

El equipo Atlassian Williams F1 asegura el acceso crítico a sistemas privilegiados con KeeperPAM®



Antecedentes

El equipo Atlassian Williams F1 es uno de los equipos más históricos 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', lo que lo convierte en uno de los equipos más condecorados en 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 tecnología de vanguardia y análisis de datos para competir al frente de la parrilla en el mundo en rápida evolución del automovilismo.

Industria
Deportes de motor

Empleados
1,000+

Soluciones
KeeperPAM



El desafío

En Fórmula 1, proteger los datos confidenciales de rendimiento es vital para mantener una ventaja competitiva. Para el equipo Atlassian Williams F1, el desafío es proteger el acceso privilegiado a través de una fuerza laboral global que opera cientos de dispositivos durante fines de semana de carrera de alta presión, así como las operaciones comerciales regulares fuera de los fines de semana de carrera. Con sistemas críticos en uso en múltiples continentes y en entornos de red variados, el equipo debe mantener segura su información más valiosa cerciorando que las operaciones funcionen a máxima velocidad y los datos críticos permanezcan protegidos.

"Hoy en día, es fundamental contar con un socio que nos ayude a proteger y salvaguardar todos los datos extremadamente confidenciales que producimos en la pista."

Carlos Sainz | Piloto de Fórmula 1, Atlassian Williams F1 Team

Operando en más de 20 países cada temporada, Williams depende de dispositivos y credenciales que viajan constantemente entre continentes. Las medidas de seguridad deben seguir siendo efectivas independientemente de la ubicación, red o punto final, protegiendo al equipo tanto si estaba en la sede central como conectado a una red temporal en la vía.

Gestionar este acceso presentó sus propios desafíos. Aprovisionar y desaprovisionar credenciales en numerosos equipos internos, funciones, sistemas y geografías requería muchos recursos y mucho tiempo.

"Normalmente, una computadora permanece dentro de un solo edificio – pero la nuestra viaja por todo el mundo. Dondequiero que vayamos, tenemos que garantizar de que nuestra tecnología siga siendo segura."

James Vowles | Director de equipo, Atlassian Williams F1 Team



La solución Keeper

El equipo F1 de Atlassian Williams se asoció con Keeper Security para desplegar **KeeperPAM**, una plataforma integral de gestión de acceso privilegiado (PAM) de confianza cero y conocimiento cero. La plataforma unificada de KeeperPAM brindo la visibilidad, seguridad y agilidad operativa que Williams necesita para gestionar el acceso privilegiado a través de una fuerza laboral distribuida globalmente y de rápida evolución. El equipo necesitaba una solución fácil de desplegar que protegiera sus datos confidenciales y les permitiera monitorizar de cerca el acceso.

Acceso basado en roles y con menos privilegios – los **controles de acceso basados en roles (RBAC)** detallados de KeeperPAM garantizan que cada miembro del equipo en el departamento de Tecnología, Innovación y Crecimiento tenga acceso solo a las credenciales, sistemas y datos necesarios para su función. Al limitar estrictamente los privilegios, Williams reduce las amenazas internas y minimiza la exposición a datos confidenciales.

Credenciales Privilegiadas Seguras – Las credenciales privilegiadas como contraseñas y claves de acceso están abovedadas y aseguradas dentro de la **arquitectura de conocimiento cero y confianza cero** de Keeper. Esto elimina prácticas de almacenamiento arriesgadas, garantiza que las credenciales nunca se expongan en texto plano y protege los inicios de sesión confidenciales sin importar en qué parte del mundo esté compitiendo el equipo.

“Cuando un usuario se apunta a Keeper, se da cuenta inmediatamente de lo que se estaba perdiendo en su vida. Con Keeper, nunca tendrán que lidiar con contraseñas ni preocuparse de cómo compartir información de forma segura. La productividad aumenta significativamente junto con la seguridad para cada usuario debido a lo fácil que es de usar.”

Craig Lurey | CTO y cofundador, Keeper Security

Acceso sin contraseña – Las capacidades de gestión de sesiones privilegiadas permiten a los equipos de seguridad de Williams otorgar acceso a sistemas sensibles sin exponer nunca las credenciales. Con KeeperPAM, Williams puede monitorizar, registrar y auditar actividades privilegiadas en tiempo real, proporcionando visibilidad y control completos.

Integración Fluida con los Sistemas Existentes – KeeperPAM **se integra directamente** con el proveedor de identidad de Williams para la provisión y desaprovisionamiento automatizado de cuentas privilegiadas. Esto garantiza cambios de acceso inmediatos y precisos cuando el personal se une o abandona el equipo, reduciendo la carga administrativa y eliminando los riesgos de acceso persistentes.

La mejor seguridad de su clase – La arquitectura de seguridad de confianza cero y conocimiento cero de Keeper no tiene rival a la hora de proteger la información y mitigar el riesgo de una violación de datos. Keeper combina la Criptografía de curva elíptica (ECC) a nivel de dispositivo con **múltiples capas de cifrado** (a nivel bóveda, carpeta y registro), autenticación multifactor y biométrica y cifrado AES validado FIPS 140-3 de 256 bits, además de PBKDF2. Keeper **cumple con SOC 2, ISO 27001, 27017 y 27018** – con el cumplimiento más antiguo de la industria — así como está autorizado por FedRAMP y GovRAMP, certificado PCI DSS y certificado por TrustArc en cuanto a privacidad.

“En comparación con otras herramientas que usamos antes, encontramos que el proceso de incorporación de Keeper es mucho más rápido y fácil.”

Harry Wilson | Exdirector de Seguridad de la Información, Equipo de F1 Atlassian Williams





Impacto en la organización

Keeper transformó la forma en que el equipo F1 de Atlassian Williams gestiona y protege el acceso privilegiado. El equipo ahora aplica políticas PAM para sus usuarios más privilegiados, cerciorando las credenciales en una bóveda de conocimiento cero y permitiendo conexiones rápidas y seguras desde cualquier parte del mundo. Con la actividad privilegiada monitorizada y los cambios de acceso automatizados, Williams opera con mayor velocidad, confianza y control.

“Lo clave para nosotros en cualquier asociación es que existe una sinergia entre ambas marcas trabajando juntas hacia el mismo objetivo. Y eso existe absolutamente con Keeper.”

James Vowles | Director de equipo, Atlassian Williams F1 Team

Seguridad y visibilidad de acceso privilegiado mejoradas –

KeeperPAM aplica el acceso con privilegios mínimos y almacena todas las credenciales en una bóveda cifrada, y Williams puede registrar la actividad de pantalla y teclado durante sesiones remotas en todos los protocolos, incluidos SSH, RDP, VNC, base de datos y sesiones de navegador sitio web.



Higiene de credenciales más sólida – Con KeeperPAM desplegadas, Williams aplica la autenticación multifactor (MFA) en todos los sistemas, garantiza que la fuerza de contraseñas entre equipos cumpla con sus estándares e identifica proactivamente la reutilización de contraseñas entre usuarios. Al aprovechar la funcionalidad de auditoría e informes de Keeper, la organización elimina por completo las credenciales repetidas, cerciorando que sus sistemas se mantengan seguros frente a posibles amenazas ciberneticas.

Alta adopción por parte de los usuarios y reducción de tiquetes de soporte –

El diseño intuitivo de KeeperPAM impulsó una fuerte adopción en toda la organización, resultando en menos solicitudes de soporte de acceso y contraseñas por parte del equipo de TI. El **portal de documentación** de KeeperPAM también resultó útil para ayudar a los usuarios a familiarizarse con la plataforma. La alta tasa de adopción permitió una experiencia diaria más fluida y segura tanto para administradores como para usuarios finales.

“Si observamos a nuestro equipo de pista, lo que Keeper ha hecho realmente bien es convertir el camino de menor resistencia en el más seguro, lo que significa que nuestros usuarios finales están contentos, y yo también lo estoy”.

Harry Wilson | Exdirector de Seguridad de la Información, Equipo de F1 Atlassian Williams

Confianza Operativa Global – Keeper sigue permitiendo a Williams operar de forma segura en todo el mundo, en cualquier red y con cualquier dispositivo, brindando el más alto nivel de protección ya sea que el equipo esté operando en la pista, en la sede central o viajando a la próxima carrera.



KeeperPAM

KeeperPAM es una plataforma de gestión de acceso privilegiado (PAM) de próxima generación que protege y administra el acceso a recursos críticos, incluidos servidores, aplicaciones web, bases de datos y cargas de trabajo. Construido sobre una arquitectura de seguridad de cero confianza y conocimiento cero, KeeperPAM ayuda a organizaciones de cualquier tamaño a proteger cuentas privilegiadas, hacer cumplir el privilegio mínimo, proteger la infraestructura remota y cumplir con los requisitos de cumplimiento, con una facilidad de uso y una implementación rápida sin igual.

Keeper es intuitivo y fácil de implementar, independientemente del tamaño del negocio. KeeperPAM utiliza un servicio de puerta de enlace de confianza cero para acceder a cada entorno. No se necesitan actualizaciones del firewall ni cambios de entrada, lo que permite un acceso seguro y fluido sin complicaciones. Con las capacidades de sesión remota de Keeper, el usuario nunca tiene acceso a las credenciales o claves SSH. El acceso a un recurso puede tener un límite de tiempo y las credenciales rotan automáticamente después de revocar el acceso, lo que proporciona acceso JIT sin exponer nunca las credenciales.

Keeper está diseñado para escalar en organizaciones de cualquier tamaño. KeeperPAM centraliza el acceso en una única Interfaz de Usuario (UI) entre múltiples proveedores de nube, cargas de trabajo locales y entornos de cliente, permitiendo la gestión multi-nube.

Casos de uso empresarial: KeeperPAM

- Controlar y supervisar todas las cuentas privilegiadas
- Proporcionar acceso a JIT sin exponer las credenciales
- Consolide las herramientas de desarrollo en una plataforma con una interfaz de usuario intuitiva
- Permitir una gestión fluida de entornos de nube, híbridos y multinube
- Grabar sesiones multiprotocolo con detección de amenazas de IA y finalización automatizada de sesiones
- Automatizar la rotación de contraseñas
- Aplicar la protección MFA en todos los sistemas
- Desplegar sin problemas a través de la web o la aplicación de escritorio con aprovisionamiento SCIM automatizado

Protege su organización con Keeper

Para obtener más información sobre cómo Keeper puede proteger su organización con una plataforma fácil de usar, [póngase en contacto con nuestro equipo de ventas](#) para obtener una prueba gratuita o una demostración personalizada.

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.



Premio a la Excelencia en Ciberseguridad
Gestión de acceso privilegiado



Revista de defensa cibernética
Selección del editor - Gestión de acceso privilegiado (PAM)



Newsweek
Plataforma de Ciberseguridad #1



Asociados de gestión empresarial
KeeperPAM® reconocido por la resistencia del producto

Gartner

KeeperPAM® reconocido en el 2025 Gartner Magic Quadrant™ para PAM