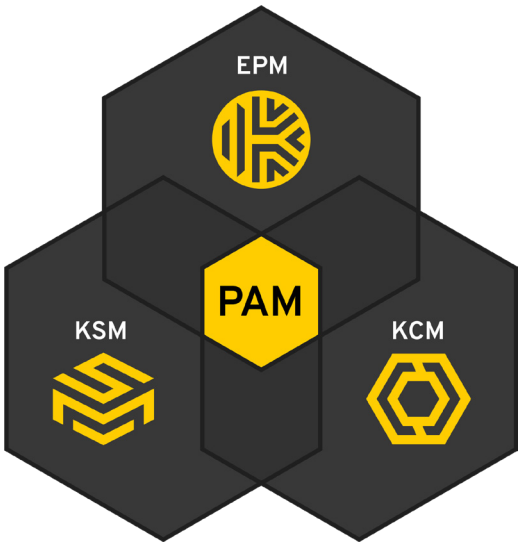
KEEPER

Fiche technique : Gestion des accès privilégiés Keeper

La solution de gestion des accès privilégiés (PAM) de nouvelle génération, Zero-Trust et Zero-Knowledge.

KeeperPAM™ a été créé pour protéger complètement les environnements sans périmètre et multi-cloud avec seulement les fonctionnalités dont vous avez besoin.

Gestion simplifiée des privilèges pour chaque utilisateur sur chaque appareil de chaque lieu.



KeeperPAM

La plateforme PAM brevetée de Keeper permet aux organisations d'obtenir une visibilité, une sécurité, un contrôle et des rapports complets sur chaque utilisateur sur chaque appareil de toute organisation. La plateforme est Cloud-Based, permet la sécurité Zero-Trust et Zero-Knowledge et répond aux exigences de conformité en unifiant trois solutions intégrées en une seule.

82 % des violations impliquent l'élément humain, la majorité étant dues à des mots de passe, des identifiants et des secrets volés ou faibles.[1]

KEEPER PASSWORD MANAGER

Permet aux organisations de gérer, protéger, découvrir, partager et faire tourner les mots de passe en toute sécurité, avec un contrôle et une visibilité complets pour simplifier l'audit et la conformité.

KEEPER SECRETS MANAGER

Fournit une solution entièrement gérée et basée sur le Cloud pour sécuriser les secrets d'infrastructure tels que les clés API, les identifiants de la base de données, les clés d'accès et les certificats.

KEEPER CONNECTION MANAGER

Fournit une passerelle de PC de bureau à distance sans agent pour la gestion instantanée des sessions à privilèges, l'accès à l'infrastructure à distance et l'accès sécurisé aux bases de données à distance pour les points de terminaison RDP, les clés SSH, les bases de données et Kubernetes, sans VPN requis.

[1] Rapport d'enquête sur les violation de données 2022

Réduisez votre surface d'attaque pour protéger les employés et les appareils.

Keeper fournit les composants les plus critiques de la gestion des accès privilégiés (PAM) sans la complexité des solutions PAM traditionnelles.

- Gestion des comptes et des sessions à privilèges (PASM)
- Gestion des secrets
- Intégration de l'authentification unique (SSO)
- Gestion des mots de passe
- Gestion des identifiants des comptes à privilèges
- Protection des identifiants et contrôle des accès
- Gestion, suivi et enregistrement des sessions
- Sécurité Zero-Trust

Les produits PAM traditionnels sont laids, coûteux, difficiles à déployer, difficiles à utiliser et ne surveillent et ne protègent pas chaque utilisateur sur chaque appareil en tout lieu.

Réduction des coûts opérationnels. Comprend la gestion des mots de passe, des secrets et des connexions, le tout sur une seule plateforme, ainsi qu'un personnel informatique minimal requis.

Approvisionnement rapide. Se déploie en toute fluidité en quelques heures, et non quelques mois.

Facile à utiliser. Fournit une console d'administration unifiée et une interface utilisateur moderne pour chaque employé sur tous les types d'appareils. Le temps de formation total moyen est inférieur à 2 heures.

Visibilité omniprésente. Simplifie l'audit et la conformité avec le contrôle des accès en fonction des rôles (RBAC) à l'échelle de l'organisation, la journalisation des événements et la création de rapports.

Sécurité de classe mondiale. Utilise la meilleure sécurité de sa catégorie avec une infrastructure Zero-Trust et une architecture de sécurité Zero-Knowledge.

Plus de 50 intégrations. S'intègre à votre pile technologique et IAM existante pour obtenir une couverture et une visibilité à l'échelle de l'entreprise.

ISO 27001 | SOC 2 | FedRAMP | StateRAMP | HIPAA | GDPR

PCI DSS Level 1 | TRUSTe | Level 1 | FIPS-140-2 | EU-US Privacy Shield