KEEPER | Pressemitteilung

Williams Racing entscheidet sich für Keeper Security, um Informationen in der datengetriebenen und hochriskanten Welt der Formel 1 zu schützen

Die Zero-Trust- und Zero-Knowledge-Cybersicherheitslösungen von Keeper Security ermöglichen es Williams Racing, sensible Daten sicher zu verwalten, Abläufe zu optimieren und kritische Ressourcen zu schützen.

München, 28. November 2024 – Die neue Fallstudie von Keeper Security und Williams Racing verdeutlicht, wie hoch die Bedeutung einer Zero-Trust- und Zero-Knowledge-Cybersicherheitssoftware zum Schutz von Passwörtern, Zugangsdaten, privilegierten Zugängen, Geheimnissen und Remote-Verbindungen, in der wettbewerbsintensiven Welt der Formel 1 ist. Als eine der am meisten datengetriebenen Sportarten der Welt, müssen sich Formel-1-Teams auf fortschrittliche Analysen, Telemetrie- und Leistungsdaten verlassen, um ihre Wettbewerbsfähigkeit zu sichern – was Cybersicherheit zu einem zentralen Anliegen macht.

Keeper spielt eine entscheidende Rolle bei der Sicherung des Geschäftsbetriebs von Williams Racing, einschließlich Verträgen, Geschäftsinformationen, Finanzdaten und mehr. Darüber hinaus generiert Williams Racing an jedem Rennwochenende Terabytes an Daten – von Rennstrategien über Fahrzeugdesigns bis hin zu Leistungskennzahlen. Ein erfolgreicher Cyberangriff auf das Team könnte verheerende Folgen haben: geistiges Eigentum könnte gefährdet, sensible Daten kompromittiert und der Betrieb sowohl am Hauptsitz als auch an der Rennstrecke unterbrochen werden. Für Williams Racing ist der Schutz dieser Informationen unverzichtbar und die Lösungen von Keeper Security bieten die optimale Absicherung für die wertvollen Ressourcen.

„Die Formel 1 ist ein hochgradig wettbewerbsorientiertes Umfeld, in dem jeder Vorteil zählt“, sagt Darren Guccione, CEO und Mitgründer von Keeper Security. „Unsere Partnerschaft mit Williams Racing geht über den reinen Schutz ihrer IT-Infrastruktur und sensiblen Informationen hinaus - es geht darum, eine sichere Grundlage zu schaffen, damit das Team Daten nutzen kann, um die Leistung zu steigern und gleichzeitig die mit Cyberbedrohungen verbundenen Risiken zu minimieren.“

„Wir brauchen Daten“, sagt James Vowles, Teamchef bei Williams Racing. „Wir brauchen Cybersicherheit. Wir brauchen eine IT-Infrastruktur. Und wir brauchen für unsere Mitarbeiter die Möglichkeit, in einer sicheren Umgebung zu arbeiten – und zwar unabhängig davon, ob sie sich in Großbritannien oder irgendwo anders auf der Welt befinden.“

Zu den wichtigsten Ergebnissen für Williams Racing mit den Keeper Sicherheitslösungen gehören:

- **Verbesserter Schutz für kritische Daten** – Mit der Zero-Knowledge-Architektur von Keeper kann Williams Racing Rennstrategien, Designs und Telemetriedaten vor unbefugtem Zugriff schützen, wodurch sensible Informationen vollständig abgesichert bleiben. Die fortschrittliche Passwortverwaltung von Keeper stellt sicher,

dass der Geschäftsbetrieb des Teams sicher und widerstandsfähig gegen unbefugten Zugriff bleibt.
- **Steigerung der Betriebseffizienz** – Das zentrale Passwortmanagementsystem von Keeper rationalisiert die Verwaltung von Zugangsdaten, spart dem Team wertvolle Zeit an stressigen Rennwochenenden und ermöglicht es, sich auf die Kernziele zu konzentrieren.
- **Nahtloser globaler Zugriff mit hohem Schutz** – Durch die Verfügbarkeit der Keeper-Lösungen für die globale Belegschaft von Williams Racing können Teammitglieder sicher auf die benötigten Daten zugreifen – sei es an der Rennstrecke, an entfernten Standorten oder im Hauptquartier. Dabei bleiben sensible Informationen vor potenziellen Cyberbedrohungen geschützt.

Die vollständige Fallstudie zeigt umfassend, wie die Lösungen von Keeper Security das Team von Williams Racing dabei unterstützen, ein Höchstmaß an Cybersicherheit aufrechtzuerhalten. Dadurch kann das Team sowohl auf als auch abseits der Strecke mit Vertrauen und Präzision agieren. In diesem Video von Williams Racing erfahren Sie, wie Williams Racing Keeper einsetzt.

###

Über Keeper Security:
Keeper Security verändert weltweit die Cybersicherheit für Menschen und Organisationen. Die intuitiven Lösungen von Keeper basieren auf einer End-to-End-Verschlüsselung, um jeden Anwender auf jedem Gerät und an jedem Standort zu schützen. Die Keeper Zero-Trust-Plattform für die Verwaltung von privilegierten Zugängen ist in wenigen Minuten einsatzbereit. Sie lässt sich nahtlos in jeden Technologie-Stack integrieren, um Sicherheitsverletzungen zu verhindern, Helpdesk-Kosten zu senken und Compliance zu gewährleisten. Keeper genießt das Vertrauen von Millionen von Einzelnutzern und Tausenden von Unternehmen und ist führend bei der Verwaltung von Passwörtern, Passkeys und Geheimnissen, privilegiertem Zugriff, sicherem Fernzugriff und verschlüsseltem Messaging. Erfahren Sie, wie die Zero-Trust- und Zero-Knowledge-Lösungen vor Cyber-Bedrohungen schützen auf KeeperSecurity.com.

Folgen Sie Keeper auf Facebook Instagram LinkedIn X YouTube TikTok

Pressekontakt für Keeper in DACH:
Alexandra Schmidt, +49 170 387 10 64
Thilo Christ, +49 171 622 06 10
keeper@tc-communications.de