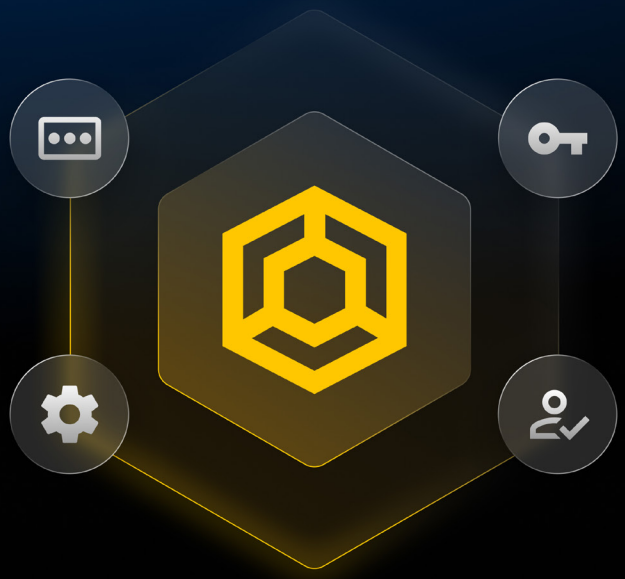
FALLSTUDIE

Asite sichert unternehmensweit Zugangsdaten, Geheimnisse und privilegierte Zugriffe mit KeeperPAM®



Hintergrund

Asite ist ein SaaS-Unternehmen, das die Bauindustrie bedient und Organisationen bei der Verwaltung komplexer Projekte unterstützt – von 3D-Modellen und digitalen Zwillingen bis hin zur Dokumentenkontrolle und Lieferantenzusammenarbeit – über globale Teams und Regionen hinweg. Asite ist in verschiedenen Regionen aktiv und betreibt Rechenzentren an neun Standorten mit mehr als 500 Mitarbeitern.

Branche
Bautechnologie (SaaS)

Mitarbeiter
500+

Lösungen
KeeperPAM

Die Herausforderung

Für ein globales SaaS-Unternehmen, das große Bauprojekte unterstützt, darunter Kunden in kritischen Infrastrukturen und verteidigungsnahen Bereichen, ist die sichere Verwaltung von Zugangsdaten und privilegierten Zugriffen unerlässlich. Asite benötigte einen zentralisierteren und besser durchsetzbaren Ansatz für Passwörter, Geheimnisse und Privileged Access Management (PAM) im gesamten Unternehmen.

Legacy-Tools mit fragmentierter Transparenz -Die Abhängigkeit von browserbasierten Passwortmanagern schränkt die Transparenz und Kontrolle ein und erhöht das Risiko durch die Wiederverwendung von Passwörtern, schwache Zugangsdaten und eine reduzierte Fähigkeit zur Durchsetzung von Sicherheitskontrollen für Compliance und Kundenzufriedenheit. Die vorherigen Geheimnisverwaltungs- und PAM-Anbieter der Organisation waren kostspielig und schwierig zu implementieren.

Neben der Sicherung der internen Benutzer musste Asite das gleiche Schutzniveau auch auf externe Partner und Lieferanten ausdehnen, die an komplexen Bauprojekten mitarbeiten, um sicherzustellen, dass diese die Kundenerwartungen und vertraglichen Verpflichtungen erfüllen. Die Organisation suchte eine sichere, benutzerfreundliche Lösung, die alle ihre Cybersicherheitsanforderungen auf einer zentralen Plattform abdecken konnte.

> **„Die (Sicherheits-)Architektur und die Flexibilität von KeeperPAM sind unübertroffen.“**
>
> **Tiago Rosado | Chief Information Security Officer**

Die Keeper-Lösung

Asite wählte **KeeperPAM** als seine einheitliche Plattform zur Sicherung privilegierter Zugriffe, Zugangsdaten, Verbindungen und Geheimnisse im gesamten Unternehmen. Durch die Konsolidierung seines Cybersicherheits-Technologiestacks in eine einzige Zero-Trust- und Zero-Knowledge-Plattform reduzierte Asite die Komplexität und verbesserte gleichzeitig Sicherheit und Compliance.

Zentralisierter privilegierter Zugriff bei geringem Betriebsaufwand - KeeperPAM bietet sicheren, nachvollziehbaren privilegierten Zugriff auf Server, Infrastruktur und empfindliche Systeme, ohne Zugangsdaten preiszugeben. Die Sitzungsaktivitäten werden zentral protokolliert und aufgezeichnet, was Untersuchungen, Verantwortlichkeit und die Einhaltung von Vorschriften im Kunden- und Regulierungsbereich unterstützt. KeeperAI beendet automatisch Sitzungen mit hohem Risiko und generiert Aktivitätszusammenfassungen mit präzisen forensischen Details für Prüfungs- und Vorfallsreaktionszwecke.

Dank schneller Bereitstellung und flexibler Architektur ersetzte KeeperPAM sowohl die veralteten PAM- als auch die Geheimnisverwaltungstools von Asite, und erweiterte gleichzeitig die Abdeckung des privilegierten Zugriffs auf zusätzliche Systeme, ohne die Kosten oder die Komplexität zu erhöhen.

> **„Die Implementierung von KeeperPAM war extrem einfach, eine der besten, die ich je erlebt habe. Ich wünschte, andere Tools wären genauso einfach einzusetzen."**
>
> **Tiago Rosado | Chief Information Security Officer**

Integrierte Enterprise Passwortverwaltung in KeeperPAM - Als Teil der KeeperPAM-Plattform standardisierte Asite die unternehmensweite **Passwortverwaltung** für alle Mitarbeiter, ersetzte browserbasierten Passwortmanager und etablierte einen zentralisierten, durchsetzbaren Ansatz für die Zugangsdatensicherheit.

Dies ermöglichte die vom Administrator kontrollierte Festlegung von Passwortrichtlinien hinsichtlich der Länge und Komplexität, und verhinderte die Wiederverwendung von Anmeldeinformationen in verschiedenen Anwendungen. Das IT-Team kann jetzt kompromittierte Zugangsdaten mithilfe des Dark-Web-Überwachungstools BreachWatch® von Keeper identifizieren und so die Sicherheitslage des Unternehmens weiter stärken. Der Zugriff auf die Passwortverwaltung innerhalb desselben Tresors wie KeeperPAM gewährleistet eine einheitliche Governance sowohl für Endbenutzer als auch für privilegierte Zugangsdaten und sorgt für eine einfache Benutzererfahrung.

Moderne Geheimnisverwaltung mit Keeper Secrets Manager - Um Anwendungs- und Infrastrukturgeheimnisse zu schützen, hat Asite Keeper Secrets Manager als native Komponente der KeeperPAM-Plattform eingeführt und damit sein bisheriges Geheimnisverwaltungstool ersetzt. Keeper Secrets Manager automatisiert die Erstellung und Rotation von Passwörtern, Schlüsseln und Geheimnissen, entfernt langlebige oder manuell verwaltete Zugangsdaten und lässt sich dank **klarer APIs und robuster Dokumentation** problemlos integrieren – und das alles mit minimalem operativem Aufwand für IT- und Sicherheitsteams.

> **„Der Aufwand ist minimal. die Automatisierung und Rotation von Passwörtern und Schlüsseln ist fantastisch."**
>
> **Tiago Rosado | Chief Information Security Officer**

Die Verwaltung von Geheimnissen neben Passwörtern und privilegierter Zugriffe innerhalb von KeeperPAM ermöglichte eine konsistente Verwaltung sowohl menschlicher als auch nicht-menschlicher Identitäten.

Erstklassige Sicherheit - Die Zero-Trust- und Zero-Knowledge-Sicherheitsarchitektur von Keeper ist unübertroffen, wenn es darum geht, Informationen zu schützen und das Risiko einer Datenschutzverletzung zu mindern. Keeper kombiniert Elliptic-Curve-Kryptographie (ECC) auf Geräteebene mit **mehreren Verschlüsselungsebenen** (auf Tresor-, Ordner- und Datensatzebene), Multi-Faktor- und biometrischer Authentifizierung sowie FIPS 140-3-validierter AES-256-Bit-Verschlüsselung plus PBKDF2. Keeper ist **SOC 2- und ISO 27001-konform** — mit der am längsten anhaltenden Compliance in der Branche – sowie FedRAMP High- und GovRAMP-autorisiert.

Auswirkungen auf die Organisation

Durch den Einsatz der umfassenden PAM-Plattform von Keeper zur Verwaltung von Passwörtern, Geheimnissen und privilegierten Zugriffen hat Asite ein einheitliches, skalierbares Sicherheitsframework geschaffen, das den Schutz verbessert und gleichzeitig die betriebliche Komplexität für die IT- und Sicherheitsteams verringert.

Verbesserte Sicherheitslage mit messbaren Ergebnissen - Die Zentralisierung von Zugangsdaten- und Zugriffsmanagement ermöglichte es Asite, seine allgemeine Sicherheitslage deutlich zu verbessern. Stärkere Passworthygiene, automatisierte Geheimnisrotation und kontrollierter privilegierter Zugriff verringern die Anfälligkeit für externe Bedrohungen und Insiderrisiken. Zugangsdaten werden nicht mehr manuell erstellt, weitergegeben oder wiederverwendet, wodurch eine einheitliche Durchsetzung der Sicherheitsrichtlinien im gesamten Unternehmen unterstützt wird.

Entscheidend ist, dass diese Kontrollen messbar und überprüfbar sind und somit dazu beitragen, regulatorische und vertragliche Anforderungen in verschiedenen Regionen und Kundenumgebungen zu erfüllen.

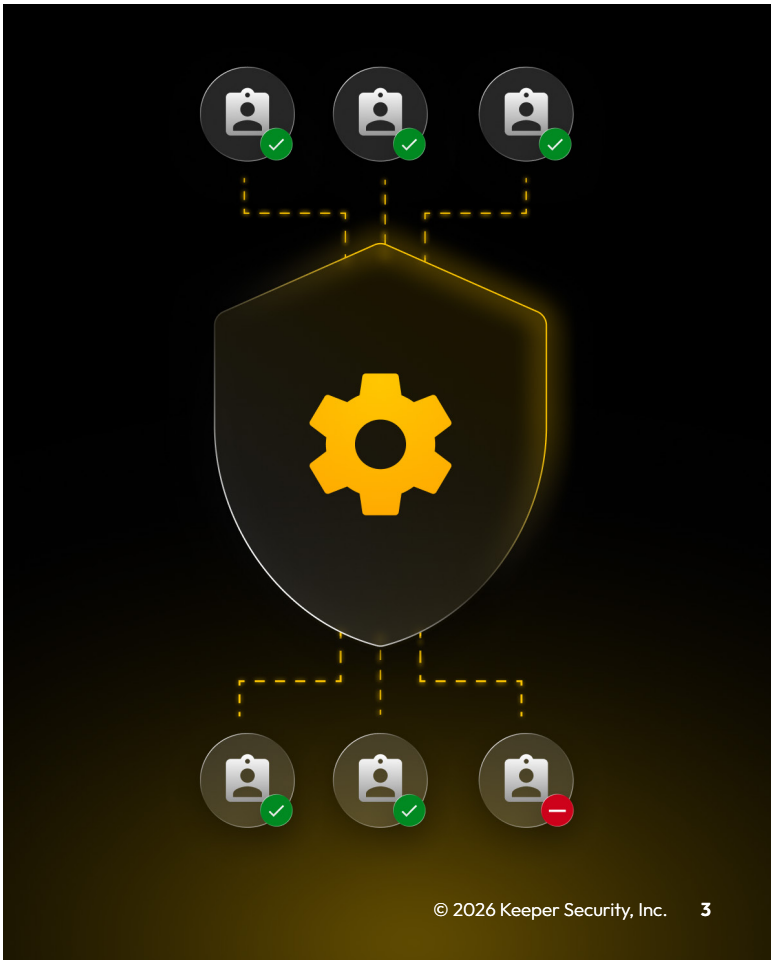
> **„Die wichtigsten Vorteile der KeeperPAM-Plattform sind die Senkung der Kosten, die Verringerung des Verwaltungsaufwands für Systeme, die Verbesserung der Einhaltung von Sicherheitsanforderungen und definitiv die Steigerung des Sicherheitsniveaus."**
>
> **Tiago Rosado | Chief Information Security Officer**

Reduzierter Betriebsaufwand und Konsolidierung der Tools– Durch die Konsolidierung von Passwortmanagement, Geheimnisverwaltung und PAM auf einer einzigen Plattform reduzierte Asite die Tool-Vielfalt und vereinfachte die Administration, wodurch der Betriebsaufwand gesenkt wurde. Dieser Ansatz ermöglichte es schlanken IT- und Sicherheitsteams, Zugriffskontrollen effizienter zu verwalten, ohne die Mitarbeiterzahl oder den operativen Aufwand zu erhöhen, und gleichzeitig die Abdeckung zu skalieren, um ein breiteres Spektrum an Systemen und Umgebungen zu schützen. Geringeres Insiderrisiko und stärkere.

Kontinuierliche Partnerschaft und Befähigung - Neben der Technologie hob Asite die Bedeutung verlässlicher Unterstützung und Befähigung während der gesamten Implementierungs- und Einführungsphase hervor. Die Support- und Enablement-Teams von Keeper spielten eine entscheidende Rolle dabei, sicherzustellen, dass die Plattform effektiv implementiert und auf die betrieblichen Bedürfnisse der Organisation abgestimmt wurde.

> **„Die Qualität des Supports – selbst bei hochtechnischen Fragen gehen sie der Sache gründlich nach [...] Das Schulungsteam [war] absolut entscheidend und hat die Schulung an unsere Gegebenheiten angepasst."**
>
> **Tiago Rosado | Chief Information Security Officer**

KeeperPAM wurde zur Grundlage der Zugangssicherheitsstrategie von Asite und ermöglichte eine zentralisierte Kontrolle über menschliche und nicht-menschliche Identitäten in globalen Umgebungen. Durch die Zusammenführung von privilegiertem Zugriff, Passwortverwaltung und Geheimnisverwaltung auf einer einzigen Plattform hat Asit die Sicherheit gestärkt, betriebliche Effizienz verbessert und eine skalierbare Grundlage für zukünftiges Wachstum geschaffen.



KeeperPAM

KeeperPAM ist eine Plattform zur privilegierten Zugriffsverwaltung der nächsten Generation, die den Zugriff auf kritische Ressourcen wie Server, Webanwendungen, Datenbanken und Workloads sichert und verwaltet. KeeperPAM basiert auf einer Zero-Trust- und Zero-Knowledge-Sicherheitsarchitektur und unterstützt Organisationen jeder Größe beim Schutz privilegierter Konten, bei der Durchsetzung des Prinzips der minimalen Berechtigungen, der Sicherung der Remote-Infrastruktur und der Erfüllung von Compliance-Anforderungen – mit unübertroffener Benutzerfreundlichkeit und schneller Bereitstellung.

Keeper ist intuitiv und einfach zu implementieren, unabhängig von der Unternehmensgröße. KeeperPAM verwendet einen Gateway-Dienst mit Zero-Trust für den Zugriff auf die jeweiligen Umgebungen. Es sind keine Firewall-Updates oder Änderungen am Eingangssignal erforderlich, wodurch ein nahtloser, sicherer Zugriff ohne Komplexität ermöglicht wird. Mit den Remote-Sitzungsfunktionen von Keeper hat der Benutzer niemals Zugriff auf die Zugangsdaten oder SSH-Schlüssel. Der Zugriff auf eine Ressource kann zeitlich begrenzt sein, und die Zugangsdaten werden nach dem Entzug des Zugriffs automatisch rotiert, wodurch ein JIT-Zugriff (Just in Time) ermöglicht wird, ohne dass die Anmeldedaten jemals offengelegt werden.

Keeper ist so konzipiert, dass es für Organisationen jeder Größe skaliert werden kann. KeeperPAM zentralisiert den Zugriff über mehrere Cloud-Anbieter, lokale Workloads und Client-Umgebungen hinweg in einer einzigen Benutzeroberfläche und ermöglicht so das Multi-Cloud-Management.

Anwendungsfälle im Geschäftsleben: KeeperPAM

- Alle privilegierten Konten kontrollieren und überwachen
- JIT-Zugriff gewähren, ohne Zugangsdaten preiszugeben
- Konsolidierung der Entwicklungswerkzeuge auf einer Plattform mit intuitiver Benutzeroberfläche
- Nahtlose Verwaltung von Cloud-, Hybrid- und Multi-Cloud-Umgebungen ermöglichen
- Aufzeichnung von Multiprotokoll-Sitzungen mit KI-Bedrohungserkennung und automatischer Sitzungsbeendigung
- Automatisierte Passwortrotation
- Setzen Sie MFA-Schutz auf jedem System durch
- Nahtlose Bereitstellung über Web- oder Desktop-App mit automatisierter SCIM-Bereitstellung

Schützen Sie Ihre Organisation mit Keeper

Um mehr darüber zu erfahren, wie Keeper Ihre Organisation mit einer benutzerfreundlichen Plattform schützen kann, **kontaktieren Sie unser Vertriebsteam** für eine kostenlose Testversion oder eine personalisierte Demo.

Über Keeper

Keeper Security ist eines der am schnellsten wachsenden Unternehmen für Cybersicherheitssoftware, das Tausende von Organisationen und Millionen von Menschen in über 150 Ländern schützt. Keeper ist ein Pionier der Zero-Knowledge- und Zero-Trust-Sicherheit für jede IT-Umgebung. Das Herzstück, KeeperPAM®, ist eine KI-fähige, Cloud-native Plattform, die alle Benutzer, Geräte und Infrastrukturen vor Cyberangriffen schützt. Keeper wurde für seine Innovationen im Gartner Magic Quadrant für Privileged Access Management (PAM) ausgezeichnet und sichert Passwörter und Passkeys, Infrastrukturgeheimnisse, Remote-Verbindungen und Endpunkte mit rollenbasierten Durchsetzungsrichtlinien, Least-Privilege und Just-in-Time-Zugriff.

Auf Keeper vertrauen Tausende Unternehmen und Millionen Menschen weltweit.

Gartner

KeeperPAM® wurde im Gartner Magic Quadrant™ 2025 für PAM ausgezeichnet

Auszeichnung für herausragende Leistungen im Bereich Cybersicherheit **Privileged Access Management**

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

Newsweek **#1 Cybersecurity-Plattform**

Enterprise Management Associates **KeeperPAM® wurde für seine Produktstärke ausgezeichnet**