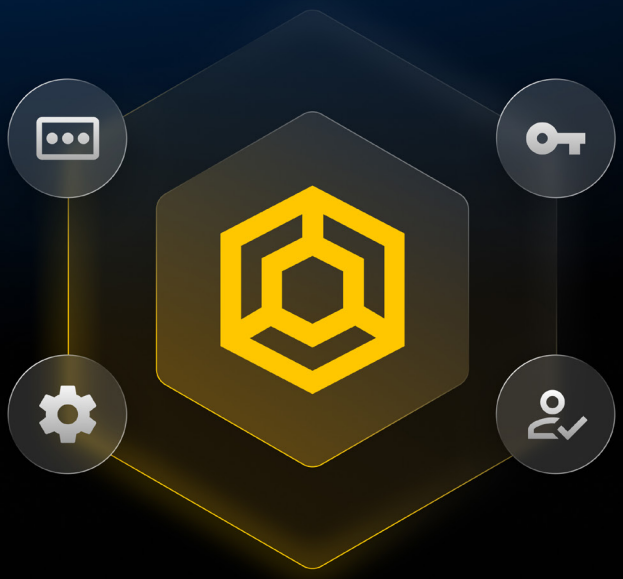
ÉTUDE DE CAS

Asite sécurise les identifiants, les secrets et les accès privilégiés à l'échelle de l'entreprise avec KeeperPAM®



Contexte

Asite est une société SaaS au service du secteur de la construction, qui aide les organisations à gérer des projets complexes — des modèles 3D et des jumeaux numériques au contrôle des documents et à la collaboration avec les fournisseurs — au sein d'équipes et de régions internationales. Asite est présent dans de nombreuses régions du monde, avec des centres de données répartis sur neuf sites et un effectif de plus de 500 personnes.

Industrie
Technologie de la construction (SaaS)

Effectif
Plus de 500 employés

Solutions
KeeperPAM

Le défi

Pour une entreprise SaaS internationale qui soutient des programmes de construction majeurs, y compris des clients opérant dans des infrastructures critiques et des environnements proches de la défense, la gestion sécurisée des identifiants et des accès privilégiés est essentielle. Asite avait besoin d'une approche plus centralisée et applicable aux mots de passe, aux secrets et à la gestion des accès privilégiés (PAM) dans l'ensemble de l'organisation.

Des outils anciens avec une visibilité fragmentée - Le recours aux gestionnaires de mots de passe basés sur le navigateur limitait la visibilité et le contrôle, augmentant les risques liés à la réutilisation des mots de passe, à la faiblesse des identifiants et à une capacité réduite à appliquer des contrôles de sécurité pour la conformité et la garantie de la satisfaction client. Les précédents fournisseurs de gestion des secrets et de PAM de l'organisation étaient coûteux et difficiles à déployer.

Au-delà de la sécurisation des utilisateurs internes, Asite devait étendre le même niveau de protection aux partenaires et fournisseurs externes collaborant à des projets de construction complexes, en veillant à ce qu'ils répondent aux attentes des clients et aux obligations contractuelles. L'organisation recherchait une solution sécurisée et facile à utiliser, capable de répondre à tous ses besoins en matière de cybersécurité au sein d'une plateforme centralisée.

> **« L'architecture (de sécurité) et la flexibilité de KeeperPAM sont inégalées. »**
>
> **Tiago Rosado | Responsable de la sécurité des systèmes d'information**

La solution Keeper

Asite a choisi **KeeperPAM** comme plateforme unifiée pour sécuriser les accès privilégiés, les identifiants, les connexions et les secrets à travers l'organisation. En consolidant son ensemble de technologies de cybersécurité dans une plateforme unique zero trust et zero knowledge, Asite a réduit la complexité tout en améliorant la sécurité et la conformité.

Accès privilégié centralisé avec faibles coûts opérationnels - KeeperPAM fournit un accès privilégié sécurisé et contrôlable aux serveurs, à l'infrastructure et aux systèmes sensibles sans exposer les identifiants. L'activité de la session est enregistrée de manière centralisée, ce qui facilite les enquêtes, la responsabilisation et la conformité des clients et des environnements réglementaires. KeeperAI met automatiquement fin aux sessions à haut risque et génère des résumés d'activité avec des détails précis pour l'audit et les réponses aux incidents.

Avec un déploiement rapide et une architecture flexible, KeeperPAM a remplacé les outils de gestion des secrets et de PAM d'Asite tout en étendant la couverture des accès privilégiés à d'autres systèmes sans augmenter les coûts ou la complexité.

> **« Le déploiement de KeeperPAM a été extrêmement facile, l'un des meilleurs de mon expérience. J'aimerais que d'autres outils soient aussi faciles à déployer. »**
>
> **Tiago Rosado | Responsable de la sécurité des systèmes d'information**

Gestion des mots de passe d'entreprise, intégrée à KeeperPAM - Dans le cadre de la plateforme KeeperPAM, Asite a normalisé la **gestion des mots de passe** à l'échelle de l'entreprise pour tous les employés, en remplaçant les gestionnaires de mots de passe basés sur un navigateur et en établissant une approche centralisée et exécutoire de sécurité des identifiants.

Cela a permis de mettre en place des politiques de mot de passe contrôlées par l'administrateur en ce qui concerne la longueur et la complexité, et d'empêcher la réutilisation des identifiants de connexions dans les applications. L'équipe informatique peut désormais identifier les identifiants compromis à l'aide de l'outil de surveillance du dark-web de Keeper, BreachWatch®, et renforcer ainsi la posture de sécurité de l'organisation. L'accès à la gestion des mots de passe dans le même coffre-fort que KeeperPAM garantit une gouvernance cohérente pour les utilisateurs finaux et les identifiants privilégiés, ainsi qu'une expérience utilisateur simple.

Gestion moderne des secrets avec Keeper Secrets Manager - Pour protéger les secrets des applications et de l'infrastructure, Asite a déployé **Keeper Secrets Manager** en tant que composant natif de la plateforme KeeperPAM, en remplacement de son précédent outil de gestion des secrets. Keeper Secrets Manager automatise la création et la rotation des mots de passe, des clés et des secrets, supprime les identifiants à longue durée de vie ou gérés manuellement et s'intègre facilement grâce à des **API claires et une documentation solide**, le tout avec une charge opérationnelle minimale pour les équipes informatiques et de sécurité.

> **« Les frais généraux sont minimes... l'automatisation et la rotation des mots de passe et des clés sont fantastiques. »**
>
> **Tiago Rosado | Responsable de la sécurité des systèmes d'information**

La gestion des secrets, des mots de passe et des accès privilégiés au sein de KeeperPAM a permis une gouvernance cohérente entre les identités humaines et non humaines.

Sécurité de premier ordre - L'architecture de sécurité zero trust et zero knowledge de Keeper est inégalée pour protéger les informations et atténuer le risque de violation de données. Keeper associe la cryptographie à courbe elliptique (ECC) au niveau de l'appareil à **plusieurs couches de chiffrement** (au niveau du coffre-fort, des dossiers et des entrées), une authentification multifactorielle et biométrique, ainsi qu'un chiffrement AES 256 bits validé par la norme FIPS 140-3 et PBKDF2. Keeper est **conforme aux normes SOC 2 et ISO 27001** — dont la conformité est la plus ancienne du secteur — ainsi qu'aux normes FedRAMP High et GovRAMP.

Impact sur l'organisation

En déployant la plateforme PAM complète de Keeper pour permettre la gestion des mots de passe, des secrets et des accès privilégiés, Asite a mis en place un cadre de sécurité unifié et évolutif qui renforce la protection tout en réduisant la complexité opérationnelle pour ses équipes informatiques et de sécurité.

Amélioration de la posture de sécurité avec des résultats mesurables - La centralisation la gestion des identifiants et des accès a permis à Asite de renforcer considérablement sa posture de sécurité globale. Le renforcement de l'hygiène des mots de passe, l'automatisation de rotation des secrets et le contrôle des accès privilégiés ont permis de réduire l'exposition aux menaces externes et aux risques internes. Les identifiants ne sont plus créés, partagés ou réutilisés manuellement, ce qui favorise une application cohérente des politiques de sécurité dans l'ensemble de l'organisation.

Surtout, ces contrôles sont mesurables et vérifiables, ce qui permet de répondre aux exigences réglementaires et contractuelles dans toutes les régions du monde et dans tous les environnements des clients.

> **« Les principaux avantages de la plateforme KeeperPAM sont la réduction des coûts, la réduction des frais généraux de gestion des systèmes, l'amélioration de la conformité aux exigences de sécurité et l'amélioration de la posture de sécurité. »**
>
> **Tiago Rosado | Responsable de la sécurité des systèmes d'information**

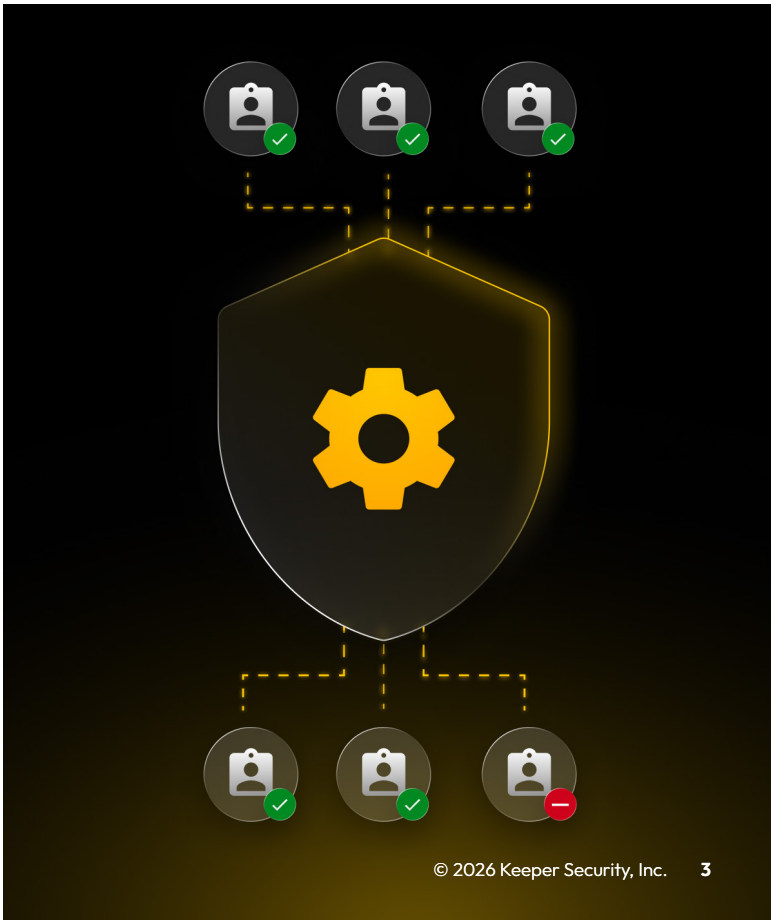
Réduction des frais généraux et consolidation des outils - En consolidant la gestion des mots de passe, la gestion des secrets et la PAM en une seule plateforme, Asite a réduit la prolifération des outils et simplifié l'administration, réduisant ainsi les frais généraux. Cette approche a permis aux équipes informatiques et de sécurité allégées de gérer les contrôles d'accès plus efficacement sans augmenter les effectifs ou les frais généraux, tout en élargissant la couverture pour protéger un plus large éventail de systèmes et d'environnements.

Diminution de l'exposition au risque d'initié et renforcement de la responsabilité - Grâce à la gestion et au contrôle centralisés des accès privilégiés, Asite a renforcé sa capacité à détecter, enquêter et répondre aux activités à haut risque. Le contrôle des sessions et la piste d'audit favorisent la responsabilisation et réduisent la probabilité d'une utilisation abusive, qu'elle soit intentionnelle ou accidentelle.

Partenariat et assistance continus - Au-delà de la technologie, Asite a souligné l'importance d'une assistance fiable et d'une assistance tout au long du déploiement et de l'adoption. Les équipes de soutien et d'habilitation de Keeper ont joué un rôle essentiel en veillant à ce que la plateforme soit mise en œuvre efficacement et alignée sur les besoins opérationnels de l'organisation.

> **« La qualité de l'assistance - même s'il s'agit de la question la plus technique, ils feront une analyse approfondie [...] L'équipe de formation [a été] absolument essentielle, en adaptant la formation à notre réalité. »**
>
> **Tiago Rosado | Responsable de la sécurité des systèmes d'information**

KeeperPAM est devenue le fondement de la stratégie d'Asite en matière d'accès à la sécurité, offrant un contrôle centralisé des identités humaines et non humaines dans des environnements mondiaux. En regroupant l'accès privilégié, la gestion des mots de passe et la gestion des secrets au sein d'une plateforme unique, Asite a renforcé la sécurité, amélioré l'efficacité opérationnelle et établi une base évolutive pour soutenir la croissance future.



KeeperPAM

KeeperPAM est une plateforme de gestion des accès privilégiés (PAM) de nouvelle génération qui sécurise et gère l'accès aux ressources critiques, y compris les serveurs, les applications web, les bases de données et les charges de travail. Basé sur une architecture de sécurité zero trust et zero knowledge, KeeperPAM aide les organisations de toute taille à protéger les comptes privilégiés, à appliquer le moindre privilège, à sécuriser l'infrastructure distante et à répondre aux exigences de conformité, avec une facilité d'utilisation inégalée et un déploiement rapide.Keeper est intuitif et facile à déployer, quelle que soit la taille de l'entreprise. KeeperPAM utilise un service de passerelle zero trust pour accéder à chaque environnement. Aucune mise à jour des paramètres de pare-feu ou d'entrée n'est nécessaire, ce qui permet un accès transparent et sécurisé sans complexité. Grâce aux capacités de session à distance de Keeper, l'utilisateur n'a jamais accès aux identifiants ou aux clés SSH. L'accès à une ressource peut être limité dans le temps et les identifiants changent automatiquement après la révocation de l'accès, ce qui permet l'accès juste-à-temps (JIT) sans jamais exposer les identifiants.Keeper est conçu pour être mis à l'échelle pour les organisations de toutes tailles. KeeperPAM centralise l'accès dans une interface utilisateur (UI) unique à travers plusieurs fournisseurs de cloud, charges de travail sur site et environnements clients, ce qui permet une gestion multicloud.

Cas d'utilisation professionnelle : KeeperPAM

- Contrôler et surveiller tous les comptes privilégiés
- Fournir un accès JIT sans exposer les identifiants
- Consolider les outils de développement en une seule plateforme avec une interface utilisateur intuitive
- Permettre une gestion transparente des environnements cloud, hybrides et multicloud
- Enregistrer les sessions multiprotocoles avec la détection des menaces par l'IA et la terminaison automatisée des sessions
- Automatiser la rotation des mots de passe
- Appliquer la protection MFA sur tous les systèmes
- Déployer en toute transparence via le web ou une application de bureau avec un approvisionnement SCIM automatisé

Protégez votre organisation avec Keeper

Pour en savoir plus sur la façon dont Keeper peut protéger votre organisation avec une plateforme facile à utiliser, **contactez notre équipe commerciale** pour un essai gratuit ou une démonstration personnalisée.

A propos du Keeper

Keeper Security est l'une des entreprises de logiciels de cybersécurité à la croissance la plus rapide, qui protège des milliers d'organisations et des millions de personnes dans plus de 150 pays. Keeper est pionnier de la sécurité zero knowledge et zero trust, conçu pour tout environnement informatique. Son offre principale, KeeperPAM®, est une plateforme conçue sur le cloud et basée sur l'IA qui protège tous les utilisateurs, appareils et infrastructures contre les cyberattaques. Reconnu pour son innovation dans le Gartner Magic Quadrant pour la gestion des accès privilégiés (PAM), Keeper sécurise les mots de passe et les clés d'accès, les secrets d'infrastructure, les connexions à distance et les terminaux avec des politiques d'application basées sur le rôle, le moindre privilège et l'accès juste-à-temps.

Keeper est une solution de confiance, appréciée par des milliers d'entreprises et des millions d'utilisateurs dans le monde.

Gartner

KeeperPAM® reconnue dans le 2025 Gartner Magic Quadrant™ pour la PAM

Prix d'excellence en matière de cybersécurité
Gestion des accès privilégiés

Cyber Defense Magazine
Choix de la rédaction - Gestion des accès privilégiés (PAM)

Newsweek
Plateforme de cybersécurité n° 1

Enterprise Management Associates
KeeperPAM® reconnu pour la solidité de son produit