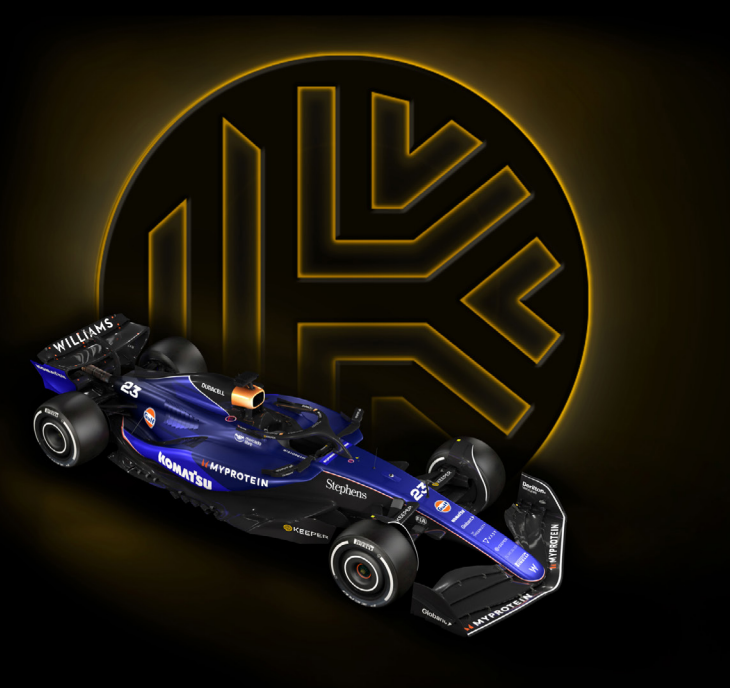
KEEPER | WILLIAMS RACING

OFFICIAL PARTNER



Case Study

Williams Racing Fortifies Global Operations With Keeper's Zero-Trust Cybersecurity Platform

Background

Williams Racing is one of the most historic and successful teams in Formula 1, founded in 1977 by Sir Frank Williams and Patrick Head. Based in Grove, Oxfordshire, UK, the team has won nine Constructors' Championships and seven Drivers' Championships, making it one of the most decorated teams in F1 history. Known for its engineering excellence and competitive spirit, Williams is focused on innovation and performance, leveraging cutting-edge technology and data analytics to reach the front of the grid in the ever-evolving world of motorsport.

Industry
Motorsports

Employees
1,000+

Solutions
Keeper Password Manager

- Enterprise

The Challenge

In the world of Formula 1, technology and data are essential for maintaining a competitive advantage. Williams Racing, one of the oldest and most renowned F1 teams, faces an immense challenge in protecting its valuable intellectual property. With a globally distributed workforce utilizing hundreds of devices during races around the globe, as well as sophisticated day-to-day operations, the team must ensure that their sensitive information remains secure from cyber threats while maintaining seamless workflows.

Formula 1 cars are high-tech assets for the team, refined by constant engineering. Vehicle development is driven by data, and teams collect an increasingly large amount of new data with each race, including telemetry data and video footage. Williams Racing gathers terabytes of data each race weekend, which is then transferred, stored and analyzed by the team to be leveraged to refine strategies for upcoming races and the years to come. With the increased reliance on data, along with the sheer volume, storing and accessing it in a secure way is crucial to ensure all highly confidential intellectual property is protected.

Equally important is the security of financial and commercial data, including the allocation of cost-cap budgets, which are directly linked to performance. This sensitive information plays a critical role in maintaining a competitive edge, ensuring compliance with regulations and protecting strategic decisions.

The mobile nature of Formula 1, in which teams travel to 21 different countries over the 10-month season — some of which are prone to heightened cybersecurity threats — adds another layer of complexity. Securing a distributed workforce while ensuring uninterrupted access to essential data is a nonnegotiable priority for Williams Racing.

> **Cybersecurity, your threats and how you protect yourself is of fundamental importance. And it's not spoken about often enough at all.**
>
> **James Vowles | Team Principal, Williams Racing**

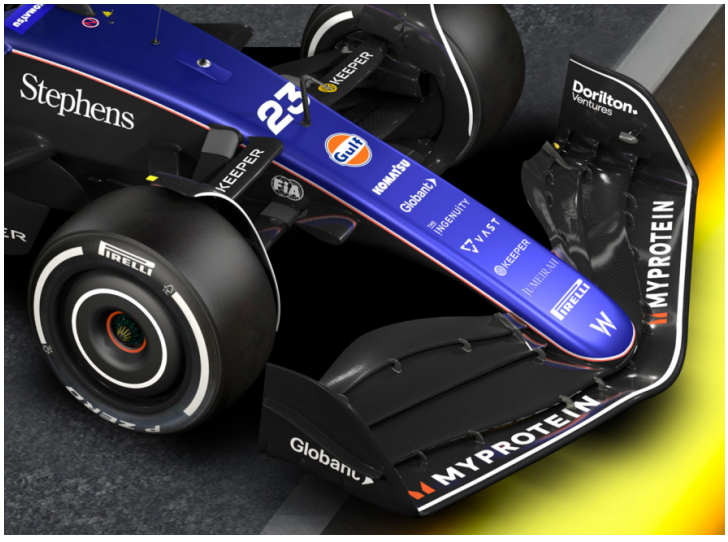
Without a robust password management solution in place, the team risked exposing its systems to data breaches, which could paralyze operations or see sensitive information fall into the wrong hands. The challenges with previous password management methods included:

Password Management Practices: With hundreds of team members accessing critical data on race strategies, car designs and performance metrics around the globe, this increased the risk of unauthorized access to sensitive information and led to limited visibility and access control.

Limited Visibility and Access Control: The Information Technology (IT) team struggled to maintain control over password access and usage, particularly when it came to managing access for a large number of remote workers. Decommissioning users and transferring credentials securely when team members left the organization was especially difficult and time-consuming, resulting in gaps in security along with wasted resources.

Inconsistent Security Across Devices: As the team traveled to races around the world, including high-risk cybersecurity regions, the lack of a unified password management solution created inconsistencies in how devices were protected. This exposed the team to potential breaches while operating from a variety of different countries.

> **We need an infrastructure that works across every location, whether it's the UK or countries with elevated cybersecurity risks. Keeper allows us to confidently give the team access to critical systems, no matter where they are.**
>
> **Harry Wilson | Head of Information Security, Williams Racing**



The Keeper Solution

Williams Racing turned to Keeper Security for a reliable and secure password management solution. Keeper's zero-trust and zero-knowledge architecture ensured the highest level of security for the team's data, allowing Williams to safeguard its sensitive records. The solution delivered key benefits in several areas, including:

Centralized Password Management: Keeper provided Williams Racing with a single, secure platform for storing and managing passwords. This eliminated the need for risky practices and ensured that all credentials were protected with Keeper's zero-trust and zero-knowledge architecture.

Seamless Integration with Existing Systems: Keeper integrated easily with Williams Racing's existing Identity Provider (IdP), allowing for automated provisioning and deprovisioning of user accounts. This integration ensures that credentials are securely transferred when staff leave or join the team, reducing the burden on IT and eliminating potential security gaps.

Advanced Security Features: Keeper's robust security measures, including Multi-Factor Authentication (MFA) and end-to-end encryption, ensure that sensitive internal communications and data are protected. The ability to securely and seamlessly share credentials among team members without exposing sensitive data adds an extra layer of protection.

User Adoption and Training: Keeper is recognized as the leading password manager for organizations of all sizes and is designed to be easy to use and quick to deploy. Keeper's extensive documentation portal provides detailed instructions and system best practices to help administrators get the most out of their deployment. For end-users, detailed product guides and training videos drive high end-user adoption.

Additionally, Keeper's award-winning User Interface (UI) provides an intuitive and accessible platform that is easy for non-technical employees to understand and adopt. Keeper also supports cross-platform use on Windows, Mac, Linux, iOS and Android, ensuring that the solution works seamlessly no matter the platform or device.

Role-Based Access Controls (RBAC): Keeper provides granular sharing enforcement for administrators to leverage Role-Based Access Controls (RBAC) that ensure organization-wide security policies are adhered to and compliance is met. Designating roles within the organization streamlines provisioning for administrators and allows for specific rule sets to be leveraged to maintain least privilege access and increase the organization's security posture.

Organization Impact

The deployment of Keeper had a transformative effect on Williams Racing, improving both security and efficiency across the organization. The key impacts include:

Increased Security and Data Protection: Keeper's robust security architecture improved Williams Racing's ability to safeguard its highly sensitive data. The IT team now has full visibility into password usage and password complexity and can monitor for any security threats, ensuring that all credentials are protected from unauthorized access.

> **We need data. We need cybersecurity. We need IT infrastructure. And we need the ability for people to work in a safe environment. And that's irrespective of whether they are here in the United Kingdom or anywhere else in the world.**
>
> **James Vowles | Team Principal, Williams Racing**

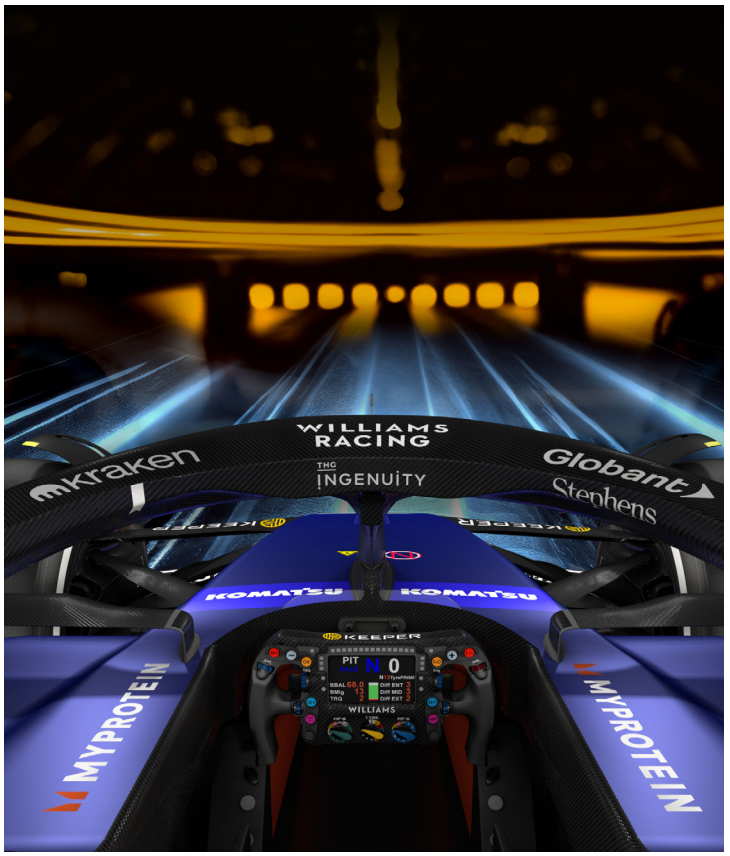
Improved Operational Efficiency: By centralizing password management and streamlining access controls, Williams Racing significantly reduced the time spent managing credentials. This allowed engineers, mechanics and other personnel to focus on their core tasks without delays caused by access issues – particularly during race weekends.

Reduced Risk of Cyber Attacks: With strong password management practices and advanced security features in place, Williams Racing minimized the risk of a data breach or cyber attack. The seamless integration of Keeper's solution across all devices, even in high-risk regions, provides the team with an additional layer of confidence as they travel globally.

Positive Feedback and User Adoption: Keeper's ease of use and intuitive interface led to a high adoption rate among team members, including non-technical staff. As a result, the organization saw a significant reduction in password-related help desk tickets and a more secure, organized approach to password management.

Enhanced Usability for Non-Technical Staff: Keeper's user-friendly interface and browser extension simplified password management for non-technical teams like marketing, finance and logistics. This improved user adoption across departments and reduced friction during high-pressure race weekends, when every second counts.

> **Once we had Keeper up and running, we were able to use the built-in capability to assess password strength, password reuse across different users and different vaults, to report on that... and run a project to remove any reused passwords across our infrastructure.**
>
> **Harry Wilson | Head of Information Security, Williams Racing**



Keeper Password Manager

Most businesses have limited visibility into the password practices of their employees, which greatly increases cyber risk. Password hygiene cannot be improved without critical information regarding password usage and compliance. Keeper solves this by providing ultimate security, visibility and control.

Data is protected with Keeper's zero-knowledge security architecture and world-class encryption. Zero-knowledge means that only the user has knowledge of and access to their master password and the encryption key that is used to encrypt and decrypt their information.

Keeper is intuitive and easy to deploy, regardless of the size of a business. Keeper integrates with Active Directory and LDAP servers, which streamline provisioning and onboarding. Keeper SSO Connect® integrates into existing SSO solutions and is FedRAMP and StateRAMP Authorized.

Keeper is designed to scale for any sized organization. Features such as role-based permissions, team sharing, departmental auditing and delegated administration, support organizations as they grow. Keeper Commander provides robust APIs to integrate into current and future systems.

Business Use Cases: Keeper Password Manager

- Prevent password-related data breaches and cyber attacks
- Support passkeys for effortless authentication
- Strengthen compliance
- Boost employee productivity
- Enforce password policies and procedures
- Reduce help desk costs
- Minimize training with fast time-to-security
- Improve employee security awareness and behavior

About Keeper

Keeper Security is transforming cybersecurity for people and organizations around the world with next-generation privileged access management. Keeper's easy-to-use cybersecurity solutions are built with zero-trust and zero-knowledge security to protect every user on every device. Trusted by millions of individuals and thousands of organizations, Keeper is the leader for password management, secrets management, privileged access, secure remote access and encrypted messaging. Learn more at KeeperSecurity.com.

Keeper is trusted and loved by thousands of companies and millions of people globally.

G2
Enterprise Leader

PCMag
Editor's Choice

App Store
Top-Rated Productivity

Google Play
Over 10 Million Installs