KEEPER | WILLIAMS RACING

OFFICIAL PARTNER

FALLSTUDIE

Williams Racing schützt globale Betriebsabläufe mit der Zero-Trust-Cybersicherheitsplattform von Keeper

Hintergrund

Williams Racing ist eines der ältesten und erfolgreichsten 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, was es zu einem der erfolgreichsten Teams in der Geschichte der Formel 1 macht. Williams ist für technische Exzellenz und seinen Wettbewerbsgeist bekannt und konzentriert sich voll auf Innovation und Leistung. Es kommen modernste Technologie und Datenanalysen zum Einsatz, damit das Team in der sich ständig weiterentwickelnden Welt des Motorsports weiter ganz vorn bleiben kann.

Branche
Motorsport

Mitarbeiter
Über 1.000

Lösungen
Keeper Password Manager

- Enterprise

Die Herausforderung

In der Welt der Formel 1 sind Technologien und Daten unerlässlich, wenn sich Teams Vorteile im Wettkampf sichern möchten. Williams Racing, eines der ältesten und renommiertesten Formel 1-Teams der Welt, steht vor der immensen Herausforderung, sein wertvolles geistiges Eigentum umfassend zu schützen. Angesichts einer weltweit tätigen Belegschaft, die bei Rennen rund um die Erde Hunderte von Geräten nutzt, sowie eines anspruchsvollen Tagesablaufs muss das Team sicherstellen, dass sensible Daten vor Cyberbedrohungen geschützt bleiben, und gleichzeitig für nahtlose Workflows sorgen.

Die Formel 1-Fahrzeuge stellen für das Team High-Tech-Assets dar, die durch ständige Weiterentwicklung verfeinert werden. Dabei wird die Fahrzeugentwicklung von Daten getragen. Deswegen erfassen Teams bei jedem Rennen neuen Daten, einschließlich Telemetriedaten und Videoaufnahmen. So sammelt Williams Racing jedes Rennwochenende Terabyte an Daten, die dann vom Team übertragen, gespeichert und analysiert werden müssen, um Strategien für anstehende Rennen und die kommenden Jahre zu optimieren. Angesichts der zunehmenden Bedeutung und Mengen von Daten ist es wichtig, dass sie sich sicher speichern und aufrufen lassen, um zu gewährleisten, dass hochvertrauliches geistiges Eigentum geschützt bleibt.

Ebenso wichtig ist die Sicherheit finanzieller und kommerzieller Daten, einschließlich der Zuweisung von Kostenobergrenzenbudgets, die direkt mit der Leistung verknüpft sind. Diese vertraulichen Informationen spielen eine entscheidende Rolle bei der Wahrung des Wettbewerbsvorteils, der Gewährleistung der Einhaltung von Vorschriften und dem Schutz strategischer Entscheidungen.

Aufgrund der hochmobilen Natur der Formel 1, in deren Rahmen Teams in zehn Monaten 21 Länder bereisen – wovon manche besonders anfällig für Cyberbedrohungen sind – wird die Aufgabe noch komplexer. Der Schutz der global verteilten Belegschaft sowie ununterbrochener Zugriff auf essentielle Daten stellen für Williams Racing eine nicht verhandelbare Priorität dar.

> **Cybersicherheit, Bedrohungen und entsprechende Schutzmaßnahmen sind von grundlegender Bedeutung. Darüber kann man gar nicht oft genug sprechen.**
>
> **James Vowles | Teamchef, Williams Racing**

Ohne leistungsstarke Lösung zur Passwortverwaltung riskierte das Team, seine Systeme Datenschutzverletzungen auszusetzen, was Abläufe lahmlegen oder dazu führen könnte, dass sensible Daten in die falschen Hände gelangen. Zu den Herausforderungen mit früher verwendeten Passwortverwaltungsmethoden gehörten:

Passwortverwaltungspraktiken: Da Hunderte von Teammitgliedern weltweit Zugriff auf kritische Daten zu Rennstrategien, Fahrzeugdesigns und Leistungsmetriken haben, war das Risiko für unbefugte Zugriffe auf sensible Daten erhöht. Gleichzeitig waren Transparenz und Zugriffskontrolle eingeschränkt.

Begrenzte Transparenz und Zugriffskontrolle: Dem IT-Team fiel es schwer, die Kontrolle über den Zugriff und die Verwendung von Passwörtern zu behalten, insbesondere angesichts einer Zugriffsverwaltung für eine große Anzahl von Remote-Mitarbeitern. Das Deaktivieren von Benutzern und sichere Übertragen von Anmeldeinformationen nach Austritten aus dem Unternehmen waren besonders schwierig und zeitaufwendig, was zu Sicherheitslücken und verschwendeten Ressourcen führte.

Uneinheitliche Sicherheit bei verschiedenen Geräten: Da das Team zu Rennen rund um die Welt reist, darunter auch in Regionen mit besonders großen Cybersicherheitsrisiken, brachte das Fehlen einer einheitlichen Passwortverwaltungslösung Unstimmigkeiten beim Schutz von Geräte mit sich. Dadurch war das Team potenziellen Sicherheitsverletzungen ausgesetzt, während es in verschiedenen Ländern operierte.

> **Wir benötigen eine Infrastruktur, die an jedem Ort funktioniert, unabhängig davon, ob es sich um Großbritannien oder Länder mit einem erhöhten Cybersicherheitsrisiko handelt. Mit Keeper können wir dem Team Zugriff auf kritische Systeme bieten, egal wo sie sich die Mitarbeiter befinden.**
>
> **Harry Wilson | Leiter der Informationssicherheit, Williams Racing**

Die Lösung von Keeper

Williams Racing wandte sich an Keeper Security, um eine zuverlässige und sichere Passwortverwaltungslösung zu erhalten. Die Zero-Trust- und Zero-Knowledge-Architektur von Keeper gewährleistet für Daten des Teams ein Höchstmaß an Sicherheit, sodass Williams sensible Datensätze zuverlässig schützen kann. Die Lösung bot verschiedene wichtige Vorteile, darunter:

Zentralisierte Passwortverwaltung: Keeper stellte Williams Racing eine zentrale, sichere Plattform zum Speichern und Verwalten von Passwörtern zur Verfügung. Dadurch wurden riskante Praktiken überflüssig und ist sichergestellt, dass alle Anmeldeinformationen mit der Zero-Trust- und zero-knowledge Architektur von Keeper geschützt bleiben.

Nahtlose Integration mit bestehenden Systemen: Keeper ließ sich problemlos in den vorhandenen Identitätsanbieter (IdP) von Williams Racing integrieren, was eine automatisierte Bereitstellung und Deprovisionierung von Benutzerkonten möglich machte. Die Integration sorgt dafür, dass Anmeldeinformationen sicher übertragen werden, wenn Mitarbeiter das Team verlassen bzw. dem Team beitreten. Das reduziert den Aufwand für die IT und beseitigt potenzielle Sicherheitslücken.

Erweiterte Sicherheitsfunktionen: Keepers robuste Sicherheitsmaßnahmen, darunter Multi-Faktor-Authentifizierung (MFA) und End-to-End-Verschlüsselung, sorgen dafür, dass vertrauliche interne Kommunikation und Daten geschützt sind. Die Möglichkeit, Anmeldeinformationen sicher und nahtlos zwischen Teammitgliedern auszutauschen, ohne vertrauliche Daten preiszugeben, bietet eine zusätzliche Schutzebene.

Benutzerakzeptanz und Schulungen: Keeper gilt als führender Password Manager für Unternehmen jeder Größe und ist einfach zu bedienen sowie schnell zu implementieren. Das umfangreiche Dokumentationsportal von Keeper stellte Williams Racing detaillierte Anweisungen und Best Practices für das System zur Verfügung, um Administratoren dabei zu helfen, die Bereitstellung zu optimieren. Bei Endbenutzern führten detaillierte Produkthandbücher und Schulungsvideos zu einer hohen Akzeptanz.

Rollenbasierte Zugriffskontrollen (RBAC): Keeper erlaubt Administratoren eine granulare Durchsetzung von Freigaben. Sie können rollenbasierte Zugriffskontrollen (RBAC) nutzen, um dafür zu sorgen, dass Sicherheitsrichtlinien und Compliance-Anforderungen im gesamten Williams Racing-Team eingehalten werden. Durch Festlegung von Rollen innerhalb des Teams wird die Bereitstellung für Administratoren vereinfacht. Außerdem können bestimmte Regelsätze genutzt werden, um Zugriff mit den geringsten Privilegien zu unterstützen und den Sicherheitsstatus des Teams zu erhöhen.

Vorteile für das Unternehmen

Die Bereitstellung von Keeper hatte einen transformativen Effekt auf Williams Racing und erhöhte im gesamten Unternehmen die Sicherheit und Effizienz. Zu den wichtigsten Vorteilen gehören:

Mehr Sicherheit und Datenschutz: Die robuste Sicherheitsarchitektur von Keeper verbesserte die Fähigkeit von Williams Racing, hochsensible Daten umfassend zu schützen. Das IT-Team verfügt jetzt über volle Transparenz hinsichtlich der Passwortnutzung und Passwortkomplexität und kann auf Sicherheitsbedrohungen überwachen, um sicherzustellen, dass alle Anmeldeinformationen vor unbefugtem Zugriff geschützt sind.

> **Wir brauchen Daten. Wir brauchen Cybersicherheit. Wir brauchen IT-Infrastruktur. Und wir brauchen die Möglichkeit, dass Menschen in einer sicheren Umgebung arbeiten können. Und zwar unabhängig davon, ob sie sich in Großbritannien oder irgendwo anders auf der Welt befinden.**
>
> **James Vowles | Teamchef, Williams Racing**

Verbesserte Betriebseffizienz: Durch die Zentralisierung der Passwortverwaltung und Rationalisierung von Zugriffskontrollen konnte Williams Racing den Zeitaufwand für das Verwalten von Anmeldeinformationen erheblich reduzieren. So können sich Ingenieure, Mechaniker und anderes Personal auf ihre Kernaufgaben konzentrieren, ohne dass es wegen Zugriffsproblemen zu Verzögerungen kommt – insbesondere an Rennwochenenden.

Geringeres Risiko für Cyberangriffe: Dank starker Passwortverwaltungspraktiken und erweiterter Sicherheitsfunktionen konnte Williams Racing das Risiko für Datenlecks und Cyberangriffe deutlich minimieren. Die nahtlose Integration der Keeper-Lösung auf allen Geräten und auch in Regionen mit hohem Risiko bietet dem Team zusätzlichen Schutz, wenn es weltweit unterwegs ist.

Positives Feedback und hohe Benutzerakzeptanz: Die einfache Bedienung und intuitive Benutzeroberfläche von Keeper führten zu einer hohen Akzeptanz unter den Teammitgliedern, auch bei nicht-technischem Personal. Somit profitierte das Unternehmen von einer erheblichen Reduzierung der passwortbezogenen Helpdesk-Tickets und einem sichereren, organisierteren Ansatz für die Verwaltung von Passwörtern.

Bessere Benutzerfreundlichkeit für nicht-technische Mitarbeiter: Die benutzerfreundliche Oberfläche von Keeper und die Browser-Erweiterung vereinfachen die Passwortverwaltung für nicht-technische Teams wie Marketing, Finanzen und Logistik. Das hat die Benutzerakzeptanz in allen Abteilungen erhöht und Reibung an Wochenenden mit hohem Druck, an denen jede Sekunde zählt, spürbar reduziert.

> **Nach der Einrichtung von Keeper konnten wir die integrierte Funktion nutzen, um die Passwortstärke, die Wiederverwendung von Passwörtern bei verschiedenen Benutzern und Tresoren zu bewerten, entsprechende Berichte zu erstellen. und ein Projekt durchzuführen, das in unserer gesamten Infrastruktur wiederverwendete Passwörter entfernt.**
>
> **Harry Wilson | Leiter für Informationssicherheit, Williams Racing**

Keeper Password Manager

Die meisten Unternehmen haben nur einen begrenzten Einblick in die Passwortpraktiken ihrer Mitarbeiter, was das Cyberrisiko erheblich erhöht. Die Passworthygiene kann nicht verbessert werden, wenn keine wichtigen Informationen über die Verwendung von Passwörtern und deren Einhaltung vorliegen. Keeper löst dieses Problem, indem es für ultimative Sicherheit, Transparenz und Kontrolle sorgt.

Die Daten sind mit der Zero-Knowledge-Sicherheitsarchitektur und der erstklassigen Verschlüsselung von Keeper geschützt. Zero-Knowledge bedeutet, dass ausschließlich der jeweilige Benutzer Wissen und Zugriff auf sein Master-Passwort sowie den Verschlüsselungsschlüssel hat, der zur Ver- und Entschlüsselung seiner Daten dient.

Keeper ist unabhängig von der Größe eines Unternehmens intuitiv und einfach zu implementieren. Keeper kann mit Active Directory- und LDAP-Servern integriert werden, was die Bereitstellung und das Onboarding deutlich vereinfacht. Keeper SSO Connect® lässt sich in bestehende SSO-Lösungen integrieren und ist FedRAMP- und StateRAMP-autorisiert.

Keeper ist für Unternehmen jeder Größe skalierbar. Funktionen wie rollenbasierte Berechtigungen, Team-Sharing, Abteilungsaudits und delegierte Verwaltung unterstützen Organisationen bei ihrem Wachstum. Keeper Commander bietet robuste APIs, die sich in vorhandene und zukünftige Systeme integrieren lassen.

Geschäftsbezogene Anwendungsfälle: Keeper Password Manager

- Verhindern Sie passwortbezogene Datenschutzverletzungen und Cyberangriffe
- Unterstützen Sie Passkeys für mühelose Authentifizierung
- Stärken Sie die Compliance
- Steigern Sie die Produktivität der Mitarbeiter
- Setzen Sie Passwortrichtlinien und -verfahren durch
- Reduzieren Sie die Helpdesk-Kosten
- Minimieren Sie Schulungen mit schnellen Sicherheitszeitsmaßnahmen
- Verbessern Sie das Sicherheitsbewusstsein und das Verhalten der Mitarbeiter

Über Keeper

Keeper Security transformiert Cybersicherheit für Privatanwender und Unternehmen auf der ganzen Welt durch Privileged Access Management der nächsten Generation. Die benutzerfreundlichen Cybersicherheitslösungen von Keeper basieren auf Zero-Trust- und Zero-Knowledge-Sicherheit, damit alle Benutzer auf allen Geräten geschützt werden. Auf Keeper vertrauen Millionen von Privatanwendern und Tausende von Unternehmen. Damit ist Keeper führend in den Bereichen Passwortverwaltung, Geheimnisverwaltung, privilegierter Zugriff, sicherer Fernzugriff und verschlüsselte Nachrichten. Erfahren Sie mehr unter KeeperSecurity.com.

Keeper wird von Tausenden von Unternehmen und Millionen von Menschen weltweit geschätzt.

G2
Unternehmensführer

PCMag
Editor's Choice

App Store
Top-Rated Productivity

Google Play
Über 10 Millionen Installationen