Fiche technique

Keeper Connection Manager (KCM)

Fournit un accès à distance sans agent, sans client et sécurisé aux points de terminaison RDP, SSH, base de données et Kubernetes via un navigateur Web.

Défis

Les organisations de toutes tailles doivent fournir un accès sécurisé et fiable à l'infrastructure informatique, aux bases de données et aux sites Web en back-end. Cependant, les solutions d'accès à distance existantes se traduisent souvent par une évolutivité limitée, des frais administratifs élevés, la frustration de l'utilisateur final et de graves lacunes en matière de sécurité.

1. Les réseaux privés virtuels (VPN) fournissent généralement trop d'accès, en particulier pour les sous-traitants, les fournisseurs et les employés occasionnels.
2. Les VPN ne protègent pas contre le suivi des cookies, les virus ou autres logiciels malveillants.
3. Les VPN sont coûteux et notoirement difficiles à configurer et à entretenir pour le personnel informatique, ainsi qu'à utiliser pour les utilisateurs finaux.
4. Certaines solutions reposent sur des combinaisons d'agents, de clients et de serveurs bastion distribués, ce qui accroît la complexité du système et nuit à l'adoption par les utilisateurs.

Les employés doivent pouvoir établir des connexions à distance sécurisées, fiables et faciles à utiliser, où qu'ils se trouvent, afin de minimiser le risque d'accès non autorisé à des ressources sensibles.

Solution

Keeper Connection Manager (KCM) résout le dilemme de la complexité et de la sécurité avec une solution moderne, sans agent, qui offre la sécurité, la facilité d'utilisation et la rapidité requises dans les environnements de télétravail distant d'aujourd'hui.

Keeper Connection Manager est conçu pour fonctionner selon le principe du moindre privilège. Les droits d'accès sont délégués par le biais d'utilisateurs et de groupes, qui sont automatiquement créés par les paquets de Keeper Connection Manager, et par le biais de permissions strictes sur les fichiers.

Tout le trafic passe par une passerelle sécurisée et authentifiée. Les ordinateurs de bureau ne sont jamais exposés à l'Internet public. Conformément aux principes Zero-Trust, seules les connexions autorisées et authentifiées sont permises.

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.

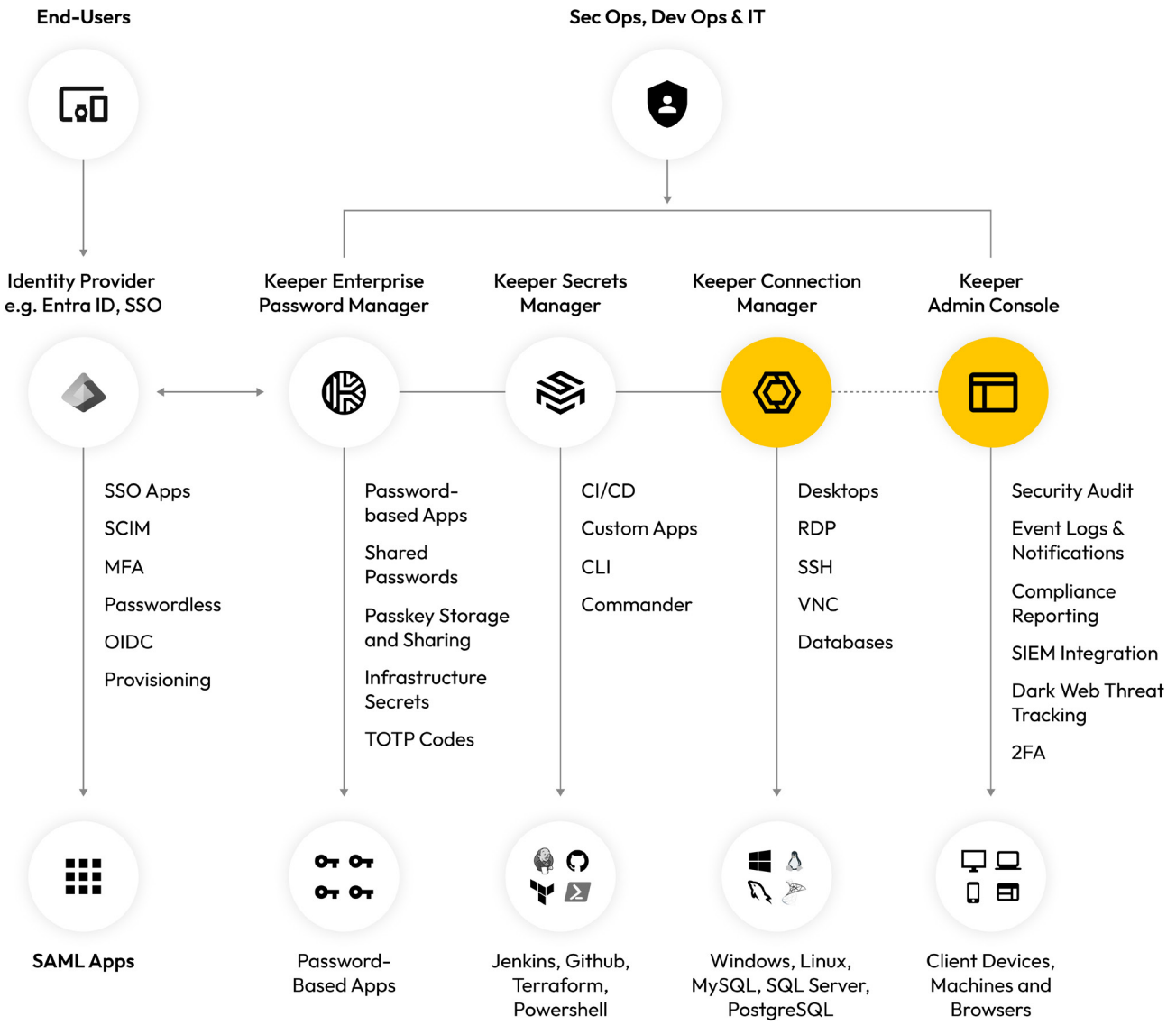
Keeper Security est soutenu par des sociétés de capital-investissement de premier plan, Insight Partners et Summit Partners.

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

Isolation du navigateur à distance
Atténuez les menaces de cybersécurité en hébergeant des sessions de navigation dans un environnement distant et contrôlé.

Accès à la base de données à distance
Protégez les données propriétaires et les PII grâce à un accès sécurisé à la base de données à distance.

Accès sécurisé à l'infrastructure à distance
Établissez des connexions à distance sécurisées de n'importe où sans exposer les identifiants.

Gestion des sessions des comptes à privilèges
Répondez aux exigences de conformité grâce à des sessions auditées et enregistrées.

Capacités clés

- Accès basé sur le Web avec chiffrement de bout en bout
- Authentification multifacteur
- Accès sans agent (aucun VPN requis)
- Plusieurs magasins de données
- Sécurité Zero-Knowledge
- Cadre Zero-Trust
- Moteur de politique du contrôle d'accès basé sur les rôles (RBAC)
- Surveillance des événements et enregistrement de session
- Authentification sans mot de passe
- Prise en charge multi-protocoles
- Intégration avec Keeper Secrets Manager