KEEPER PAM

Apportez à l'ensemble de votre entreprise visibilité, sécurité, contrôle d'accès et conformité.

Aujourd'hui, les entreprises sont confrontées à de plus en plus de risques de sécurité, qu'il s'agisse de la compromission des identifiants et des privilèges permanents, des menaces internes ou de la complexité excessive des plateformes PAM. Face aux cyberattaques visant en permanence les comptes privilégiés, la sécurisation des ressources critiques constitue une priorité absolue.

Pour assurer leur sécurité, les entreprises disposent souvent de plusieurs solutions existantes qui sont coûteuses et difficiles à déployer et à intégrer. Qui plus est, elles ne surveillent ni ne protègent chaque utilisateur sur chaque appareil, où qu'il se trouve. Une approche rationalisée et zero-trust en matière de gestion des accès privilégiés est essentielle afin de réduire la surface d'attaque, d'appliquer le principe du moindre privilège et de garantir la conformité réglementaire. Cela permet de mettre en place un accès sécurisé et efficace pour les équipes distribuées dans les environnements hybrides et multicloud.

### L'infrastructure moderne d'aujourd'hui nécessite une solution PAM moderne

KeeperPAM sécurise et gère l'accès à vos ressources critiques, notamment les serveurs, les applications web, les bases de données et les charges de travail. Tous les utilisateurs et les appareils de votre entreprise sont autorisés, authentifiés et pris en charge par des services de surveillance, de suivi des menaces et de génération de rapports.

En tant que plateforme cloud-native et zero-knowledge brevetée, KeeperPAM unifie la gestion des mots de passe, des secrets et des connexions de l'entreprise avec un accès réseau zero-trust, la gestion des privilèges au niveau des terminaux et l'isolation du navigateur à distance.

# Beneficios de KeeperPAM

### Mise en place d'une gestion multicloud

Centralisez l'accès au sein d'une même interface utilisateur à travers de multiples fournisseurs de services cloud, charges de travail sur site et environnements client.

### Enregistrement de chaque session privilégiée

Enregistrez l'activité de l'écran et du clavier sur tous les protocoles, notamment SSH, RDP, VNC, les bases de données ainsi que les sessions de navigateur web, avec détection des menaces par IA et arrêt automatique des sessions.

### Application d'une protection MFA sur tous les systèmes

Ajoutez une couche MFA à votre infrastructure cloud et sur site, y compris aux ressources qui ne la prennent pas en charge nativement.

### Rotation automatique des mots de passe

Verrouillez les comptes de service au niveau de l'infrastructure sur site et dans le cloud.

### Concesión de privilegios controlada y justo a tiempo

Éliminez les droits administrateur permanents en instaurant une élévation temporaire à la demande, basée sur des politiques. Toutes les actions privilégiées sont consignées, limitées dans le temps et protégées par une authentification multifacteur ainsi que des workflows d'approbation.

### Respect des exigences de conformité

Bénéficiez d'une visibilité totale grâce à des journaux détaillés, à l'enregistrement des sessions et à des rapports automatisés qui vous garantissent un accès instantané à toutes les données nécessaires pour les audits.

En savoir plus
**keepersecurity.com**

Demandez une démo
**keeper.io/demo**

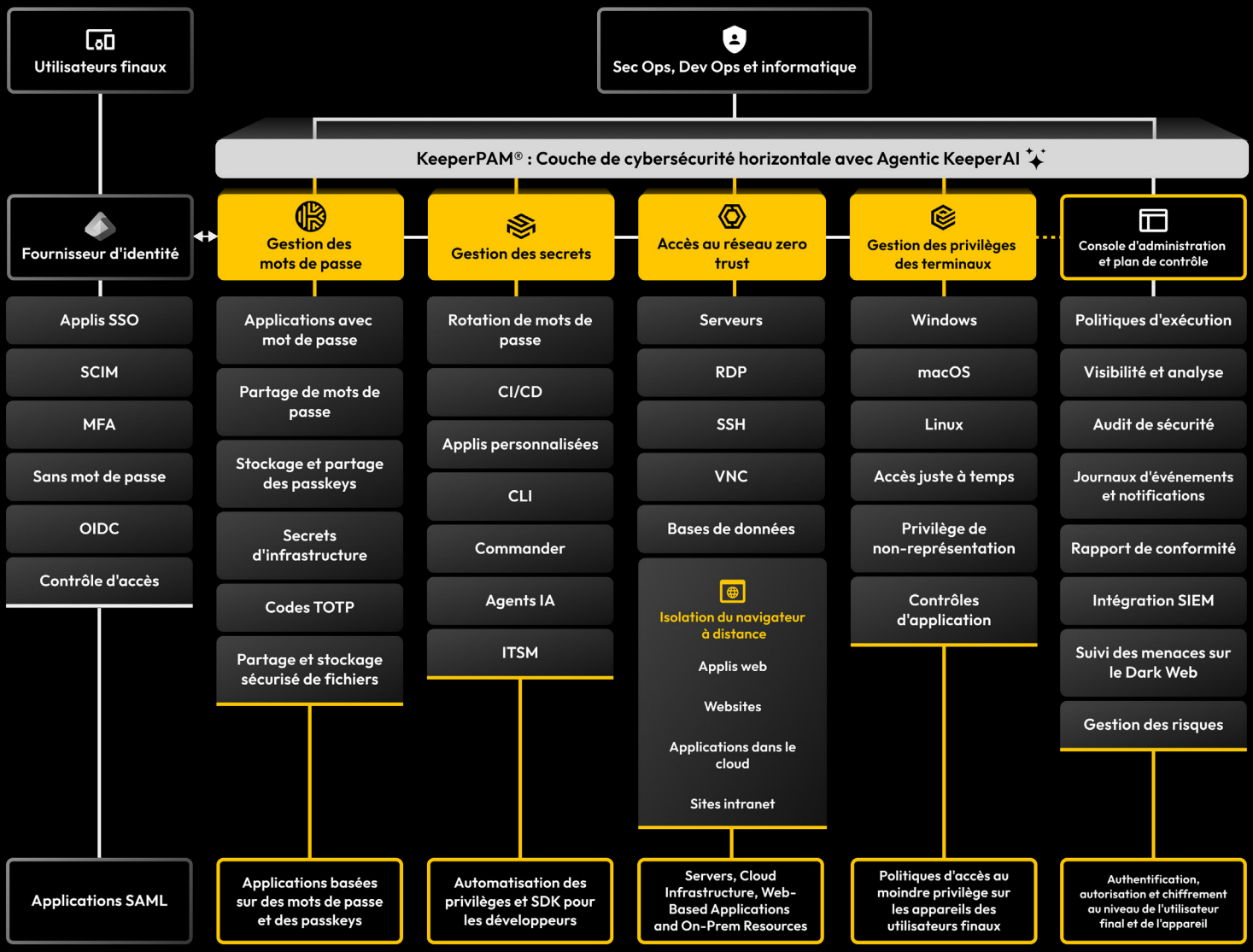
Demandes de partenaires
**partners@keepersecurity.com**

# 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.

KEEPER PAM

# Plateforme de gestion des accès à privilèges de Keeper




## Une plateforme PAM de nouvelle génération conçue pour les environnements de travail à distance multicloud et distribués

KeeperPAM est la toute première solution à intégrer les fonctionnalités PAM critiques dans un coffre-fort cloud capable de fournir un accès sécurisé à toute ressource protégée. La plateforme permet aux entreprises d'adopter une approche zero-trust et de supprimer les privilèges permanents pour tous les employés.

La plateforme peut être entièrement personnalisée afin de répondre aux besoins de votre entreprise. Il est notamment possible de configurer les méthodes de provisionnement, d'appliquer des politiques d'accès granulaires par rôle ou par équipe, et d'intégrer des centaines d'autres plateformes IAM telles que vos outils SIEM, CI/CD, DevOps ou encore vos logiciels personnalisés.

## Comment déployer KeeperPAM

1. **Déployer le coffre-fort** - Déployez Keeper avec votre SSO, tel qu'Entra ID ou Okta. Provisionnez via SCIM, SAML ou AD.
2. **Despliegue el agente de punto final** - Envíe el agente a los sistemas Windows, macOS y Linux para controlar los derechos de administrador local con concesión JIT.
3. **Déployer la passerelle** - Installez une passerelle allégée dans chaque environnement afin de bénéficier d'un accès sans agent et de sessions privilégiées.
4. **Définir la politique** - Appliquez des politiques MFA, RBAC et à moindre privilèges en fonction des responsabilités du poste.