ATLASSIAN Williams F1 TEAM | KEEPER OFFICIAL PARTNER

Case Study

Atlassian Williams F1 Team Secures Critical Access to Privileged Systems With KeeperPAM®

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, making it one of 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 at the front of the grid in the fast-changing world of motorsport.

Industry
Motorsports

Employees
1,000+

Solution
KeeperPAM

The Challenge

In Formula 1, safeguarding sensitive performance data is vital to maintaining a competitive edge. For Atlassian Williams F1 Team, the challenge is protecting privileged access across a global workforce operating hundreds of devices during high-pressure race weekends, as well as regular business operations outside of race weekends. With critical systems in use on multiple continents and in varied network environments, the team needs to keep its most valuable information secure while ensuring operations run at peak speed and critical data remains protected.

> **"Nowadays, it's fundamental to have a partner that helps us protect and safeguard all of the extremely confidential data that we produce on the track."**
>
> **Carlos Sainz | Formula 1 Driver, Atlassian Williams F1 Team**

Operating across more than 20 countries each season, Williams relies on devices and credentials that travel constantly between continents. Security measures needed to remain effective regardless of location, network or endpoint, protecting the team whether they are at headquarters or connected to a temporary network trackside.

Managing this access presented its own challenges. Provisioning and deprovisioning credentials across numerous internal teams, functions, systems and geographies was both resource-intensive and time-consuming.

> **"Normally, a computer remains inside one building – but ours travel all over the world. Wherever we go, we have to ensure our technology remains secure."**
>
> **James Vowles | Team Principal, Atlassian Williams F1 Team**

The Keeper Solution

Atlassian Williams F1 Team partnered with Keeper Security to deploy KeeperPAM, a comprehensive zero-trust, zero-knowledge Privileged Access Management (PAM) platform. KeeperPAM's unified platform delivered the visibility, security and operational agility Williams requires to manage privileged access across a fast-moving, globally distributed workforce. The team needed an easy-to-deploy solution that would secure its sensitive data and allow them to closely monitor access.

Role-Based, Least-Privilege Access – KeeperPAM's fine-grained Role-Based Access Controls (RBAC) ensure each team member in the Technology, Innovation & Growth department has access only to the credentials, systems and data required for their role. By strictly limiting privileges, Williams reduces insider threats and minimises exposure to sensitive data.

Secure Privileged Credentials – Privileged credentials like passwords and passkeys are vaulted and secured within Keeper's zero-knowledge and zero-trust architecture. This eliminates risky storage practices, ensures credentials are never exposed in plaintext and protects sensitive logins no matter where in the world the team is competing.

> **"When a user signs up for Keeper, they realise right away what they were missing in their lives. With Keeper, they never have to fumble with passwords or worry about how to share information securely. Productivity increases significantly alongside security for every user because of how easy it is to use."**
>
> **Craig Lurey | CTO and Co-founder, Keeper Security**

Passwordless Access – Privileged session management capabilities allow Williams' security teams to grant access to sensitive systems without ever exposing credentials. With KeeperPAM, Williams can monitor, record and audit privileged activity in real time, providing full visibility and control.

Seamless Integration With Existing Systems – KeeperPAM integrates directly with Williams' identity provider for automated provisioning and deprovisioning of privileged accounts. This ensures immediate and accurate access changes when personnel join or leave the team, reducing administrative overhead and eliminating lingering access risks.

Best-in-Class Security - Keeper's zero-trust and zero-knowledge security architecture is unmatched in safeguarding information and mitigating the risk of a data breach. Keeper combines device-level Elliptic-Curve Cryptography (ECC) with multiple layers of encryption (at the vault, folder and record levels), multi-factor and biometric authentication and FIPS 140-3 validated AES 256-bit encryption, plus PBKDF2. Keeper is SOC2, ISO 27001, 27017 and 27018 compliant — with the longest-standing compliance in the industry — as well as FedRAMP and GovRAMP Authorised, PCI DSS certified and certified by TrustArc for privacy.

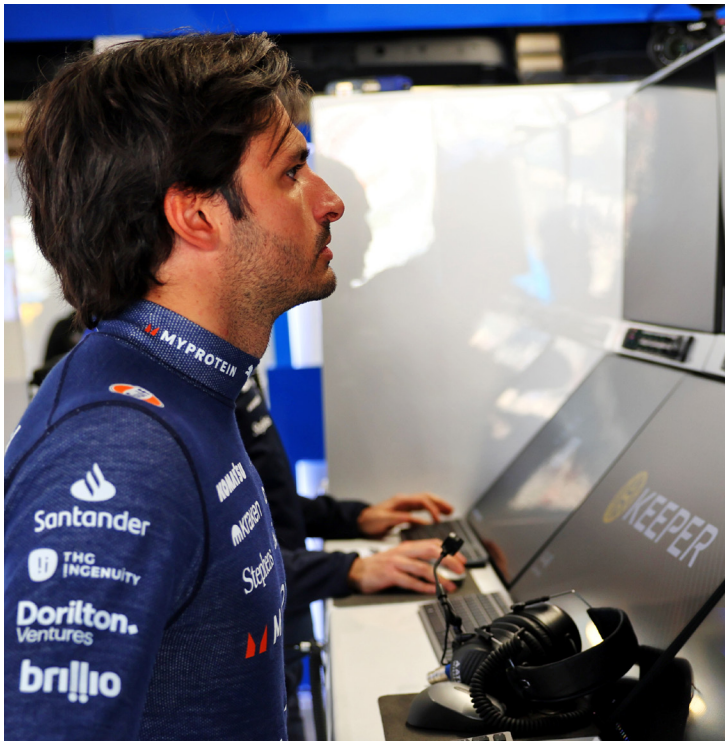
> **"Relative to other tools that we used previously, we found the Keeper onboarding process much quicker and easier."**
>
> **Harry Wilson | Former Head of Information Security, Atlassian Williams F1 Team**

Organisation Impact

Keeper transformed how Atlassian Williams F1 Team manages and protects privileged access. The team now enforces PAM policies for its most privileged users, securing credentials in a zero-knowledge vault and enabling fast, secure connections from anywhere in the world. With privileged activity monitored and access changes automated, Williams operates with greater speed, confidence and control.

> **"What's key to us with any partnership is that there's a synergy between both brands working together towards the same goal. And that absolutely exists with Keeper."**
>
> **James Vowles | Team Principal, Atlassian Williams F1 Team**

Enhanced Privileged Access Security and Visibility – KeeperPAM enforces least-privilege access and stores all credentials in an encrypted vault, and Williams can record screen and keyboard activity during remote sessions across all protocols, including SSH, RDP, VNC, databases and web browser sessions.



Stronger Credential Hygiene – With KeeperPAM deployed, Williams enforces Multi-Factor Authentication (MFA) on every system, ensures password strength across teams meets its standards and proactively identifies password reuse across users. By leveraging Keeper's auditing and reporting functionality, the organisation eliminates repeated credentials entirely, ensuring its systems stay secure against potential cyber threats.

High User Adoption and Reduced Support Tickets – KeeperPAM's intuitive design has driven strong adoption across the organisation, resulting in fewer password and access-related help desk requests for the IT team. The KeeperPAM documentation portal also proved useful in helping users familiarise themselves with the platform. The high adoption rate led to a smoother, more secure daily experience for both admins and end users alike.

> **"When you look at our trackside team, what Keeper has done really well is made the path of least resistance also the most secure path, which means our end users are happy, meaning I'm happy as well."**
>
> **Harry Wilson | Former Head of Information Security, Atlassian Williams F1 Team**

Global Operational Confidence – Keeper continues to enable Williams to operate securely worldwide, on any network and with any device, providing the highest level of protection whether the team is operating trackside, at headquarters or traveling to the next race.

KeeperPAM

KeeperPAM is a next-generation Privileged Access Management (PAM) platform that secures and manages access to critical resources, including servers, web apps, databases and workloads. Built on a zero-trust and zero-knowledge security architecture, KeeperPAM helps organisations of any size protect privileged accounts, enforce least privilege, secure remote infrastructure and meet compliance requirements, with unmatched ease of use and fast deployment.

Keeper is intuitive and easy to deploy, regardless of business size. KeeperPAM uses a zero-trust gateway service to access each environment. No firewall updates or ingress changes are needed, enabling seamless, secure access without complexity. With remote session capabilities, the user never has access to the credentials or SSH keys. Access to a resource can be time-limited, and credentials automatically rotate after access has been revoked, providing JIT access without ever exposing credentials.

Keeper is designed to scale for organisations of any size. KeeperPAM centralises access in a single User Interface (UI) across multiple cloud providers, on-premises workloads and client environments, enabling multi-cloud management.

Business Use Cases: KeeperPAM

- Control and monitor all privileged accounts
- Provide JIT access without exposing credentials
- Consolidate development tools in one platform with an intuitive UI
- Enable seamless management of cloud, hybrid and multi-cloud environments
- Record multi-protocol sessions with AI threat detection and automated session termination
- Automate password rotation
- Enforce MFA protection on every system
- Deploy seamlessly via web or desktop app with automated SCIM provisioning

Protect your organisation with Keeper

To learn more about how Keeper can protect your organisation with an easy-to-use platform, contact our sales team for a free trial or personalised demo.

About Keeper

Keeper Security is one of the fastest-growing cybersecurity software companies that protects thousands of organisations 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. Recognised 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.

Cybersecurity Excellence Award **Privileged Access Management**

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

Newsweek **#1 Cybersecurity Platform**

Enterprise Management Associates **KeeperPAM® recognised for product strength**

KeeperPAM® recognised in the 2025 Gartner Magic Quadrant™ for PAM