

Il team Atlassian Williams F1 garantisce l'accesso critico ai sistemi privilegiati con KeeperPAM®



Contesto

L'Atlassian Williams F1 Team è un team storico tra i più noti della Formula 1, fondato nel 1977 da Sir Frank Williams e Patrick Head. Con sede a Grove, nell'Oxfordshire, Regno Unito, il team ha vinto nove campionati nella categoria Costruttori e sette campionati in quella Piloti, il che lo rende uno dei team più premiati della storia della Formula 1. Nota per la sua eccellenza nell'ingegneria e il suo spirito competitivo, Williams si concentra sull'innovazione e sulle prestazioni, sfruttando tecnologie e analisi dati all'avanguardia per essere sempre in prima linea nel mondo in continua evoluzione degli sport motoristici.

Settore

Sport motoristici

Dipendenti

1,000+

Soluzioni

KeeperPAM



La sfida

In Formula 1, proteggere i dati sensibili sulle prestazioni è fondamentale per mantenere un vantaggio competitivo. Per l'Atlassian Williams F1 Team, la sfida è quella di proteggere gli accessi privilegiati di una forza lavoro globale che utilizza centinaia di dispositivi durante gli intensi weekend di gara, oltre alle operazioni aziendali ordinarie. Con sistemi critici in uso in più continenti e in ambienti di rete diversi, il team ha bisogno di mantenere al sicuro le informazioni più preziose, assicurando al contempo che le operazioni vengano svolte alla massima velocità e che i dati critici rimangano protetti.

“Al giorno d'oggi, è fondamentale avere un partner che ci aiuti a proteggere tutti i dati estremamente riservati che produciamo in pista.”

Carlos Sainz | Pilota di Formula 1, Atlassian Williams F1 Team

Operando in più di 20 paesi ogni stagione, Williams si affida a dispositivi e credenziali che viaggiano costantemente tra i continenti. Era importante garantire misure di sicurezza efficaci indipendentemente dalla posizione, dalla rete o dall'endpoint, proteggendo il team sia che fosse nella sede centrale sia che fosse connesso a una rete temporanea a bordo pista.

La gestione di questi accessi presentava delle sfide. Il provisioning e il deprovisioning delle credenziali tra numerosi team interni, funzioni, sistemi e aree geografiche richiedeva molte risorse e molto tempo.

“Normalmente i computer rimangono all'interno di un edificio, ma i nostri viaggiano in tutto il mondo. Ovunque andiamo, dobbiamo garantire che la nostra tecnologia sia sempre sicura.”

James Vowles | Team Principal, Atlassian Williams F1 Team



La soluzione Keeper

Il team Atlassian Williams F1 ha collaborato con Keeper Security per implementare **KeeperPAM**, una piattaforma completa di gestione degli accessi con privilegi (PAM) zero-trust e zero-knowledge. La piattaforma unificata di KeeperPAM ha fornito la visibilità, la sicurezza e l'agilità operativa di cui Williams aveva bisogno per gestire gli accessi privilegiati con una forza lavoro in rapida evoluzione e distribuita a livello globale. Il team aveva bisogno di una soluzione facile da implementare che proteggesse i dati sensibili e consentisse di monitorare da vicino gli accessi.

Accesso basato sui ruoli e con privilegi minimi – i **controlli degli accessi basati sui ruoli (RBAC)** di KeeperPAM garantiscono che ogni membro del team del reparto Tecnologia, innovazione e crescita abbia accesso solo alle credenziali, ai sistemi e ai dati di cui ha bisogno per il proprio ruolo. Limitando rigorosamente i privilegi, Williams riduce le minacce interne e riduce al minimo l'esposizione dei dati sensibili

Credenziali privilegiate sicure – le credenziali privilegiate come password e passkey sono custodite e protette all'interno dell'**architettura zero-knowledge e zero-trust di Keeper**. In questo modo si eliminano le pratiche di archiviazione rischiose, si garantisce che le credenziali non siano mai esposte in chiaro e si proteggono i login sensibili in qualsiasi parte del mondo il team stia gareggiando.

“Quando un utente si iscrive a Keeper, si rende subito conto di cosa si stava perdendo. Con Keeper, non è più necessario armeggiare con le password o preoccuparsi di come condividere le informazioni in modo sicuro. La produttività aumenta in modo significativo, insieme alla sicurezza di ogni utente, grazie alla sua facilità d'uso.”

Craig Lurey | CTO e co-fondatore, Keeper Security

Accesso senza password – Le funzionalità di gestione delle sessioni con privilegi consentono ai team di sicurezza di Williams di concedere l'accesso a sistemi sensibili senza mai esporre le credenziali. Con KeeperPAM, Williams può monitorare, registrare e verificare le attività privilegiate in tempo reale, garantendo piena visibilità e controllo.

Integrazione perfetta con i sistemi esistenti – KeeperPAM **si integra direttamente** con il provider di identità di Williams per il provisioning e il deprovisioning automatizzati degli account privilegiati. In questo modo si garantisce una modifica immediata e accurata degli accessi quando il personale entra o esce dal team, riducendo i costi amministrativi ed eliminando i rischi di accesso persistenti.

Sicurezza all'avanguardia – l'architettura di sicurezza zero-trust e zero-knowledge di Keeper offre una protezione senza eguali, tutelando le informazioni e riducendo al minimo il rischio di violazioni dei dati. Keeper combina la crittografia ellittica (ECC) a livello di dispositivo con una **crittografia a più livelli** (a livello di cassaforte, cartella e voce), l'autenticazione a più fattori e biometrica e la crittografia AES a 256 bit certificata secondo FIPS 140-3 e PBKDF2. Keeper è **conforme a SOC 2, ISO 27001, 27017 e 27018**, con la conformità più longeva del settore, nonché autorizzato FedRAMP e GovRAMP, certificato PCI DSS e certificato da TrustArc per la privacy.

“il processo di onboarding di Keeper è stato molto più rapido e semplice di quello di altri strumenti che abbiamo utilizzato in passato.”

Harry Wilson | Ex responsabile della sicurezza informatica, Atlassian Williams F1 Team



Impatto sull'organizzazione

Keeper ha trasformato il modo in cui Atlassian Williams F1 Team gestisce e protegge gli accessi con privilegi. Il team ora applica i criteri PAM per i suoi utenti più privilegiati, proteggendo le credenziali in una cassaforte zero-knowledge e consentendo connessioni veloci e sicure da qualsiasi parte del mondo. Grazie al monitoraggio delle attività privilegiate e all'automazione delle modifiche di accesso, Williams opera con maggiore velocità, sicurezza e controllo.

“La cosa fondamentale per noi in ogni partnership è che vi sia una sinergia tra i due marchi e che entrambi lavorino insieme per lo stesso obiettivo. E questo è quello che accade con Keeper.”

**James Vowles | Team Principal,
Atlassian Williams F1 Team**

Maggiore sicurezza e visibilità degli accessi privilegiati –

KeeperPAM applica il principio del privilegio minimo e memorizza tutte le credenziali in una cassaforte criptata, mentre Williams può registrare l'attività dello schermo e della tastiera durante le sessioni remote su tutti i protocolli, inclusi SSH, RDP, VNC, database e sessioni di browser web.



Migliore gestione delle credenziali – con KeeperPAM implementato, Williams applica l'autenticazione a più fattori (MFA) su tutti i sistemi, garantisce che l'efficacia delle password dei team rispetti gli standard aziendali e identifica proattivamente eventuali riutilizzi di password tra gli utenti. Sfruttando la funzionalità di audit e reporting di Keeper, l'organizzazione elimina completamente le credenziali ripetute, garantendo che i suoi sistemi siano protetti da potenziali minacce informatiche.

Elevata adozione da parte degli utenti e ticket di assistenza ridotti –

il design intuitivo di KeeperPAM ha favorito una forte adozione in tutta l'organizzazione, con un numero minore di richieste di help desk relative a password e accessi per il team IT. Anche il [portale di documentazione](#) di KeeperPAM si è rivelato utile per aiutare gli utenti a familiarizzare con la piattaforma. L'alto tasso di adozione ha consentito un'esperienza quotidiana più fluida e sicura sia per gli amministratori che per gli utenti finali.

“Per il nostro team a bordo pista, ciò che Keeper ha fatto davvero bene è rendere il percorso più semplice anche il più sicuro, il che significa che i nostri utenti finali sono soddisfatti, e di conseguenza lo sono anch'io.”

**Harry Wilson | Ex responsabile della sicurezza
informatica, Atlassian Williams F1 Team**

Fiducia operativa globale – Keeper continua a consentire a Williams di operare in modo sicuro in tutto il mondo, su qualsiasi rete e con qualsiasi dispositivo, offrendo il massimo livello di protezione sia che il team operi a bordo pista, presso la sede centrale o mentre è in viaggio per la prossima gara.



KeeperPAM

KeeperPAM è una piattaforma gestione degli accessi con privilegi (PAM) di nuova generazione che protegge e gestisce l'accesso alle risorse critiche, tra cui server, applicazioni web, database e carichi di lavoro. Basato su un'architettura di sicurezza zero-trust e zero-knowledge, KeeperPAM aiuta le organizzazioni di ogni dimensione a proteggere gli account privilegiati, applicare il principio del privilegio minimo, proteggere l'infrastruttura remota e soddisfare i requisiti di conformità, con una facilità d'uso senza pari e una rapida implementazione.

Keeper è intuitivo e facile da implementare, a prescindere dalle dimensioni dell'azienda. KeeperPAM utilizza un servizio gateway zero-trust per accedere a ogni ambiente. Non sono necessari aggiornamenti del firewall o modifiche all'accesso, il che consente un accesso semplice e sicuro senza complessità. Con le funzionalità di sessione remota, l'utente non ha mai accesso alle credenziali o alle chiavi SSH. L'accesso a una risorsa può essere limitato nel tempo e le credenziali vengono ruotate automaticamente dopo che l'accesso è stato revocato, fornendo un accesso JIT senza mai esporre le credenziali.

Keeper è stato pensato per la crescita delle organizzazioni di qualsiasi dimensione. KeeperPAM centralizza l'accesso in un'unica interfaccia utente (UI) tra più provider cloud, carichi di lavoro on-premise e ambienti client, consentendo una gestione multi-cloud.

Casi d'uso aziendali: KeeperPAM

- Controlla e monitora tutti gli account con privilegi
- Fornisci l'accesso JIT senza esporre le credenziali
- Unifica gli strumenti di sviluppo in un'unica piattaforma con un'interfaccia utente intuitiva
- Abilita una gestione senza interruzioni degli ambienti cloud, ibridi e multi-cloud
- Registra sessioni multi-protocollo con rilevamento delle minacce tramite AI e interruzione automatica delle sessioni
- Automatizza la rotazione delle password
- Applica la protezione MFA su ogni sistema
- Implementa senza problemi tramite app web o desktop con provisioning SCIM automatizzato

Proteggi la tua organizzazione con Keeper

Per maggiori informazioni su come Keeper può proteggere la tua organizzazione con una piattaforma facile da usare, [contatta il nostro team di vendita](#) per una prova gratuita o una demo personalizzata.

Informazioni su Keeper

Keeper Security è una delle società di software per la sicurezza informatica in più rapida crescita, che protegge migliaia di organizzazioni e milioni di persone in oltre 150 paesi. Keeper è un pioniere della sicurezza zero-knowledge e zero-trust, realizzata per qualsiasi ambiente IT. La sua offerta principale, KeeperPAM®, è una piattaforma cloud-native abilitata all'intelligenza artificiale che protegge tutti gli utenti, i dispositivi e le infrastrutture dagli attacchi informatici. Riconosciuto per la sua innovazione nel Magic Quadrant di Gartner per il Privileged Access Management (PAM), Keeper protegge password e passkey, segreti delle infrastrutture, connessioni remote ed endpoint con politiche di applicazione basate sui ruoli, privilegi minimi e accesso just-in-time.

Keeper è apprezzata e amata da migliaia di aziende e da milioni di persone in tutto il mondo.



Cybersecurity
Excellence Award

Gestione degli accessi
con privilegi



Cyber Defense
Magazine

Scelta dalla redazione
- Privileged Access
Management (PAM)



Newsweek

Piattaforma di sicurezza
informatica n.1



Enterprise

Management Associates
KeeperPAM® premiata
per le prestazioni del
prodotto

Gartner

KeeperPAM® riconosciuta nel
Gartner Magic Quadrant™
2025 per il PAM