



Mettez en œuvre des politiques d'accès selon le principe du moindre privilège, éliminez les droits d'administrateur permanents et activez l'accès juste-à-temps (JIT) pour les processus et les machines avec la gestion des privilégiés au niveau des terminaux sur Windows, Linux et macOS.

Des contrôles d'accès privilégiés robustes sont essentiels pour les organisations afin de renforcer leur posture de sécurité, assurer l'efficacité opérationnelle et respecter les exigences de conformité réglementaire.

Keeper Endpoint Privilege Manager sécurise les terminaux grâce à des agents légers qui suppriment les droits d'administrateur permanents tout en permettant une élévation temporaire des privilégiés basée sur des politiques, uniquement lorsque cela est nécessaire. Le système applique des politiques de sécurité personnalisables grâce à un accès juste-à-temps avec des flux de travail d'approbation optionnels et l'application de l'authentification multifactor (MFA).

Les actions privilégiées peuvent être exécutées soit via des comptes éphémères qui sont automatiquement provisionnés et déprovisionnés pour chaque session, soit en élevant temporairement les privilégiés sur les comptes utilisateur standard. Les entreprises peuvent choisir l'une ou l'autre méthode en fonction de leur posture de sécurité et de leurs besoins opérationnels.

Keeper Endpoint Privilege Manager fonctionne dans les environnements Windows, macOS et Linux. Il offre une visibilité grâce à un tableau de bord centralisé qui enregistre toutes les activités d'élévation à des fins d'audit et de conformité.

Avantages de Keeper Endpoint Privilege Manager

Sécurité

Élimine les droits d'administrateur permanents et autorise l'élévation juste-à-temps uniquement pour les applications approuvées afin de réduire les surfaces d'attaque et d'améliorer la sécurité.

Conformité

Fournit des pistes d'audit complètes sur l'utilisation des privilégiés et garantit le respect des exigences réglementaires grâce à un contrôle d'accès administratif documenté.

Efficacité opérationnelle

Réduit la charge de travail du service d'assistance en automatisant les approbations pour les tâches d'administration courantes.

Expérience utilisateur

Permet aux utilisateurs d'effectuer les tâches nécessaires sans délai d'intervention du service informatique grâce à l'élévation automatisée des privilégiés pour les applications approuvées.

Évolutivité

Permet aux entreprises d'appliquer efficacement des politiques d'accès à moindre privilège et de gérer les accès privilégiés sur des milliers de points de terminaison Windows, macOS et Linux à partir d'une plateforme centralisée.

Auditabilité et visibilité

Fournit des informations exploitables sur les activités d'élévation, les approbations et l'application des politiques au niveau des terminaux grâce à une journalisation détaillée et à l'intégration à des outils SIEM pour une réponse plus rapide aux incidents.

En savoir plus
keepersecurity.com

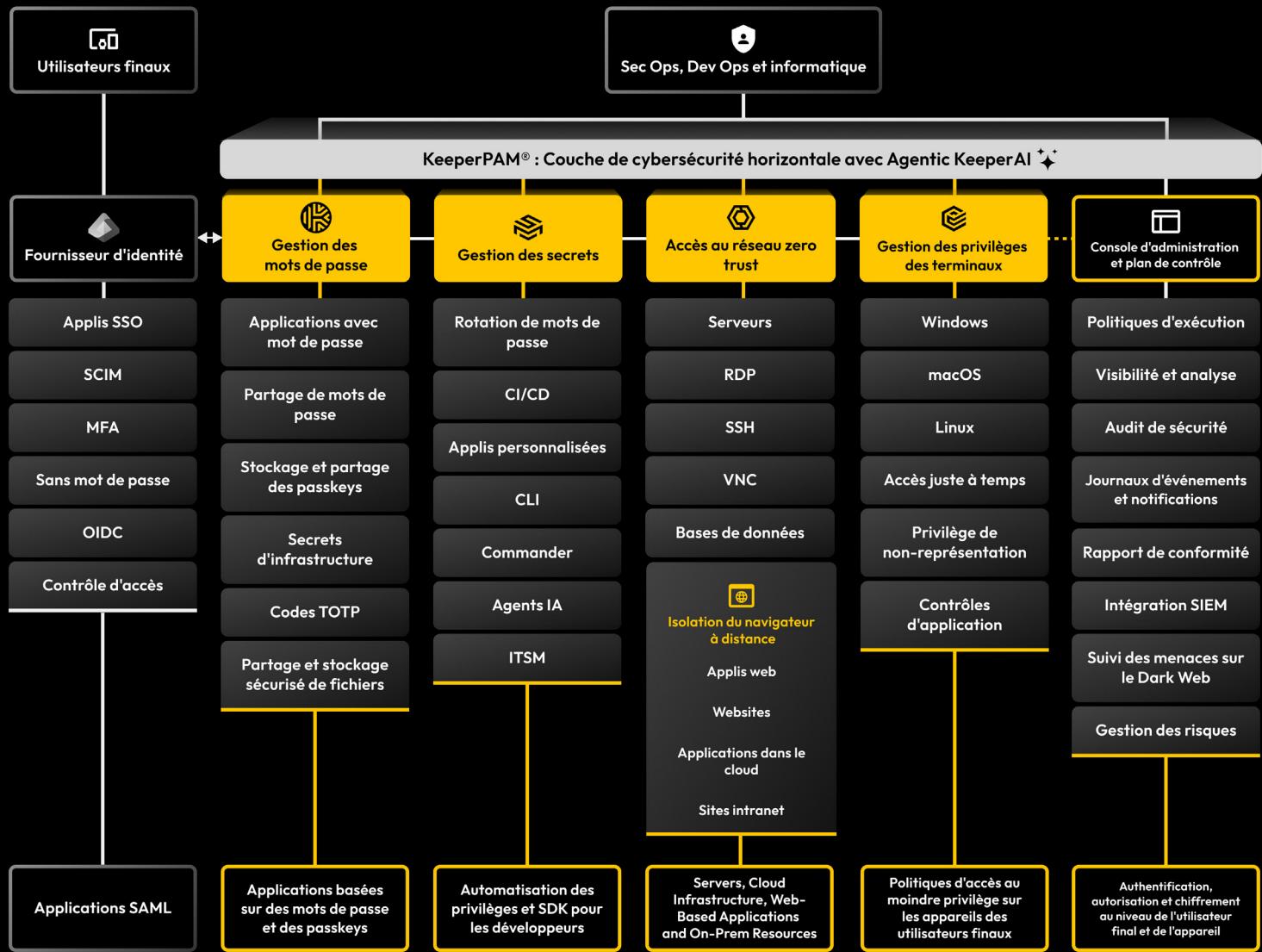
Demandez une démo
keeper.io/demo

Demandes de partenaires
partners@keepersecurity.com



À propos de Keeper Security

Keeper Security transforme la cybersécurité pour les particuliers et les entreprises du monde entier. Les solutions intuitives de Keeper sont conçues avec un chiffrement de bout en bout pour protéger chaque utilisateur sur chaque appareil, où qu'il se trouve. Bénéficiant de la confiance de millions d'individus et de milliers d'organisations, Keeper est le leader en matière de gestion des accès privilégiés.



Étendez le modèle zero-trust aux terminaux

Endpoint Privilege Manager étend l'approche zero-trust de KeeperPAM en contrôlant l'élévation des priviléges directement sur les terminaux, complétant ainsi les capacités de connexion sécurisée de la solution PAM dans son ensemble. Alors que le reste de la plateforme KeeperPAM sécurise la manière dont les utilisateurs se connectent aux systèmes, Endpoint Privilege Manager régit les droits administratifs qu'ils peuvent exercer une fois connectés.

Comment Keeper élève les priviléges

- Politique**: si une application ou un processus requiert une élévation, l'agent Keeper vérifie la politique correspondante.
- Approbation**: si une approbation est requise, la demande est acheminée vers un administrateur via la console d'administration ou l'interface de ligne de commande (CLI).
- Option MFA**: si aucune approbation n'est requise, l'élévation s'effectue automatiquement. L'application de la MFA est une étape supplémentaire facultative.