KEEPER®
CONNECTION MANAGER

Fiche technique : accès à distance pour les équipes DevOps et informatiques

Accédez instantanément à votre infrastructure à distance avec une sécurité zero-trust

Keeper Connection Manager permet aux équipes DevOps et informatiques d'accéder facilement aux points de terminaison RDP, SSH et Kubernetes par le biais d'un navigateur web.

Accéder de façon à la fois simple et sécurisée à toute l'infrastructure interne a toujours été un défi. L'accès à un système suit souvent un principe de « on installe et on oublie ». Avec le temps, vous pouvez vous retrouver avec un nombre inconnu de personnes ayant accès à ces systèmes critiques.

Il est difficile d'effectuer des modifications ou de vérifier les autorisations. En cas de problème, il est souvent difficile de savoir après coup ce qui a été fait sur un système.

Certaines solutions tentent de pallier ce problème au moyen d'agents, de clients, de serveurs bastion distribués ou d'une combinaison de ces éléments. Ces approches augmentent la complexité des systèmes, affectent la sécurité et sont difficilement applicables à grande échelle.

Keeper Connection Manager résout le dilemme de la complexité et de la sécurité grâce à une solution moderne et sans agent offrant la sécurité, la simplicité d'utilisation et la rapidité indispensables aux environnements de travail distribués et à distance d'aujourd'hui.

Pourquoi choisir Keeper Connection Manager pour vos équipes informatiques et DevOps ?

- Intégration simple à Keeper Secrets Manager. Gestion des identifiants d'accès à des systèmes privilégiés dans le coffre-fort Keeper.
- Prise en charge de l'authentification sans mot de passe sur des serveurs à distance via toutes les solutions d'authentification connues avec ou sans solution IdP.
- Accès instantané à la session de console de vos systèmes privilégiés. Il n'est pas nécessaire d'accéder physiquement à un appareil, ce qui réduit les frais d'assistance.
- Pour atteindre et maintenir la conformité aux normes SOX, HIPAA, RGPD, FINRA et autres règlementations propres à ce secteur d'activité, les administrateurs peuvent enregistrer les sessions privilégiées et utiliser des journaux détaillés.
- Des fonctionnalités avancées et à la pointe permettent un accès multi-utilisateur, le partage de plusieurs sessions, les sessions ouvertes multiples ainsi le changement rapide de session.
- Il est possible de verrouiller complètement l'accès aux systèmes critiques, garantissant ainsi l'absence de point d'entrée inconnu ou non autorisé.
- Atténuez et réduisez les risques pour les fournisseurs et prestataires tiers grâce à un accès sécurisé, temporaire et surveillé aux appareils et machines autorisés.

KEEPER
CONNECTION MANAGER

Fiche technique

Accès à distance pour les équipes DevOps et informatiques

Une connexion rapide, simple et sécurisée à votre infrastructure à distance. Vous bénéficiez de la sécurité zero-trust et zero-knowledge et d'une assistance de qualité exceptionnelle.

En quoi Keeper Connection Manager est plus sûr que les solutions de bureau à distance traditionnelles ?

- Tout le trafic transite par une passerelle sécurisée et authentifiée. La session à distance n'est jamais exposée à l'Internet public.
- Conformément aux principes zero-trust, seules les connexions autorisées et authentifiées sont permises.
- Toutes les fonctions à distance sont exécutées derrière le pare-feu de l'entreprise. Les utilisateurs à distance bénéficient de la même protection que s'ils travaillaient dans un bureau sur le réseau de l'entreprise.
- Il est possible d'appliquer des certificats clients et l'authentification à plusieurs facteurs pour encore plus de sécurité.
- Keeper Connection Manager est conçu pour fonctionner selon le principe de moindre privilège. Les droits d'accès sont attribués avec discernement par le biais d'utilisateurs et de groupes créés automatiquement par les paquets de Keeper Connection Manager, et avec des permissions de fichiers strictes.
- Les utilisateurs finaux communiquent avec des postes de travail à distance via une session sécurisée depuis leur navigateur. C'est un moyen simple et efficace de chiffrer le trafic entre les utilisateurs finaux et la passerelle sans affecter les performances.
- Il est possible d'accorder l'accès à des systèmes privilégiés sans divulguer les identifiants de connexion à l'utilisateur final.
- Fonctionne avec les points de terminaison RDP, SSH, VNC, K8s et MySQL.

Cas d'utilisation	Keeper Connection Manager
Accès basé sur le web	✓
Validation multi-étapes	✓
Accès sans agent	✓
Banques de données multiples	✓
Sécurité à connaissance nulle	✓
Cadre zero-trust	✓
Enregistrement des sessions	✓
Authentification sans mot de passe	✓
Prise en charge multiprotocole	✓
Intégration à Keeper Secrets Manager	✓

À propos de Keeper Security, Inc.

Keeper Security, Inc. (Keeper) est la plateforme de cybersécurité leader du marché pour la prévention des cybermenaces et violations de données associées à des mots de passe. Des millions de particuliers et des milliers d'entreprises du monde entier font confiance au logiciel de chiffrement et de sécurité zero-trust et zero-knowledge de Keeper. Keeper a été nommé Meilleur gestionnaire de mots de passe de l'année et Choix de l'équipe par PC Magazine, Choix de l'équipe par PCWorld et a remporté plusieurs récompenses de meilleur logiciel G2. Keeper est certifié SOC-2 et ISO 27001 et est homologué par le gouvernement fédéral des États-Unis via le système SAM (System for Award Management). Pour en savoir plus, consultez https://keepersecurity.com.