

ESTUDIO DE CASO

Atlassian Williams F1 Team mantiene los datos sensibles protegidos desde la fábrica hasta el pit lane



Antecedentes

Atlassian Williams F1 Team es uno de los equipos con más historia de la Fórmula 1, fundado en 1977 por Sir Frank Williams y Patrick Head. Con sede en Grove, Oxfordshire, Reino Unido, el equipo ha ganado nueve Campeonatos de Constructores y siete Campeonatos de Pilotos – entre los equipos más laureados de la historia de la Fórmula 1. Reconocido por su excelencia en ingeniería y su espíritu competitivo, Williams se centra en la innovación y el rendimiento, aprovechando tecnología de vanguardia y análisis de datos para competir en el cambiante mundo del automovilismo.

Industria

Deportes de motor

Empleados

1,000+

Soluciones

Keeper Enterprise
Password Manager



El desafío

La Fórmula 1 es el deporte con mayor uso intensivo de datos del planeta, lo que la convierte en un objetivo de alto valor para los ciberataques. Atlassian Williams F1 Team genera más de 1 TB de datos de telemetría, aerodinámica y simulación en cada fin de semana de carrera, con más de 400 sensores en cada monoplaza que envían 30 000 canales de datos en vivo a los ingenieros en el circuito y en Grove simultáneamente. Las credenciales que protegen el acceso a esos datos pueden tener el mismo valor estratégico que los propios datos.

“La F1 es un deporte de equipo — si no todos los equipos trabajan juntos en la misma tarea, nada funciona. No queremos que la seguridad sea el obstáculo. Las personas necesitan acceder a lo que necesitan, cuando lo necesitan”.

**Chris Hicks | Ingeniero sénior de seguridad de la información,
Atlassian Williams F1 Team**

Alrededor de 1,200 personas trabajan en toda la organización, desde el túnel de viento hasta las operaciones de carrera en pista. Cada una requiere un acceso preciso y adecuado a su rol durante una temporada que abarca más de 20 países. Cada libra esterlina gastada está sujeta al límite de costos de la Fórmula 1, que limita cuánto pueden invertir los equipos en personal, equipos y operaciones cada temporada. Esto significa que el gasto en seguridad se evalúa directamente frente a las inversiones destinadas a mejorar el rendimiento del propio monoplaza.

“Es una conversación real en la que se sopesa la compra de una herramienta de seguridad frente a un nuevo alerón delantero o un nuevo ingeniero mecánico. Debemos demostrar el valor tangible de la herramienta cuando la proponemos”.

**Chris Hicks | Ingeniero sénior de seguridad de la información,
Atlassian Williams F1 Team**



La solución Keeper

Atlassian Williams F1 Team implementó el Enterprise Password Manager de Keeper junto con BreachWatch®, centralizando la gestión de credenciales en torno a dos prioridades: la colaboración segura entre todos los equipos y funciones, y un cifrado de primer nivel diseñado para las amenazas de hoy y del mañana.

Colaboración: compartir a la velocidad de la F1

Las carpetas compartidas y los permisos basados en roles de Keeper garantizan que el personal sea aprovisionado automáticamente con exactamente las credenciales que necesita para desempeñar su trabajo. One-Time Share proporciona a los contratistas y terceros acceso por tiempo limitado que vence automáticamente, sin necesidad de intervención manual. Keeper es accesible en todos los navegadores, dispositivos y sistemas operativos administrados, lo que garantiza que los usuarios puedan acceder a las credenciales que necesitan cuando y donde las necesiten. Desde el equipo en pista hasta el equipo de marketing, Keeper reduce la fricción para los usuarios.

“Se generan completamente en Keeper y se aplican automáticamente, reconociendo el sitio y completando automáticamente en un instante.”

James Yexley | Ejecutivo de redes sociales,
Atlassian Williams F1 Team

Cifrado: protección diseñada para datos de alto valor

La **arquitectura de zero-knowledge y zero-trust** de Keeper significa que las claves de cifrado se generan del lado del cliente y nunca se almacenan en los servidores de Keeper. 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.

“Le tomaría a un ciberdelincuente más de 2,000 años descifrar los datos cifrados. Las claves se generan del lado del cliente con Atlassian Williams F1 Team. Nosotros almacenamos unos y ceros. Eso es todo.”

Darren Guccione | CEO y cofundador,
Keeper Security

Keeper también incorpora cifrado resistente a la computación cuántica mediante **el algoritmo Kyber** para defenderse de la amenaza de ‘recolectar ahora, descifrar después’, en la que los adversarios almacenan datos cifrados hoy para descifrarlos una vez que la computación cuántica sea viable.

“En la F1, siempre hay que estar pensando en el próximo ciclo de regulaciones. Es genial ver que Keeper adopta esa misma filosofía de pensar con anticipación sobre cómo protegernos de lo que sabemos que viene.”

Chris Hicks | Ingeniero sénior de seguridad de la información, Atlassian Williams F1 Team



Impacto en la organización

Keeper brinda a los equipos de Williams acceso inmediato y de autoservicio a las credenciales que necesitan, lo que reduce la carga de soporte de TI y libera al equipo para enfocarse en trabajo de mayor valor. Con el aprovisionamiento y desaprovisionamiento gestionados de forma automática, el equipo de TI dedica menos tiempo a las solicitudes de acceso rutinarias y más tiempo a las prioridades técnicas que impulsan al equipo.

“Cuando los equipos se incorporan a Keeper, se sienten empoderados en lugar de tener que contactar al servicio de asistencia. Eso libera al equipo de soporte para las tareas cruciales que realmente marcan la diferencia en el monoplaza”.

Chris Hicks | Ingeniero sénior de seguridad de la información, Atlassian Williams F1 Team

Rendimiento durante el fin de semana de carrera

En pista, una configuración de infraestructura más rápida significa más tiempo para el análisis de datos y la estrategia de carrera — que es exactamente donde se logran las ventajas marginales. Los ingenieros que llegan a un circuito pueden poner los sistemas en línea de forma rápida y segura, sabiendo que cada credencial que necesitan está al alcance de inmediato.

“Si los chicos en la pista levantan la infraestructura antes, ese tiempo se destina a los ingenieros para desarrollar estrategias de carrera y realizar el análisis de datos con mayor anticipación. Esas diferencias de fracciones de segundo marcan una gran diferencia durante el fin de semana de carrera.”

Chris Hicks | Ingeniero sénior de seguridad de la información, Atlassian Williams F1 Team



Confianza en la seguridad global

Ya sea que el equipo esté en Grove o en pista al otro lado del mundo, Keeper ofrece acceso coherente y conforme a las políticas en cada país, red y dispositivo. Con BreachWatch monitoreando continuamente la web oscura y el cifrado de conocimiento cero protegiendo cada credencial, Williams cuenta con la base de seguridad necesaria para competir sin compromisos.

“La gestión de credenciales ya no es donde se encuentra el margen de mejora”.

Chris Hicks | Ingeniero sénior de seguridad de la información, Atlassian Williams F1 Team

Una base segura para cada equipo

El impacto de Keeper va mucho más allá de TI. En Williams, el personal en roles tan variados como experiencia del cliente, redes sociales, administración de viajes e ingeniería de costos describe el mismo beneficio fundamental: un lugar único, seguro y organizado para gestionar cada credencial en la que confían. La seguridad se ha convertido en algo que las personas notan porque funciona, no porque entorpece el trabajo.

“La seguridad es de suma importancia en la Fórmula 1. Manejamos una gran cantidad de datos de clientes — queremos asegurarnos de que estén en una única fuente de información centralizada, protegida mediante Keeper”.

Tom Iverson | Gerente sénior de experiencia de invitados en la sede, Atlassian Williams F1 Team



La mayoría de las compañías tienen una visibilidad limitada sobre las prácticas de contraseñas de los empleados, lo que aumenta significativamente el riesgo cibernético. La higiene de contraseñas no se puede mejorar sin información crítica sobre el uso y cumplimiento de las contraseñas. Keeper resuelve esto al ofrecer máxima seguridad, visibilidad y control.

Los datos están protegidos con la arquitectura de seguridad de conocimiento cero de Keeper y un cifrado de clase mundial resistente a la computación cuántica. Conocimiento cero significa que solo el usuario conoce y tiene acceso a su contraseña maestra y a la clave de cifrado empleada para encriptar y descifrar su información.

Keeper es intuitivo y fácil de implementar, independientemente del tamaño del negocio. Keeper se integra con servidores Active Directory y LDAP, lo que agiliza el aprovisionamiento y la incorporación. **Keeper SSO Connect**® se integra en las soluciones de SSO existentes y cuenta con la certificación FedRAMP High y la autorización GovRAMP High.

Keeper está diseñado para escalar en organizaciones de cualquier tamaño. Funciones como permisos basadas en roles, uso compartido de equipos, auditoría departamental y administración delegada apoyan a las organizaciones a medida que crecen. **Keeper Commander** ofrece API sólidas para se integran en los sistemas actuales y futuros.

Casos de uso empresaria: KeeperPAM

- Prevenir brechas de datos y ciberataques relacionados con credenciales
- Admite claves de acceso para una autenticación sin esfuerzo
- Fortalecer el cumplimiento
- Aumentar la productividad de los empleados
- Hacer cumplir las políticas y procedimientos de contraseñas
- Reducir los costos de la mesa de ayuda
- Minimiza la capacitación con un rápido tiempo de seguridad
- Mejorar la conciencia y el comportamiento de los empleados en materia de seguridad

Acerca de Keeper

Keeper Security es una de las compañías de software de ciberseguridad de más rápido crecimiento que protege a miles de organizaciones y millones de personas en más de 150 países. Keeper es un pionero de la seguridad de conocimiento cero y confianza cero creada para cualquier entorno de TI. Su oferta principal, KeeperPAM®, es una plataforma nativa de la nube habilitada para IA que protege a todos los usuarios, dispositivos e infraestructura de los ataques cibernéticos. Reconocido por su innovación en el Gartner Magic Quadrant para la gestión de accesos privilegiados (PAM), Keeper protege contraseñas y claves de acceso, secretos de infraestructura, conexiones remotas y puntos finales con políticas de aplicación basadas en roles, privilegios mínimos y acceso justo a tiempo.

Miles de empresas y millones de personas de todo el mundo confían en Keeper.

Gartner

Keeper Security® fue reconocida en 2026 como la segunda empresa de software de seguridad de más rápido crecimiento a nivel mundial



Cybersecurity Stars Awards 2026

Innovador de seguridad de IA del año, mejor plataforma de gestión de acceso privilegiado para empresas



Premio a la Excelencia en Ciberseguridad

Gestión de acceso privilegiado



Global InfoSec Awards

Solución de ciberseguridad impulsada por IA, empresa de ciberseguridad, gestión de acceso privilegiado (PAM)



Globe Awards 2026

Ganador de plata en ciberseguridad