

Atlassian Williams F1-team beveiligt kritieke toegang tot geprivilegieerde systemen met KeeperPAM®



Achtergrond

Atlassian Williams F1 Team is een van de meest historische teams in de Formule 1, opgericht in 1977 door Sir Frank Williams en Patrick Head. Het team is gevestigd in Grove, Oxfordshire, VK, en heeft negen constructeurskampioenschappen en zeven coureurskampioenschappen gewonnen, waardoor het een van de meest succesvolle teams in de geschiedenis van de Formule 1 is. Williams staat bekend om zijn uitstekende techniek en competitieve geest en richt zich op innovatie en prestaties, waarbij gebruik wordt gemaakt van geavanceerde technologie en gegevensanalyse om vooraan mee te doen in de snel veranderende wereld van de autosport.

Branche
Motorsport

Medewerkers
1,000+

Oplossingen
KeeperPAM



De uitdaging

In de Formule 1 is het beschermen van gevoelige prestatiegegevens van cruciaal belang voor het behoud van een concurrentievoordeel. Voor het Atlassian Williams F1-team is het een uitdaging om bevoorrechte toegang te beschermen voor een wereldwijd personeelsbestand dat tijdens raceweekenden onder hoge druk honderden apparaten bedient en voor reguliere bedrijfsactiviteiten buiten de raceweekenden. Met kritieke systemen op meerdere continenten en in diverse netwerkomgevingen in gebruik, moet het team zijn meest waardevolle informatie veilig houden terwijl de bedrijfsvoering op pieksnelheid verloopt en kritieke data beschermd blijft.

“Tegenwoordig is het essentieel om een partner te hebben die ons helpt uiterst vertrouwelijke gegevens die we op het circuit produceren te beschermen en te beveiligen”.

Carlos Sainz | Formule 1-coureur, Atlassian Williams F1 Team

Williams is elk seizoen actief in meer dan 20 landen en is daarom afhankelijk van apparatuur en aanmeldingsgegevens die constant tussen continenten reizen. Beveiligingsmaatregelen moesten effectief blijven, ongeacht locatie, netwerk of eindpunt, zodat het team beschermd is ongeacht of ze nu op het hoofdkantoor zijn of aangesloten op een tijdelijk netwerk langs het circuit.

Het beheren van deze toegang bracht zijn eigen uitdagingen met zich mee. Het inrichten en intrekken van aanmeldingsgegevens voor diverse interne teams, functies, systemen en geografische locaties was zowel arbeidsintensief als tijdrovend.

“Normaal gesproken blijft een computer in één gebouw – maar die van ons reizen de hele wereld over. Waar we ook gaan, we moeten ervoor zorgen dat onze technologie beveiligd is”.

James Vowles | Teambaas, Atlassian Williams F1 Team



De oplossing van Keeper

Het F1-team van Atlassian Williams is een samenwerking aangegaan met Keeper Security om **KeeperPAM** te implementeren, een uitgebreid platform voor zero-trust en zero-knowledge Privileged Access Management (PAM). Het uniforme platform van KeeperPAM bood Williams het inzicht, de beveiliging en de operationele flexibiliteit die nodig zijn om bevoorrechte toegang te beheren binnen een snel veranderende, wereldwijd verspreide werkomgeving. Het team had een eenvoudig te implementeren oplossing nodig die de gevoelige gegevens zou beveiligen en waarmee ze de toegang nauwgezet kummern controleren.

Rolgebaseerde toegang met minimale privileges – KeeperPAM's verfijnde **rolgebaseerde toegangscontroles (RBAC)** zorgen ervoor dat elk teamlid op de afdeling Technologie, innovatie & groei alleen toegang heeft tot de aanmeldingsgegevens, systemen en gegevens die voor hun rol vereist zijn. Door privileges strikt te beperken, vermindert Williams interne bedreigingen en minimaliseren ze de blootstelling aan gevoelige gegevens.

Beveiligde geprivilegieerde aanmeldingsgegevens – Geprivilegieerde aanmeldingsgegevens zoals wachtwoorden en passkeys worden opgeslagen en beveiligd binnen de **zero-knowledge en zero-trust architectuur** van Keeper. Dit elimineert riskante opslagpraktijken, zorgt ervoor dat aanmeldingsgegevens nooit in platte tekst worden weergegeven en beschermt gevoelige inlogpogingen, ongeacht waar ter wereld het team zich bevindt.

“Wanneer gebruikers zich aanmelden voor Keeper, beseffen ze meteen wat ze in hun leven misten. Met Keeper hoeven ze nooit meer te worstelen met wachtwoorden of zich zorgen te maken over hoe ze informatie veilig kunnen delen. De productiviteit en beveiliging neemt voor elke gebruiker toe, omdat de software zo eenvoudig te gebruiken is”.

Craig Lurey | CTO en medeoprichter, Keeper Security

Wachtwoordloze toegang – Bevoorrechte sessiebeheermogelijkheden stellen de beveiligingsteams van Williams in staat toegang te verlenen tot gevoelige systemen zonder ooit aanmeldingsgegevens bloot te stellen. Met KeeperPAM kan Williams geprivilegieerde activiteiten in realtime monitoren, vastleggen en controleren, wat zorgt voor volledig inzicht en controle.

Naadloze integratie met bestaande systemen – KeeperPAM **integreert direct** met de identiteitsprovider van Williams voor geautomatiseerd inrichten en intrekken van bevoorrechte accounts. Dit zorgt voor onmiddellijke en nauwkeurige toegangswijzigingen wanneer personeel zich bij het team voegt of het verlaat, waardoor de administratieve overhead wordt verminderd en risico's van blijvende toegang worden geëlimineerd.

Beveiliging van wereldklasse – De zero-trust en zero-knowledge beveiligingsarchitectuur van Keeper is ongeëvenaard in het beschermen van informatie en het beperken van het risico op een datalek. Keeper combineert Elliptic-Curve Cryptography (ECC) op apparaatniveau met **meerdere lagen van versleuteling** (op kluis-, map- en recordniveau), multi-factor- en biometrische authenticatie en FIPS 140-3 gevalideerde AES 256-bits versleuteling, evenals PBKDF2. Keeper is **SOC 2-, ISO 27001-, 27017- en 27018-compliant** – met de langst bestaande naleving in de sector – en tevens FedRAMP- en GovRAMP-geautoriseerd, PCI DSS-gecertificeerd en gecertificeerd door TrustArc voor privacy.

“Vergeleken met andere tools die we eerder hebben gebruikt, vonden we het onboardingproces van Keeper veel sneller en eenvoudiger”.

Harry Wilson | Voormalig hoofd informatiebeveiliging, Atlassian Williams F1 Team



Impact op de organisatie

Keeper heeft de manier waarop Atlassian Williams F1 Team bevoorrechte toegang beheert en beschermt, volledig veranderd. Het team handhaaft nu PAM-beleidsregels voor de meest bevoorrechte gebruikers, beveiligt aanmeldingsgegevens in een zero-knowledge kluis en maakt snelle, veilige verbindingen mogelijk vanaf elke locatie ter wereld. Williams werkt sneller, betrouwbaarder en met meer controle, omdat bevoorrechte activiteiten worden bewaakt en toegangswijzigingen worden geautomatiseerd.

“Wat voor ons essentieel is bij elke samenwerking, is dat er synergie ontstaat tussen beide merken en dat ze samenwerken aan hetzelfde doel. En dat is bij Keeper absoluut het geval”.

James Vowles | Teambaas, Atlassian Williams F1 Team

Verbeterde beveiliging en zichtbaarheid van geprivilegieerde toegang – KeeperPAM handhaaft toegang met het minste privilege en slaat alle aanmeldingsgegevens op in een versleutelde kluis, en Williams kan scherm- en toetsenbordactiviteit opnemen tijdens sessies op afstand over alle protocollen, waaronder SSH, RDP, VNC, databases en webbrowsersessies.



Sterkere aanmeldingsgegevenshygiëne – Nu KeeperPAM is geïmplementeerd, handhaaft Williams multi-factor authenticatie (MFA) op elk systeem, zorgen ze ervoor dat de wachtwoordsterkte van alle teams voldoet aan de normen en identificeren ze proactief het hergebruik van wachtwoorden bij gebruikers. Door gebruik te maken van de audit- en rapportagefunctionaliteit van Keeper elimineert de organisatie herhaalde aanmeldingsgegevens volledig, zodat haar systemen beschermd blijven tegen potentiële cyberbedreigingen.

Hoge gebruikersacceptatie en minder supporttickets – Het intuïtieve ontwerp van KeeperPAM heeft geleid tot een sterke acceptatie binnen de organisatie, resulterend in minder wachtwoord- en toegangsgelateerde helpdeskaanvragen voor het IT-team. Het KeeperPAM [documentatieportal](#) bleek ook nuttig om gebruikers te helpen vertrouwd te raken met het platform. De hoge acceptatiegraad leidde tot een soepelere, veiligere dagelijkse ervaring voor zowel beheerders als eindgebruikers.

“Als je kijkt naar ons team langs de baan, dan heeft Keeper het uitstekend voor elkaar gekregen om de weg van de minste weerstand óók de veiligste weg te maken. Dat betekent dat onze eindgebruikers tevreden zijn en dus ben ik dat ook”.

Harry Wilson | Voormalig hoofd informatiebeveiliging, Atlassian Williams F1 Team

Wereldwijde operationele zekerheid – Keeper stelt Williams in staat om wereldwijd veilig te opereren, op elk netwerk en met elk apparaat, en biedt het hoogste niveau van bescherming, of het team nu langs het circuit opereert, op het hoofdkantoor is of onderweg is naar de volgende race.



KeeperPAM

KeeperPAM is een next-gen Privileged Access Management (PAM)-platform dat de toegang tot kritieke bronnen, waaronder servers, webapps, databases en workloads, beveiligt en beheert. KeeperPAM is gebouwd op een zero-trust en zero-knowledge beveiligingsarchitectuur en helpt organisaties van elk formaat om bevoorrechte accounts te beschermen, minimale privilege te handhaven, externe infrastructuur te beveiligen en te voldoen aan compliance-eisen, met ongeëvenaard gebruiksgemak en snelle implementatie.

Keeper is intuïtief en eenvoudig te implementeren, ongeacht het bedrijfsformaat. KeeperPAM gebruikt een zero-trust gateway-service om toegang te krijgen tot elke omgeving. Er zijn geen firewallupdates of wijzigingen nodig, waardoor naadloze, veilige toegang zonder complexiteit mogelijk is. Met de mogelijkheden voor sessies op afstand heeft de gebruiker nooit toegang tot de aanmeldingsgegevens of SSH-sleutels. De duur van toegang tot een bron kan beperkt worden en aanmeldingsgegevens worden automatisch geroteerd nadat de toegang is ingetrokken, waardoor JIT-toegang wordt geboden zonder ooit aanmeldingsgegevens bloot te stellen.

Keeper is ontworpen om mee te schalen met organisaties van elke omvang. KeeperPAM centraliseert de toegang in één gebruikersinterface (UI) voor meerdere cloudproviders, lokale workloads en clientomgevingen, waardoor multi-cloudbeheer mogelijk wordt.

Zakelijke toepassingsvoorbeelden: KeeperPAM

- Beheer en controleer alle geprivilegieerde accounts
- Bied Just-in-time toegang zonder aanmeldingsgegevens bloot te stellen
- Bundel ontwikkeltools op één platform met een intuïtieve gebruikersinterface
- Maak naadloos beheer mogelijk van cloud-, hybride en multi-cloudomgevingen
- Neem multiprotocol-sessies op met AI-detectie van bedreigingen en automatische sessiebeëindiging
- Automatische wachtwoordrotatie
- Handhaaf MFA-bescherming op elk systeem
- Implementeer naadloos via web- of desktop-app met geautomatiseerde SCIM-inrichting

Bescherm uw organisatie met Keeper

Wilt u meer weten over hoe Keeper uw organisatie kan beschermen met een gebruiksvriendelijk platform?

Neem contact op met ons verkoopteam voor een gratis proefperiode of een gepersonaliseerde demo.

Over Keeper

Keeper Security is een van de snelst groeiende cyberbeveiligingssoftwarebedrijven die duizenden organisaties en miljoenen mensen in meer dan 150 landen beschermt. Keeper is een pionier op het gebied van zero-knowledge en zero-trust beveiliging, gebouwd voor elke IT-omgeving. Het kernaanbod, KeeperPAM®, is een AI-gebaseerd, cloud-native platform dat alle gebruikers, apparaten en infrastructuur beschermt tegen cyberaanvallen. Keeper, erkend voor zijn innovatie in het Gartner Magic Quadrant voor Privileged Access Management (PAM), beveiligt wachtwoorden en sleutels, infrastructuurgeheimen, externe verbindingen en eindpunten met rolgebaseerd handhavingsbeleid, minimale privileges en just-in-time toegang.

**Keeper wordt wereldwijd vertrouwd en
gewaardeerd door duizenden bedrijven en
miljoenen mensen.**



Prijs voor uitmuntende
cyberbeveiliging
**Privileged Access
Management**



Cyber Defense
Magazine
**Editor's Choice –
Privileged Access
Management (PAM)**



Newsweek
#1 Cyberbeveiligingsplatform



Enterprise
Management Associates
**KeeperPAM® erkend voor
productsterkte**

Gartner

**KeeperPAM® erkend in
het 2025 Gartner Magic
Quadrant™ voor PAM**