ATLASSIAN Williams F1 TEAM | KEEPER OFFICIAL PARTNER

ÉTUDE DE CAS

Atlassian Williams F1 Team sécurise les accès critiques aux systèmes privilégiés avec KeeperPAM®

Contexte

Atlassian Williams F1 Team est l'une des équipes les plus historiques de Formule 1, fondée en 1977 par Sir Frank Williams et Patrick Head. Basée à Grove, dans l'Oxfordshire, au Royaume-Uni, l'équipe a remporté neuf championnats des constructeurs et sept championnats des pilotes, ce qui en fait l'une des équipes les plus décorées de l'histoire de la Formule 1. Connue pour son excellence en matière d'ingénierie et son esprit de compétition, Williams se concentre sur l'innovation et la performance, en tirant parti de la technologie de pointe et de l'analyse des données pour rivaliser en tête de grille dans le monde du sport automobile – ce qui évolue rapidement.

Secteur
Sports mécaniques

Employés
1,000+

Solutions
KeeperPAM

Le défi

En Formule 1, la protection des données sensibles relatives aux performances est essentielle pour conserver un avantage concurrentiel. Pour Atlassian Williams F1 Team, le défi consiste à protéger les accès privilégiés d'une main-d'œuvre internationale utilisant des centaines d'appareils pendant les week-ends de course sous haute pression, ainsi que les opérations commerciales normales en dehors des week-ends de course. Avec des systèmes critiques utilisés sur plusieurs continents et dans des environnements réseau variés, l'équipe doit sécuriser ses informations les plus précieuses tout en veillant à ce que les opérations se déroulent à une vitesse maximale et à ce que les données critiques restent protégées.

> **« Aujourd'hui, il est fondamental d'avoir un partenaire qui nous aide à protéger et à sauvegarder toutes les données extrêmement confidentielles que nous produisons sur la piste. »**
>
> **Carlos Sainz | Pilote de Formule 1, Atlassian Williams F1 Team**

Opérant dans plus de 20 pays chaque saison, Williams s'appuie sur des appareils et des identifiants qui voyagent constamment d'un continent à l'autre. Les mesures de sécurité devaient rester efficaces quels que soient le lieu, le réseau ou le terminal, afin de protéger l'équipe, qu'elle se trouve au siège ou qu'elle soit connectée à un réseau temporaire en bord de piste.

La gestion de cet accès a présenté ses propres défis. L'approvisionnement et le déprovisionnement des identifiants au sein de nombreuses équipes internes, fonctions, systèmes et zones géographiques ont exigé beaucoup de ressources et de temps.

> **« Normalement, un ordinateur reste à l'intérieur d'un bâtiment, mais les nôtres voyagent dans le monde entier. Où que nous allions, nous devons nous assurer que notre technologie reste sécurisée. »**
>
> **James Vowles | Directeur d'équipe, Atlassian Williams F1 Team**

La solution Keeper

Atlassian Williams F1 Team s'est associé à Keeper Security pour déployer **KeeperPAM**, une plateforme complète de gestion des accès privilégiés (PAM) zero trust et zero knowledge. La plateforme unifiée de KeeperPAM offre la visibilité, la sécurité et l'agilité opérationnelle dont Williams a besoin pour gérer les accès privilégiés au sein d'une main-d'œuvre en constante évolution et répartie dans le monde entier. L'équipe avait besoin d'une solution facile à déployer qui sécuriserait ses données sensibles et lui permettrait de contrôler étroitement l'accès.

Accès de moindre privilège basé sur les rôles – **Le contrôle d'accès basé sur les rôles (RBAC)** de Keeper assure que chaque membre de l'équipe du département de Technologie, innovation & croissance n'a accès qu'aux identifiants, systèmes et données nécessaires à son rôle. En limitant strictement les privilèges, Williams réduit la menace interne et minimise l'exposition aux données sensibles.

Identifiants privilégiés sécurisés – Les identifiants privilégiés tels que les mots de passe et les clés d'accès sont protégés et sécurisés dans le cadre de **l'architecture zero knowledge et zero trust** de Keeper. Cela élimine les pratiques de stockage risquées, garantit que les identifiants ne sont jamais exposés en clair et protège les connexions sensibles, quel que soit l'endroit du monde où l'équipe participe à la compétition.

> **« Lorsqu'un utilisateur s'inscrit à Keeper, il réalise immédiatement ce qui lui manquait dans sa vie. Avec Keeper, ils n'ont plus à se battre avec des mots de passe ou à s'inquiéter de la manière de partager des informations en toute sécurité. Grâce à sa simplicité d'utilisation, la productivité augmente considérablement, tout comme la sécurité pour chaque utilisateur. »**
>
> **Craig Lurey | Directeur technique et cofondateur, Keeper Security**

Accès sans mot de passe – Les capacités de gestion des sessions privilégiées permet aux équipes de sécurité de Williams d'accorder l'accès aux systèmes sensibles sans jamais exposer les identifiants. Avec KeeperPAM, Williams peut surveiller, entrer et auditer les activités privilégiées en temps réel, offrant ainsi une visibilité et un contrôle complets.

Intégration transparente avec les systèmes existants – KeeperPAM **s'intègre directement** avec le fournisseur d'identité de Williams pour l'approvisionnement et le déprovisionnement automatisés des comptes privilégiés. Cela garantit des changements d'accès immédiats et précis lorsque le personnel rejoint ou quitte l'équipe, réduisant ainsi les frais administratifs et éliminant les risques d'accès persistants.

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 enregistrements), 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, ISO 27001, 27017 et 27018** - avec la conformité la plus ancienne de l'industrie - ainsi qu'autorisé par FedRAMP et GovRAMP, certifié PCI DSS et certifié par TrustArc pour la protection de la confidentialité.

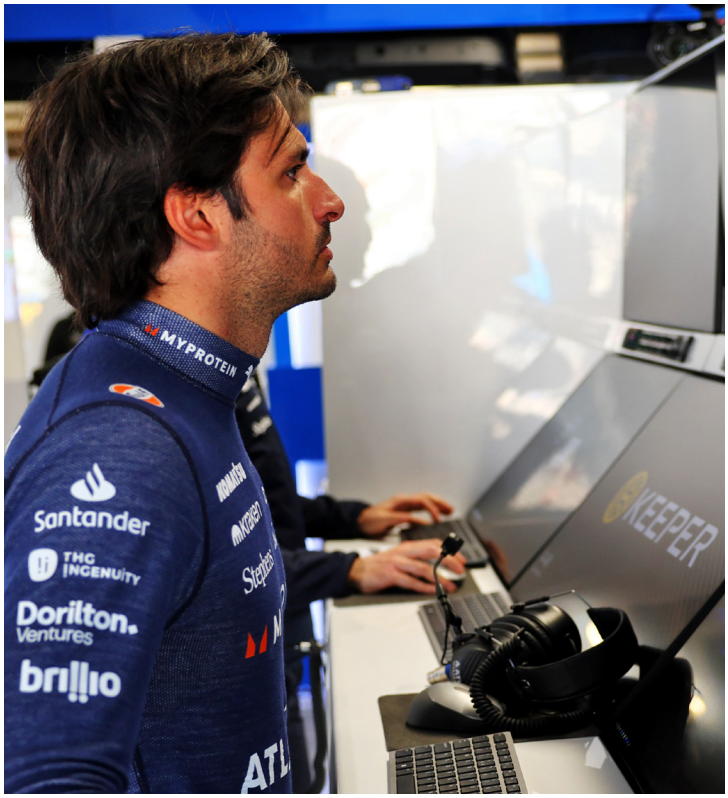
> **« Par rapport à d'autres outils que nous utilisions auparavant, nous avons trouvé le processus d'intégration de Keeper beaucoup plus rapide et facile. »**
>
> **Harry Wilson | Ancien responsable de la sécurité de l'information, Atlassian Williams F1 Team**

Impact sur l'organisation

Keeper a transformé la façon dont Atlassian Williams F1 Team gère et protège les accès privilégiés. L'équipe applique désormais les politiques PAM pour ses utilisateurs les plus privilégiés, en sécurisant les identifiants dans un coffre-fort zero knowledge et en permettant des connexions rapides et sécurisées depuis n'importe où dans le monde. Grâce à la surveillance des activités privilégiées et à l'automatisation des changements d'accès, Williams opère avec plus de rapidité, de confiance et de contrôle.

> **« Ce qui est essentiel pour nous dans tout partenariat, c'est qu'il y ait une synergie entre les deux marques qui travaillent ensemble pour atteindre le même objectif. Et c'est tout à fait le cas avec Keeper. »**
>
> **James Vowles | Directeur d'équipe, Atlassian Williams F1 Team**

Sécurité et visibilité accrues des accès privilégiés – KeeperPAM applique l'accès de moindre privilège et stocke tous les identifiants dans un coffre-fort chiffré, et Williams peut enregistrer l'activité de l'écran et du clavier pendant les sessions à distance à travers tous les protocoles, y compris SSH, RDP, VNC, base de données et sessions web du navigateur.



Hygiène fortifiée des identifiants – Avec KeeperPAM déployé, Williams applique l'authentification multifactorielle (MFA) sur chaque système, s'assure que la force des mots de passe à travers les équipes répond à ses normes et identifie proactivement la réutilisation des mots de passe à travers les utilisateurs. En tirant parti des fonctionnalités d'audit et de reporting de Keeper, l'organisation élimine totalement les identifiants répétés, garantissant ainsi la sécurité de ses systèmes contre les cybermenaces potentielles.

Forte adoption par les utilisateurs et réduction des tickets d'assistance – La conception intuitive de KeeperPAM a entraîné une forte adoption dans l'ensemble de l'organisation, ce qui s'est traduit par une réduction des demandes d'assistance liées à l'accès et aux mots de passe pour l'équipe informatique. Le **portail de documentation de** KeeperPAM s'est également avéré utile pour aider les utilisateurs à se familiariser avec la plateforme. Le taux d'adoption élevé a conduit à une expérience quotidienne plus fluide et plus sûre, tant pour les administrateurs que pour les utilisateurs finaux.

> **« Si vous regardez notre équipe de piste, ce que Keeper a vraiment fait, c'est que le chemin de moindre résistance est aussi le chemin le plus sûr, ce qui signifie que nos utilisateurs finaux sont satisfaits, ce qui signifie que je suis également satisfait. »**
>
> **Harry Wilson | Ancien responsable de la sécurité de l'information, Atlassian Williams F1 Team**

Confiance opérationnelle globale – Keeper continue de permettre à Williams d'opérer en toute sécurité dans le monde entier, sur n'importe quel réseau et avec n'importe quel appareil, offrant ainsi le plus haut niveau de protection, que l'équipe opère sur le bord de la piste, au siège ou en voyageant vers la prochaine course.

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 d'accéder à 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 unique (UI) 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 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 Magic Quadrant de Gartner pour la gestion des accès privilégiés (PAM), Keeper sécurise les mots de passe et les clés d'accès, l'infrastructure de secrets, la connexion à distance et les terminaux avec des politiques d'application basées sur le rôle, le moindre privilège et l'accès juste-à-temps.

Des milliers d'entreprises et des millions de personnes dans le monde font confiance à Keeper et l'apprécient.

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

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