KEEPER | DrillDocs

Case Study

DrillDocs beveiligt wereldwijde offshore operaties en 24/7 engineeringtoegang met KeeperPAM®

Achtergrond

DrillDocs is een technologische startup in een beginstadium die software voor computervisie levert voor offshore boortoepassingen. Het platform bewaakt het boorproces in real-time en analyseert steenfragmenten om operators te helpen de veiligheid, efficiëntie en prestaties op offshore platforms te verbeteren.

Branche
Olie en gas

Werknemers
20+

Oplossingen
KeeperPAM
Keeper Secrets Manager

De uitdaging

Naarmate DrillDocs zich ontwikkeld van een engineeringteam in oprichting naar een gedistribueerde, productieondersteunende organisatie, werd toegangsbeheer steeds complexer. In de beginfase verzorgde een klein intern team zowel de ontwikkeling als de ondersteuning, waarbij aanmeldingsgegevens veilig werden opgeslagen en de toegang strikt werd gecontroleerd via informele, handmatige processen. Naarmate de vraag van klanten toenam en systemen internationaal werden ingezet, schakelde DrillDocs een extern engineeringbureau in om nachtelijke ondersteuning te bieden en voor daadwerkelijke 24/7 operationele paraatheid te zorgen. De organisatie vertrouwde op Keeper Secrets Manager om het ophalen van aanmeldingsgegevens tijdens implementaties te automatiseren. Aanmeldingsgegevens werden programmatisch geïnjecteerd tijdens het bouwen van systemen en in het geheugen bewaard tijdens runtime workflows, zodat ze nooit in leesbare tekst op productiesystemen werden opgeslagen.

Hoewel deze aanpak effectief veilige DevOps-workflows ondersteunde, vereiste het beheer van interactieve geprivilegieerde sessies voor gedistribueerde interne en externe gebruikers een veilige oplossing voor geprivilegieerd toegangsbeheer (PAM, Privileged Access Management). Door de uitbreiding van de operationele reikwijdte ontstonden nieuwe governancevereisten voor het toekennen, monitoren en intrekken van geprivilegieerde toegang voor wereldwijde teams en onbeheerde apparaten. Het management had behoefte aan meer zichtbaarheid, strengere toegangscontroles en een oplossing die veilig kon meegroeien met de wereldwijde activiteiten van het bedrijf.

> **“We begonnen ons zorgen te maken over hoe we de beveiliging het beste konden beheren wanneer er op persoonlijke machines wordt gewerkt. We vertrouwen onze partners, maar we moesten overschakelen op een vertrouwen-maar-verifiëren-cultuur.”**
>
> **Francois Ruel | Medeoprichter en Chief Science Officer, DrillDocs**

De oplossing van Keeper

DrillDocs heeft **KeeperPAM** geïmplementeerd, een uitgebreid zero-trust en zero-knowledge PAM-platform, om geprivilegieerde toegang te centraliseren, aanmeldingsgegevens te beveiligen en gecontroleerd beheer van externe sessies te bieden zonder engineeringworkflows te verstoren.

Snelle implementatie met onmiddellijke waarde - Het implementatieproces van Keeper is eenvoudig en overzichtelijk, waardoor zowel interne engineers als externe supportteams naadloos kunnen overstappen op een veiliger toegangsmodel. Keeper biedt uitgebreide **productdocumentatie**, implementatiebronnen en begeleiding voor eindgebruikers ter ondersteuning van een succesvolle uitrol. Gedetailleerde **productgidsen** en **trainingsvideo's** helpen om voor een hoge gebruikersacceptatie te zorgen.

> **"De dag dat we besloten onze proefperiode te starten, lukte het ons om alles op te zetten in een sessie van twee uur. Vanaf dat moment zijn we meteen met Keeper aan de slag gegaan."**
>
> **Francois Ruel | Medeoprichter en Chief Science Officer, DrillDocs**

Beveiligde virtuele toegang zonder beheer van eindpunten - KeeperPAM stroomlijnt het beheer van de gebruikerslevenscyclus door beheerders in staat te stellen geprivilegieerde toegang binnen enkele seconden in te richten, te wijzigen en in te trekken. Via gecentraliseerde, op rollen gebaseerde toegangscontroles en beleidshandhaving kunnen organisaties onmiddellijk toegang verlenen tot kritieke systemen of machtigingen verwijderen wanneer rollen veranderen of gebruikers vertrekken. Deze realtime inrichting vermindert de administratieve overhead, elimineert de risico's van permanente toegang en zorgt ervoor dat geprivilegieerde accounts op elk moment streng gecontroleerd blijven.

Onmiddellijke inrichting en intrekking van toegang - KeeperPAM stroomlijnt het beheer van de gebruikerslevenscyclus door beheerders in staat te stellen geprivilegieerde toegang binnen enkele seconden in te richten, te wijzigen en in te trekken. Via gecentraliseerde, **op rollen gebaseerde toegangscontroles** en beleidshandhaving kunnen organisaties onmiddellijk toegang verlenen tot kritieke systemen of machtigingen verwijderen wanneer rollen veranderen of gebruikers vertrekken. Deze realtime inrichting vermindert de administratieve overhead, elimineert de risico's van permanente toegang en zorgt ervoor dat geprivilegieerde accounts op elk moment streng gecontroleerd blijven.

Veilige geautomatiseerde implementaties zonder aanmeldingsgegevens bloot te stellen - Keeper Secrets Manager beveiligt de toegang van machine tot machine door geautomatiseerde implementaties en systeemupdates mogelijk te maken zonder aanmeldingsgegevens bloot te stellen of hard te coderen. Tijdens buildprocessen worden aanmeldingsgegevens programmatisch opgehaald en rechtstreeks in het geheugen geïnjecteerd, zodat ze nooit in leesbare tekst worden opgeslagen of op systemen achterblijven. Deze aanpak versterkt de DevOps-beveiliging door de wildgroei aan geheimen te elimineren en tegelijkertijd de efficiëntie van automatisering te behouden.

> **"Ik gebruik de kluis meerdere keren per dag. We gebruiken Keeper Secrets Manager ook voor geautomatiseerde implementaties en updates. "Het werkt erg goed voor ons."**
>
> **David Momberger | Senior Systems Engineer, DrillDocs**

Beveiliging van wereldklasse - de zero-trust en zero-knowledge beveiligingsarchitectuur van Keeper is ontworpen om informatie te beschermen en het risico van datalekken te verminderen. Keeper combineert Elliptic-Curve Cryptography (ECC) op apparaatniveau met **meerdere versleutelingslagen** (op kluis-, map- en recordniveau), kwantumbestendige cryptografie, meerledige en biometrische verificatie en FIPS 140-3-gevalideerde AES 256-bits versleuteling, plus PBKDF2. Keeper **voldoet aan de SOC 2- en ISO/IEC 27001-normen en ondersteunt tevens ISO/IEC 27017 en 27018**, met de langstlopende naleving in de branche. Keeper is FedRAMP en GovRAMP High Authorized, PCI DSS-gecertificeerd en TrustArc-gecertificeerd voor privacy.

Impact op de organisatie

Sinds de implementatie van KeeperPAM heeft DrillDocs zijn beveiliging aanzienlijk versterkt, terwijl de flexibiliteit die nodig is voor een snelgroeiende, wereldwijde start-up behouden is gebleven. Gedeelde beheerderswachtwoorden zijn afgeschaft en geprivilegieerde aanmeldingsgegevens worden nu in een kluis geplaatst, gerandomiseerd en beheerd door op rollen gebaseerde toegangscontrole. Het BYOD-model (Bring Your Own Device) van het bedrijf veroorzaakt niet langer zichtbaarheidsproblemen of operationele druk.

> **"Keeper heeft een grote verandering teweeggebracht in onze digitale beveiligingscultuur. We bewaren onze aanmeldingsgegevens niet langer op onveilige plekken."**
>
> **Francois Ruel | Medeoprichter en Chief Science Officer, DrillDocs**

Minder risico's in een extern BYOD-personeelsbestand - KeeperPAM verlaagt het risico voor het externe BYOD-personeelsbestand van DrillDocs door geprivilegieerde toegang te isoleren in beveiligde virtuele omgevingen. Engineers en externe partners kunnen overal ter wereld veilig verbinding maken met productiesystemen, zonder aanmeldingsgegevens bloot te stellen of gevoelige toegangstools rechtstreeks op persoonlijke apparaten te installeren.

Op rollen gebaseerde toegang met minimale privileges - KeeperPAM stelt DrillDocs in staat om de toegang te structureren per rol in plaats van individuele aanmeldingsgegevens te distribueren. Engineeringteams van klanten, ontwikkelaars en externe partners krijgen alleen toegang tot de systemen die nodig zijn voor hun verantwoordelijkheden. Deze aanpak geeft de administratieve overhead drastisch verminderd en heeft er tegelijkertijd voor gezorgd dat geprivilegieerde toegang streng gecontroleerd bleef.

> **"Het on- of offboarden van werknemers is nu veel gemakkelijker en sneller. Als iemand toegang tot iets nieuws nodig heeft, is het nu een kwestie van seconden en ze hebben er toegang toe."**
>
> **Mert Geveci | Chief Technology Officer, DrillDocs**

Gestroomlijnde on- en offboarding van gebruikers - KeeperPAM heeft onboarding- en offboardingprocessen getransformeerd, de efficiëntie verbeterd en de administratieve overhead verminderd. Toegang kan binnen enkele seconden worden verleend of ingetrokken, waardoor het leiderschap direct kan reageren op operationele behoeften.

Volledige zichtbaarheid in geprivilegeerde sessies - de sessieregistratie- en activiteitsregistratiemogelijkheden van KeeperPAM bieden extra inzicht in geprivilegeerde activiteit. Als zich ongewoon gedrag voordoet, kan het leiderschap de sessiegegevens bekijken om beter te begrijpen wat er is gebeurd en op de juiste manier reageren. KeeperAI maakt geautomatiseerde beëindiging van risicovolle sessies en versleutelde activiteitsoverzichten mogelijk. Dit niveau van zichtbaarheid ondersteunt het beveiligingsmodel van de organisatie over wereldwijd verspreide engineers en externe ondersteuningsteams, waardoor het leiderschap duidelijk toezicht heeft op hoe productieomgevingen worden benaderd en gebruikt.

Ingebouwde governance ter ondersteuning van compliance - nu DrillDocs doorgaat op weg naar SOC 2-conformiteit, biedt KeeperPAM een sterke basis om te voldoen aan toegangscontrolevereisten. Gecentraliseerd beheer van aanmeldingsgegevens, op rollen gebaseerde handhaving van minimale privileges en mogelijkheden voor sessiecontrole ondersteunen de bredere doelstellingen van het bedrijf op het gebied van governance en beveiliging.

DrillDocs opereert tegenwoordig met de beveiligingsvolwassenheid van een veel grotere onderneming. Engineers kunnen overal ter wereld veilig verbinding maken, op elk apparaat, zonder geprivilegeerde aanmeldingsgegevens bloot te stellen. De toegang is gestructureerd, gemonitord en centraal gecontroleerd. Onboarding is onmiddellijk en offboarding is snel en beleidsgestuurd. Externe partners kunnen veilig bijdragen. Met KeeperPAM is de organisatie in staat om veilig op te schalen en tegelijkertijd de snelheid en innovatie te behouden die kenmerkend zijn voor zijn groei.

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. Gebouwd op een zero-trust, zero-knowledge beveiligingsarchitectuur helpt KeeperPAM organisaties bij het beschermen van geprivilegieerde accounts, het handhaven van minimale privileges, het beveiligen van externe infrastructuur en het voldoen aan compliance-eisen, met ongeëvenaard gebruiksgemak en snelle implementatie.

Keeper is intuïtief en eenvoudig te implementeren, ongeacht de bedrijfsgrootte. KeeperPAM maakt gebruik van een zero-trust gatewayservice om verbinding te maken met doelomgevingen zonder dat firewallupdates of wijzigingen in de inkomende routering nodig zijn. Mogelijkheden voor externe sessies zorgen ervoor dat gebruikers nooit rechtstreeks toegang hebben tot aanmeldingsgegevens of SSH-sleutels, zodat geheimen volledig geïsoleerd blijven van eindpunten. De toegang tot een bron kan tijdsbeperkt zijn en geregeld worden door beleid, waarbij aanmeldingsgegevens automatisch worden geroteerd nadat de toegang is ingetrokken. Dit maakt veilige just-in-time (JIT) toegang mogelijk 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 gebruikssituaties: 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 en is gebouwd voor elke IT-omgeving. Het belangrijkste product, KeeperPAM®, is een AI-gestuurd, cloudeigen platform dat alle gebruikers, apparaten en infrastructuur beschermt tegen cyberaanvallen. Keeper, erkend voor zijn innovatie in het Gartner Magic Quadrant for Privileged Access Management (PAM), beveiligt wachtwoorden en sleutels, infrastructuurgeheimen, externe verbindingen en eindpunten met rolgebaseerd handhavingsbeleid, minimale privileges en just-in-time toegang. Ontdek waarom toonaangevende organisaties vertrouwen op Keeper om zich te beschermen tegen hedendaagse cyberdreigingen via **KeeperSecurity.com**.

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

Gartner

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

Prijs voor uitmuntende cyberbeveiliging
Privileged Access Management

Cyber Defense Magazine
Keuze van de redactie - Privileged Access Management (PAM)

Newsweek
#1 Cyber-beveiligingsplatform

Enterprise Management Associates
KeeperPAM® erkend voor productsterkte