KEEPER®
CONNECTION MANAGER

Fiche technique : accès aux postes de travail et aux serveurs à distance

Accès sécurisé et facile aux postes de travail et machines à distance sans VPN

Accès sécurisé à vos systèmes de n'importe où, sur n'importe quel appareil, via n'importe quel navigateur web.

Pour que le télétravail soit une réussite à long terme, les entreprises ont besoin d'un moyen sûr, fiable et évolutif pour permettre aux employés d'accéder rapidement aux postes de travail et aux applications.

Les réseaux virtuels privés (VPN) constituent un choix répandu, mais ils présentent des lacunes dans plusieurs domaines. Ils sont coûteux et réputés pour être difficiles à configurer et à entretenir pour le personnel informatique, et à utiliser pour les utilisateurs finaux. Les VPN souffrent également de problèmes de latence, de fiabilité et de disponibilité.

Lorsqu'ils sont mis en place comme il se doit, les bureaux à distance constituent une alternative séduisante aux VPN.

- La charge administrative liée au déploiement, à la prise en charge et à l'entretien d'un poste de travail à distance standardisé est significativement inférieure à celle liée à la prise en charge d'appareils physiques distribués utilisés par les utilisateurs finaux.
- Tant que la solution de poste de travail à distance ne nécessite pas d'agent aux points de terminaison, les employés peuvent utiliser quasiment n'importe quelle machine pour leur accès, y compris leur ordinateur portable et leur smartphone personnels.
- Il y a rarement besoin d'accéder physiquement à l'appareil d'un utilisateur final, ce qui réduit les frais généraux d'assistance pour les ressources de la société.
- Les postes de travail à distance renforcent la sécurité des télétravailleurs en permettant d'adopter une architecture zero-trust, ce qui n'est pas possible avec la plupart des VPN.
- Les actions effectuées par les équipes en télétravail par le biais de postes de travail à distance sont exécutées derrière le pare-feu de l'entreprise. Ceci leur permet d'être protégées par les systèmes de sécurité de l'entreprise de la même façon que si elles travaillaient dans un bureau physique.
- Les postes de travail à distance incitent les utilisateurs à stocker les données sur le réseau de l'entreprise plutôt que sur des machines locales. La protection est plus solide à l'intérieur du pare-feu, les données pouvant être sauvegardées et sécurisées correctement. De plus, le risque que des données soient perdues est bien moindre et il est bien plus facile de les partager avec d'autres personnes.
- Les postes de travail à distance sont très évolutifs, surtout lorsqu'aucun agent n'est nécessaire aux points de terminaison. Les images peuvent être facilement standardisées et les mises à jour des postes de travail et des applications peuvent être automatisées, puisqu'il est inutile d'accéder aux différents appareils.

Témoignage d'un client de Keeper Connection Manager : secteur manufacturier

Keeper Connection Manager fournit bien plus que des postes de travail à distance aux personnes travaillant chez elles. Son évolutivité, sa sûreté et sa convivialité font que de nombreuses entreprises l'utilisent pour fournir des postes de travail à des services et des environnements de formation.

Un fabricant connu d'appareils grand public a mis en place des services de formation dans ses bureaux internationaux. La fourniture de l'accès direct aux postes de travail était difficile à maintenir et source de confusion pour les utilisateurs.

Keeper Connection Manager a simplifié les systèmes internes pour la mise à jour, la sécurisation et la fourniture d'accès à son équipe et lui permettre de se former sur des postes de travail à distance basés sur un service. La sécurité et la vitesse ont transformé l'environnement de formation de ce fabricant. Les stagiaires n'avaient besoin que d'un navigateur web, d'une URL et d'identifiants de connexion.

KEEPER CONNECTION MANAGER

Fiche technique

Accès à distance aux postes de travail et aux serveurs

Une expérience de bureau entièrement à distance, quelle que soit la localisation de vos utilisateurs. 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. Les postes de travail ne sont jamais exposés à l'Internet public. Conformément aux principes zero-trust, seules les connexions autorisées et authentifiées sont permises.
- Toutes les fonctionnalités de bureau 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.