

FALLSTUDIE

Das Atlassian Williams F1 Team schützt vertrauliche Daten – vom Werk bis zur Boxengasse



Hintergrund

Das Atlassian Williams F1-Team ist eines der traditionsreichsten Teams der Formel 1 und wurde 1977 von Sir Frank Williams und Patrick Head gegründet. Das Team mit Sitz in Grove, Oxfordshire, Großbritannien, hat neun Konstrukteurs- und sieben Fahrermeisterschaften gewonnen und ist damit eines der am meisten ausgezeichneten Teams in der Geschichte der Formel 1. Williams ist für seine herausragende Ingenieurleistungen und seinen Wettbewerbsgeist bekannt. Der Fokus liegt auf Innovation und Leistung, wobei Spitzentechnologie und Datenanalysen eingesetzt werden, um in der sich schnell verändernden Welt des Motorsports mithalten zu können.

Branche
Motorsport

Mitarbeiter
Mehr als 1.000

Lösungen
Keeper Enterprise
Passwortmanager



Die Herausforderung

Die Formel 1 ist der datenintensivste Sport der Welt und damit ein wertvolles Ziel für Cyberangriffe. Das Atlassian Williams F1-Team erzeugt an jedem Rennwochenende über 1 TB an Telemetrie-, Aerodynamik- und Simulationsdaten, wobei über 400 Sensoren an jedem Auto 30.000 Datenkanäle live an die Ingenieure auf der Strecke und zurück in Grove liefern. Die Zugangsdaten, die den Zugang zu diesen Daten schützen, können denselben strategischen Wert haben wie die Daten selbst.

„F1 ist ein Mannschaftssport – wenn nicht alle Teams gemeinsam an derselben Aufgabe arbeiten, funktioniert auch nichts. Wir wollen nicht, dass Sicherheit das Hindernis ist. Menschen müssen Zugang zu dem haben, was sie brauchen, wann sie es brauchen.“

**Chris Hicks | Leitender Informationssicherheitsingenieur,
Atlassian Williams F1-Team**

Rund 1.200 Mitarbeiter arbeiten in der gesamten Organisation – vom Windkanal bis zum Streckeneinsatz. Jeder erfordert einen präzisen, rollengerechten Zugriff über eine Saison, der sich über mehr als 20 Länder erstreckt. Jedes ausgegebene Pfund wird durch die Kostenobergrenze der Formel 1 geregelt, die begrenzt, wie viel Teams in Personal, Ausrüstung und Betrieb pro Saison investieren dürfen. Das bedeutet, dass Sicherheitsausgaben direkt gegen leistungssteigernde Investitionen in das Fahrzeug selbst abgewogen werden.

„Es ist ein echtes Abwägungsgespräch zwischen dem Kauf eines Sicherheits-Tools und einem neuen Frontflügel oder einem neuen Maschinenbauingenieur. Wir müssen einen nachweisbaren Mehrwert des Tools belegen, wenn wir es vorschlagen.“

**Chris Hicks | Leitender Informationssicherheitsingenieur,
Atlassian Williams F1-Team**



Die Keeper-Lösung

Das Atlassian Williams F1-Team setzte zusammen mit BreachWatch den Enterprise-Passwortmanager von Keeper ein und zentralisierte die Verwaltung von Zugangsdaten auf zwei Prioritäten: sichere Zusammenarbeit in jedem Team und jeder Funktion sowie erstklassige Verschlüsselung, die für die Bedrohungen von heute und morgen entwickelt wurde.

Zusammenarbeit: Mit der Geschwindigkeit der F1 teilen

Die geteilten Ordner und rollenbasierte Berechtigungen von Keeper sorgen dafür, dass das Personal automatisch genau die Zugangsdaten bekommt, die sie für den Erfolg benötigen. Die einmalige Freigabe gewährt Auftragnehmern und Dritten zeitlich begrenzten Zugang, der automatisch abläuft, ohne dass ein manuelles Eingreifen erforderlich ist. Keeper ist über alle unterstützten Browser, Geräte und Betriebssysteme zugänglich, sodass Nutzer jederzeit und von überall aus auf die benötigten Zugangsdaten zugreifen können. Vom Trackside-Team bis zum Marketingteam reduziert Keeper die Reibung für Benutzer.

„Sie werden vollständig in Keeper generiert und automatisch angewendet, wobei die Website erkannt und die Daten im Handumdrehen automatisch ausgefüllt werden.“

James Yexley | Social-Media-Manager, Atlassian Williams F1-Team

Verschlüsselung: Schutz für hochwertige Daten

Die **Zero-Knowledge- und Zero-Trust-Architektur** von Keeper bedeutet, dass Verschlüsselungsschlüssel clientseitig generiert und niemals auf den Servern von Keeper gespeichert werden. Elliptic-Curve-Kryptographie, **AES-256-Bit-Verschlüsselung** und PBKDF2 sind über Tresor-, Ordner- und Datensatzebenen verteilt, wobei die MFA und biometrische Authentifizierung in allen Systemen durchgesetzt werden.

„Ein Cyberkrimineller würde über 2.000 Jahre brauchen, um die verschlüsselten Daten zu entschlüsseln. Die Schlüssel werden kundenseitig mit dem Atlassian Williams F1-Team generiert. Wir speichern Einsen und Nullen. Mehr nicht.“

Darren Guccione | CEO und Mitbegründer, Keeper Security

Keeper integriert außerdem quantenresistente Verschlüsselung mithilfe des **Kyber-Algorithmus**, um sich gegen die Bedrohung „Jetzt ernten, später entschlüsseln“ zu schützen, wobei Gegner heute verschlüsselte Daten speichern, um sie zu entschlüsseln, sobald Quantencomputing möglich wird.

„In der Formel 1 muss man immer an den nächsten Regulationszyklus denken. Es ist großartig zu sehen, wie Keeper diese gleiche Philosophie verfolgt und darüber nachdenkt, wie wir uns vor dem schützen können, was als Nächstes kommt.“

Chris Hicks | Leitender Informationssicherheitsingenieur, Atlassian Williams F1-Team



Auswirkungen auf das Unternehmen

Keeper bietet Teams in Williams sofortigen Self-Service-Zugang zu den benötigten Zugangsdaten, reduziert den IT-Supportaufwand und ermöglicht es dem Team, sich auf höherwertige Aufgaben zu konzentrieren. Da die Provisionierung und Deprovisionierung automatisch abgewickelt werden, verbringt das IT-Team weniger Zeit mit routinemäßigen Zugriffsanfragen und mehr mit den technischen Prioritäten, die das Team voranbringen.

„Wenn Teams in Keeper eingegliedert werden, fühlen sie sich gestärkt, anstatt den Serviceschalter kontaktieren zu müssen. Das entlastet das Support-Team für die entscheidenden Aufgaben, die einen wichtigen Unterschied für das Fahrzeug machen.“

Chris Hicks | Leitender Informationssicherheitsingenieur,
Atlassian Williams F1-Team

Leistung am Rennwochenende

Auf der Strecke bedeutet schnellere Infrastrukturaufbau mehr Zeit für Datenanalyse und Rennstrategie – genau dort, wo marginale Gewinne erzielt werden. Ingenieure, die an einer Rennstrecke eintreffen, können Systeme schnell und zuverlässig in Betrieb nehmen, da sie wissen, dass alle benötigten Zugangsdaten sofort verfügbar sind.

„Wenn die Leute auf der Strecke die Infrastruktur schneller aufbauen, geht diese Zeit an die Ingenieure, die Rennstrategien entwickeln und die Datenanalyse früher durchführen. Diese Sekundenbruchteile machen an einem Rennwochenende einen enormen Unterschied.“

Chris Hicks | Leitender Informationssicherheitsingenieur,
Atlassian Williams F1-Team



Globales Sicherheitsvertrauen

Egal, ob das Team in Grove oder am anderen Ende der Welt auf der Strecke ist – Keeper bietet konsistenten, richtlinienkonformen Zugang in jedem Land, Netzwerk und Gerät. Mit kontinuierlicher BreachWatch-Überwachung des Dark Web und Zero-Knowledge Verschlüsselung, die alle Zugangsdaten schützt, verfügt Williams über die Sicherheitsgrundlage, um kompromisslos zu konkurrieren.

„Die Verwaltung von Zugangsdaten ist nicht mehr der Bereich, in dem Verbesserungsmöglichkeiten bestehen.“

Chris Hicks | Leitender Informationssicherheitsingenieur,
Atlassian Williams F1-Team

Eine sichere Grundlage für jedes Team

Der Einfluss von Keeper reicht weit über IT hinaus. Bei Williams beschreiben Mitarbeiter in so unterschiedlichen Bereichen wie Gasterlebnis, Social Media, Reisemanagement und Kostentechnik denselben grundlegenden Vorteil: einen einzigen, sicheren und organisierten Ort zur Verwaltung aller Zugangsdaten, auf die sie angewiesen sind. Sicherheit ist zu etwas geworden, das den Mitarbeitern auffällt, weil sie funktioniert – nicht weil sie im Weg steht.

„Sicherheit ist in der Formel 1 enorm wichtig. Wir arbeiten mit so vielen Kundendaten – wir wollen sicherstellen, dass sie in einer zentralen Wahrheitsquelle sind, geschützt durch Keeper.“

Tom Iverson | Senior HQ Guest Experience Manager,
Atlassian Williams F1-Team

KeeperPAM

Die meisten Unternehmen haben nur begrenzten Einblick in die Passwortpraktiken ihrer Mitarbeiter, was Cyberrisiken erheblich erhöhen kann. Die Cyberhygiene kann nicht verbessert werden, ohne kritische Informationen über die Verwendung und Einhaltung von Passwörtern zu erhalten. Keeper löst dieses Problem durch ultimative Sicherheit, Visibilität und Kontrolle.

Daten werden durch die Zero-Knowledge Sicherheitsarchitektur von Keeper und die erstklassige, quantenresistente Verschlüsselung geschützt. Zero-Knowledge bedeutet, dass nur der Benutzer sein Master-Passwort und den Verschlüsselungsschlüssel kennt und darauf Zugriff hat, der zum Ver- und Entschlüsseln seiner Informationen verwendet wird.

Keeper ist intuitiv und einfach zu implementieren, unabhängig von der Unternehmensgröße. Keeper lässt sich mit Active Directory und LDAP-Servern integrieren, sodass die Bereitstellung und das Onboarding optimiert werden. **Keeper SSO Connect**® lässt sich in bestehende SSO-Lösungen integrieren und ist FedRAMP High-zertifiziert und GovRAMP High-autorisiert.

Keeper ist so konzipiert, dass es für Unternehmen jeder Größe skaliert werden kann. Funktionen wie rollenbasierte Berechtigungen, Teilen innerhalb von Teams, abteilungsbezogene Prüfungen und delegierte Verwaltung unterstützen Organisationen bei ihrem Wachstum. **Keeper Commander** bietet eine robuste API für die Integration in aktuelle und zukünftige Systeme.

Anwendungsfälle für Unternehmen: KeeperPAM

- Verhinderung zugangsdatenbezogener Datenpannen und Cyberangriffe
- Unterstützung von Passkeys für mühelose Authentifizierung
- Stärkung der Compliance
- Steigerung der Produktivität Ihrer Mitarbeiter
- Durchsetzung von Passwort-Richtlinien und -Verfahren
- Reduzierung der Helpdesk-Kosten
- Minimierung des Schulungsaufwands durch schnelle Sicherheitsmaßnahmen
- Verbesserung des Sicherheitsbewusstseins und -verhaltens der Mitarbeiter

Über Keeper

Keeper Security ist eines der am schnellsten wachsenden Unternehmen für Cybersicherheitssoftware, das Tausende von Unternehmen und Millionen von Menschen in über 150 Ländern schützt. Keeper ist ein Pionier der Zero-Knowledge- und Zero-Trust-Sicherheit für jede IT-Umgebung. Das Herzstück, KeeperPAM®, ist eine KI-fähige, Cloud-native Plattform, die alle Benutzer, Geräte und Infrastrukturen vor Cyberangriffen schützt. Keeper wurde für seine Innovationen im Gartner Magic Quadrant für Privileged Access Management (PAM) ausgezeichnet und sichert Passwörter und Passkeys, Infrastrukturgeheimnisse, Remote-Verbindungen und Endpunkte mit rollenbasierten Durchsetzungsrichtlinien, Least-Privilege und Just-in-Time-Zugriff.

Auf Keeper vertrauen Tausende Unternehmen und Millionen Menschen weltweit.

Gartner

Keeper Security® wurde 2026 als das zweitschnellst wachsende Security-Softwareunternehmen weltweit anerkannt



Cybersecurity Stars Awards 2026

KI-Sicherheitsinnovator des Jahres, Beste Privileged Access Management-Plattform für Unternehmen



Cybersecurity Excellence Awards Privileged Access Management



Global InfoSec Awards

KI-gestützte Cybersicherheitslösung, Cybersicherheitsunternehmen, Privileged Access Management (PAM)



Globe Awards 2026

Silber-Gewinner in Cybersecurity