

ESTUDIO DE CASO

DrillDocs garantiza la seguridad de las operaciones globales en alta mar y el acceso de ingeniería las 24 horas del día, los 7 días de la semana con KeeperPAM®



Antecedentes

DrillDocs es una startup tecnológica en fase inicial que ofrece software de visión por computadora para aplicaciones de perforación en alta mar. Su plataforma monitorea el proceso de perforación en tiempo real y analiza los recortes de roca para ayudar a los operadores a mejorar la seguridad, la eficiencia y el rendimiento en las plataformas en alta mar.

Industria

Petróleo y gas

Empleados

Más de 20

Soluciones

KeeperPAM

Keeper Secrets Manager



El desafío

A medida que DrillDocs evolucionó de un equipo de ingeniería fundador a una organización distribuida de soporte de producción, la gestión de accesos se volvió cada vez más compleja. En sus primeras etapas, un pequeño equipo interno se encargaba tanto del desarrollo como del soporte técnico, y las credenciales se almacenaban de forma segura, mientras que el acceso se controlaba estrictamente mediante procesos informales y manuales. A medida que aumentaba la demanda de los clientes y se implementaban los sistemas en todo el mundo, DrillDocs incorporó una empresa externa de servicios de ingeniería para ofrecer cobertura de soporte durante la noche y garantizar una verdadera disponibilidad operativa las 24 horas del día, los 7 días de la semana. La organización dependía de Keeper Secrets Manager para automatizar la recuperación de credenciales durante las implementaciones. Las credenciales se inyectaban mediante programación durante la compilación del sistema y se mantenían en la memoria durante los flujos de trabajo en tiempo de ejecución, lo que garantizaba que nunca se almacenaran en texto sin cifrar en los sistemas de producción.

Si bien este enfoque brindó soporte eficazmente a flujos de trabajo seguros de DevOps, la gestión de sesiones interactivas privilegiadas entre usuarios internos y de terceros distribuidos requería una solución segura de gestión de acceso privilegiado (PAM). La expansión de la cobertura operativa introdujo nuevos requisitos de gobernanza relacionados con la concesión, supervisión y revocación del acceso privilegiado en equipos globales y dispositivos no gestionados. El equipo de líderes necesitaba una mayor visibilidad, controles de acceso más estrictos y una solución que pudiera escalar de manera segura junto con las operaciones globales de la compañía.

“Nos preocupaba saber cómo administrar mejor la seguridad cuando el trabajo se realiza desde equipos personales. Confiamos en nuestros socios, pero necesitábamos cambiar a una cultura de ‘confiar pero verificar’”.

François Ruel | Cofundador y Director Científico de DrillDocs

La solución Keeper

DrillDocs implementó **KeeperPAM**, una plataforma PAM integral de confianza cero y conocimiento cero, para centralizar el acceso privilegiado, proteger las credenciales y ofrecer una gestión remota controlada de sesiones sin interrumpir los flujos de trabajo de ingeniería.

Implementación rápida con valor inmediato - El proceso de implementación de Keeper es sencillo y directo, lo que facilita la transición tanto de ingenieros internos como de equipos de soporte externos hacia un modelo de acceso más seguro. Keeper ofrece una amplia **documentación del producto**, recursos de implementación y orientación para el usuario final para facilitar implementaciones exitosas. **Guías de producto** detalladas y **videos de capacitación** aumentan la alta tasa de adopción por parte de los usuarios.

“El día que decidimos comenzar nuestra prueba, pudimos configurar todo en una sesión de dos horas. A partir de ahí, comenzamos a usar Keeper de inmediato”.

François Ruel | Cofundador y Director Científico de DrillDocs

Acceso virtualizado seguro sin gestionar puntos finales

- KeeperPAM permite el acceso seguro y basado en navegador a escritorios virtuales Windows y Linux a través de una puerta de enlace de confianza cero, lo cual evita la instalación de una VPN o la exposición directa a la red en dispositivos personales. Dado que la conectividad y las herramientas administrativas se mantienen en un entorno virtual seguro, KeeperPAM ayuda a garantizar que las credenciales privilegiadas nunca queden expuestas a los usuarios finales. Todo el acceso a la infraestructura se controla de manera centralizada, se encripta y se registra, lo que brinda a las organizaciones visibilidad completa y control sobre las sesiones privilegiadas remotas.

Aprovisionamiento y revocación de acceso instantáneo

- KeeperPAM agiliza la gestión del ciclo de vida del usuario al permitir a los administradores aprovisionar, modificar y revocar el acceso privilegiado en segundos. A través de **controles de acceso basados en roles** y centralizados así como la aplicación de políticas, las organizaciones pueden otorgar acceso inmediato a sistemas críticos o eliminar permisos cuando los roles cambian o los usuarios dejan la organización. Esta capacidad de aprovisionamiento en tiempo real reduce la carga administrativa, elimina los riesgos de acceso permanente y garantiza que las cuentas privilegiadas permanezcan estrictamente controladas en todo momento.

Implementaciones automatizadas y seguras sin exponer credenciales - **Keeper Secrets Manager** protege el acceso entre equipos al permitir implementaciones automatizadas y actualizaciones del sistema sin exponer ni codificar de forma estática las credenciales. Durante los procesos de compilación, las credenciales se recuperan de forma programada e inyectan directamente en la memoria, lo que asegura que nunca se almacenen en texto plano ni se dejen en los sistemas. Este enfoque refuerza la seguridad de DevOps al eliminar la proliferación de secretos, al tiempo que mantiene la eficiencia de la automatización.

“Uso la bóveda muchas veces al día. También utilizamos Keeper Secrets Manager para implementaciones y actualizaciones automatizadas. Nos funciona muy bien”.

David Momberger | Ingeniero Sénior de Sistemas de DrillDocs

Seguridad de primera clase - la arquitectura de seguridad de Keeper, basada en el principio de confianza cero y conocimiento cero, está diseñada para proteger la información y reducir el riesgo de violaciones de datos. Keeper combina la criptografía de curva elíptica (ECC) a nivel de dispositivo con **múltiples capas de cifrado** (a nivel de bóveda, carpeta y registro), criptografía resistente a la computación cuántica, autenticación multifactor y biométrica, así como cifrado AES de 256 bits validado según FIPS 140-3, además de PBKDF2. Keeper **cumple con las normas SOC 2 e ISO/IEC 27001 y también es compatible con las normas ISO/IEC 27017 y 27018**, lo que representa el período de cumplimiento más prolongado de la industria. Keeper cuenta con la autorización de nivel superior de FedRAMP y GovRAMP, la certificación PCI DSS y la certificación de privacidad de TrustArc.



Impacto en la organización

Desde que implementó KeeperPAM, DrillDocs ha reforzado considerablemente su postura de seguridad, al tiempo que ha conservado la agilidad que se requiere de una startup global en rápido crecimiento. Se eliminaron las contraseñas administrativas compartidas y las credenciales privilegiadas ahora se almacenan, aleatorizan y se regulan mediante controles de acceso basados en roles. El modelo Bring Your Own Device (BYOD) de la compañía ya no genera retos de visibilidad ni carga operativa.

“Keeper hizo un gran cambio en nuestra cultura de seguridad digital. Ya no guardamos nuestras credenciales en lugares inseguros”.

François Ruel | Cofundador y Director Científico de 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.

“Ahora, incorporar o desvincular empleados es mucho más fácil y rápido. Si alguien necesita acceso a algo nuevo, en cuestión de segundos recibe el acceso”.

Mert Geveci | Director de Tecnología, DrillDocs

Incorporación y desvinculación simplificadas de usuarios - KeeperPAM transformó los procesos de incorporación y desvinculación, lo cual mejoró la eficiencia y redujo la sobrecarga administrativa. El acceso se puede otorgar o revocar en segundos, lo que permite a los líderes responder de inmediato a las necesidades operativas.

Visibilidad completa de sesiones privilegiadas - Las capacidades de grabación de sesiones y registro de actividades de KeeperPAM otorgan mayor visibilidad sobre la actividad privilegiada. Si se produce un comportamiento inusual, los equipos de líderes pueden revisar los datos de la sesión para comprender mejor lo sucedido y responder de forma adecuada. KeeperAI permite la terminación automática de sesiones de alto riesgo y resúmenes cifrados de actividades. Este nivel de visibilidad respalda el modelo de seguridad de la organización entre los ingenieros distribuidos por todo el mundo y los equipos de soporte externos, lo que otorga a la dirección una visión clara de cómo se accede a los entornos de producción y cómo se utilizan.

Gobernanza integrada para respaldar el cumplimiento - A medida que DrillDocs continúa en el proceso hacia el cumplimiento del SOC 2, KeeperPAM ofrece una base estable para cumplir con los requisitos de control de acceso. La gestión centralizada de credenciales, la aplicación de privilegios mínimos basada en roles y las capacidades de auditoría de sesiones respaldan los objetivos más amplios de gobernanza y seguridad de la empresa.

En la actualidad, DrillDocs opera con el nivel de madurez en materia de seguridad propio de una empresa mucho más grande. Los ingenieros pueden conectarse de forma segura desde cualquier parte del mundo, en cualquier dispositivo, sin exponer credenciales privilegiadas. El acceso está estructurado, supervisado y controlado de forma centralizada. La incorporación es inmediata y la desvinculación es rápida y basada en políticas. Los socios externos pueden contribuir de forma segura. Con KeeperPAM implementado, la organización está en condiciones de crecer de forma segura sin perder la rapidez y la innovación que caracterizan su crecimiento.



KeeperPAM

KeeperPAM es una plataforma de gestión de acceso privilegiado (PAM) de próxima generación que protege y administra el acceso a recursos críticos, incluidos servidores, aplicaciones web, bases de datos y cargas de trabajo. Desarrollado sobre una arquitectura de seguridad de cero confianza y conocimiento cero, KeeperPAM ayuda a las organizaciones a proteger cuentas privilegiadas, hacer cumplir el privilegio mínimo, asegurar la infraestructura remota y cumplir con los requisitos de cumplimiento, con una facilidad de uso y una implementación rápida sin igual.

Keeper es intuitivo y fácil de implementar, independientemente del tamaño del negocio. KeeperPAM utiliza un servicio de puerta de enlace de confianza cero para conectarse a entornos de destino sin requerir actualizaciones de firewall ni cambios de entrada. Las capacidades de sesión remota garantizan que los usuarios nunca tengan acceso directo a las credenciales o claves SSH, lo cual mantiene los secretos completamente aislados de los puntos finales. El acceso a los recursos puede estar limitado en el tiempo y regirse por políticas, con credenciales que giran automáticamente después de revocar el acceso. Esto permite un acceso seguro justo a tiempo (JIT) sin exponer nunca las credenciales.

Keeper está diseñado para escalar en organizaciones de cualquier tamaño. KeeperPAM centraliza el acceso en una única Interfaz de Usuario (UI) entre múltiples proveedores de nube, cargas de trabajo locales y entornos de cliente, lo cual permite la gestión multinube.

Casos de uso empresarial: KeeperPAM

- Controla y supervisa todas las cuentas privilegiadas
- Otorga acceso JIT sin exponer las credenciales
- Consolida las herramientas de desarrollo en una plataforma con una interfaz de usuario intuitiva
- Permite una gestión fluida de entornos de nube, híbridos y multinube
- Graba sesiones multiprotocolo con detección de amenazas de IA y finalización automatizada de sesiones
- Automatiza la rotación de contraseñas
- Aplica la protección MFA en todos los sistemas
- Se implementa sin problemas a través de la web o la aplicación de escritorio con aprovisionamiento SCIM automatizado

Proteja su organización con Keeper

Para obtener más información sobre cómo Keeper puede proteger su organización con una plataforma fácil de usar, **póngase en contacto con nuestro equipo de ventas** para obtener una prueba gratuita o una demostración personalizada.

Acerca de Keeper

Keeper Security es una de las compañías de software de ciberseguridad de más rápido crecimiento que protege a miles de organizaciones y millones de personas en más de 150 países. Keeper es un pionero de la seguridad de conocimiento cero y confianza cero creada para cualquier entorno de TI. Su oferta principal, KeeperPAM®, es una plataforma nativa de la nube habilitada para IA que protege a todos los usuarios, dispositivos e infraestructura de los ataques cibernéticos. Reconocido por su innovación en el Gartner Magic Quadrant para la gestión de accesos privilegiados (PAM), Keeper protege contraseñas y claves de acceso, secretos de infraestructura, conexiones remotas y puntos finales con políticas de aplicación basadas en roles, privilegios mínimos y acceso justo a tiempo. Descubra por qué las organizaciones líderes confían en Keeper para defenderse de las amenazas cibernéticas modernas en [KeeperSecurity.com](https://www.keepersecurity.com).

Miles de empresas y millones de personas de todo el mundo confían en Keeper.

Gartner

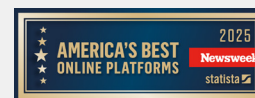
KeeperPAM® reconocido en el 2025
Gartner Magic Quadrant™ para PAM



Premio a la Excelencia
en Ciberseguridad
**Gestión de acceso
privilegiado**



Revista de defensa
cibernética
**Selección del editor
- Gestión de acceso
privilegiado (PAM)**



Newsweek
**Plataforma de
Ciberseguridad #1**



Asociados de
gestión empresarial
**KeeperPAM® reconocido por
la resistencia del producto**