Fiche technique

Gestionnaire de mots de passe d'entreprise (EPM)

Empêchez les failles, réduisez les coûts de service d'assistance et garantissez la conformité.

Défis

Les mots de passe, les identifiants et les secrets DevOps faibles et volés sont l'une des principales causes des violations de données. La plupart des organisations manquent de visibilité sur ces menaces et n'ont aucun moyen d'appliquer les meilleures pratiques de sécurité à chaque employé, dans chaque lieu, sur chaque appareil, application et système. Cela crée une série de défis pour les administrateurs informatiques :

1. Une organisation se compose d'identifiants des personnes et de machines qui doivent être protégés.
2. Le télétravail distribué et l'informatique multi-cloud ont rendu obsolètes les périmètres informatiques traditionnels.
3. Les surfaces d'attaque s'étendent de manière exponentielle à mesure que des milliards d'appareils, d'identifiants et de secrets supplémentaires sont connectés à des réseaux distribués, à la fois sur site et hors site.
4. Les solutions conventionnelles de cybersécurité sont hétérogènes et cloisonnées par nature, ce qui crée des lacunes critiques en matière de visibilité, de sécurité, de contrôle, de conformité et de rapports.

Les organisations qui ne s'attaquent pas à ces défis fondamentaux s'exposent à un risque accru de violations de données, de non-respect de la conformité et de problèmes opérationnels.

Solution

Le gestionnaire de mots de passe Keeper Enterprise surveille et protège chaque utilisateur sur chaque appareil au sein d'une organisation avec des capacités de cloud et d'applications natives. Keeper EPM s'intègre de manière transparente avec les technologies informatiques existantes, y compris la gestion des informations et des événements de sécurité (SIEM), l'authentification multifacteur (MFA), les solutions sans mot de passe et les fournisseurs d'identité (IdP).

Keeper EPM fournit une authentification et un chiffrement complets sur chaque site Web, application et système avec lesquels les employés interagissent. Keeper EPM est facile à déployer, facile à adopter pour des utilisateurs non techniques et constitue le produit le plus sûr de sa catégorie. Keeper détient la conformité SOC 2 Type I et II la plus ancienne du secteur, la certification ISO 27001 et est autorisé par FedRAMP et StateRAMP.

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.

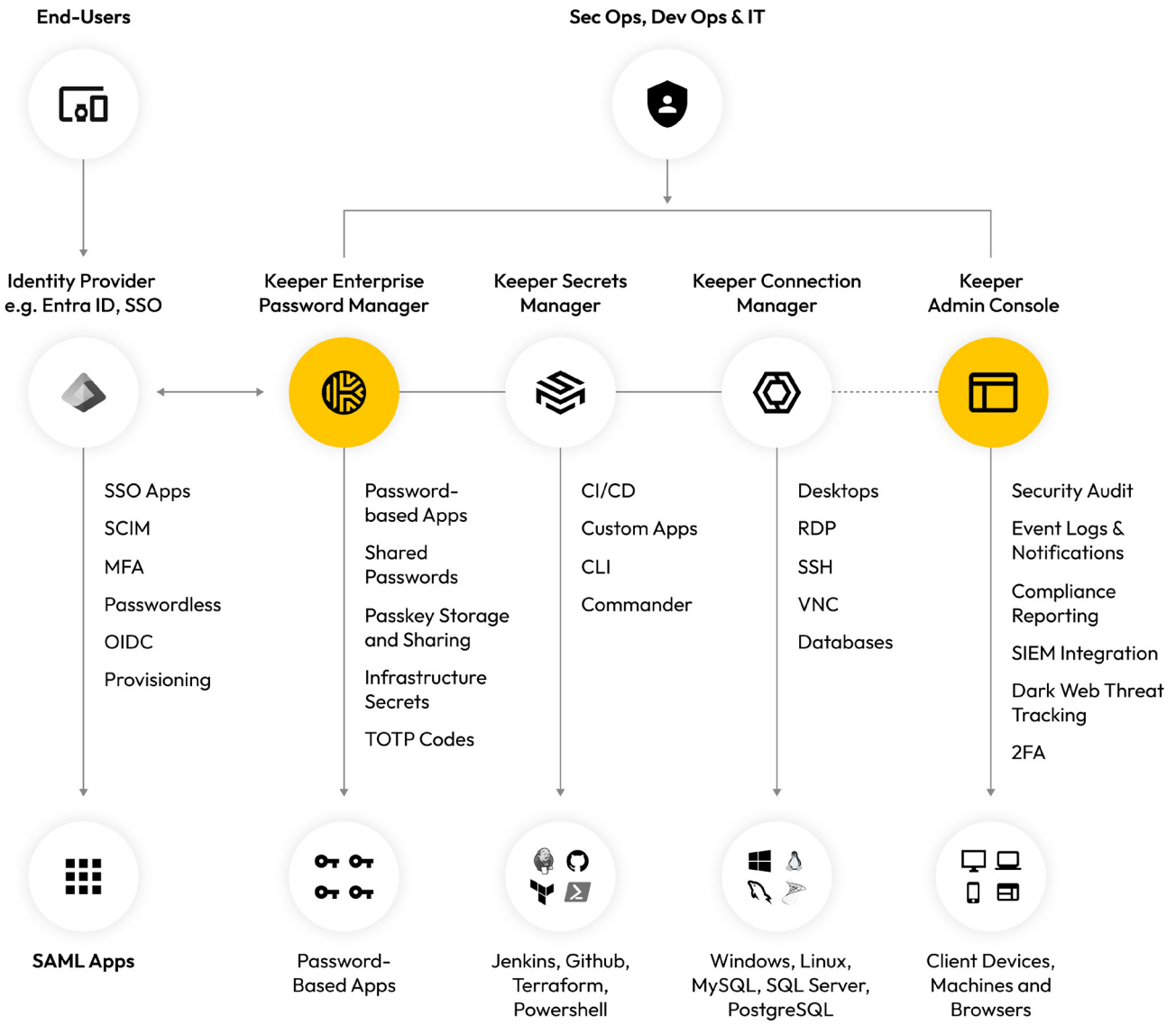
Keeper Security est soutenu par des sociétés de capital-investissement de premier plan, Insight Partners et Summit Partners.

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

- Prévenez les cyberattaques liées aux ransomwares et aux identifiants.
- Protégez chaque utilisateur sur chaque appareil depuis chaque emplacement.
- Bénéficiez d'une visibilité complète, appliquez les meilleures pratiques et contrôles de sécurité et rationalisez les audits de conformité.
- Améliorez et étendez le déploiement de votre système d'authentification unique (SSO) existant.
- Améliorez la productivité de vos employés et réduisez le nombre de tickets liés aux mots de passe pour votre service d'assistance et vos équipes informatiques.

Capacités clés

- Coffres-forts chiffrés de l'utilisateur final
- Stockage, gestion et partage des mots de passe et des clés d'accès
- Extension de navigateur KeeperFill® alimentée par KeeperAI™
- Applications Web, de bureau et mobiles
- Surveillance du Dark Web avec BreachWatch
- Console d'administration intuitive
- Approvisionnement et intégrations fluides
- Contrôles d'accès basés sur les rôles (RBAC)