ATLASSIAN Williams F1 TEAM | KEEPER OFFICIAL PARTNER

CASE STUDY

Atlassian Williams F1 Team Keeps Sensitive Data Protected From Factory to Pit Lane

Background

Atlassian Williams F1 Team is one of the most historic 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 – among the most decorated teams in Formula 1 history. Known for its engineering excellence and competitive spirit, Williams focuses on innovation and performance, leveraging cutting-edge technology and data analytics to compete in the fast-changing world of motorsport.

Industry
Motorsports

Employees
1,000+

Solution
Keeper Enterprise Password Manager

The Challenge

Formula 1 is the most data-intensive sport on the planet, making it a high-value target for cyber attacks. Atlassian Williams F1 Team generates upwards of 1TB of telemetry, aerodynamic and simulation data every race weekend, with over 400 sensors on each car feeding 30,000 data channels live to engineers at the circuit and back at Grove simultaneously. The credentials protecting access to that data can carry the same strategic value as the data itself.

> **"F1 is a team sport — without all the teams working together on the same task, nothing works. We don't want security to be the blocker. People need to access what they need, when they need it."**
>
> **Chris Hicks | Senior Information Security Engineer, Atlassian Williams F1 Team**

Around 1,200 personnel work across the entire organisation - from the wind tunnel to trackside race operations. Each requires precise, role-appropriate access throughout a season spanning more than 20 countries. Every pound spent is governed by Formula 1's cost cap, which limits how much teams can invest in personnel, equipment and operations each season. That means security spending is weighed directly against performance-driving investments in the car itself.

"It's a real conversation weighing the purchase of a security tool versus a new front wing or a new mechanical engineer. We have to prove demonstrable value from the tool when we put it forward."

Chris Hicks | Senior Information Security Engineer, Atlassian Williams F1 Team

© 2026 Keeper Security, Inc.

The Keeper Solution

Atlassian Williams F1 Team deployed Keeper's Enterprise Password Manager alongside BreachWatch®, centralizing credential management around two priorities: secure collaboration across every team and function, and best-in-class encryption built for the threats of today and tomorrow.

Collaboration: Sharing at the Speed of F1
Keeper's shared folders and role-based permissions ensure personnel are automatically provisioned with exactly the credentials they need to succeed. One-Time Share provides contractors and third parties with time-limited access that expires automatically, requiring no manual intervention. Keeper is accessible across all managed browsers, devices and operating systems, ensuring users can access the credentials they need when and where they need them. From the trackside team to the marketing team, Keeper reduces friction for users.

> **"They're generated entirely in Keeper and applied automatically, recognizing the site and autofilling in an instant."**
>
> **James Yexley | Social Media Executive, Atlassian Williams F1 Team**

Encryption: Protection Built for High-Value Data
Keeper's **zero-knowledge, zero-trust architecture** means encryption keys are generated client-side and never stored on Keeper's servers. Elliptic-Curve Cryptography, **AES-256-bit encryption** and PBKDF2 are layered across the vault, folder and record levels, with MFA and biometric authentication enforced across all systems.

> **"It would take a cybercriminal over 2,000 years to decrypt the encrypted data. The keys are generated client-side with Atlassian Williams F1 Team. We store ones and zeros. That's it."**
>
> **Darren Guccione | CEO and Co-Founder, Keeper Security**

Keeper also layers in quantum-resistant encryption using the **Kyber algorithm** to defend against the "harvest now, decrypt later" threat, where adversaries store encrypted data today to decrypt it once quantum computing becomes viable.

"In F1, you've always got to be thinking about the next regulation cycle. It's great to see Keeper taking that same philosophy of thinking down the line about how to protect us from what we know is coming next."

Chris Hicks | Senior Information Security Engineer, Atlassian Williams F1 Team

© 2026 Keeper Security, Inc.

Organization Impact

Keeper gives teams across Williams immediate, self-service access to the credentials they need, reducing IT support overhead and freeing up the team to focus on higher-value work. With provisioning and deprovisioning handled automatically, the IT team spends less time on routine access requests and more time on the technical priorities that move the team forward.

> **"When teams get rolled into Keeper, they feel empowered rather than needing to contact the service desk. That frees up the support team for the crucial jobs that make an important difference to the car."**
>
> **Chris Hicks | Senior Information Security Engineer, Atlassian Williams F1 Team**

Race Weekend Performance
Trackside, faster infrastructure setup means more time for data analysis and race strategy — exactly where marginal gains are made. Engineers arriving at a circuit can bring systems online quickly and confidently, knowing every credential they need is immediately at hand.

"If the guys at the track get the infrastructure up sooner, that time goes to engineers developing race strategies and doing the data analysis earlier. Those split-second differences make a huge difference on a race weekend."

Chris Hicks | Senior Information Security Engineer, Atlassian Williams F1 Team

Global Security Confidence
Whether the team is at Grove or trackside on the other side of the world, Keeper delivers consistent, policy-compliant access across every country, network and device. With BreachWatch continuously monitoring the dark web and zero-knowledge encryption protecting every credential, Williams has the security foundation to compete without compromise.

> **"Credential management is no longer where the room for improvement sits."**
>
> **Chris Hicks | Senior Information Security Engineer, Atlassian Williams F1 Team**

A Secure Foundation for Every Team
The impact of Keeper extends well beyond IT. Across Williams, personnel in roles as varied as guest experience, social media, travel administration and cost engineering describe the same fundamental benefit: a single, secure and organized place to manage every credential they rely on. Security has become something people notice because it works, not because it gets in the way.

"Security is hugely important in Formula One. We deal with a lot of customer data – we want to make sure it's in one centralised source of truth, protected through Keeper."

Tom Iverson | Senior HQ Guest Experience Manager, Atlassian Williams F1 Team

© 2026 Keeper Security, Inc.

Keeper Password Manager

Most businesses have limited visibility into employees' password practices, which can significantly increase cyber risk. Cyber 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, quantum-resistant encryption. Zero-knowledge means only the user knows and has access to their master password and the encryption key used to encrypt and decrypt their information.

Keeper is intuitive and easy to deploy, regardless of business size. Keeper integrates with Active Directory and LDAP servers, which streamlines provisioning and onboarding. **Keeper SSO Connect®** integrates into existing SSO solutions and is FedRAMP High Certified and GovRAMP High Authorized.

Keeper is designed to scale for organizations of any size. Features such as role-based permissions, team sharing, departmental auditing and delegated administration support organizations as they grow. **Keeper Commander** provides robust APIs for integration with current and future systems.

Business Use Cases: Keeper Password Manager

- Prevent credential-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 one of the fastest-growing cybersecurity software companies, protecting thousands of organizations and millions of people in over 150 countries. Keeper is a pioneer of zero-knowledge and zero-trust security built for any IT environment. Its core offering, KeeperPAM®, is an AI-enabled, cloud-native platform that protects all users, devices and infrastructure from cyber attacks. Recognized for its innovation in the Gartner Magic Quadrant for Privileged Access Management (PAM), Keeper secures passwords and passkeys, infrastructure secrets, remote connections and endpoints with role-based enforcement policies, least privilege and just-in-time access.

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

Gartner

Keeper Security® was recognized in 2026 as the second fastest-growing security software company globally.

Cybersecurity Stars Awards 2026
AI Security Innovator of the Year, Best Privileged Access Management Platform for Enterprises.

Cybersecurity Excellence Awards
Privileged Access Management.

Global InfoSec Awards
AI-Powered Cybersecurity Solution, Cybersecurity Company, Privileged Access Management (PAM)

Globee Awards 2026
Cybersecurity Silver Winner

© 2026 Keeper Security, Inc.