

ÉTUDE DE CAS

L'équipe Atlassian Williams F1 protège les données sensibles de l'usine jusqu'aux stands



Le 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 constructeurs et sept championnats pilotes – parmi les équipes les plus décorées de l'histoire de la Formule 1. Réputée pour son excellence en ingénierie et son esprit de compétition, Williams met l'accent sur l'innovation et la performance, s'appuyant sur les technologies de pointe et l'analyse de données pour concourir dans le monde en pleine évolution du sport automobile.

Secteur

Sports mécaniques

Employés

Plus de 1 000

Solutions

Keeper Enterprise
Password Manager



Le défi

La Formule 1 est le sport le plus gourmand en données au monde, ce qui en fait une cible de grande valeur pour les cyberattaques. L'équipe Atlassian Williams F1 génère plus de 1 To de données télémétriques, aérodynamiques et de simulation chaque week-end de course, avec plus de 400 capteurs sur chaque voiture fournissant simultanément 30 000 canaux de données aux ingénieurs présents sur le circuit ainsi qu'à ceux basés à Grove. Les identifiants protégeant l'accès à ces données peuvent avoir la même valeur stratégique que les données elles-mêmes.

« La F1 est un sport d'équipe — sans que toutes les équipes travaillent ensemble sur la même tâche, rien ne fonctionne. Nous ne voulons pas que la sécurité soit le blocage. Les gens ont besoin d'accéder à ce dont ils ont besoin, quand ils en ont besoin. »

Chris Hicks | Ingénieur principal en sécurité de l'information, équipe Atlassian Williams F1

Environ 1 200 personnes travaillent dans toute l'organisation – de la soufflerie aux opérations de course en bord de piste. Chacune nécessite un accès précis et adapté au rôle tout au long d'une saison couvrant plus de 20 pays. Chaque livre dépensée est régie par le plafond des coûts de la Formule 1, qui limite combien les équipes peuvent investir en personnel, équipement et opérations chaque saison. Cela signifie que les dépenses de sécurité sont directement mises en balance par rapport aux investissements performants dans la voiture elle-même.

« C'est une vraie conversation entre l'achat d'un outil de sécurité et un nouvel aileron avant ou un nouvel ingénieur mécanique. Nous devons prouver une valeur démontrable de l'outil lorsque nous le proposons. »

Chris Hicks | Ingénieur principal en sécurité de l'information, équipe Atlassian Williams F1



La solution Keeper

L'équipe F1 d'Atlassian Williams a déployé le gestionnaire de mots de passe d'entreprise de Keeper en parallèle avec BreachWatch, centralisant la gestion des identifiants autour de deux priorités : une collaboration sécurisée entre toutes les équipes et fonctions, et un chiffrement de premier ordre conçu pour les menaces d'aujourd'hui et de demain.

Collaboration : Partager à la vitesse de la F1

Les dossiers partagés et les autorisations basées sur les rôles de Keeper garantissent que le personnel est automatiquement équipé des identifiants nécessaires pour réussir. Le partage ponctuel offre aux entrepreneurs et aux tiers un accès limité dans le temps qui expire automatiquement, sans intervention manuelle. Keeper est accessible sur tous les navigateurs, appareils et systèmes d'exploitation gérés, garantissant ainsi que les utilisateurs peuvent accéder aux identifiants dont ils ont besoin, quand et où ils en ont besoin. De l'équipe en bord de piste à l'équipe marketing, Keeper réduit les frictions pour les utilisateurs.

« Ils sont générés entièrement au sein de Keeper et appliqués automatiquement, la reconnaissance du site et la saisie automatique s'effectuent en un instant. »

James Yexley | Responsable des réseaux sociaux, équipe Atlassian Williams F1

Chiffrement : Protection conçue pour les données de grande valeur

L'architecture **zero knowledge et zero trust** de Keeper signifie que les clés de chiffrement sont générées côté client et jamais stockées sur les serveurs de Keeper. Cryptographie à courbe elliptique, **chiffrement AES-256 bits** et PBKDF2 sont superposés sur les niveaux de coffre-fort, de dossier et d'entrée, avec une authentification MFA et biométrie appliquée sur tous les systèmes.

« Il faudrait plus de 2 000 ans à un cybercriminel pour déchiffrer les données chiffrées. Les clés sont générées côté client avec l'équipe Atlassian Williams F1. Nous stockons les uns et les zéros. C'est tout. »

Darren Guccione | PDG et cofondateur, Keeper Security

Keeper ajoute aussi des chiffrements résistants au quantique en utilisant **l'algorithme de Kyber** pour se défendre contre la menace de « collecter maintenant, déchiffrer plus tard », où les adversaires stockent aujourd'hui des données chiffrées pour les déchiffrer une fois que l'informatique quantique devient viable.

« En F1, il faut toujours penser au prochain cycle réglementaire. C'est formidable de voir Keeper adopter cette même philosophie de réflexion sur la façon de nous protéger de ce que nous savons qui va suivre. »

Chris Hicks | Ingénieur principal en sécurité de l'information, équipe Atlassian Williams F1



L'impact sur l'organisation

Keeper offre aux équipes de Williams un accès immédiat en libre-service aux identifiants dont elles ont besoin, réduisant ainsi la charge de support informatique et libérant l'équipe pour se concentrer sur des tâches à plus grande valeur. Avec le provisionnement et le déprovisionnement gérés automatiquement, l'équipe informatique consacre moins de temps aux demandes d'accès de routine et plus de temps aux priorités techniques qui font avancer l'équipe.

« Quand les équipes sont intégrées au Keeper, elles se sentent puissantes plutôt que de devoir contacter le service d'assistance. Cela libère l'équipe de support pour les tâches cruciales qui font une différence importante pour la voiture. »

Chris Hicks | Ingénieur principal en sécurité de l'information, équipe Atlassian Williams F1

Performances du week-end de course

En bord de piste, une installation plus rapide de l'infrastructure signifie plus de temps pour l'analyse des données et la stratégie de course — précisément là où des gains marginaux sont réalisés. Les ingénieurs arrivant à un circuit peuvent mettre en ligne les systèmes rapidement et en toute confiance, sachant que chaque identifiant dont ils ont besoin est immédiatement à portée de main.

« Si les équipes du circuit mettent l'infrastructure en place plus tôt, ce temps est consacré aux ingénieurs pour élaborer des stratégies de course et faire l'analyse des données plus tôt. Ces différences de fractions de seconde font une énorme différence lors d'un week-end de course. »

Chris Hicks | Ingénieur principal en sécurité de l'information, équipe Atlassian Williams F1



Confiance en matière de sécurité mondiale

Que l'équipe soit à Grove ou en bord de piste à l'autre bout du monde, Keeper offre un accès cohérent et conforme aux politiques sur tous les pays, réseaux et appareils. Grâce à la surveillance continue du dark web assurée par BreachWatch et au chiffrement zero knowledge protégeant chaque identifiant, Williams dispose des fondations de sécurité nécessaires pour rivaliser sans compromis.

« La gestion des identifiants n'est plus le domaine où une marge de progression existe. »

Chris Hicks | Ingénieur principal en sécurité de l'information, équipe Atlassian Williams F1

Une base solide pour chaque équipe

L'impact de Keeper va bien au-delà de l'informatique. Chez Williams, les collaborateurs occupant des postes aussi variés que la gestion de l'expérience client, les réseaux sociaux, l'administration des déplacements et l'ingénierie des coûts évoquent le même avantage fondamental : un espace unique, sécurisé et organisé pour gérer toutes les identifiants dont ils ont besoin. La sécurité est devenue quelque chose que les gens remarquent parce qu'elle fonctionne, pas parce qu'elle gêne.

« La sécurité est extrêmement importante en Formule 1. Nous traitons beaucoup de données clients – nous voulons nous assurer qu'elles soient dans une source centralisée de vérité, protégée via Keeper. »

Tom Iverson | Responsable principal de l'expérience client (siège), Atlassian Williams F1 Team





La plupart des entreprises n'ont qu'une visibilité limitée sur les pratiques des employés en matière de mots de passe, ce qui accroît considérablement le risque cybernétique. L'hygiène cybernétique ne peut pas être améliorée sans informations critiques concernant l'utilisation et la conformité des mots de passe. Keeper résout ce problème en fournissant la sécurité, la visibilité et le contrôle ultime.

Les données sont protégées par l'architecture de sécurité zero knowledge de Keeper et un chiffrement de classe mondiale résistant au quantique. Le modèle zero knowledge signifie que seul l'utilisateur connaît et détient son mot de passe principal ainsi que la clé de chiffrement utilisée pour chiffrer et déchiffrer ses informations.

Keeper est intuitif et facile à déployer, quelle que soit la taille de l'entreprise. Keeper s'intègre aux serveurs Active Directory et LDAP, ce qui rationalise le provisionnement et l'intégration. **Keeper SSO Connect®** s'intègre aux solutions SSO existantes et est certifié FedRAMP High et autorisé GovRAMP High.

Keeper est conçu pour être mis à l'échelle pour les organisations de toutes tailles. Des fonctionnalités telles que les autorisations basées sur les rôles, le partage d'équipe, l'audit départemental et l'administration déléguée accompagnent les organisations dans leur croissance. **Keeper Commander** fournit des API robustes pour l'intégration avec les systèmes actuels et futurs.

Cas d'utilisation professionnelle: KeeperPAM

- Prévenir les cyberattaques et les violations de données liées aux identifiants
- Prendre en charge les clés d'accès pour une authentification sans effort
- Renforcer la conformité
- Augmenter la productivité des employés
- Appliquer les procédures et les politiques de mots de passe
- Réduire les coûts d'assistance technique
- Minimiser la formation grâce à une mise en place rapide de la sécurité
- Améliorer la sensibilisation et le comportement des employés en matière de sécurité

A propos de Keeper

Keeper Security est l'une des entreprises de logiciels de cybersécurité à la croissance la plus rapide, protégeant 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, l'infrastructure de secrets, les connexions à distance et les terminaux avec des politiques d'application basées sur les rôles, 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

Keeper Security® a été reconnue en 2026 comme la deuxième entreprise de logiciels de sécurité à la croissance la plus rapide au monde



Prix Cybersecurity Stars 2026

Innovateur de l'année en matière de sécurité de l'IA, Meilleure plateforme de gestion des accès privilégiés pour les entreprises



Cybersecurity Excellence Awards

Gestion des accès privilégiés



Global InfoSec Awards

Solution de cybersécurité alimentée par l'IA, Entreprise de cybersécurité, Gestion des accès privilégiés (PAM)



Globe Awards 2026

Lauréat argent en cybersécurité