Case Study

DrillDocs Secures Global Offshore Operations and 24/7 Engineering Access With KeeperPAM®

Background

DrillDocs is a seed-stage technology startup that delivers computer vision software for offshore drilling applications. Its platform monitors the drilling process in real time, analyzing rock cuttings to help operators improve safety, efficiency and performance on offshore rigs.

Industry
Oil and Gas

Employees
20+

Solutions
KeeperPAM
Keeper Secrets Manager

The Challenge

As DrillDocs evolved from a founding engineering team into a distributed, production-support organization, access management became increasingly complex. In its early stages, a small internal team handled both development and support, with credentials stored securely and access tightly controlled through informal, manual processes. As customer demand increased and systems were deployed internationally, DrillDocs introduced an external engineering services firm to provide overnight support coverage and ensure true 24/7 operational readiness. The organization relied on Keeper Secrets Manager to automate credential retrieval during deployments. Credentials were programmatically injected during system builds and kept in memory during runtime workflows, ensuring they were never stored in plaintext on production systems.

While this approach effectively supported secure DevOps workflows, managing interactive privileged sessions across distributed internal and third-party users required a secure Privileged Access Management (PAM) solution. Expanding operational coverage introduced new governance requirements around granting, monitoring and revoking privileged access across global teams and unmanaged devices. Leadership needed greater visibility, tighter access controls and a solution that could scale securely alongside the company's global operations.

> **"We were getting worried about how to best manage security when work is done from personal machines. We trust our partners, but we needed to make a switch to a trust-but-verify culture."**
>
> **Francois Ruel | Co-founder and Chief Science Officer, DrillDocs**

The Keeper Solution

DrillDocs deployed **KeeperPAM** a comprehensive zero-trust, zero-knowledge PAM platform, to centralize privileged access, secure credentials and provide controlled remote session management without disrupting engineering workflows.

Rapid Deployment With Immediate Value - Keeper's implementation process is simple and straightforward, making it seamless to transition both internal engineers and third-party support teams to a more secure access model. Keeper offers extensive **product documentation**, implementation resources and end-user guidance to support successful rollouts. Detailed **product guides** and **training videos** help drive high user adoption.

> **"The day we decided to go start our trial, we were able to get everything set up in a two-hour session. From there, we started using Keeper right away."**
>
> **Francois Ruel | Co-founder and Chief Science Officer, DrillDocs**

Secure Virtualized Access Without Managing Endpoints- KeeperPAM enables secure, browser-based access to Windows and Linux virtual desktops through its zero-trust gateway, eliminating the need for VPN installations or direct network exposure on personal devices. By keeping connectivity and administrative tools contained within a secure virtual environment, KeeperPAM helps ensure that privileged credentials are never exposed to end users. All infrastructure access is centrally controlled, encrypted and logged, providing organizations with full visibility and governance over remote privileged sessions.

Instant Access Provisioning and Revocation - KeeperPAM streamlines user lifecycle management by enabling administrators to provision, modify and revoke privileged access in seconds. Through centralized, **role-based access controls** and policy enforcement, organizations can immediately grant access to critical systems or remove permissions when roles change or users depart. This real-time provisioning capability reduces administrative overhead, eliminates standing access risks and ensures privileged accounts remain tightly controlled at all times.

Secure Automated Deployments Without Exposing Credentials - Keeper Secrets Manager secures machine-to-machine access by enabling automated deployments and system updates without exposing or hardcoding credentials. During build processes, credentials are programmatically retrieved and injected directly into memory, ensuring they are never stored in plaintext or left behind on systems. This approach strengthens DevOps security by eliminating secrets sprawl while maintaining automation efficiency.

> **"I use the vault many times every day. We also use Keeper Secrets Manager for automated deployments and updates. It works very well for us."**
>
> **David Momberger | Senior Systems Engineer, DrillDocs**

Best-in-Class Security - Keeper's zero-trust, zero-knowledge security architecture is designed to safeguard information and reduce the risk of data breaches. Keeper combines device-level Elliptic-Curve Cryptography (ECC) with **multiple layers of encryption** (at the vault, folder and record levels), quantum-resistant cryptography, multi-factor and biometric authentication and FIPS 140-3 validated AES 256-bit encryption, plus PBKDF2. Keeper is **SOC 2 and ISO/IEC 27001 compliant and also supports ISO/IEC 27017 and 27018**, with the longest-standing compliance in the industry. Keeper is FedRAMP and GovRAMP High Authorized, PCI DSS certified and certified by TrustArc for privacy.

Organization Impact

Since implementing KeeperPAM, DrillDocs has significantly strengthened its security posture while preserving the agility required of a fast-growing global startup. Shared administrative passwords have been eliminated, and privileged credentials are now vaulted, randomized and governed by role-based access controls. The company's Bring Your Own Device (BYOD) model no longer creates visibility challenges or operational strain.

> **"Keeper made a big change in our digital security culture. We're not keeping our credentials in unsafe places anymore."**
>
> **Francois Ruel | Co-founder and Chief Science Officer, DrillDocs**

Reduced Risk Across a Remote BYOD Workforce - KeeperPAM reduces risk across DrillDocs' remote BYOD workforce by isolating privileged access within secure virtual environments. Engineers and third-party partners can securely connect to production systems from anywhere in the world without exposing credentials or installing sensitive access tools directly on personal devices.

Role-Based, Least-Privilege Access - KeeperPAM enables DrillDocs to structure access by role rather than distributing individual credentials. Customer engineering teams, developers and external partners are granted access only to the systems required for their responsibilities. This approach dramatically reduced administrative overhead while ensuring that privileged access remained tightly controlled.

> **"Onboarding or offboarding employees is now much easier and faster. If someone needs access to something new, now it's a matter of seconds and they have access to it."**
>
> **Mert Geveci | Chief Technology Officer, DrillDocs**

Streamlined User Onboarding and Offboarding - KeeperPAM transformed onboarding and offboarding processes, improving efficiency and reducing administrative overhead. Access can be granted or revoked in seconds, enabling leadership to respond immediately to operational needs.

Complete Visibility Into Privileged Sessions - KeeperPAM's session recording and activity logging capabilities grant additional visibility into privileged activity. If unusual behavior occurs, leadership can review session data to better understand what happened and respond appropriately. KeeperAI enables automated termination of high-risk sessions and encrypted activity summaries. This level of visibility supports the organization's security model across globally distributed engineers and third-party support teams, giving leadership clear oversight into how production environments are accessed and used.

Built-In Governance to Support Compliance - As DrillDocs continues on its path toward SOC 2 compliance, KeeperPAM provides a strong foundation for meeting access control requirements. Centralized credential management, role-based least-privilege enforcement and session auditing capabilities support the company's broader governance and security objectives.

Today, DrillDocs operates with the security maturity of a much larger enterprise. Engineers can securely connect from anywhere in the world, on any device, without exposing privileged credentials. Access is structured, monitored and centrally controlled. Onboarding is immediate, and offboarding is rapid and policy-driven. External partners can contribute safely. With KeeperPAM in place, the organization is positioned to scale securely while maintaining the speed and innovation that define its growth.

KeeperPAM

KeeperPAM is a next-generation Privileged Access Management (PAM) platform that secures and manages access to critical resources, including servers, web apps, databases and workloads. Built on a zero-trust, zero-knowledge security architecture, KeeperPAM helps organizations protect privileged accounts, enforce least privilege, secure remote infrastructure and meet compliance requirements with unmatched ease of use and fast deployment.

Keeper is intuitive and easy to deploy, regardless of business size. KeeperPAM uses a zero-trust gateway service to connect to target environments without requiring firewall updates or ingress changes. Remote session capabilities ensure users never have direct access to credentials or SSH keys, keeping secrets fully isolated from endpoints. Access to resources can be time-limited and governed by policy, with credentials automatically rotating after access is revoked. This enables secure Just-in-Time (JIT) access without ever exposing credentials.

Keeper is designed to scale for organizations of any size. KeeperPAM centralizes access in a single User Interface (UI) across multiple cloud providers, on-premises workloads and client environments, enabling multi-cloud management.

Business Use Cases: KeeperPAM

- Control and monitor all privileged accounts
- Provide JIT access without exposing credentials
- Consolidate development tools in one platform with an intuitive UI
- Enable seamless management of cloud, hybrid and multi-cloud environments
- Record multi-protocol sessions with AI threat detection and automated session termination
- Automate password rotation
- Enforce MFA protection on every system
- Deploy seamlessly via web or desktop app with automated SCIM provisioning

Protect your organisation with Keeper

To learn more about how Keeper can protect your organization with an easy-to-use platform, **contact our sales team** for a free trial or personalised demo.

About Keeper

Keeper Security is one of the fastest-growing cybersecurity software companies that protects thousands of organizations and millions of people in over 150 countries. Keeper is a pioneer of zero-knowledge and zero-trust security built for any IT environment. Its core offering, KeeperPAM®, is an AI-enabled, cloud-native platform that protects all users, devices and infrastructure from cyber attacks. Recognized for its innovation in the Gartner Magic Quadrant for Privileged Access Management (PAM), Keeper secures passwords and passkeys, infrastructure secrets, remote connections and endpoints with role-based enforcement policies, least privilege and just-in-time access. Learn why Keeper is trusted by leading organizations to defend against modern cyber threats at **KeeperSecurity.com**.

Keeper is trusted and loved by thousands of companies and millions of people globally.

Gartner

KeeperPAM® recognized in the 2025 Gartner Magic Quadrant™ for PAM

Cybersecurity Excellence Award **Privileged Access Management**

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

Newsweek **#1 Cybersecurity Platform**

Enterprise Management Associates **KeeperPAM® recognized for product strength**