

ESTUDO DE CASO

Atlassian Williams F1 Team mantém dados sensíveis protegidos da fábrica ao pit lane



Contexto

A Atlassian Williams F1 Team é uma das equipes mais históricas da Fórmula 1, fundada em 1977 por Sir Frank Williams e Patrick Head. Com sede em Grove, Oxfordshire (Reino Unido), a equipe ganhou nove Campeonatos de Construtores e sete Campeonatos de Pilotos – entre as equipes mais condecoradas na história da Fórmula 1. Reconhecida pela excelência em engenharia e espírito competitivo, a Williams tem foco em inovação e desempenho, utilizando tecnologia de ponta e análise de dados para competir no mundo do automobilismo em constante transformação.

Setor

Automobilismo

Funcionários

Mais de 1.000

Soluções

Gerenciador de senhas
Keeper Enterprise



O desafio

A Fórmula 1 é o esporte mais intensivo em dados do planeta, sendo um alvo de alto valor para ciberataques. A Atlassian Williams F1 Team gera mais de 1TB de dados de telemetria, aerodinâmica e simulação a cada fim de semana de corrida, com mais de 400 sensores em cada carro alimentando 30 mil canais de dados ao vivo para os engenheiros no circuito e de volta a Grove ao mesmo tempo. As credenciais que protegem o acesso a esses dados podem ter o mesmo valor estratégico que os próprios dados.

“A F1 é um esporte de equipe — sem todas as equipes trabalhando juntas na mesma tarefa, nada funciona. Não queremos que a segurança seja um obstáculo. As pessoas precisam acessar o que precisam, quando precisam.”

Chris Hicks | Engenheiro sênior de segurança da informação da Atlassian Williams F1 Team

Cerca de 1.200 funcionários trabalham em toda a organização, do túnel de vento às operações de corrida na pista. Cada um exige acesso preciso e adequado à sua função durante uma temporada que abrange mais de 20 países. Cada libra gasta é regida pelo teto de gastos da Fórmula 1, que limita o quanto as equipes podem investir em pessoal, equipamentos e operações a cada temporada. Isso significa que os gastos com segurança são ponderados diretamente em relação aos investimentos no desempenho do próprio carro.

“É uma conversa real que pondera a compra de uma ferramenta de segurança, uma nova asa dianteira ou um novo engenheiro mecânico. Temos que comprovar o valor demonstrável da ferramenta quando a apresentamos.”

Chris Hicks | Engenheiro sênior de segurança da informação da Atlassian Williams F1 Team



A Solução da Keeper

A Atlassian Williams F1 Team implementou o Gerenciador de Senhas Corporativas da Keeper juntamente com o BreachWatch®, centralizando o gerenciamento de credenciais em torno de duas prioridades: colaboração segura entre todas as equipes e funções, e a melhor criptografia da categoria, desenvolvida para as ameaças de hoje e de amanhã.

Colaboração: compartilhamento na velocidade da F1

As pastas compartilhadas e as permissões baseadas em funções do Keeper garantem que os funcionários sejam automaticamente provisionados com exatamente as credenciais de que precisam. O compartilhamento único oferece ao contratados e terceiros acesso com tempo limitado que vence automaticamente, sem exigir intervenção manual. O Keeper está acessível em todos os navegadores, aparelhos e sistemas operacionais gerenciados, garantindo que os usuários possam acessar as credenciais quando e onde precisarem delas. Da equipe na pista à equipe de marketing, o Keeper reduz o atrito para os usuários.

“Tudo é gerado inteiramente no Keeper e aplicado automaticamente, reconhecendo o site e fazendo o preenchimento automático em um instante.”

James Yexley | Executivo de mídias sociais da Atlassian Williams F1 Team

Criptografia: proteção desenvolvida para dados de alto valor

A **arquitetura de conhecimento zero** e confiança zero do Keeper significa que as chaves de criptografia são geradas no lado do cliente e nunca armazenadas nos servidores do Keeper. A criptografia de curva elíptica, **criptografia AES de 256 bits** e PBKDF2 são aplicadas em camadas nos níveis de cofre, pasta e registro, com MFA e autenticação biométrica aplicadas em todos os sistemas.

“Levaria mais de dois mil anos para um cibercriminoso descriptografar os dados criptografados. As chaves são geradas no lado do cliente com a Atlassian Williams F1 Team. Nós armazenamos uns e zeros. É isso.”

Darren Guccione | CEO e cofundador da Keeper Security

A Keeper também adiciona camadas de criptografia resistente a ataques quânticos usando o **algoritmo Kyber** para se defender da ameaça de “coletar agora, descriptografar depois”, em que adversários armazenam dados criptografados hoje para descriptografá-los assim que a computação quântica for viável.

“Na F1, é preciso estar sempre pensando no próximo ciclo regulatório. É ótimo ver a Keeper adotando essa mesma filosofia de pensar à frente sobre como nos proteger daquilo que sabemos que está por vir.”

Chris Hicks | Engenheiro sênior de segurança da informação da Atlassian Williams F1 Team



Impacto organizacional

O Keeper oferece às equipes da Williams acesso imediato e de autoatendimento às credenciais de que precisam, reduzindo a sobrecarga de suporte de TI e liberando a equipe para atividades de maior valor. Com o provisionamento e desprovisionamento tratados automaticamente, a equipe de TI passa menos tempo nas solicitações de acesso rotineiras e mais tempo nas prioridades técnicas que fazem a equipe avançar.

“Quando são integradas ao Keeper, as equipes se sentem capacitadas em vez de precisarem entrar em contato com a central de suporte. Isso libera a equipe de suporte para as tarefas cruciais que fazem uma diferença importante para o carro.”

Chris Hicks | Engenheiro sênior de segurança da informação da Atlassian Williams F1 Team

Desempenho no fim de semana de prova

Na pista, uma configuração mais rápida da infraestrutura significa mais tempo para análise de dados e estratégia de corrida — exatamente onde os ganhos marginais são conquistados. Os engenheiros que chegam ao circuito podem colocar os sistemas em operação com rapidez e confiança, sabendo que todas as credenciais de que precisam estão imediatamente à mão.

“Se o pessoal na pista colocar a infraestrutura em funcionamento antes, esse tempo é destinado aos engenheiros para desenvolver estratégias de corrida e fazer a análise de dados mais cedo. Essa diferença de frações de segundo realmente contam no fim de semana de prova.”

Chris Hicks | Engenheiro sênior de segurança da informação da Atlassian Williams F1 Team



Confiança na segurança global

Esteja a equipe na Grove ou na pista do outro lado do mundo, o Keeper oferece acesso consistente e dentro das políticas em cada país, rede e aparelho. Com o BreachWatch monitorando continuamente a dark web e a criptografia com conhecimento zero protegendo cada credencial, a Williams tem a base de segurança para competir tranquilamente.

“O gerenciamento de credenciais não é mais onde reside a margem para melhorias.”

Chris Hicks | Engenheiro sênior de segurança da informação da Atlassian Williams F1 Team

Uma base segura para todas as equipes

O impacto do Keeper vai muito além da TI. Em toda a Williams, pessoas com funções tão variadas quanto experiência do cliente, mídias sociais, administração de viagens e engenharia de custos descrevem o mesmo benefício fundamental: um local único, seguro e organizado para gerenciar todas as credenciais das quais dependem. A segurança virou algo que as pessoas notam porque funciona, não porque atrapalha.

“A segurança é extremamente importante na Fórmula 1. Lidamos com muitos dados de clientes – queremos garantir que eles estejam em uma fonte única da verdade centralizada, protegidos pelo Keeper.”

Tom Iverson | Gerente sênior de experiência de hóspedes da sede da Atlassian Williams F1 Team





A maioria das empresas tem visibilidade limitada nas práticas de senhas dos funcionários. Isso aumenta muito o risco cibernético. A higiene cibernética não pode ser aprimorada sem informações críticas sobre uso e conformidade de senhas. O Keeper resolve isso fornecendo segurança, visibilidade e controle definitivos.

Os dados são protegidos com a arquitetura de segurança com conhecimento zero e a melhor criptografia, resistente à computação quântica, tudo no Keeper. Conhecimento zero significa que somente o usuário conhece e tem acesso à sua senha-mestra e à chave de criptografia usada para criptografar e descriptografar as informações dele.

O Keeper é intuitivo e fácil de implantar, independentemente do tamanho da empresa. O Keeper se integra aos servidores Active Directory e LDAP, o que simplifica o provisionamento e a integração. **O Keeper SSO Connect®** se integra a soluções SSO existentes e tem certificação FedRAMP High e autorização GovRAMP High.

O Keeper foi projetado para escalar em organizações de qualquer tamanho. Recursos como permissões baseadas em funções, compartilhamento entre equipes, auditoria departamental e administração delegada resulta no crescimento das organizações. O **Keeper Commander** fornece APIs robustas para integração com sistemas atuais e futuros.

Casos de uso corporativo: KeeperPAM

- Evite violações de dados relacionadas a credenciais e ciberataques
- Use passkeys para autenticação fácil
- Fortaleça a conformidade
- Aumente a produtividade dos funcionários
- Imponha políticas e procedimentos de senhas
- Reduza os custos com o suporte técnico
- Minimize o treinamento com tempo rápido para segurança
- Melhore a consciência e o comportamento de segurança dos funcionários

Sobre a Keeper

A Keeper Security é uma das empresas de software de cibersegurança que mais cresce, protegendo milhares de organizações e milhões de pessoas em mais de 150 países. A Keeper é pioneira em segurança com conhecimento zero e confiança zero, desenvolvida para qualquer ambiente de TI. O principal serviço da Keeper, o KeeperPAM®, é uma plataforma com IA nativa da nuvem que protege todos os usuários, aparelhos e a infraestrutura dos ciberataques. Reconhecido pela inovação no Gartner Magic Quadrant para gerenciamento de acesso privilegiado (PAM), o Keeper protege senhas e passkeys, segredos de infraestrutura, conexões remotas e endpoints com políticas de aplicação baseadas em funções, privilégio mínimo e acesso just-in-time.

O Keeper é confiável e admirado por milhares de empresas e milhões de pessoas no mundo inteiro.

Gartner

Keeper Security® foi reconhecida em 2026 como a segunda empresa de software de segurança que mais cresce no mundo



Cybersecurity Stars Awards 2026

Inovadora do ano em segurança de IA, Melhor plataforma de gerenciamento de acesso privilegiado para empresas



Prêmios de excelência em cibersegurança

Gerenciamento de acesso privilegiado



Global InfoSec Awards

Solução em cibersegurança com IA, Empresa de cibersegurança, Gerenciamento de Acesso Privilegiado (PAM)



Globe Awards 2026

Vencedor prata em cibersegurança