque utilisateur sur chaque appareil. Des millions de personnes et des milliers d'organisations font confiance à Keeper pour la gestion de leur mot de passe, des clés d'accès et des secrets de pointe, la gestion des accès à privilèges (PAM), l'accès à distance sécurisé et la messagerie chiffrée. Notre plateforme de cybersécurité de nouvelle génération se déploie en quelques minutes et s'intègre de manière transparente à n'importe quelle pile technologique pour prévenir les violations, réduire les coûts du service d'assistance et garantir la conformité.

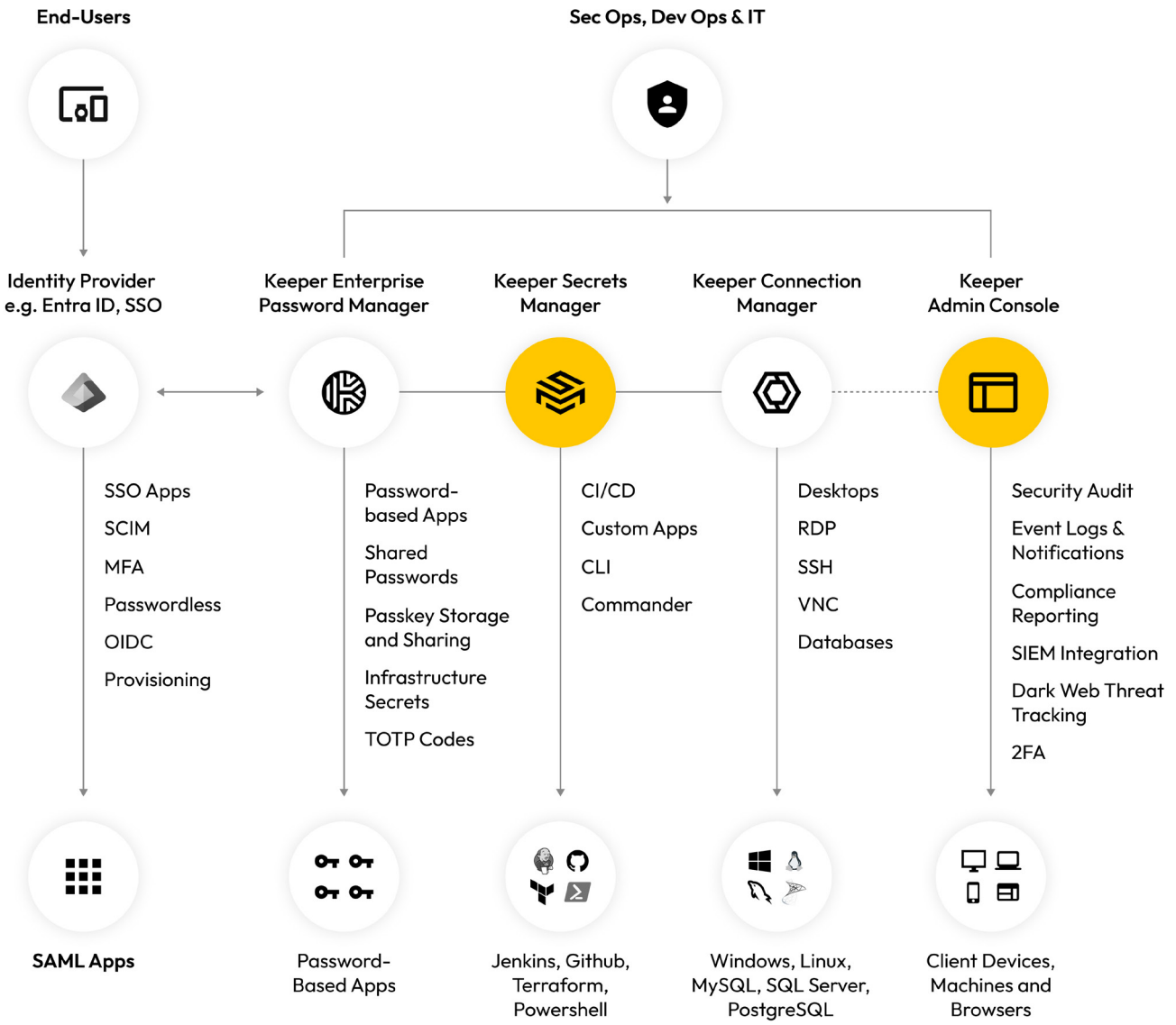
Keeper Security est soutenu par des sociétés de capital-investissement de premier plan, Insight Partners et Summit Partners.

Keeper Security
Ne vous faites pas hacked.

En savoir plus
keepersecurity.com

Commencez un essai gratuit dès aujourd'hui
keepersecurity.com/start-business-trial.html

Plateforme de gestion des accès à privilèges Keeper



Valeur de l'entreprise

Sécurisez vos systèmes et vos données à privilèges élevés
Consolidez vos secrets dans une plateforme unifiée et éliminez la prolifération des secrets en supprimant les identifiants hard-coded dans le code source, les fichiers de configuration et les systèmes CI/CD.

Intégration flexible et rapide
Intégration prête à l'emploi avec toutes les plateformes CI/CD courantes telles que Github Actions, Jenkins et Ansible.

Facile à déployer et facile à utiliser
Plateforme entièrement cloud-based, Zero-Trust et Zero-Knowledge, qui ne nécessite aucune configuration complexe de réseau, de stockage ou d'HA.

Capacités clés

- Effectuez une rotation automatique des identifiants pour les comptes de service et d'administration, les identités des utilisateurs, les comptes API basés sur REST, les machines et les comptes d'utilisateurs dans votre infrastructure et vos environnements multi-cloud.
- Gérez les droits d'accès et les autorisations avec des contrôles d'accès basés sur les rôles.
- Les appareils clients déchiffrent localement les secrets du coffre-fort après leur récupération. Keeper n'a pas la capacité de déchiffrer les données stockées dans le coffre-fort.
- Keeper Secrets Manager est un service entièrement géré avec une capacité d'évolution illimitée.