Fiche technique

KEEPER SECRETS MANAGER

Protégez-vous contre les cyberattaques en sécurisant les secrets de l'infrastructure tels que les clés API, les mots de passe des 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 config et les systèmes CI/CD, exposant les organisations aux pirates. Cette surface d'attaque élargie crée plusieurs défis pour les professionnels du DevOps, de la sécurité et de l'informatique :

01

La productivité est privilégiée par rapport à la sécurité et les employés bien intentionnés finissent par coder en dur les identifiants dans l'environnement.

02

La main-d'œuvre moderne et distribuée collabore entre les régions, les systèmes et les environnements, ce qui entraîne un risque potentiel plus élevé en l'absence de contrôles adéquats.

03

En l'absence de contrôles d'accès gérés de manière centralisée, les employés risquent d'obtenir des privilèges excessifs, ce qui ouvre la voie à des vecteurs de menace et réduit la conformité.

04

Souvent, les politiques internes et de conformité imposent une rotation régulière des identifiants, ce qui n'est possible qu'avec un coffre-fort complet.

Les entreprises ont besoin d'un moyen sûr, facile à utiliser et rentable de stocker des secrets et d'appliquer l'accès selon le principe de moindre privilège. En coordonnant l'accès, en appliquant une rotation automatisée des identifiants et en garantissant un chiffrement de bout en bout, les équipes peuvent réduire considérablement le risque d'une violation dévastatrice.

Solution

Keeper Secrets Manager permet à vos équipes d'intégrer des pipelines CI/CD, des outils DevOps, des logiciels personnalisés et des environnements multi-cloud dans une plateforme entièrement gérée, Zero-Knowledge et Zero-Trust, afin de sécuriser les secrets de l'infrastructure et de réduire la prolifération des secrets.

Keeper Secrets Manager centralise les 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, couvrant ainsi l'accès des machines et des humains aux secrets.

Protégez-vous contre le piratage informatique.

En savoir plus
keepersecurity.com

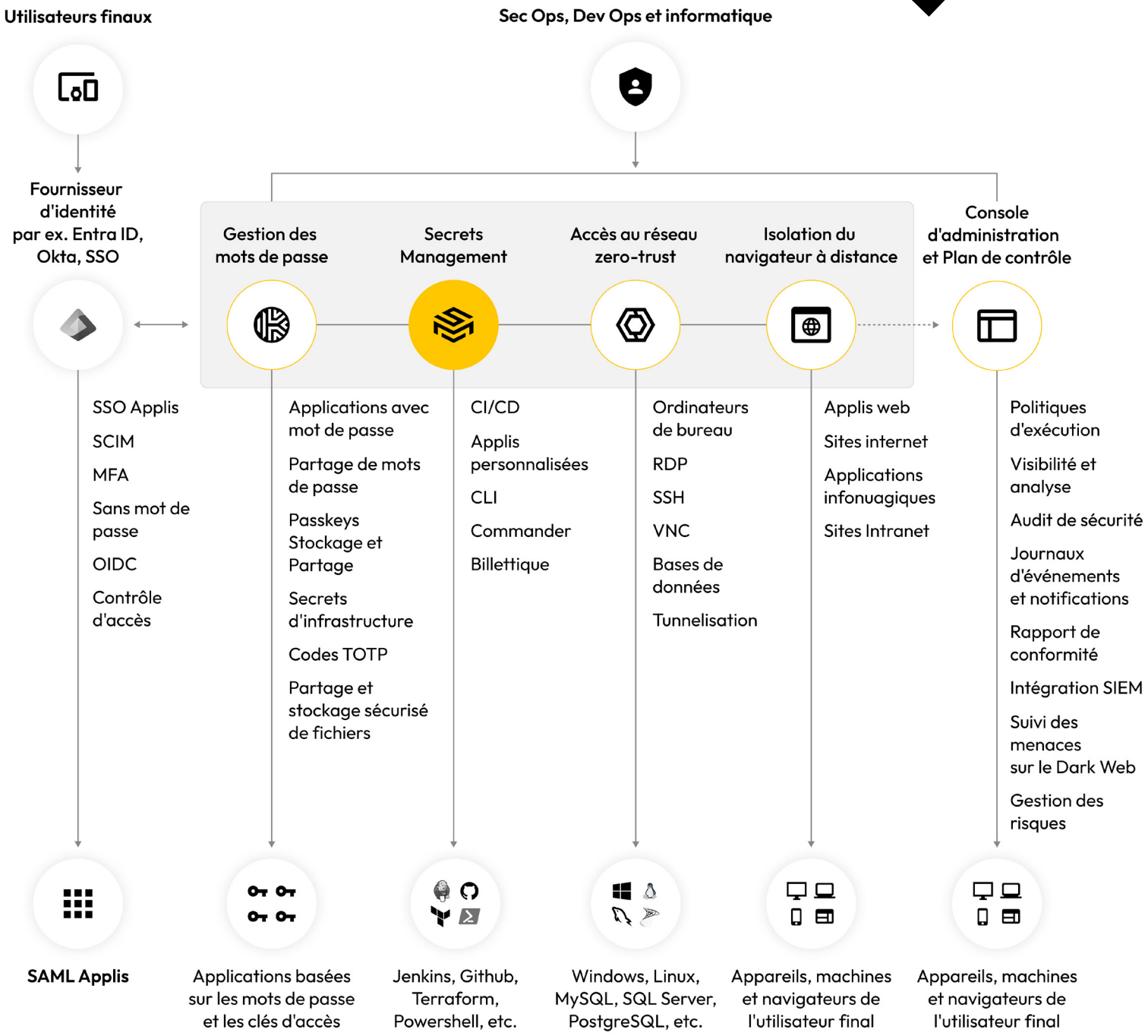
Demander une démo
keeper.io/ksm

À propos de nous

Keeper Security transforme la cybersécurité pour les organisations dans le 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. 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.

KEEPER SECRETS MANAGER

Plateforme de gestion des accès à privilèges de 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.