

ケーススタディ

ウィリアムズ・レーシングがKeeperによる
ゼロトラストのサイバーセキュリティプラット
フォームでグローバルオペレーションを強化

背景

ウィリアムズ・レーシングは、フォーミュラ1 (F1) で最も歴史的な成功を収めてきた名門チームの1つで、フランク・ウィリアムズ卿とパトリック・ヘッドによって1977年に設立されました。イギリス、オックスフォードシャーのグローブに拠点を置くこのチームは、コントラクターズチャンピオンのタイトルを9回、ドライバーズチャンピオンのタイトルを7回獲得しており、F1史上最も勝利をあげてきたチームの1つに数えられています。卓越したエンジニアリング技術と競争心で知られるウィリアムズは、イノベーションとパフォーマンスに力を注ぎ、最新鋭のテクノロジーとデータ分析を活用することで、進化を続けるモータースポーツの世界でグリッドの先頭を走っています。

業界
モータースポーツ

従業員
1,000人以上

ソリューション
Keeperパスワードマネージャー

• 企業



課題

フォーミュラ1の世界で競争力を維持するには、技術とデータが必要不可欠です。F1チームの中でも最も歴史がある名門チームの1つであるウィリアムズ・レーシングは、貴重な知的財産を保護するという大きな課題を背負っています。世界各地で開催されるレース中には、世界中に分散して数百台に及ぶデバイスを利用する従業員を抱えているほか、日常的にも複雑な業務が行われており、チームは円滑なワークフローを維持すると同時に、サイバー脅威から機密情報の安全を守らなければなりません。

フォーミュラ1のレースカーはチームにとってのかけがえのない資産であり、エンジニアリングによって常に改良が重ねられます。車両部門の業務はデータに支えられています。チームは、レースごとにテレメトリデータやビデオ映像など、常に増え続ける大量のデータを収集します。ウィリアムズ・レーシングは、レース開催の週末ごとにテラバイト規模のデータを収集します。チームは、このデータを転送、保管、分析して、その後すぐに開催されるレースや数年先のレースに向けた戦略に磨きをかけるために活用します。データへの依存度が高まりデータ容量が増大するにつれて、非常に機密性の高い知的財産を守るためデータの保管とアクセスを安全に行うことはきわめて重要です。

多要素認証 (MFA) やエンドツーエンドの暗号化など、Keeperの強力なセキュリティ対策により、機密性の高い社内通信とデータが確実に保護されます。機密データを公開することなく、チームメンバー間で認証情報を安全かつシームレスに共有できるため、保護の層がさらに強化されます。

フォーミュラ1は1か所にとどまりません。チームは10か月間のシーズン中に21か国に移動しなければならず、中にはサイバーセキュリティ脅威の危険度が高い国もあるため、複雑さを増大させます。分散した従業員の安全を確保しつつ、重要なデータに中断なくアクセスできるようにすることは、ウィリアムズ・レーシングにとって妥協できない優先事項です。

サイバーセキュリティ、脅威、さらに自分の身を守る方法は、根本的な重要事項です。これについて十分な議論がなされていません。

- ジェームズ・ヴォウルズ | ウィリアムズ・レーシング、チーム代表

高度なセキュリティレベルのパスワード管理ソリューションの整備を行わない限り、システムはデータ漏洩の危険にさらされます。データ漏洩が発生すれば、業務が停滞したり、機密情報が渡ってはいけない人物の手に渡ったりする可能性があります。それまでのパスワード管理手法には、以下のような課題がありました。

パスワード管理の習慣: 世界中にいる数百人のチームメンバーがレース戦略や車両設計、パフォーマンス指標に関する最重要データにアクセスできたことで、機密情報への不正アクセスの危険性が増し、それにより可視性とアクセス制御も限定的でした。

限られた可視性とアクセス制御: 情報テクノロジー (IT) チームは、パスワードへのアクセスと使用の管理に苦労していました。特に、多数のリモート勤務の従業員向けのアクセス管理を行うのが困難でした。チームメンバーが組織を離れる際に該当ユーザーアカウントを停止して認証情報を安全に移行させる作業が特に難しくして時間を要したため、セキュリティにギャップが生まれ、リソースが浪費されていました。

デバイス間で一貫性のないセキュリティ: チームは、レースのためにサイバーセキュリティの危険性が高い地域を含む世界各地を移動しなければならず、一元化されたパスワード管理ソリューションがないことで、デバイス保護の方法に一貫性を保つことができませんでした。このため、チームがさまざまな国で活動する際、データ漏洩の危険にさらされていました。

英国においても、サイバーセキュリティのリスクが高い国においても、あらゆる場所で機能するインフラストラクチャが不可欠です。チームがどこにいるかに関わらず、最重要システムへのアクセスをチームに自信を持って付与できるのは、Keeperのおかげです。

ハリー・ウィルソン | ウィリアムズ・レーシング、
情報セキュリティ責任者



Keeperソリューション

ウィリアムズ・レーシングは、信頼性と安全性が高いパスワード管理ソリューションとしてKeeper Securityを選択しました。Keeperのゼロトラストとゼロ知識のアーキテクチャは、チームのデータに最高レベルのセキュリティを提供するため、ウィリアムズは機密性の高い記録や情報の安全を守ることができました。ソリューションは、いくつかの分野で大きなメリットをもたらしました。

一元化されたパスワード管理: Keeperは、パスワードを保存して管理するための安全な単一プラットフォームをウィリアムズ・レーシングに提供しました。これにより危険な習慣が不要となり、すべての認証情報がKeeperのゼロトラストと[ゼロ知識](#)のアーキテクチャによって保護されるようになりました。

既存システムとの円滑な統合: ウィリアムズ・レーシングの既存のアイデンティティプロバイダ (IdP) とKeeperが容易に[統合された](#)ことで、ユーザーアカウントの自動プロビジョニングとデプロビジョニングが可能になりました。この統合により、スタッフが退社または入社する際に認証情報が安全に転送されるため、ITの負担が軽減され、潜在的なセキュリティギャップが解消されました。

高度なセキュリティ機能: 多要素認証 (MFA) やエンドツーエンド暗号化を初めとするKeeperの高度なセキュリティ対策は、内部の機密情報やコミュニケーションを確実に保護します。機密データを危険にさらさず、チームメンバー間で認証情報を安全かつチームレスに共有できるようになったことで、保護の層が強化されました。

ユーザー向け導入支援とトレーニング: Keeperは、あらゆる規模の組織に最適な一流のパスワードマネージャーとして認知されており、使いやすさと迅速な展開を実現するよう設計されています。Keeperの広範な[ドキュメントポータル](#)から詳細な手順やシステムのベストプラクティスを手入手できるため、ウィリアムズ・レーシングの管理者はシステムを最大限に利用することができました。エンドユーザー向けには、詳細な[製品ガイド](#)と[トレーニング動画](#)もあり、ユーザーによる導入が促進されました。

ロール単位のアクセス制御 (RBAC): Keeperは粒度の細かい共有制限機能を提供するため、管理者は[ロール単位のアクセス制御 \(RBAC\)](#) を活用して、ウィリアムズ・レーシングの組織全体におけるセキュリティポリシーおよびコンプライアンス準拠を確保できます。組織内の役割を設定することで、管理者のプロビジョニング作業が合理化され、さらに特定の連続のルールを利用して最小特権アクセスを維持し、チームのセキュリティ体制を強化できます。

組織への影響

Keeperの導入はウィリアムズ・レーシングに劇的な影響を与え、組織全体の安全性と効率性が改善されました。主な影響には、以下が挙げられます。

安全性の改善とデータの保護: Keeperの高度なセキュリティアーキテクチャにより、きわめて機密性の高いデータの安全を保護するウィリアムズ・レーシングの能力が向上しました。ITチームは、パスワードの使用状況やパスワードの複雑さを完全に可視化して、あらゆるセキュリティ脅威を監視できるため、すべての認証情報を不正アクセスから保護できます。

データが必要です。サイバーセキュリティが必要です。ITインフラストラクチャが必要です。そして、従業員が安全に作業できる環境を整える必要があります。これは、従業員が英国にいても世界のどこにいても変わりません

ジェームズ・ヴォウルズ | ウィリアムズ・レーシング、
チーム代表

業務効率の向上: ウィリアムズ・レーシングは、パスワード管理を一元化しアクセス制御を合理化することで、認証情報の管理に要する時間を大幅に短縮しました。これにより、エンジニアや整備士、その他の担当者は、特にレース開催の週末にアクセスの問題による遅れなく、重要な作業に専念できるようになりました。

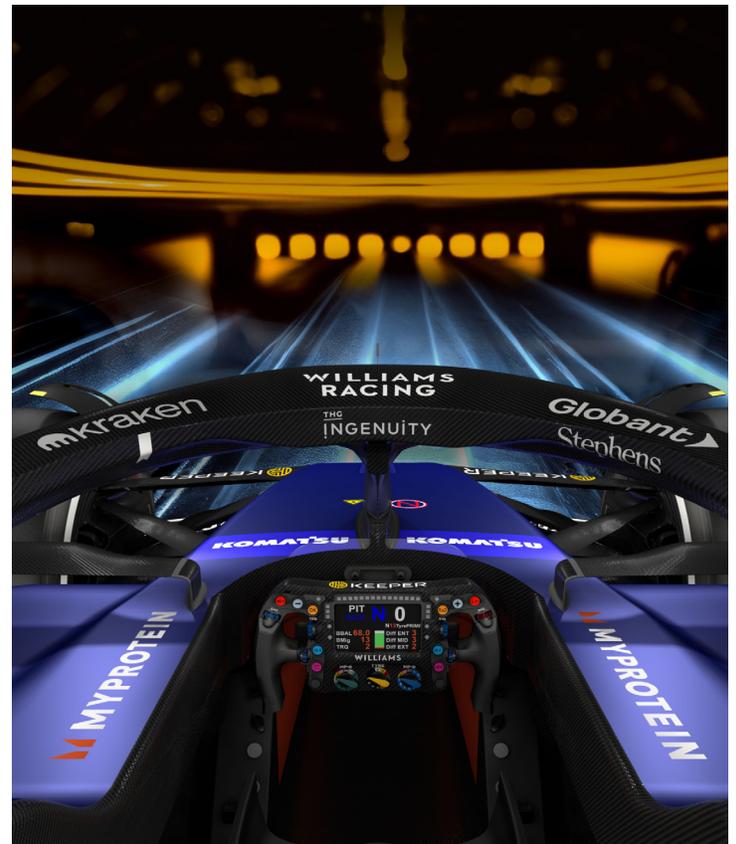
サイバー攻撃リスクの軽減: ウィリアムズ・レーシングは、強力なパスワード管理慣行と高度なセキュリティ機能を導入したことで、データ漏洩やサイバー攻撃のリスクを最小限に抑えることができました。Keeperのソリューションをリスクの高い地域でもすべてのデバイスにシームレスに統合したことで、世界を移動するチームにさらなる安心をもたらしています。

ユーザーからのポジティブなフィードバックと導入: Keeperの使いやすさと直感的なインターフェースにより、技術者ではないスタッフを含む従業員の間で高い導入率を実現しました。その結果、パスワードに関連したヘルプデスクチケットが大幅に減少し、より安全で体系的なパスワード管理のアプローチが可能になりました。

技術者(IT関連)ではないユーザー向けの使いやすさ: Keeperのユーザーフレンドリーなインターフェースとブラウザ拡張機能は、マーケティング、財務、物流部門の技術者(IT関連)ではない従業員にとってもシンプルなパスワード管理を提供します。これにより、あらゆる部門でのユーザーによる導入が改善され、1秒1秒が重要となりプレッシャーが高まるレース開催の週末のあつれきを軽減しました。

Keeperの稼働後には、内蔵機能を使用してパスワード強度の評価、異なるユーザーや異なるデジタル保管庫間でのパスワードの使い回しについての評価を行い、報告書をまとめ、インフラストラクチャ全体で使い回されているパスワードを削除するプロジェクトを実行できました

ハリー・ウィルソン | ウィリアムズ・レーシング、
情報セキュリティ責任者



Keeperパスワードマネージャー

ほとんどの企業は、従業員のパスワード習慣への可視性を制限しており、これがサイバーリスクを増大させます。パスワード習慣は、パスワードの使用とコンプライアンスに関する重要な情報なしに改善することはできません。Keeperは、究極のセキュリティ、可視性、および制御を提供することで、これを解決します。

データは、Keeperのゼロ知識セキュリティアーキテクチャと、世界クラスの暗号化で保護されます。ゼロ知識とは、情報を暗号化および復号化するのに使用される暗号鍵とマスターパスワードを知っているのがユーザーのみで、それらにアクセスできるのもユーザーのみであることを意味します。

Keeperは、直感的に操作でき、ビジネスの規模に関係なく簡単に導入できます。KeeperはActive DirectoryとLDAPサーバーとの統合が可能で、プロビジョニングとオンボーディングが効率化されます。[Keeper SSOコネク](#)®は既存のSSOソリューションと統合し、FedRAMPおよびStateRAMPの認証を受けています。

Keeperは、あらゆる規模の組織に対応できる設計です。役割ベースの権限、チーム共有、部門監査、および委任管理などの機能が、組織が成長するにつれそれらをサポートします。[Keeper Commander](#)は、現在と将来のシステムに統合するための堅牢なAPIを提供します。

ビジネスユースケース: Keeperパスワードマネージャー

- パスワード関連のデータ漏洩やサイバー攻撃を防止
- パスキー対応で手間のかからない認証を実現
- コンプライアンスを強化
- 従業員の生産性を向上
- パスワードポリシーと手続きの遵守を確保
- ヘルプデスクのコストを削減
- 迅速な安全性実現でトレーニングを最小限に
- 従業員のセキュリティ意識と行動を改善

Keeperについて

Keeper Securityは、世界中の人々や組織のためにゼロトラスト特権アクセス管理によるサイバーセキュリティ変革を行っています。Keeperの使いやすいサイバーセキュリティソリューションはゼロトラストとゼロ知識のセキュリティによってあらゆるデバイスであらゆるユーザーを保護します。数百万人のユーザーと数千の組織に信頼されているKeeperは、パスワード管理、シークレット管理、特権アクセス、安全なリモートアクセス、暗号化メッセージ送信におけるリーダーです。詳しくはKeeperSecurity.comをご覧ください。

Keeperは、世界中の数千もの企業、数百万人のユーザーによって信頼され愛されています。



G2
エンタープライズリーダー



PCMag
エディターズチョイス



App Store
トップ評価の生産性



Google Play
インストール数100万
以上