ÉTUDE DE CAS

DrillDocs sécurise les opérations offshore mondiales et l'accès à l'ingénierie 24h/24 et 7j/7 avec KeeperPAM®

Contexte

DrillDocs est une start-up technologique en phase d'amorçage qui fournit des logiciels de vision par ordinateur pour les applications de forage offshore. Sa plateforme surveille le processus de forage en temps réel et analyse les déblais de roche pour aider les opérateurs à améliorer la sécurité, l'efficacité et les performances des plateformes de forage offshore.

Secteur
Pétrole et gaz

Employés
20+

Solutions
KeeperPAM
Keeper Secrets Manager

Le défi

Au fur et à mesure que DrillDocs évoluait, passant d'une équipe d'ingénieurs fondateurs à une organisation distribuée de soutien à la production, la gestion des accès est devenue de plus en plus complexe. Dans les premiers temps, une petite équipe interne s'est chargée du développement et de l'assistance, les identifiants étant stockés en toute sécurité et l'accès étroitement contrôlé par des processus manuels informels. Au fur et à mesure que la demande des clients augmentait et que les systèmes étaient déployés à l'échelle internationale, DrillDocs a fait appel à une société de services d'ingénierie externe pour assurer une couverture d'assistance de nuit et garantir une véritable disponibilité opérationnelle 24 heures sur 24 et 7 jours sur 7. L'organisation s'est appuyée sur Keeper Secrets Manager pour automatiser la récupération des identifiants de connexion lors des déploiements. Les identifiants ont été injectés par programme lors de la construction des systèmes et conservés en mémoire pendant les processus d'exécution, ce qui garantit qu'ils ne sont jamais stockés en clair sur les systèmes de production.

Bien que cette approche ait efficacement pris en charge les flux de travail DevOps sécurisés, la gestion des sessions privilégiées interactives à travers des utilisateurs internes et tiers distribués nécessitait une solution de gestion sécurisée des accès privilégiés (PAM). L'extension de la couverture opérationnelle a introduit de nouvelles exigences en matière de gouvernance concernant l'octroi, le contrôle et la révocation des accès privilégiés au sein des équipes mondiales et des appareils non gérés. La direction avait besoin d'une plus grande visibilité, de contrôles d'accès plus stricts et d'une solution capable de s'adapter en toute sécurité aux opérations mondiales de l'entreprise.

> **« Nous nous demandions comment gérer au mieux la sécurité lorsque le travail est effectué à partir d'une machine personnelle. Nous faisons confiance à nos partenaires, mais nous devions passer à une culture fondée sur le principe « faire confiance, mais vérifier ».**
>
> **Francois Ruel | Co-fondateur et directeur scientifique, DrillDocs**

La solution Keeper

DrillDocs a déployé **KeeperPAM**, une plateforme PAM complète zero trust et zero knowledge, pour centraliser les accès privilégiés, sécuriser les identifiants et fournir une gestion contrôlée des sessions à distance sans perturber les flux de travail d'ingénierie.

Déploiement rapide avec valeur immédiate - le processus de mise en œuvre de Keeper est simple et direct, ce qui facilite la transition des ingénieurs internes et des équipes d'assistance tierces vers un modèle d'accès plus sécurisé. Keeper offre une **documentation complète sur les produits**, des ressources de mise en œuvre et des conseils aux utilisateurs finaux pour soutenir des déploiements réussis. Des **guides détaillés sur les produits** et des **vidéos de formation** favorisent l'adoption par les utilisateurs.

> **« Le jour où nous avons décidé de commencer notre essai, nous avons pu tout mettre en place en deux heures. A partir de là, nous avons commencé à utiliser Keeper tout de suite. »**
>
> **Francois Ruel | Co-fondateur et directeur scientifique, DrillDocs**

Accès virtualisé sécurisé sans gestion des terminaux - KeeperPAM permet un accès sécurisé, basé sur un navigateur, aux bureaux virtuels Windows et Linux via sa passerelle zero trust, éliminant ainsi le besoin d'installations VPN ou d'exposition directe au réseau sur les appareils personnels. En maintenant la connectivité et les outils d'administration dans un environnement virtuel sécurisé, KeeperPAM permet de s'assurer que les identifiants privilégiés ne sont jamais exposés aux utilisateurs finaux. Tous les accès à l'infrastructure sont contrôlés, chiffrés et enregistrés de manière centralisée, ce qui permet aux entreprises de bénéficier d'une visibilité et d'une gouvernance totales sur les sessions privilégiées à distance.

Approvisionnement et révocation d'accès instantanés - KeeperPAM rationalise la gestion du cycle de vie des utilisateurs en permettant aux administrateurs d'approvisionner, de modifier et de révoquer les accès privilégiés en quelques secondes. Grâce à des **contrôles d'accès centralisés basés sur les rôles** et l'application des politiques, les organisations peuvent immédiatement accorder l'accès aux systèmes critiques ou supprimer les autorisations en cas de changement de rôle ou de départ des utilisateurs. Cette capacité d'approvisionnement en temps réel réduit la charge administrative, élimine les risques d'accès permanent et garantit que les comptes privilégiés restent étroitement contrôlés à tout moment.

Déploiements sécurisés automatisés sans exposition d'identifiants - Keeper Secrets Manager sécurise l'accès de machine à machine en permettant des déploiements automatisés et des mises à jour du système sans exposer ou coder en dur les identifiants. Au cours des processus de construction, les identifiants sont récupérés par programme et injectés directement dans la mémoire, ce qui garantit qu'ils ne sont jamais stockés en clair ou laissés sur les systèmes. Cette approche renforce la sécurité DevOps en éliminant l'étalement des secrets tout en maintenant l'efficacité de l'automatisation.

> **« J'utilise le coffre-fort plusieurs fois par jour. Nous utilisons également Keeper Secrets Manager pour les déploiements et les mises à jour automatisés. Cela fonctionne très bien pour nous. »**
>
> **David Momberger | Ingénieur système principal, DrillDocs**

Sécurité de premier ordre - l 'architecture de sécurité zero trust et zero knowledge de Keeper est conçue pour protéger les informations et réduire le risque de violations de données. Keeper combine la cryptographie à courbe elliptique (ECC) avec **plusieurs couches de chiffrement** (au niveau du coffre-fort, du dossier et de l'entrée), la cryptographie résistante aux quanta, l'authentification biométrique et multifacteur et le chiffrement AES 256 bits validé par FIPS 140-3, ainsi que le PBKDF2. Keeper est **conforme aux normes SOC 2 et ISO/IEC 27001 et supporte également les normes ISO/IEC 27017 et 27018**, avec la conformité la plus ancienne de l'industrie. Keeper est autorisé par FedRAMP et GovRAMP High, certifié PCI DSS et certifié par TrustArc pour la confidentialité.

Impact sur l'organisation

Depuis l'implémentation de KeeperPAM, DrillDocs a considérablement renforcé sa posture de sécurité tout en préservant l'agilité nécessaire à une start-up internationale à croissance rapide. Les mots de passe administratifs partagés ont été éliminés et les identifiants privilégiés sont désormais protégés par des coffres-forts, randomisés et régis par les contrôles d'accès basés sur les rôles. Le modèle « Bring Your Own Device » (apporter votre propre appareil ou BYOD) de l'entreprise ne pose plus de problèmes de visibilité ni de contraintes opérationnelles.

> **« Keeper a apporté un grand changement dans notre culture de la sécurité numérique. Nous ne garderons plus nos identifiants dans des endroits peu sûrs. »**
>
> **Francois Ruel | Co-fondateur et directeur scientifique, DrillDocs**

Réduction des risques au sein d'une équipe BYOD distante – KeeperPAM réduit les risques au sein de l'équipe BYOD distante de DrillDocs en isolant les accès privilégiés au sein d'environnements virtuels sécurisés. Les ingénieurs et les partenaires tiers peuvent se connecter en toute sécurité aux systèmes de production depuis n'importe où dans le monde, sans exposer d'identifiants ni installer d'outils d'accès sensibles directement sur les appareils personnels.

Accès de moindre privilège basé sur le rôle – KeeperPAM permet à DrillDocs de structurer l'accès par rôle plutôt que de distribuer des identifiants individuels. Les équipes d'ingénieurs clients, les développeurs et les partenaires externes n'ont accès qu'aux systèmes nécessaires à l'exercice de leurs responsabilités. Cette approche a permis de réduire considérablement les frais administratifs tout en garantissant un contrôle strict des accès privilégiés.

> **« L'intégration ou le départ des employés est désormais beaucoup plus facile et plus rapide. Si quelqu'un a besoin d'accéder à quelque chose de nouveau, c'est maintenant une question de secondes et il y a accès ».**
>
> **Mert Geveci | Directeur de la technologie, DrillDocs**

Rationalisation de l'intégration et du départ des utilisateurs – KeeperPAM a transformé les processus d'intégration et de départ, en améliorant l'efficacité et en réduisant les frais administratifs. L'accès peut être accordé ou révoqué en quelques secondes, ce qui permet aux dirigeants de répondre immédiatement aux besoins opérationnels.

Visibilité complète des sessions privilégiées – les capacités d'enregistrement des sessions et des activités de KeeperPAM offrent une visibilité supplémentaire sur les activités privilégiées. En cas de comportement inhabituel, les responsables peuvent examiner les données de la session pour mieux comprendre ce qui s'est passé et réagir de manière appropriée. KeeperAI permet d'interrompre automatiquement les sessions à haut risque et d'obtenir des résumés d'activité chiffrés. Ce niveau de visibilité soutient le modèle de sécurité de l'organisation pour les ingénieurs répartis dans le monde entier et les équipes d'assistance tierces, en donnant à la direction un contrôle clair sur la façon dont les environnements de production sont accessibles et utilisés.

Une gouvernance intégrée pour soutenir la conformité – alors que DrillDocs poursuit son chemin vers la conformité SOC 2, KeeperPAM fournit une base solide pour répondre aux exigences des contrôles d'accès. La gestion centralisée des identifiants, l'application du principe du moindre privilège basée sur le rôle et les capacités d'audit des sessions soutiennent les objectifs plus larges de l'entreprise en matière de gouvernance et de sécurité.

Aujourd'hui, DrillDocs fonctionne avec la maturité de sécurité d'une entreprise beaucoup plus grande. Les ingénieurs peuvent se connecter en toute sécurité depuis n'importe où dans le monde, sur n'importe quel appareil, sans exposer d'identifiants privilégiés. L'accès est structuré, surveillé et contrôlé de manière centralisée. L'intégration est immédiate, et le départ est rapide et régi par des règles. Les partenaires extérieurs peuvent apporter leur contribution en toute sécurité. Avec KeeperPAM en place, l'organisation est en mesure d'évoluer en toute sécurité tout en maintenant la vitesse et l'innovation qui définissent sa croissance.

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 se connecter aux environnements cibles sans nécessiter de mises à jour du pare-feu ou de changements au niveau de l'entrée. Les fonctionnalités de session à distance garantissent que les utilisateurs n'ont jamais d'accès direct aux identifiants ou aux clés SSH, ce qui permet d'isoler totalement les secrets du terminal. L'accès aux ressources peut être limité dans le temps et régi par une politique, les identifiants étant automatiquement remplacés après la révocation de l'accès. Cela permet un accès sécurisé et 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 à 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 de la session
- Automatiser la rotation des mots de passe
- Appliquer la protection MFA sur chaque système
- 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 de 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 cloud-native et basée sur l'IA qui protège l'ensemble des utilisateurs, des appareils et des 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. Découvrez pourquoi des organisations de premier plan font confiance à Keeper pour se défendre contre les adversaires modernes en visitant le site **KeeperSecurity.com**.

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

Gartner

KeeperPAM® reconnu dans le Gartner Magic Quadrant™ de 2025 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