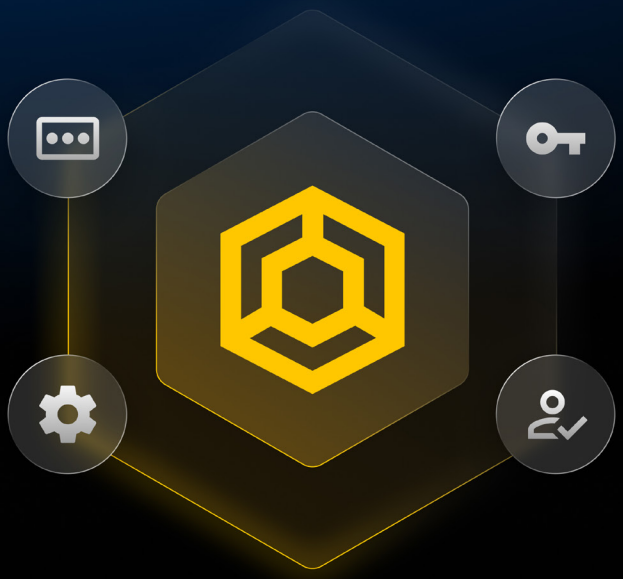
CASESTUDY

# Asite beveiligt de aanmeldingsgegevens, geheimen en geprivilegieerde toegang van het hele bedrijf met KeeperPAM®



## Achtergrond

**Asite** is een SaaS-bedrijf dat actief is in de bouwsector en organisaties helpt bij het beheren van complexe projecten – van 3D-modellen en digitale tweelingen tot documentbeheer en samenwerking met leveranciers – in wereldwijde teams en regio's. Asite opereert in meerdere regio's met datacenters op negen locaties en een personeelsbestand van 500+ medewerkers.

**Industrie**
Bouwtechnologie (SaaS)

**Werknemers**
500+

**Oplossingen**
KeeperPAM

## De uitdaging

Voor een internationaal SaaS-bedrijf dat grote bouwprojecten ondersteunt, waaronder klanten die actief zijn in kritieke infrastructuur en defensiegerelateerde omgevingen, is het veilig beheer van aanmeldingsgegevens en geprivilegieerde toegang van essentieel belang. Asite had behoefte aan een meer gecentraliseerde en afdwingbare aanpak van wachtwoorden, geheimen en geprivilegieerd toegangsbeheer (PAM) binnen de hele organisatie.

**Verouderde tools met gefragmenteerde zichtbaarheid -** De afhankelijkheid van wachtwoordbeheerders in de browser beperkte zichtbaarheid en controle, waardoor het risico toenam door hergebruik van wachtwoorden, zwakke aanmeldingsgegevens en een verminderde mogelijkheid om beveiligingscontroles af te dwingen voor naleving en zekerheid voor klanten. De vorige leveranciers van geheimenbeheer en PAM van de organisatie waren duur en moeilijk te implementeren.

Asite moest niet alleen interne gebruikers beveiligen, maar ook externe partners en leveranciers die samenwerken aan complexe bouwprojecten hetzelfde niveau van bescherming bieden, zodat zij konden voldoen aan de verwachtingen van klanten en contractuele verplichtingen. De organisatie zocht een veilige, gebruiksvriendelijke oplossing die al haar cybersecuritybehoeften kon ondersteunen via een gecentraliseerd platform.

> **"De (Beveiligings)architectuur en de flexibiliteit van KeeperPAM zijn ongeëvenaard."**
>
> **Tiago Rosado | Hoofd Informatiebeveiliging**

## De Keeper-oplossing

Asite heeft **KeeperPAM** geselecteerd als haar uniforme platform om geprivilegieerde toegang, aanmeldingsgegevens, verbindingen en geheimen binnen de hele organisatie te beveiligen. Door de cybersecuritytechnologie te consolideren in één zero-trust, zero-knowledge platform, heeft Asite de complexiteit verminderd en tegelijkertijd de beveiliging en naleving verbeterd.

**Gecentraliseerde geprivilegieerde toegang met lage operationele overhead -** KeeperPAM biedt veilige, controleerbare geprivilegieerde toegang tot servers, infrastructuur en gevoelige systemen zonder aanmeldingsgegevens bloot te stellen. Sessieactiviteiten worden centraal geregistreerd en vastgelegd ter ondersteuning van onderzoeken, verantwoording en naleving in klant- en regelgevende omgevingen. KeeperAI beëindigt automatisch risicosessies en genereert activiteitenoverzichten met nauwkeurige forensische details voor audits en incidentrespons.

KeeperPAM kon dankzij de snelle implementatie en flexibele architectuur zowel de verouderde PAM- als geheimenbeheertools van Asite vervangen en tegelijkertijd de dekking van geprivilegieerde toegang uitbreiden naar extra systemen, zonder dat dit extra kosten of complexiteit met zich meebracht.

> **"De implementatie van KeeperPAM was buitengewoon eenvoudig en behoort tot de beste die ik heb meegemaakt. Ik wou dat andere tools net zo makkelijk te implementeren waren."**
>
> **Tiago Rosado | Hoofd informatiebeveiliging**

**Wachtwoordbeheer voor ondernemingen, geïntegreerd in KeeperPAM -** Is onderdeel van het KeeperPAM-platform heeft Asite **wachtwoordbeheer** voor alle medewerkers binnen de gehele organisatie gestandaardiseerd. Hiermee zijn browsergebaseerde wachtwoordbeheerders vervangen en is een gecentraliseerde, afdwingbare aanpak voor de beveiliging van aanmeldingsgegevens geïntroduceerd.

Dit maakte door de beheerder gecontroleerd wachtwoordbeleid voor lengte en complexiteit mogelijk en voorkwam hergebruik van aanmeldingsgegevens in verschillende applicaties. Het IT-team kan nu gecompromitteerde aanmeldingsgegevens identificeren met behulp van BreachWatch®, de dark web-monitoringtool van Keeper, wat de beveiligingshouding van de organisatie verder versterkt. De toegang tot wachtwoordbeheer binnen dezelfde kluis als KeeperPAM zorgt voor consistent beheer van de aanmeldingsgegevens van zowel eindgebruikers als geprivilegieerde gebruikers, in combinatie met een eenvoudige gebruikerservaring.

**Modern geheimenbeheer met Keeper Secrets Manager -** Om applicatie- en infrastructuurgeheimen te beschermen, heeft Asite **Keeper Secrets Manager** geïmplementeerd als een systeemeigen component van het KeeperPAM-platform en verving zo de vorige tool voor geheimenbeheer. Keeper Secrets Manager automatiseert het aanmaken en rouleren van wachtwoorden, sleutels en geheimen, verwijdert lang bestaande of handmatig beheerde aanmeldingsgegevens en integreert eenvoudig via duidelijke **API's en robuuste documentatie**. Dit wordt allemaal uitgevoerd met minimale operationele overhead voor IT- en beveiligingsteams.

> **"De overhead is minimaal... De automatisering en roulatie van wachtwoorden en sleutels is fantastisch."**
>
> **Tiago Rosado | Hoofd informatiebeveiliging**

Het beheer van geheimen, wachtwoorden en geprivilegieerde toegang binnen KeeperPAM maakte consistent beheer mogelijk voor zowel menselijke als niet-menselijke identiteiten.

**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 gegevenslek. Keeper combineert Elliptic-Curve Cryptography (ECC) op apparaatniveau met **meerdere lagen van versleuteling** (op kluis-, map- en recordniveau), multi-factor- en biometrische authenticatie, evenals FIPS 140-3 gevalideerde AES 256-bits versleuteling plus PBKDF2. Keeper is **SOC 2- en ISO 27001-conform** — met de langste aaneengesloten naleving in de sector — en tevens FedRAMP High- en GovRAMP-geautoriseerd.

## Impact op de organisatie

Doordat Asite het volledige PAM-platform van Keeper heeft geïmplementeerd voor het beheer van wachtwoorden, geheimen en geprivilegieerde toegang, heeft het bedrijf een uniform, schaalbaar beveiligingsraamwerk opgezet dat de bescherming verbetert en tegelijkertijd de operationele complexiteit voor zijn IT- en beveiligingsteams vermindert.

**Verbeterd beveiligingsniveau met meetbare resultaten -** Het centraliseren van het beheer van aanmeldingsgegevens en toegang stelde Asite in staat haar algehele beveiligingspositie aanzienlijk te versterken. Sterkere wachtwoordhygiëne, automatische roulatie van geheimen en gecontroleerde geprivilegieerde toegang verminderden de blootstelling aan zowel externe bedreigingen als risico's van binnenuit. Aanmeldingsgegevens worden niet langer handmatig aangemaakt, gedeeld of hergebruikt, wat consistente handhaving van beveiligingsbeleid binnen de organisatie ondersteunt.

Het is cruciaal dat deze controles meetbaar en controleerbaar zijn, zodat ze voldoen aan de wettelijke en contractuele vereisten in verschillende regio's en klantomgevingen.

> **"De belangrijkste voordelen van het KeeperPAM-platform zijn kostenbesparing, vermindering van het beheer van systeemoverhead, verbetering van de naleving van beveiligingsvereisten en een aanzienlijke verbetering van de beveiligingsstatus."**
>
> **Tiago Rosado | Hoofd Informatiebeveiliging**

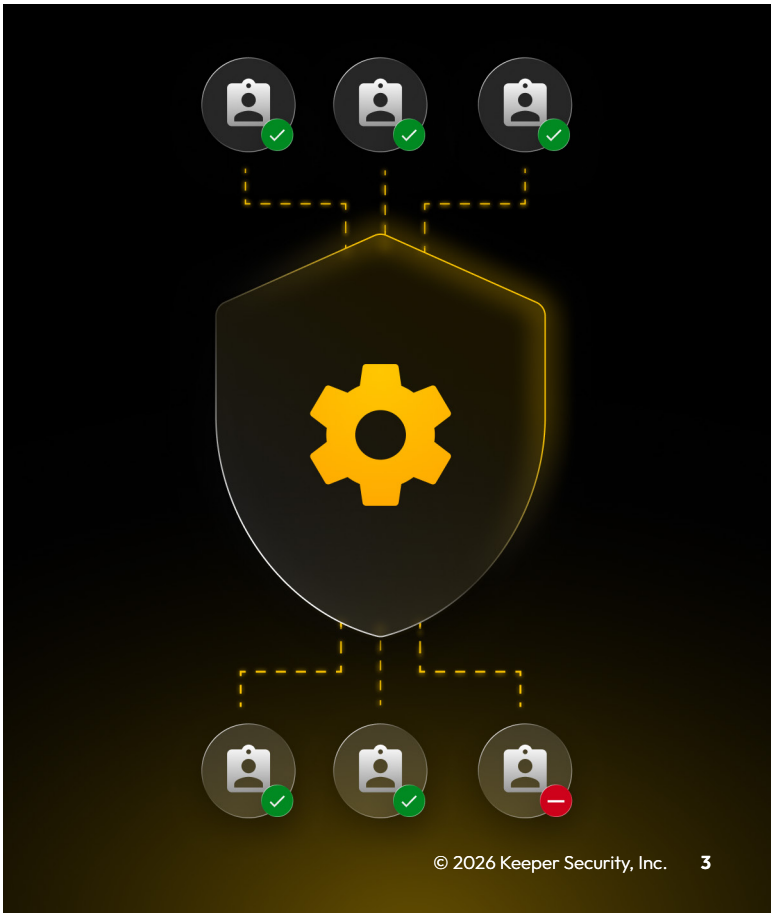
**Verminderde operationele overhead en consolidatie van tools -** Door wachtwoordbeheer, geheimenbeheer en PAM te consolideren in één platform, verminderde Asite de uitbreiding van tools en vereenvoudigde het beheer, waardoor de operationele overhead daalde. Deze aanpak stelde slanke IT- en beveiligingsteams in staat om toegangscontroles efficiënter te beheren zonder extra personeel of operationele lasten, terwijl de dekking werd uitgebreid om een breder scala aan systemen en omgevingen te beschermen.

**Verminderde blootstelling aan interne risico's en sterkere verantwoordelijkheid -** Met centraal beheerde en gemonitorde geprivilegieerde toegang versterkte Asite het vermogen om risicovolle activiteiten te detecteren, onderzoeken en erop te reageren. Sessie-monitoring en audittrails ondersteunen de controleerbaarheid en verkleinen de kans op opzettelijk of onopzettelijk misbruik.

**Voortdurende samenwerking en mogelijkheden -** Asite benadrukte niet alleen het belang van technologie, maar ook het belang van betrouwbare ondersteuning en begeleiding tijdens de implementatie en acceptatie. De ondersteunings- en implementatieteams van Keeper speelden een cruciale rol bij het waarborgen van een effectieve implementatie van het platform en de afstemming ervan op de operationele behoeften van de organisatie.

> **"De kwaliteit van de ondersteuning — zelfs als het de meest technische vraag is, zullen ze een diepgaande analyse doen [...] Het trainingsteam [was] absoluut van cruciaal belang en paste de training aan om zich aan ons aan te passen."**
>
> **Tiago Rosado | Hoofd Informatiebeveiliging**

KeeperPAM vormde de basis van de toegangsbeveiligingsstrategie van Asite en bood centrale controle over menselijke en niet-menselijke identiteiten in wereldwijde omgevingen. Door geprivilegieerde toegang, wachtwoordbeheer en geheimenbeheer samen te brengen in één platform, heeft Asite de beveiliging versterkt, de operationele efficiëntie verbeterd en een schaalbare basis gelegd voor toekomstige groei.



## KeeperPAM

KeeperPAM is een next-gen platform voor geprivilegieerd toegangsbeheer 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 geprivilegieerde accounts te beschermen, minimale privileges te handhaven, externe infrastructuur te beveiligen en te voldoen aan nalevingsvereisten, 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. De gebruiker heeft dankzij de mogelijkheden voor externe sessies nooit toegang tot de aanmeldingsgegevens of SSH-sleutels. De toegang tot een bron kan tijdelijk zijn en aanmeldingsgegevens worden automatisch gewijzigd nadat de toegang is ingetrokken, waardoor just-in-time (JIT) toegang wordt geboden zonder dat aanmeldingsgegevens ooit worden blootgesteld.

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 monitor alle geprivilegieerde accounts
- Bied JIT-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
- Registreer sessies met meerdere protocollen met AI-dreigingsdetectie en geautomatiseerde beëindiging van sessies
- Automatiseer wachtwoordroulatie
- Dwing MFA-bescherming af op elk systeem
- Implementeer naadloos via web- of desktop-app met geautomatiseerde SCIM-inrichting

**Bescherm uw organisatie met Keeper**

Als u meer informatie wilt over hoe Keeper uw organisatie kan beschermen met een gebruiksvriendelijk platform, **neemt u contact op met ons verkoopteam** voor een gratis proefperiode of een gepersonaliseerde demo.

## Over Keeper

Keeper Security is een van de snelst groeiende cybersecurity-softwarebedrijven 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 is erkend voor zijn innovatie in het Gartner Magic Quadrant voor Privileged Access Management (PAM) en 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.**

Gartner

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

Prijs voor uitmuntende cyberbeveiliging
**Privileged Access Management**

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

Newsweek
**#1 Cybersecurity platform**

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