

A equipa Atlassian Williams F1 garante o acesso crítico a sistemas privilegiados com o KeeperPAM®



Contexto

A Atlassian Williams F1 Team é uma das equipas mais históricas da Fórmula 1, fundada em 1977 por Sir Frank Williams e Patrick Head. Sediada em Grove, Oxfordshire, Reino Unido, a equipa conquistou nove Campeonatos de Construtores e sete Campeonatos de Pilotos, tornando-se uma das equipas mais premiadas da história da Fórmula 1. Conhecida pela sua excelência em engenharia e espírito competitivo, a Williams foca-se na inovação e no desempenho, aproveitando tecnologia de ponta e análises de dados para competir na frente da grelha no mundo em rápida mudança do desporto motorizado.

Indústria

Desportos Motorizados

Funcionários

1 000+

SOLUÇÕES

KeeperPAM



O Desafio

Na Fórmula 1, a proteção de dados de desempenho sensíveis é vital para manter uma vantagem competitiva. Para a equipa Atlassian Williams F1, o desafio é proteger o acesso privilegiado numa força de trabalho global que opera centenas de dispositivos durante fins de semana de corrida de alta pressão, bem como as operações comerciais regulares fora dos fins de semana de corrida. Com sistemas críticos em uso em múltiplos continentes e em ambientes de rede variados, a equipa precisa de manter a sua informação mais valiosa segura, garantindo ao mesmo tempo que as operações decorrem à velocidade máxima e que os dados críticos permanecem protegidos.

“Hoje em dia, é fundamental ter um parceiro que nos ajude a proteger e salvaguardar todos os dados extremamente confidenciais que produzimos na pista.”

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

Operando em mais de 20 países a cada temporada, a Williams depende de dispositivos e credenciais que viajam constantemente entre continentes. As medidas de segurança precisam de se manter eficazes independentemente da localização, rede ou dispositivo, protegendo a equipa, quer esteja na sede ou ligada a uma rede temporária na pista.

Gerir este acesso apresentou os seus próprios desafios. O aprovisionamento e o desprovisionamento de credenciais em diversas equipas internas, funções, sistemas e regiões geográficas eram processos que exigiam muitos recursos e que consumiam muito tempo.

“Normalmente, um computador permanece dentro de um único edifício – mas os nossos viajam por todo o mundo.” Onde quer que vamos, temos de garantir que a nossa tecnologia se mantém segura.”

James Vowles | Chefe de Equipa, Atlassian Williams F1 Team



A Solução Keeper

A equipa Atlassian Williams F1 fez uma parceria com a Keeper Security para implementar o **KeeperPAM**, uma plataforma abrangente de Gestão de Acesso Privilegiado (PAM) de confiança zero e conhecimento zero. A plataforma unificada do KeeperPAM forneceu a visibilidade, a segurança e a agilidade operacional de que a Williams precisa para gerenciar o acesso privilegiado em uma força de trabalho distribuída globalmente e em rápida evolução. A equipa precisava de uma solução fácil de implementar que protegesse os seus dados sensíveis e lhe permitisse monitorizar de perto o acesso.

Acesso baseado em função e privilégio mínimo – Os controles de acesso baseados em função (RBAC) refinados do KeeperPam garantem que cada membro da equipa no departamento de Tecnologia, Inovação & Growth tenha acesso apenas às credenciais, sistemas e dados necessários para a sua função. Ao limitar estritamente os privilégios, a Williams reduz as ameaças internas e minimiza a exposição a dados confidenciais.

Credenciais Privilegiadas Seguras – Credenciais privilegiadas como palavras-passe e chaves de acesso são guardadas e protegidas dentro da **arquitetura zero-knowledge e zero-trust** do Keeper. Isto elimina práticas de armazenamento arriscadas, garante que as credenciais nunca são expostas em texto não encriptado e protege os logins confidenciais, independentemente de onde a equipa está a competir no mundo.

“Quando um utilizador se inscreve no Keeper, percebe imediatamente o que estava a perder na sua vida. Com o Keeper, nunca têm de se preocupar com palavras-passe ou com a forma de partilhar informações com segurança. A produtividade aumenta significativamente, assim como a segurança para todos os utilizadores, devido à facilidade de utilização.”

Craig Lurey | Diretor de Tecnologia e Cofundador, Keeper Security

Acesso sem palavra-passe – As capacidades de gestão de sessões privilegiadas permitem às equipas de segurança da Williams conceder acesso a sistemas sensíveis sem nunca expor credenciais. Com o KeeperPAM, a Williams pode monitorizar, registar e auditar atividades privilegiadas em tempo real, proporcionando total visibilidade e controlo.

Integração Perfeita com os Sistemas Existentes – O KeeperPAM **integra-se diretamente** com o fornecedor de identidade da Williams para o provisionamento e desprovisionamento automatizado de contas privilegiadas. Isto garante alterações de acesso imediatas e precisas quando os colaboradores entram ou saem da equipa, reduzindo a sobrecarga administrativa e eliminando os riscos persistentes de acesso.

A melhor segurança da categoria – A arquitetura de segurança de confiança zero e conhecimento zero do Keeper é incomparável na proteção de informações e na mitigação do risco de uma violação de dados. O Keeper combina a Criptografia de Curva Elíptica (ECC) a nível do dispositivo com **várias camadas de encriptação (no cofre, pasta e níveis de registo), autenticação multifator e biométrica e encriptação AES** de 256 bits validada pelo FIPS 140-3, mais PBKDF2. O Keeper está em conformidade com **SOC 2, ISO 27001, 27017 e 27018** — com a conformidade mais antiga do setor — bem como FedRAMP e GovRamp Autorizado, certificado PCI DSS e certificado pela TrustArc para privacidade.

“Em comparação com outras ferramentas que utilizámos anteriormente, descobrimos que o processo de integração do Keeper é muito mais rápido e fácil.”

Harry Wilson | Ex-chefe de Segurança da Informação da equipa Atlassian Williams F1



Impacto na Organização

O Keeper transformou a forma como a Atlassian Williams F1 Team gere e protege o acesso privilegiado. A equipa agora aplica políticas de PAM para os seus utilizadores mais privilegiados, protegendo as credenciais num cofre de conhecimento zero e permitindo ligações rápidas e seguras de qualquer lugar do mundo. Com a atividade privilegiada monitorizada e as alterações de acesso automatizadas, a Williams opera com maior velocidade, confiança e controlo.

“O que é fundamental para nós em qualquer parceria é que haja sinergia entre as duas marcas a trabalharem em conjunto em prol do mesmo objetivo.”
E isso existe definitivamente com o Keeper.”

James Vowles | Chefe de Equipa, Atlassian Williams F1 Team

Segurança e visibilidade aprimoradas de acesso privilegiado –
O KeeperPAM impõe o acesso de privilégios mínimos e armazena todas as credenciais em um cofre criptografado, e Williams pode gravar a atividade da tela e do teclado durante sessões remotas em todos os protocolos, incluindo SSH, RDP, VNC, bancos de dados e sessões de navegador da Web.



Higiene Credencial Mais Forte – Com o KeeperPAM implementado, a Williams aplica a Autenticação Multifator (MFA) em todos os sistemas, garante que a força das palavras-passe entre as equipas cumpre os seus padrões e identifica proativamente a reutilização de palavras-passe entre os utilizadores. Ao tirar partido da funcionalidade de auditoria e reporte do Keeper, a organização elimina por completo credenciais repetidas, garantindo que os seus sistemas se mantêm seguros contra potenciais ameaças cibernéticas.

Alta adoção do usuário e redução de tickets de suporte – O design intuitivo do KeeperPAM levou a uma forte adoção em toda a organização, resultando em menos solicitações de help desk relacionadas a senhas e acesso para a equipe de TI. O [portal de documentação](#) do KeeperPAM também se mostrou útil para ajudar os usuários a se familiarizarem com a plataforma. A elevada taxa de adoção conduziu a uma experiência diária mais fácil e segura, tanto para os administradores como para os utilizadores finais.

“Quando olhas para a nossa equipa à beira da pista, o que o Keeper fez muito bem foi tornar o caminho de menor resistência também o caminho mais seguro, o que significa que os nossos utilizadores finais estão satisfeitos, ou seja, eu também estou feliz.”

Harry Wilson | Ex-chefe de Segurança da Informação da equipa Atlassian Williams F1

Confiança Operacional Global – A Keeper continua a permitir que a Williams opere de forma segura em todo o mundo, em qualquer rede e com qualquer dispositivo, proporcionando o mais alto nível de proteção, quer a equipa opere à beira da pista, na sede ou a viajar para a próxima corrida.



O KeeperPAM é uma plataforma de Gestão de Acesso Privilegiado (PAM) de próxima geração que protege e gere o acesso a recursos críticos, incluindo servidores, aplicações web, bases de dados e cargas de trabalho. Construído sobre uma arquitetura de segurança zero-trust e zero-knowledge, o KeeperPAM ajuda organizações de qualquer dimensão a proteger contas privilegiadas, aplicar o privilégio mínimo, proteger infraestruturas remotas e cumprir os requisitos de conformidade, com facilidade de utilização incomparável e implementação rápida.

O Keeper é intuitivo e fácil de implementar, independentemente da dimensão da empresa. O KeeperPAM utiliza um serviço de gateway de confiança zero para aceder a cada ambiente. Nenhuma atualização de firewall ou alterações de entrada são necessárias, permitindo um acesso contínuo e seguro sem complexidade. Com capacidades de sessão remota, o utilizador nunca tem acesso às credenciais ou chaves SSH. O acesso a um recurso pode ser limitado no tempo, e as credenciais rodam automaticamente após o acesso ter sido revogado, fornecendo acesso just-in-time sem nunca expor as credenciais.

O Keeper foi concebido para ser escalável para organizações de qualquer dimensão. O KeeperPAM centraliza o acesso numa única Interface de Utilizador (UI) entre múltiplos fornecedores de cloud, cargas de trabalho on-premises e ambientes de clientes, permitindo a gestão multi-cloud.

Casos de utilização comercial: KeeperPAM

- Controlar e monitorize todas as contas privilegiadas
- Forneça acesso JIT sem expor credenciais
- Consolide as ferramentas de desenvolvimento numa única plataforma com uma interface de utilizador intuitiva
- Permitir a gestão integrada de ambientes de cloud, híbridos e multi cloud
- Grave sessões multi protocolo com deteção de ameaças por IA e fecho automático de sessões
- Automatizar a rotação de palavra-passe
- Impor a proteção MFA em todos os sistemas
- Implemente facilmente através de aplicação web ou desktop com provisionamento SCIM automatizado

Proteja a sua organização com o Keeper

Para saber mais sobre como a Keeper pode proteger a sua organização com uma plataforma fácil de usar, [contacte a nossa equipa de vendas](#) para um teste gratuito ou demonstração personalizada.

Acerca do Keeper

A Keeper Security é uma das empresas de software de cibersegurança que mais rapidamente tem crescido, protegendo milhares de organizações e milhões de pessoas em mais de 150 países. A Keeper é pioneira em segurança de conhecimento zero e confiança zero, desenvolvida para qualquer ambiente de TI. A sua oferta principal, KeeperPAM®, é uma plataforma nativa da cloud habilitada por IA que protege todos os utilizadores, dispositivos e infraestruturas contra ataques cibernéticos. Reconhecido pela sua inovação no Quadrante Mágico da Gartner para Gestão de Acessos Privilegiados (PAM), o Keeper protege palavras-passe e chaves de acesso, segredos de infraestrutura, ligações remotas e endpoints com políticas de aplicação baseadas em funções, privilégio mínimo e acesso just-in-time.

A Keeper é uma plataforma fiável e apreciada por milhares de empresas e milhões de pessoas em todo o mundo.



Prémio Excelência em
Cibersegurança
**Gestão de Acesso
Privilegiado**



Revista de Ciberdefesa
**Escolha do Editor –
Gestão de Acesso
Privilegiado (PAM)**



Newsweek
**Plataforma de
Cibersegurança nº 1**



Associados de
Gestão Empresarial
**KeeperPAM® reconhecido
pela resistência
do produto**

Gartner

**KeeperPAM® reconhecido
no Quadrante Mágico™ da
Gartner® de 2025 para PAM**