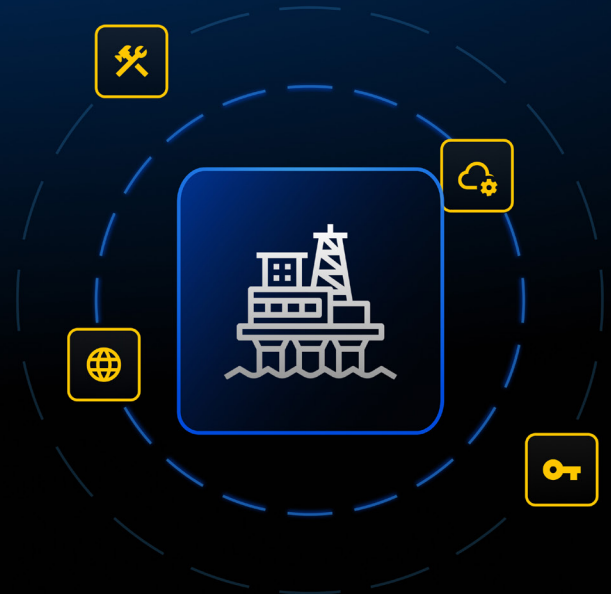


FALLSTUDIE

DrillDocs gewährleistet weltweiten Offshore-Betrieb und technischen Support rund um die Uhr mit KeeperPAM®



Hintergrund

DrillDocs ist ein Technologie-Start-up-Unternehmen in der Gründungsphase, das Computer-Vision-Software für Anwendungen im Bereich der Offshore-Bohrungen anbietet. Die Plattform überwacht den Bohrvorgang in Echtzeit und analysiert das Bohrgut, um den Betreibern bei der Verbesserung der Sicherheit, Effizienz und Leistung auf Offshore-Bohrinseln zu unterstützen.

Branche
Öl und Gas

Mitarbeiter
Über 20

Lösungen
KeeperPAM
Keeper Secrets Manager



Die Herausforderung

Mit der Entwicklung von DrillDocs von einem ursprünglichen Ingenieurteam zu einem verteilten Produktionsunterstützungsunternehmen wurde die Zugriffsverwaltung immer komplexer. In der Anfangsphase kümmerte sich ein kleines internes Team sowohl um die Entwicklung als auch um den Support, wobei die Zugangsdaten sicher gespeichert und der Zugriff durch informelle, manuelle Prozesse streng kontrolliert wurde. Angesichts der steigenden Kundennachfrage und der internationalen Einführung der Systeme beauftragte DrillDocs ein externes Unternehmen für technische Dienstleistungen mit der Bereitstellung von Support-Diensten über Nacht, um eine echte Betriebsbereitschaft rund um die Uhr zu gewährleisten. Das Unternehmen setzte auf Keeper Secrets Manager, um den Abruf von Zugangsdaten während der Bereitstellung zu automatisieren. Die Zugangsdaten wurden während der Systembildung programmgesteuert eingefügt und während der Laufzeit-Workflows im Speicher gehalten, wodurch sichergestellt wurde, dass sie auf den Produktionssystemen niemals im Klartext gespeichert wurden.

Während dieser Ansatz sichere DevOps-Workflows effektiv unterstützte, erforderte die Verwaltung interaktiver privilegierter Sitzungen über verteilte interne und externe Benutzer hinweg eine sichere PAM-Lösung (Privileged Access Management). Durch die Ausweitung der Betriebsabdeckung wurden neue behördliche Anforderungen in Bezug auf die Gewährung, Überwachung und Sperrung von privilegiertem Zugriff für globale Teams und nicht verwaltete Geräte eingeführt. Die Führungsebene benötigte mehr Transparenz, strengere Zugriffskontrollen und eine Lösung, die sicher mit den globalen Aktivitäten des Unternehmens skaliert werden konnte.

„Wir machten uns Gedanken darüber, wie wir die Sicherheit bei der Arbeit mit privaten Computern am besten gewährleisten können. Wir vertrauen unseren Partnern, mussten aber zu einer Kultur übergehen, in der wir zwar vertrauen, aber dennoch überprüfen.“

Francois Ruel | Mitbegründer und Wissenschaftlicher Leiter, DrillDocs

Die Keeper-Lösung

DrillDocs setzte **KeeperPAM** ein, eine umfassende PAM-Plattform mit Zero-Trust- und Zero-Knowledge-Architektur, um den privilegierten Zugriff zu zentralisieren, Zugangsdaten zu sichern und eine kontrollierte Remote-Sitzungsverwaltung zu ermöglichen, ohne technische Workflows zu stören.

Schnelle Bereitstellung mit sofortigem Nutzen - Der Implementierungsprozess von Keeper ist einfach und unkompliziert, sodass sowohl interne Ingenieure als auch externe Supportteams nahtlos auf ein sichereres Zugriffsmodell umsteigen können. Keeper bietet umfangreiche **Produktdokumentation**, Implementierungsressourcen und Endbenutzeranleitungen, um eine erfolgreiche Einführung zu unterstützen. Ausführliche **Produktanleitungen** und **Schulungsvideos** tragen maßgeblich zu einer hohen Akzeptanz bei den Benutzern bei.

„An dem Tag, an dem wir beschlossen, unsere Testversion zu starten, konnten wir alles innerhalb von zwei Stunden einrichten. Von da an haben wir sofort mit der Verwendung von Keeper begonnen.“

Francois Ruel | Mitbegründer und
Wissenschaftlicher Leiter, DrillDocs

Sicherer virtualisierter Zugriff ohne Verwaltung von Endpunkten - KeeperPAM ermöglicht über ein Zero-Trust-Gateway einen sicheren, browserbasierten Zugriff auf virtuelle Windows- und Linux-Desktops, wodurch die Installation von VPNs oder die direkte Netzwerkesposition auf privaten Geräten entfällt. Durch die Speicherung von Konnektivitäts- und Verwaltungstools in einer sicheren virtuellen Umgebung trägt KeeperPAM dazu bei, dass privilegierte Zugangsdaten niemals dem Endbenutzer zugänglich gemacht werden. Der gesamte Infrastrukturzugriff wird zentral gesteuert, verschlüsselt und protokolliert, wodurch Unternehmen volle Transparenz und Kontrolle über privilegierte Remote-Sitzungen erhalten.

Sofortige Zugriffsbereitstellung und -entziehung - KeeperPAM optimiert die Verwaltung des Benutzerlebenszyklus, indem es Administratoren ermöglicht, privilegierte Zugriffe innerhalb von Sekunden bereitzustellen, zu ändern und zu entziehen. Durch zentralisierte, rollenbasierte Zugriffskontrollen und die Durchsetzung von Richtlinien können Unternehmen den Zugriff auf kritische Systeme sofort gewähren oder Berechtigungen entziehen, wenn sich Rollen ändern oder Benutzer das Unternehmen verlassen. Diese Echtzeit-Bereitstellungsfunktion reduziert den administrativen Aufwand, beseitigt beständige Zugriffsrisiken und gewährleistet, dass privilegierte Konten jederzeit streng kontrolliert werden.

Sichere automatische Bereitstellungen ohne Offenlegung von Zugangsdaten - **Keeper Secrets Manager** sichert den Maschinen-zu-Maschinen-Zugriff, indem automatisierte Bereitstellungen und Systemaktualisierungen ermöglicht werden, ohne dass Zugangsdaten offengelegt oder hartcodiert werden müssen. Während der Erstellungsprozesse werden Zugangsdaten programmgesteuert abgerufen und direkt in den Speicher geladen, wodurch sichergestellt wird, dass sie niemals im Klartext gespeichert oder auf den Systemen zurückbleiben. Dieser Ansatz stärkt die DevOps-Sicherheit durch die Beseitigung der Geheimnisverbreitung (Secrets Sprawl) und erhält gleichzeitig die Effizienz der Automatisierung aufrecht.

„Ich nutze den Tresor mehrmals täglich. Wir verwenden außerdem den Keeper Secrets Manager für automatisierte Bereitstellungen und Updates. Das funktioniert für uns sehr gut.“

David Momberger | Leitender Systemingenieur,
DrillDocs

Erstklassige Sicherheit - Die Zero-Trust- und Zero-Knowledge-Sicherheitsarchitektur von Keeper ist darauf ausgelegt, Informationen zu schützen und das Risiko von Datenschutzverletzungen zu reduzieren. Keeper kombiniert Elliptic-Curve-Kryptographie (ECC) auf Geräteebene mit **mehreren Verschlüsselungsebenen** (auf Tresor-, Ordner- und Datensatzebene), quantensicherer Kryptographie, Multi-Faktor- und biometrischer Authentifizierung sowie FIPS 140-3-validierter AES-256-Bit-Verschlüsselung plus PBKDF2. Keeper ist **SOC 2- und ISO/IEC 27001-konform und unterstützt zudem ISO/IEC 27017 und 27018**, wobei es sich um die branchenweit am längsten bestehende Konformität handelt. Keeper ist FedRAMP- und GovRAMP-High-autorisiert, PCI-DSS-zertifiziert und von TrustArc für den Datenschutz zertifiziert.



Auswirkungen auf das Unternehmen

Seit der Implementierung von KeeperPAM hat DrillDocs seine Sicherheitslage deutlich verbessert und gleichzeitig die für ein schnell wachsendes globales Start-up-Unternehmen erforderliche Agilität bewahrt. Gemeinsam genutzte Administratorpasswörter wurden abgeschafft, und privilegierte Zugangsdaten werden nun in einem Tresor gespeichert, zufällig generiert und durch rollenbasierte Zugriffskontrollen geregelt. Das BYOD-Modell (Bring Your Own Device) des Unternehmens verursacht keine Probleme mehr in Bezug auf Transparenz oder betriebliche Belastungen.

„Keeper hat unsere digitale Sicherheitskultur stark verändert. Wir bewahren unsere Zugangsdaten nicht mehr an unsicheren Orten auf.“

François Ruel | Mitbegründer und Wissenschaftlicher Leiter, DrillDocs

Riesgo reducido en una fuerza laboral remota con BYOD - KeeperPAM reduce el riesgo en la fuerza laboral remota con BYOD de DrillDocs al aislar el acceso privilegiado dentro de entornos virtuales seguros. Los ingenieros y socios externos pueden conectarse de forma segura a los sistemas de producción desde cualquier parte del mundo sin exponer credenciales ni instalar herramientas de acceso confidenciales directamente en dispositivos personales.

Acceso basado en roles, con privilegios mínimos - KeeperPAM permite a DrillDocs estructurar el acceso por rol en lugar de distribuir credenciales individuales. A los equipos de ingeniería de clientes, a los desarrolladores y a los socios externos se les concede acceso únicamente a los sistemas necesarios para el desempeño de sus funciones. Este enfoque redujo drásticamente los gastos administrativos, al tiempo que garantizó que el acceso privilegiado se mantuviera bajo un estricto control.

„Das Onboarding oder Offboarding von Mitarbeitern ist jetzt viel einfacher und schneller. Wenn eine Person Zugriff auf etwas Neues benötigt, dauert es nur noch wenige Sekunden, bis der Zugriff gewährt ist.“

Mert Geveci | Technische Direktor, DrillDocs

Optimiertes Onboarding und Offboarding der Benutzer- KeeperPAM hat Onboarding- und Offboarding-Prozesse transformiert, die Effizienz verbessert und den Verwaltungsaufwand reduziert. Der Zugriff kann innerhalb von Sekunden gewährt oder entzogen werden, sodass die Führungsebene umgehend auf operative Erfordernisse reagieren kann.

Vollständige Transparenz privilegierter Sitzungen - Die Sitzungsaufzeichnung und Aktivitätsprotokollierung von KeeperPAM ermöglichen umfassende Einblicke in privilegierte Aktivitäten. Bei ungewöhnlichem Verhalten kann die Führungsebene die Sitzungsdaten analysieren, um die Ursachen besser zu verstehen und angemessen zu reagieren. KeeperAI ermöglicht die automatische Beendigung risikoreicher Sitzungen und verschlüsselte Aktivitätszusammenfassungen. Diese Transparenz unterstützt das Sicherheitsmodell des Unternehmens für weltweit verteilte Ingenieure und externe Supportteams und bietet der Führungsebene einen klaren Überblick über den Zugriff auf und die Nutzung von Produktionsumgebungen.

Integrierte Governance zur Unterstützung der Compliance - Im Zuge der weiteren Bemühungen von DrillDocs um die SOC-2-Konformität bietet KeeperPAM eine solide Grundlage für die Erfüllung der Anforderungen an die Zugriffskontrolle. Die zentralisierte Zugangsdatenverwaltung, die rollenbasierte Durchsetzung des Least-Privilege-Prinzips und die Sitzungsüberwachungsfunktionen unterstützen die übergeordneten Governance- und Sicherheitsziele des Unternehmens.

Heute arbeitet DrillDocs mit dem Sicherheitsniveau eines viel größeren Unternehmens. Ingenieure können sich von überall auf der Welt und mit jedem Gerät sicher verbinden, ohne vertrauliche Zugangsdaten offenzulegen. Der Zugriff ist strukturiert, überwacht und zentral gesteuert. Das Onboarding erfolgt umgehend, das Offboarding zügig und richtlinienbasiert. Externe Partner können sicher ihren Beitrag leisten. Mit KeeperPAM ist das Unternehmen in der Lage, sicher zu skalieren und dabei die Geschwindigkeit und Innovationskraft beizubehalten, die sein Wachstum auszeichnen.



KeeperPAM

KeeperPAM ist eine PAM-Plattform (Privileged Access Management) der nächsten Generation, die den Zugriff auf kritische Ressourcen wie Server, Webanwendungen, Datenbanken und Workloads schützt und verwaltet. KeeperPAM basiert auf einer Zero-Trust- und Zero-Knowledge-Sicherheitsarchitektur und unterstützt Unternehmen beim Schutz privilegierter Konten, bei der Durchsetzung des Least-Privilege-Prinzips, bei der Absicherung der Remote-Infrastruktur und bei 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 Zero-Trust-Gateway-Dienst, um Verbindungen zu Zielumgebungen herzustellen, ohne dass Firewall-Updates oder Änderungen am Ingress erforderlich sind. Dank der Remote-Sitzungsfunktionen haben Benutzer niemals direkten Zugriff auf Zugangsdaten oder SSH-Schlüssel, sodass vertrauliche Daten vollständig von Endpunkten isoliert bleiben. Der Zugriff auf Ressourcen kann zeitlich begrenzt und durch Richtlinien geregelt sein, wobei die Zugangsdaten nach Entzug der Zugriffsberechtigung automatisch geändert werden. Dadurch wird ein sicherer JIT-Zugriff (Just-in-Time) ermöglicht, ohne Zugangsdaten jemals offenzulegen.

Keeper ist so konzipiert, dass es für Unternehmen 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
- Multiprotokoll-Sitzungen mit KI-Bedrohungserkennung und automatischer Sitzungsbeendigung aufnehmen
- Passwortrotation automatisieren
- MFA-Schutz auf jedem System durchsetzen
- Nahtlose Bereitstellung über Web- oder Desktop-App mit automatisierter SCIM-Bereitstellung

Schützen Sie Ihr Unternehmen mit Keeper

Um mehr darüber zu erfahren, wie Keeper Ihrem Unternehmen 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 Unternehmen 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-Prinzip und Just-in-Time-Zugriff. Erfahren Sie auf [KeeperSecurity.com](#), warum führende Unternehmen auf Keeper vertrauen, um sich gegen moderne Cyberbedrohungen zu verteidigen.

Auf Keeper vertrauen Tausende Unternehmen und Millionen Menschen weltweit.

Gartner

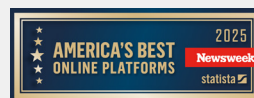
KeeperPAM® wurde im Gartner Magic Quadrant™2025 für PAM ausgezeichnet.



Auszeichnung für herausragende Leistungen im Bereich Cybersicherheit
Privileged Access Management



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



Newsweek
Nr. 1 Cyber-sicherheitsplattform



Enterprise Management Associates
KeeperPAM® wurde für seine Produktstärke ausgezeichnet