ATLASSIAN Williams F1 TEAM | KEEPER OFFICIAL PARTNER

FALLSTUDIE

Das Atlassian Williams F1-Team sichert kritische Zugriffe auf privilegierte Systeme mit KeeperPAM®

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 herausragenden Ingenieursleistungen 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 ganz vorne mitzumischen.

Branche
Motorsport

Mitarbeiter
Mehr als 1.000

Lösungen
KeeperPAM

Die Herausforderung

In der Formel 1 ist der Schutz vertraulicher Leistungsdaten von entscheidender Bedeutung für die Aufrechterhaltung der Wettbewerbsfähigkeit. Für das Atlassian Williams F1-Team besteht die Herausforderung darin, den privilegierten Zugriff auf Hunderten von Geräten während der stressigen Rennwochenenden sowie im regulären Geschäftsbetrieb außerhalb der Rennwochenenden zu schützen. Da kritische Systeme auf mehreren Kontinenten und in unterschiedlichen Netzwerkumgebungen im Einsatz sind, muss das Team seine wertvollsten Informationen schützen und gleichzeitig sicherstellen, dass der Betrieb mit maximaler Geschwindigkeit abläuft und kritische Daten geschützt bleiben.

> **„Heutzutage ist es von grundlegender Bedeutung, einen Partner zu haben, der uns dabei hilft, alle strengst vertraulichen Daten, die wir auf der Rennstrecke produzieren, zu schützen und zu sichern."**
>
> **Carlos Sainz | Formel-1-Fahrer, Atlassian Williams F1-Team**

Williams ist jede Saison in mehr als 20 Ländern aktiv und nutzt dafür Geräte und Anmeldedaten, die ständig zwischen den Kontinenten ausgetauscht werden. Die erforderlichen Sicherheitsmaßnahmen müssen unabhängig von Standort, Netzwerk oder Umgebung wirksam bleiben und das Team schützen, egal ob es sich im Hauptquartier befindet oder mit einem temporären Netzwerk an der Rennstrecke verbunden ist.

Die Verwaltung dieses Zugangs stellte ihre eigenen Herausforderungen dar. Die Bereitstellung und Deaktivierung von Zugangsdaten über zahlreiche interne Teams, Funktionen, Systeme und Regionen hinweg war sowohl ressourcenintensiv als auch zeitaufwändig.

> **„Normalerweise bleibt ein Computer in einem Gebäude – unsere reisen aber um die ganze Welt." Wo immer wir hingehen, müssen wir sicherstellen, dass unsere Technologie sicher bleibt."**
>
> **James Vowles | Teamchef, Atlassian Williams F1-Team**

Die Keeper-Lösung

Das Atlassian Williams F1-Team hat sich mit Keeper Security zusammengetan, um **KeeperPAM** einzuführen, eine umfassende Zero-Trust- und Zero-Knowledge-Plattform für Privileged Access Management (PAM). Die einheitliche Plattform von KeeperPAM bot Williams die Transparenz, Sicherheit und operative Agilität, die für die Verwaltung privilegierter Zugriffe in einer schnelllebigen, global verteilten Belegschaft erforderlich sind. Das Team benötigte eine einfach zu implementierende Lösung, die seine sensiblen Daten sichert und es ihnen ermöglicht, den Zugriff genau zu überwachen.

Rollenbasierter Least-Privilege-Zugriff – Die fein abgestuften **rollenbasierte Zugriffskontrolle (Role-Based Access Controls, RBAC)** von KeeperPAM stellen sicher, dass jedes Teammitglied in der Abteilung Technologie, Innovation & Wachstum nur Zugriff auf die für seine Rolle erforderlichen Zugangsdaten, Systeme und Daten hat. Durch die strikte Beschränkung von Berechtigungen reduziert Williams die Insider-Bedrohungen und minimiert die Gefährdung vertraulicher Daten.

Sichere privilegierte Zugangsdaten – Privilegierte Zugangsdaten wie Passwörter und Passkeys werden in der **Zero-Knowledge- und Zero-Trust-Architektur** von Keeper gespeichert und gesichert. Dadurch werden riskante Speicherpraktiken vermieden, sichergestellt, dass Anmeldeinformationen niemals im Klartext offengelegt werden, und vertrauliche Logins werden geschützt, egal wo auf der Welt das Team antritt.

> **„Wenn sich ein Nutzer bei Keeper anmeldet, merkt er sofort, was ihm im Leben gefehlt hat.“ Mit Keeper muss man sich nie mehr mit Passwörtern herumschlagen oder sich Gedanken darüber machen, wie Informationen sicher geteilt werden können. ‚Die Produktivität steigt deutlich, und gleichzeitig wird die Sicherheit für jeden Benutzer erhöht, weil es so einfach zu bedienen ist.“**
>
> **Craig Lurey | CTO und Mitbegründer, Keeper Security**

Passwortloser Zugriff – Die Privileged Session Management-Funktionen ermöglichen es den Sicherheitsteams von Williams, Zugriff auf sensible Systeme zu gewähren, ohne jemals Anmeldeinformationen preiszugeben. Mit KeeperPAM kann Williams privilegierte Aktivitäten in Echtzeit überwachen, protokollieren und prüfen, und so vollständige Transparenz und Kontrolle gewährleisten.

Nahtlose Integration mit bestehenden Systemen – KeeperPAM **integriert sich direkt** in den Identitätsanbieter von Williams für die automatisierte Bereitstellung und Deaktivierung privilegierter Konten. Dies gewährleistet eine sofortige und präzise Änderung der Zugriffsrechte, wenn Mitarbeiter dem Team beitreten oder es verlassen, wodurch der administrative Aufwand reduziert und verbleibende Zugriffsrisiken beseitigt werden.

Erstklassige Sicherheit - Die Zero-Trust- und Zero-Knowledge-Sicherheitsarchitektur von Keeper ist unübertroffen, wenn es darum geht, Informationen zu schützen und das Risiko einer Datenschutzverletzung zu mindern. Keeper kombiniert Elliptic-Curve-Kryptographie (ECC) auf Geräteebene mit **mehreren Verschlüsselungsebenen** (auf Tresor-, Ordner- und Datensatzebene), Multi-Faktor- und biometrischer Authentifizierung sowie FIPS 140-3-validierter AES-256-Bit-Verschlüsselung plus PBKDF2. Keeper **erfüllt die Standards SOC 2, ISO 27001, 27017 und 27018**. — mit der am längsten anhaltenden Compliance der Branche — sowie FedRAMP- und GovRAMP-Autorisierung, PCI-DSS-Zertifizierung und TrustArc-Zertifizierung für Datenschutz.

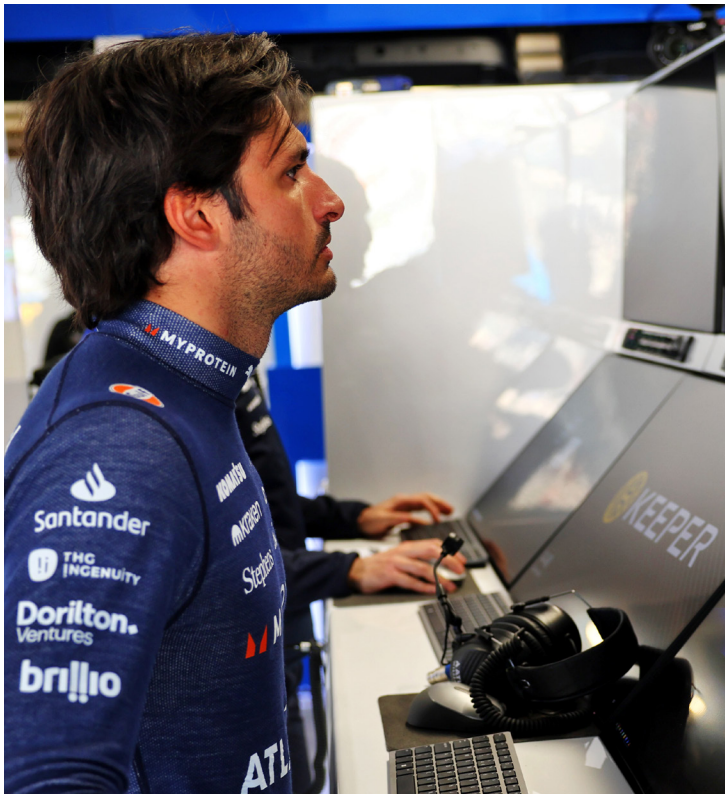
> **„Im Vergleich zu anderen Tools, die wir zuvor verwendet haben, empfanden wir den Onboarding-Prozess von Keeper als wesentlich schneller und einfacher.“**
>
> **Harry Wilson | Ehemaliger Leiter der Informationssicherheit, Atlassian Williams F1-Team**

Auswirkungen auf die Organisation

Keeper hat die Art und Weise, wie das Atlassian Williams F1-Team privilegierte Zugriffe verwaltet und schützt, grundlegend verändert. Das Team setzt nun PAM-Richtlinien für seine privilegiertesten Benutzer durch, sichert Zugangsdaten in einem Zero-Knowledge-Tresor und ermöglicht schnelle, sichere Verbindungen von überall auf der Welt aus. Durch die Überwachung privilegierter Aktivitäten und die Automatisierung von Zugriffsänderungen arbeitet Williams schneller, sicherer und kontrollierter.

> **„Für uns ist bei jeder Partnerschaft entscheidend, dass eine Synergie zwischen den beiden Marken entsteht, die gemeinsam auf dasselbe Ziel hinarbeiten." Und das trifft auf Keeper absolut zu."**
>
> **James Vowles | Teamchef, Atlassian Williams F1-Team**

Verbesserte Sicherheit und Transparenz privilegierter Zugriffe – KeeperPAM erzwingt den Zugriff nach dem Prinzip der geringsten Berechtigungen und speichert alle Anmeldedaten in einem verschlüsselten Tresor. Williams kann die Bildschirm- und Tastaturaktivitäten während Remote-Sitzungen über alle Protokolle hinweg protokollieren, einschließlich SSH-, RDP-, VNC-, Datenbank- und Webbrowser-Sitzungen.



Stärkere Zugangsdatenhygiene – Mit dem Einsatz von KeeperPAM erzwingt Williams die Multi-Faktor-Authentifizierung (MFA) auf jedem System, stellt sicher, dass die Passwortstärke teamübergreifend den Standards entspricht und identifiziert proaktiv die Wiederverwendung von Passwörtern durch Benutzer. Durch die Nutzung der Prüf- und Berichtsfunktionen von Keeper vermeidet die Organisation die wiederholte Eingabe von Anmeldeinformationen vollständig und gewährleistet so die Sicherheit ihrer Systeme vor potenziellen Cyberbedrohungen.

Hohe Benutzerakzeptanz und weniger Support-Tickets – Das intuitive Design von KeeperPAM hat zu einer starken Akzeptanz im gesamten Unternehmen geführt, was zu weniger Helpdesk-Anfragen im Zusammenhang mit Passwörtern und Zugriffsrechten für das IT-Team geführt hat. Das **Dokumentationsportal** von KeeperPAM erwies sich ebenfalls als hilfreich, um den Nutzern den Einstieg in die Plattform zu erleichtern. Die hohe Akzeptanzrate führte zu einem reibungsloseren und sichereren täglichen Nutzungserlebnis für Administratoren und Endbenutzer gleichermaßen.

> **„Was man bei unserem Streckenteam sieht, und was Keeper wirklich gut gemacht, ist, dass der Weg des geringsten Widerstands auch der sicherste Weg ist; was bedeutet, dass unsere Endnutzer zufrieden sind, was wiederum bedeutet, dass auch ich zufrieden bin."**
>
> **Harry Wilson | Ehemaliger Leiter der Informationssicherheit, Atlassian Williams F1-Team**

Globales Betriebsvertrauen – Keeper ermöglicht es Williams weiterhin, weltweit, in jedem Netzwerk und mit jedem Gerät sicher zu arbeiten und bietet ein Höchstmaß an Schutz, egal ob das Team an der Rennstrecke, im Hauptquartier oder auf dem Weg zum nächsten Rennen im Einsatz ist.

KeeperPAM

KeeperPAM ist eine Privileged Access Management (PAM)-Plattform der nächsten Generation, die den Zugriff auf kritische Ressourcen wie Server, Webanwendungen, Datenbanken und Workloads sichert und verwaltet. KeeperPAM basiert auf einer Zero-Trust- und Zero-Knowledge-Sicherheitsarchitektur und unterstützt Organisationen jeder Größe beim Schutz privilegierter Konten, bei der Durchsetzung des Prinzips der minimalen Berechtigungen, der Sicherung der Remote-Infrastruktur und der Erfüllung von Compliance-Anforderungen – mit unübertroffener Benutzerfreundlichkeit und schneller Bereitstellung.

Keeper ist intuitiv und einfach zu implementieren, unabhängig von der Unternehmensgröße. KeeperPAM verwendet einen Gateway-Dienst mit Zero-Trust für den Zugriff auf die jeweiligen Umgebungen. Es sind keine Firewall-Updates oder Änderungen am Eingangssignal erforderlich, wodurch ein nahtloser, sicherer Zugriff ohne Komplexität ermöglicht wird. Mit den Remote-Sitzungsfunktionen von Keeper hat der Benutzer niemals Zugriff auf die Zugangsdaten oder SSH-Schlüssel. Der Zugriff auf eine Ressource kann zeitlich begrenzt sein, und die Zugangsdaten werden nach dem Entzug des Zugriffs automatisch rotiert, wodurch ein JIT-Zugriff ermöglicht wird, ohne dass die Anmeldedaten jemals offengelegt werden.

Keeper ist so konzipiert, dass es für Organisationen jeder Größe skaliert werden kann. KeeperPAM zentralisiert den Zugriff über mehrere Cloud-Anbieter, lokale Workloads und Client-Umgebungen hinweg in einer einzigen Benutzeroberfläche und ermöglicht so das Multi-Cloud-Management.

Anwendungsfälle im Geschäftsleben: KeeperPAM

- Alle privilegierten Konten kontrollieren und überwachen
- JIT-Zugriff gewähren, ohne Zugangsdaten preiszugeben
- Konsolidierung der Entwicklungswerkzeuge auf einer Plattform mit intuitiver Benutzeroberfläche
- Nahtlose Verwaltung von Cloud-, Hybrid- und Multi-Cloud-Umgebungen ermöglichen
- Multiprotokoll-Sitzungen mit KI-Bedrohungserkennung und automatischer Sitzungsbeendigung aufnehmen
- Automatische Passwortrotation
- MFA-Schutz auf jedem System durchsetzen
- Nahtlose Bereitstellung über Web- oder Desktop-App mit automatisierter SCIM-Bereitstellung

Schützen Sie Ihre Organisation mit Keeper

Um mehr darüber zu erfahren, wie Keeper Ihre Organisation mit einer benutzerfreundlichen Plattform schützen kann, **kontaktieren Sie unser Vertriebsteam** für eine kostenlose Testversion oder eine personalisierte Demo.

Über Keeper

Keeper Security ist eines der am schnellsten wachsenden Unternehmen für Cybersicherheitssoftware, das Tausende von Organisationen 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.

Auszeichnung für herausragende Leistungen im Bereich Cybersicherheit
Privileged Access Management

Cyber Defense Magazine
Editor's Choice – Privileged Access Management (PAM)

Newsweek
Nr. 1 Cybersicherheitsplattform

Enterprise Management Associates
KeeperPAM® wurde für seine Produktstärke ausgezeichnet

KeeperPAM® wurde im Gartner Magic Quadrant™ 2025 für PAM ausgezeichnet