

CASE STUDY

Atlassian Williams F1 Team beschermt gevoelige gegevens, van de fabriek tot aan de pitstraat



Achtergrond

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

Branche
Autosport

Werknemers
1000+

Oplossingen
Keeper Enterprise-
wachtwoordbeheer



De uitdaging

Formule 1 is de sport waar de meeste gegevens ter wereld worden verwerkt, waardoor het een zeer aantrekkelijk doelwit is voor cyberaanvallen. Het Atlassian Williams F1 Team genereert elk raceweekend meer dan 1 TB aan telemetrie-, aerodynamische en simulatiegegevens, waarbij meer dan 400 sensoren op elke auto tegelijkertijd 30.000 gegevenskanalen live doorsturen naar technici op het circuit en op de basis in Grove. De aanmeldingsgegevens die de toegang tot die gegevens beschermen, kunnen van net zo'n strategische waarde zijn als de gegevens zelf.

“F1 is een teamsport; als niet alle teams samen aan dezelfde taak werken, lukt er niets. We willen niet dat beveiliging een blokkade vormt. Mensen moeten toegang hebben tot wat ze nodig hebben, wanneer ze het nodig hebben”.

**Chris Hicks | Senior informatiebeveiligingsingenieur,
Atlassian Williams F1 Team**

Er werken zo'n 1200 mensen in de hele organisatie, van de windtunnel tot op het circuit tijdens de races zelf. Ze hebben allemaal gedurende het hele seizoen, dat zich over meer dan 20 landen uitstrekt, nauwkeurige en rolspecifieke toegang nodig. Elke uitgegeven pond wordt beheerst door het kostenplafond van de Formule 1, dat beperkt hoeveel teams elk seizoen kunnen investeren in personeel, apparatuur en bedrijfsprocessen. Dat betekent dat uitgaven aan beveiliging direct worden afgewogen tegen prestatiebevorderende investeringen in de auto zelf.

“Het is echt een afweging tussen de aanschaf van een beveiligingstool en een nieuwe voorvleugel of een nieuwe werktuigbouwkundig ingenieur. We moeten de aantoonbare meerwaarde van de tool bewijzen als we die voorstellen”.

**Chris Hicks | Senior informatiebeveiligingsingenieur,
Atlassian Williams F1 Team**



De oplossing van Keeper

Het Atlassian Williams F1 Team is een samenwerking aangegaan met Keeper Security om naast BreachWatch® ook de Keeper Enterprise-wachtwoordbeheerder te implementeren, waardoor het beheer van aanmeldingsgegevens is gecentraliseerd rond twee prioriteiten: veilige samenwerking binnen elk team en elke functie en de beste versleuteling in zijn klasse, gebouwd voor de dreigingen van vandaag en morgen.

Samenwerking: delen op F1-snelheid

De gedeelde mappen en rolgebaseerde machtigingen van Keeper zorgen ervoor dat personeel automatisch wordt ingericht met de aanmeldingsgegevens die ze nodig hebben om te kunnen werken. Met eenmalig delen krijgen aannemers en derden tijdelijke toegang die automatisch verloopt, zonder dat daarvoor handmatige actie nodig is. Keeper is toegankelijk via alle beheerde browsers, apparaten en besturingssystemen, zodat gebruikers toegang hebben tot de aanmeldingsgegevens die ze nodig hebben, wanneer en waar ze die nodig hebben. Van het team langs het circuit tot het marketingteam: Keeper zorgt voor minder frictie voor gebruikers.

“Ze worden volledig in Keeper gegenereerd en automatisch toegepast: de website wordt herkend en de gegevens worden direct automatisch ingevuld”.

James Yexley | Social Media-manager,
Atlassian Williams F1 Team

Versleuteling: bescherming die is gebouwd voor waardevolle gegevens

De **zero-knowledge, zero-trust architectuur** van Keeper betekent dat encryptiesleutels aan de clientzijde worden gegenereerd en nooit op de servers van Keeper worden opgeslagen. Elliptic-Curve-cryptografie, **AES 256-bits versleuteling** en PBKDF2 worden in meerdere lagen toegepast op de kluizen, mappen en records, waarbij MFA en biometrische authenticatie op alle systemen worden afgedwongen.

“Het zou een cybercrimineel meer dan 2000 jaar kosten om de versleutelde gegevens te ontcijferen. De sleutels worden aan de clientzijde gegenereerd met het Atlassian Williams F1 Team. Wij slaan enen en nullen op. En verder niks”.

Darren Guccione | CEO en medeoprichter, Keeper Security

Keeper voegt ook kwantumbestendige versleuteling toe met behulp van het **Kyber-algoritme** voor de bescherming tegen de bedreiging van “nu verzamelen, later ontcijferen”, waarbij aanvallers vandaag versleutelde gegevens opslaan om die te ontcijferen zodra kwantumcomputers inzetbaar worden.

“In de F1 wordt altijd nagedacht over de volgende regelgevingscyclus. Het is geweldig om te zien dat Keeper diezelfde filosofie hanteert door vooruit te denken over hoe we beschermd kunnen worden tegen wat we weten dat komen gaat”.

Chris Hicks | Senior informatiebeveiligingsingenieur,
Atlassian Williams F1 Team



Impact op de organisatie

Keeper geeft teams binnen Williams direct en zelfstandig toegang tot de aanmeldingsgegevens die ze nodig hebben, waardoor de kosten voor IT-ondersteuning dalen en het team zich kan richten op werk dat meer waarde oplevert. Nu het inrichten en intrekken automatisch wordt afgehandeld, besteedt het IT-team minder tijd aan routinematige toegangsverzoeken en meer tijd aan de technische prioriteiten die het team vooruithelpen.

“Wanneer teams aan de slag gaan met Keeper, voelen ze zich zelfstandiger en hoeven ze geen contact meer op te nemen met de servicedesk. Daardoor kan het ondersteuningsteam zich richten op de cruciale taken die echt het verschil maken voor de auto”.

Chris Hicks | Senior informatiebeveiligingsingenieur,
Atlassian Williams F1 Team

Prestaties tijdens het raceweekend

Aan het circuit leidt een snellere installatie van de infrastructuur tot meer tijd voor gegevensanalyse en racestrategie; dit is precies waar marginale winst wordt geboekt. Ingenieurs die aankomen op een circuit, kunnen systemen snel en met vertrouwen online brengen. Ze weten namelijk dat de aanmeldingsgegevens die ze nodig hebben, direct beschikbaar zijn.

“Als de mensen op het circuit de infrastructuur sneller op orde krijgen, kan die tijd worden besteed aan technici die racestrategieën ontwikkelen en eerder de gegevensanalyse uitvoeren. Die paar seconden maken een enorm verschil tijdens een raceweekend”.

Chris Hicks | Senior informatiebeveiligingsingenieur,
Atlassian Williams F1 Team



Vertrouwen in wereldwijde beveiliging

Of het team zich nu in Grove bevindt of langs het circuit aan de andere kant van de wereld: Keeper zorgt voor consistente, aan de beleidsregels conforme toegang in elk land, op elk netwerk en op elk apparaat. Doordat BreachWatch continu het dark web monitort en de zero-knowledge versleuteling alle aanmeldingsgegevens beschermt, beschikt Williams over de nodige beveiligingsbasis om zonder concessies te kunnen concurreren.

“Het beheer van aanmeldingsgegevens is niet langer het gebied waar ruimte voor verbetering zit”.

Chris Hicks | Senior informatiebeveiligingsingenieur,
Atlassian Williams F1 Team

Een veilige basis voor elk team

De impact van Keeper reikt veel verder dan alleen IT. Overal bij Williams noemen medewerkers in allerlei functies, van gastbeleving en sociale media tot reisadministratie en kostenbeheer, hetzelfde grote voordeel: dat ze al hun aanmeldingsgegevens op één veilige en overzichtelijke plek kunnen beheren. Beveiliging is uitgegroeid tot iets wat mensen opmerken omdat het werkt, niet omdat het in de weg zit.

“Beveiliging is enorm belangrijk in de Formule 1. Wij verwerken veel klantgegevens – we willen ervoor zorgen dat deze zich in één centrale bron van waarheid bevinden, die wordt beschermd door Keeper”.

Tom Iverson | Senior HQ-manager gastbeleving,
Atlassian Williams F1 Team



KeeperPAM

De meeste bedrijven hebben beperkt inzicht in de wachtwoordpraktijken van hun werknemers, wat het cyber risico aanzienlijk kan vergroten. Het is onmogelijk om de cyberhygiëne te verbeteren als er geen cruciale informatie beschikbaar is over het gebruik van wachtwoorden en de naleving. Keeper lost dit op door ultieme beveiliging, zichtbaarheid en controle te bieden.

De gegevens worden beschermd door de zero-knowledge beveiligingsarchitectuur van Keeper en versleuteling van wereldklasse die kwantumbestendig is. Zero-knowledge houdt in dat alleen de gebruiker het hoofdwachtwoord en de encryptiesleutel kent en toegang heeft tot deze gegevens, die worden gebruikt om informatie te versleutelen en te ontcijferen.

Keeper is intuïtief en eenvoudig te installeren, ongeacht de bedrijfsgrootte. Keeper integreert met Active Directory- en LDAP-servers, wat het inrichten en onboarden stroomlijnt. **Keeper SSO Connect**® integreert met bestaande SSO-oplossingen en is FedRAMP High-gecertificeerd en GovRAMP High-geautoriseerd.

Keeper is ontworpen om mee te schalen met organisaties van elke omvang. Functies zoals rolgebaseerde machtigingen, teamdeling, afdelingsaudits en gedelegeerd beheer ondersteunen organisaties naarmate ze groeien. **Keeper Commander** biedt robuuste API's voor integratie met huidige en toekomstige systemen.

Zakelijke use cases: KeeperPAM

- voorkom gegevenslekken en cyberaanvallen met betrekking tot aanmeldingsgegevens
- ondersteunt toegangssleutels voor moeiteloze authenticatie
- versterkt de naleving
- geeft de medewerkersproductiviteit een boost
- dwingt wachtwoordbeleid en -procedures af
- verlaagt de kosten van de helpdesk
- minimaliseert training met snelle implementatie van beveiliging
- verbetert het bewustzijn en het gedrag van medewerkers op het gebied van beveiliging

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 belangrijkste product, KeeperPAM®, is een AI-gestuurd, cloud-native platform dat alle gebruikers, apparaten en infrastructuur beschermt tegen cyberaanvallen. Keeper wordt erkend voor diens innovatie in het Gartner Magic Quadrant for Privileged Access Management (PAM) en beveiligt wachtwoorden, toegangssleutels, infrastructuurgeheimen, externe verbindingen en eindpunten met rolgebaseerd handhavingbeleid, minimale privileges en just-in-time toegang.

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

Gartner

Keeper Security® werd in 2026 erkend als het op een na snelst groeiende beveiligingssoftwarebedrijf ter wereld



Cybersecurity Stars Awards 2026

AI Security Innovator of the Year, Best Privileged Access Management Platform for Enterprises



Cybersecurity Excellence Awards

Privileged Access Management



Global InfoSec Awards

AI-cyberbeveiligingsoplossing, cyberbeveiligingsbedrijf, Privileged Access Management (PAM)



Globe Awards 2026

Cybersecurity Silver-winnaar