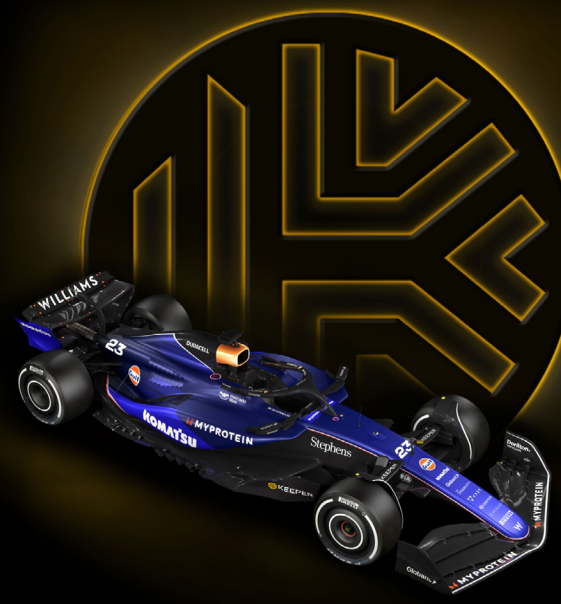
KEEPER | WILLIAMS RACING

OFFICIAL PARTNER

Estudio de Caso

Williams Racing refuerza sus operaciones globales con la plataforma de Seguridad cibernética de confianza cero de Keeper



Antecedentes

Williams Racing es uno de los equipos más históricos y exitosos en la Fórmula 1, fundado en 1977 por Sir Frank Williams y Patrick Head. El equipo Williams Racing, con sede en Grove, Oxfordshire, Reino Unido, ha ganado nueve campeonatos de constructores y siete campeonatos de pilotos, es uno de los equipos más laureados de la historia de la Fórmula 1. Conocido por su excelencia en ingeniería y espíritu competitivo, Williams se centra en la innovación y el rendimiento, aprovechando la tecnología de vanguardia y las analíticas de datos para llegar a la primera posición en el mundo en constante evolución de los deportes de motor.

Industria
Deportes de motor

Empleados
Más de 1000

Soluciones
Keeper Password Manager

- Empresarial

El reto

En el mundo de la Fórmula 1, la tecnología y los datos son esenciales para mantener una ventaja competitiva. Williams Racing, uno de los equipos de F1 más antiguos y renombrados, se enfrenta a un enorme desafío para proteger su valiosa propiedad intelectual. Con una fuerza laboral distribuida a nivel mundial que utiliza cientos de dispositivos durante las carreras en todo el mundo, así como operaciones diarias sofisticadas, el equipo debe garantizar que su información confidencial permanezca segura de las amenazas cibernéticas a la vez que mantiene flujos de trabajo sin interrupciones.

Los autos de Fórmula 1 son recursos de alta tecnología para el equipo, perfeccionados por ingeniería constante. El desarrollo de vehículos se basa en datos, y los equipos recopilan una cantidad cada vez mayor de datos nuevos en cada carrera, incluidos los datos de telemetría y las secuencias de video. Williams Racing recopila terabytes de datos cada fin de semana de carrera, que luego el equipo transfiere, almacena y analiza para utilizarlos en el perfeccionamiento de estrategias para las próximas carreras y los próximos años. Con la creciente dependencia de los datos, junto con el gran volumen, el almacenamiento y acceso a ellos de forma segura es crucial para garantizar la protección de toda la propiedad intelectual altamente confidencial.

Igualmente importante es la seguridad de los datos financieros y comerciales, incluida la asignación de presupuestos de gastos, que están directamente relacionados con el rendimiento. Esta información sensible desempeña un papel fundamental a la hora de mantener una ventaja competitiva, garantizar el cumplimiento de la normativa y proteger las decisiones estratégicas.

La naturaleza móvil de la Fórmula 1, en la que los equipos viajan a 21 países diferentes durante una temporada de 10 meses (algunos de los cuales son propensos a las amenazas de seguridad cibernética intensificadas), agrega otra capa de complejidad. Proteger una fuerza laboral distribuida a la vez que se garantiza el acceso ininterrumpido a los datos esenciales es una prioridad no negociable para Williams Racing.

> **La seguridad cibernética, sus amenazas y cómo se protege es de importancia fundamental. Y no se habla de ella con la suficiente frecuencia.**
>
> **James Vowles | Director de equipo, Williams Racing**

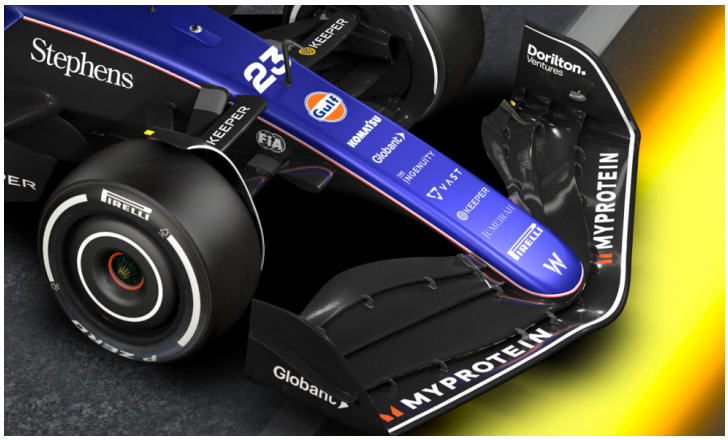
Sin una solución de gestión de contraseñas robusta, el equipo se arriesgaba a exponer sus sistemas a violaciones de datos, lo que podría paralizar las operaciones o hacer que información confidencial cayera en manos equivocadas. Los desafíos con los métodos de gestión de contraseñas anteriores incluían:

Prácticas de gestión de contraseñas: Con cientos de miembros de equipos que acceden a datos críticos sobre estrategias de carrera, diseños de autos y métricas de rendimiento en todo el mundo, esto aumentaba el riesgo de un acceso no autorizado a la información sensible y limitaba la visibilidad y el control de acceso.

Visibilidad y control de acceso limitados: El equipo de Tecnología de la Información (TI) enfrentaba dificultades para mantener el control sobre el acceso y el uso de las contraseñas, en particular cuando se trataba de gestionar el acceso de un gran número de trabajadores remotos. Cuando los miembros de un equipo abandonaban la organización, era especialmente difícil y lento dar de baja a los usuarios y transferir credenciales de forma segura, lo que provocaba fallos en la seguridad y el desperdicio de recursos.

Seguridad inconsistente en todos los dispositivos: A medida que el equipo viajaba a carreras por todo el mundo, incluidas las regiones de seguridad cibernética de alto riesgo, la falta de una solución unificada de gestión de contraseñas unificada creaba inconsistencias en la forma en que se protegían los dispositivos. Esto exponía el equipo a posibles violaciones de seguridad cuando operaba desde una variedad de países diferentes.

> **Necesitamos una infraestructura que funcione en todas las ubicaciones, ya sea en el Reino Unido o en países que presenten mayores riesgos en seguridad cibernética. Keeper nos permite ofrecer al equipo un acceso seguro a los sistemas críticos, estén donde estén.**
>
> **Harry Wilson | Jefe de seguridad de la información, Williams Racing**



La solución de Keeper

Williams Racing recurrió a Keeper Security en busca de una solución de gestión de contraseñas confiable y segura. La arquitectura de confianza cero y conocimiento cero de Keeper garantizaba el mayor nivel de seguridad para los datos del equipo, lo que permitía a Williams salvaguardar sus registros confidenciales. La solución ofreció beneficios clave en varias áreas, entre ellas:

Gestión de contraseñas centralizada: Keeper proporcionó a Williams Racing una plataforma única y segura para almacenar y gestionar contraseñas. Esto eliminó la necesidad de prácticas arriesgadas y garantizó que todas las credenciales estuvieran protegidas con la arquitectura de confianza cero y conocimiento cero de Keeper.

Integración perfecta con los sistemas existentes: Keeper se integraba fácilmente con el proveedor de identidades (IdP) existente de Williams Racing, lo que permitía el aprovisionamiento y desaprovisionamiento automatizados de las cuentas de usuario. Esta integración garantiza que las credenciales se transfieran de forma segura cuando el personal se va o se une al equipo, lo que reduce la carga de TI y elimina posibles fallos de seguridad.

Funciones de seguridad avanzadas: las sólidas medidas de seguridad de Keeper, incluida la autenticación multifactor (MFA) y el cifrado de extremo a extremo, garantiza que las comunicaciones y los datos internos sensibles estén protegidos. La posibilidad de compartir credenciales entre miembros de equipos de forma segura y sin problemas sin exponer datos sensibles añade una capa adicional de protección.

Adopción y formación de usuarios: Keeper es reconocido como el gestor de contraseñas líder para organizaciones de todos los tamaños y está diseñado para ser fácil de usar y rápido de implementar. El extenso portal de documentación de Keeper proporcionó a Williams Racing instrucciones detalladas y prácticas recomendadas del sistema para ayudar a sus administradores a aprovechar al máximo la implementación. Para los usuarios finales, las guías detalladas de productos y los videos de formación generaron una alta adopción de los usuarios.

Controles de acceso basados en roles (RBAC): Keeper ofrece una aplicación de uso compartido granular para que los administradores aprovechen los controles de acceso basados en roles (RBAC),garantizando el cumplimiento de las políticas de seguridad y se cumpla la conformidad en toda la organización de Williams Racing. Designar roles dentro de la organización facilita el aprovisionamiento para los administradores y permite aprovechar conjuntos de reglas específicos para mantener el acceso de privilegios mínimos y aumentar la postura de seguridad del equipo.

Impacto de la organización

La implementación de Keeper tuvo un efecto transformador en Williams Racing, mejorando tanto la seguridad como la eficiencia en toda la organización. Los impactos clave incluyen:

Mayor seguridad y protección de datos: la sólida arquitectura de seguridad de Keeper mejoró la capacidad de Williams Racing para proteger sus datos altamente sensibles. Ahora, el equipo de TI tiene visibilidad completa sobre el uso y la complejidad de las contraseñas y puede monitorear cualquier amenaza de seguridad, lo que garantiza que todas las credenciales estén protegidas del acceso no autorizado.

> **Necesitamos datos. Necesitamos seguridad cibernética. Necesitamos infraestructura de TI. Y necesitamos la capacidad de las personas para trabajar en un entorno seguro. Y eso es independientemente de si están aquí en el Reino Unido o en cualquier otro lugar del mundo.**
>
> **James Vowles | Director de equipo, Williams Racing**

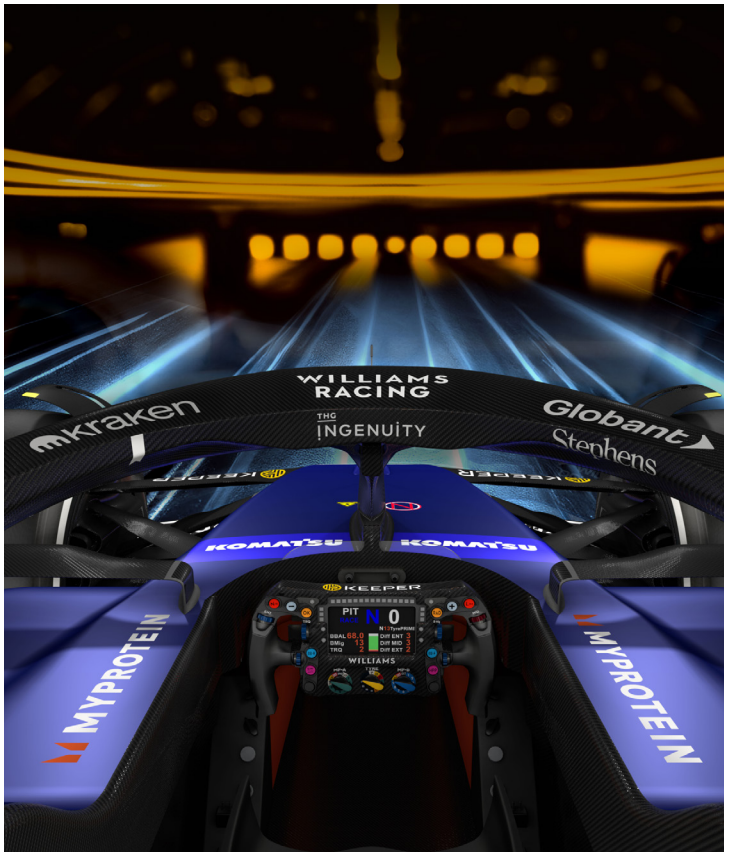
Eficiencia operativa mejorada: Al centralizar la gestión de contraseñas y optimizar los controles de acceso, Williams Racing redujo significativamente el tiempo dedicado a la gestión de credenciales. Esto permitió a los ingenieros, mecánicos y otro personal centrarse en sus tareas principales sin demoras causadas por problemas de acceso, especialmente durante los fines de semana de carreras.

Riesgo reducido de ataques cibernéticos: Con prácticas seguras de gestión de contraseñas y funciones de seguridad avanzadas, Williams Racing minimizó el riesgo de una violación de datos o un ataque cibernético. La integración perfecta de la solución de Keeper en todos los dispositivos, incluso en regiones de alto riesgo, ofrece al equipo una capa adicional de confianza a medida que viajan por todo el mundo.

Comentarios positivos y adopción por parte de los usuarios: la facilidad de uso y la interfaz intuitiva de Keeper dieron lugar a un elevado índice de adopción entre los miembros del equipo, incluido el personal no técnico. Como resultado, la organización observó una reducción significativa en los tickets de asistencia técnica relacionados con las contraseñas y un enfoque más seguro y organizado para la gestión de contraseñas.

Usabilidad mejorada para personal no técnico: la interfaz fácil de usar y la extensión del navegador de Keeper simplificaron la gestión de contraseñas para equipos no técnicos como marketing, finanzas y logística. Esto mejoró la adopción de usuarios en todos los departamentos y redujo la fricción durante los fines de semana de carreras de alta presión, cuando cada segundo cuenta.

> **Una vez que tuvimos Keeper en funcionamiento, pudimos utilizar la función integrada para evaluar la seguridad de las contraseñas, reutilizar contraseñas en diferentes usuarios y diferentes bóvedas, para informar al respecto... y ejecutar un proyecto para eliminar cualquier contraseña reutilizada en nuestra infraestructura.**
>
> **Harry Wilson | Jefe de seguridad de la información, Williams Racing**



Keeper Password Manager

La mayoría de las empresas tienen una visibilidad limitada de las prácticas que tienen sus empleados en torno a las contraseñas, lo que aumenta en gran medida los riesgos cibernéticos. La seguridad de las contraseñas no puede mejorarse sin una información crítica sobre su uso y su conformidad. Keeper resuelve esto al proporcionar la máxima seguridad, visibilidad y control.

Los datos se protegen en la arquitectura de seguridad de conocimiento cero de Keeper con un cifrado de primera categoría. El conocimiento cero significa que solo los usuarios saben y pueden acceder a su contraseña maestra y la clave de cifrado que se utiliza para cifrar y descifrar su información.

Keeper es intuitivo y fácil de implementar, independientemente del tamaño de la empresa. Keeper se integra con Active Directory y servidores LDAP, lo que agiliza el aprovisionamiento y la incorporación de usuarios. Keeper SSO Connect® se integra en las soluciones SSO existentes y está autorizado por FedRAMP y StateRAMP.

Keeper está diseñado para adaptarse a organizaciones de cualquier tamaño. Funciones como los permisos basados en roles, el uso compartido entre equipos, las auditorías de departamentos y la administración delegada respaldan a las organizaciones a medida que crecen. Keeper Commander ofrece API sólidas que se integran en sistemas actuales y futuros.

Casos de uso empresariales: Keeper Password Manager

- Evite las violaciones de datos relacionados con contraseñas y los ataques cibernéticos
- Admite claves de acceso para una autenticación sin esfuerzo
- Refuerza el cumplimiento
- Aumenta la productividad de los empleados
- Refuerza los procedimientos y las políticas de contraseñas
- Reduce los costos de asistencia técnica
- Minimice la formación con tiempo hasta seguridad
- Mejora el comportamiento y el conocimiento de los empleados en materia de seguridad

Acerca de Keeper

Keeper Security está transformando la seguridad cibernética para personas y organizaciones de todo el mundo con gestión del acceso privilegiado de nueva generación. Las soluciones de seguridad cibernética fáciles de usar de Keeper son construido con seguridad de confianza cero y conocimiento cero para proteger a todos los usuarios en todos los dispositivos. Confianza por millones de individuos y miles de organizaciones. Keeper es el líder en contraseñas gestión, gestión de secretos, privilegiados acceso, acceso remoto seguro y cifrado mensajería. Obtenga más información en KeeperSecurity.com.

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

G2
Líder empresarial

PCMag
Selección del editor

App Store
Máxima productividad

Google Play
Más de 10 millones de instalaciones