Hoja de datos

KEEPER SECRETS MANAGER

Defiéndase de los ataques cibernéticos protegiendo los secretos de infraestructura, como las claves de la API, las contraseñas de bases de datos, las claves de acceso y los certificados.

Desafíos

Los secretos de DevOps robados o poco seguros son una de las principales causas tras los ataques a la cadena de suministro. Los secretos están esparcidos por el código fuente, los archivos de configuración y los sistemas CI/CD, lo deja a las organizaciones expuestas a los hackers. Esta superficie de ataque ampliada crea varios retos para los profesionales de DevOps, Seguridad y TI:

01

Se prioriza la productividad sobre la seguridad, y los empleados, por muy bien intencionados que sean, terminan codificando las credenciales por todo el entorno.

02

La colaboración de las modernas plantillas distribuidas entre regiones, sistemas y entornos, conlleva un mayor riesgo potencial si no se implementan los controles adecuados.

03

Sin controles de acceso gestionados de forma centralizada, los empleados corren el riesgo de recibir privilegios excesivos que fomentan las amenazas y reducen la conformidad.

04

A menudo, las políticas internas y de conformidad exigen la rotación de credenciales con regularidad, lo que solo es posible con una bóveda integral.

Las organizaciones necesitan una forma segura, fácil de usar y rentable de almacenar secretos y aplicar el acceso de privilegios mínimos. Al coordinar el acceso, aplicar la rotación automatizada de credenciales y garantizar el cifrado de extremo a extremo, los equipos pueden reducir drásticamente el riesgo de que se produzca una violación de seguridad devastadora.

Solución

Keeper Secrets Manager permite a sus equipos integrar las canalizaciones CI/CD, las herramientas DevOps, el software personalizado y los entornos multinube en una plataforma totalmente gestionada, de conocimiento cero y confianza cero para proteger los secretos de infraestructura y reducir la difusión de secretos.

Keeper Secrets Manager centraliza los secretos para eliminar la expansión y evitar el acceso no autorizado y proporcionar auditorías y registros. Las amplias funciones del kit de desarrollo de software (SDK) y la interfaz de programación de aplicaciones (API) permiten inyectar credenciales justo a tiempo en cualquier lenguaje de programación, lo que cubre el acceso a los secretos tanto de máquinas como humanos.

No se convierta en una víctima de los hackers.

Más información
keepersecurity.com

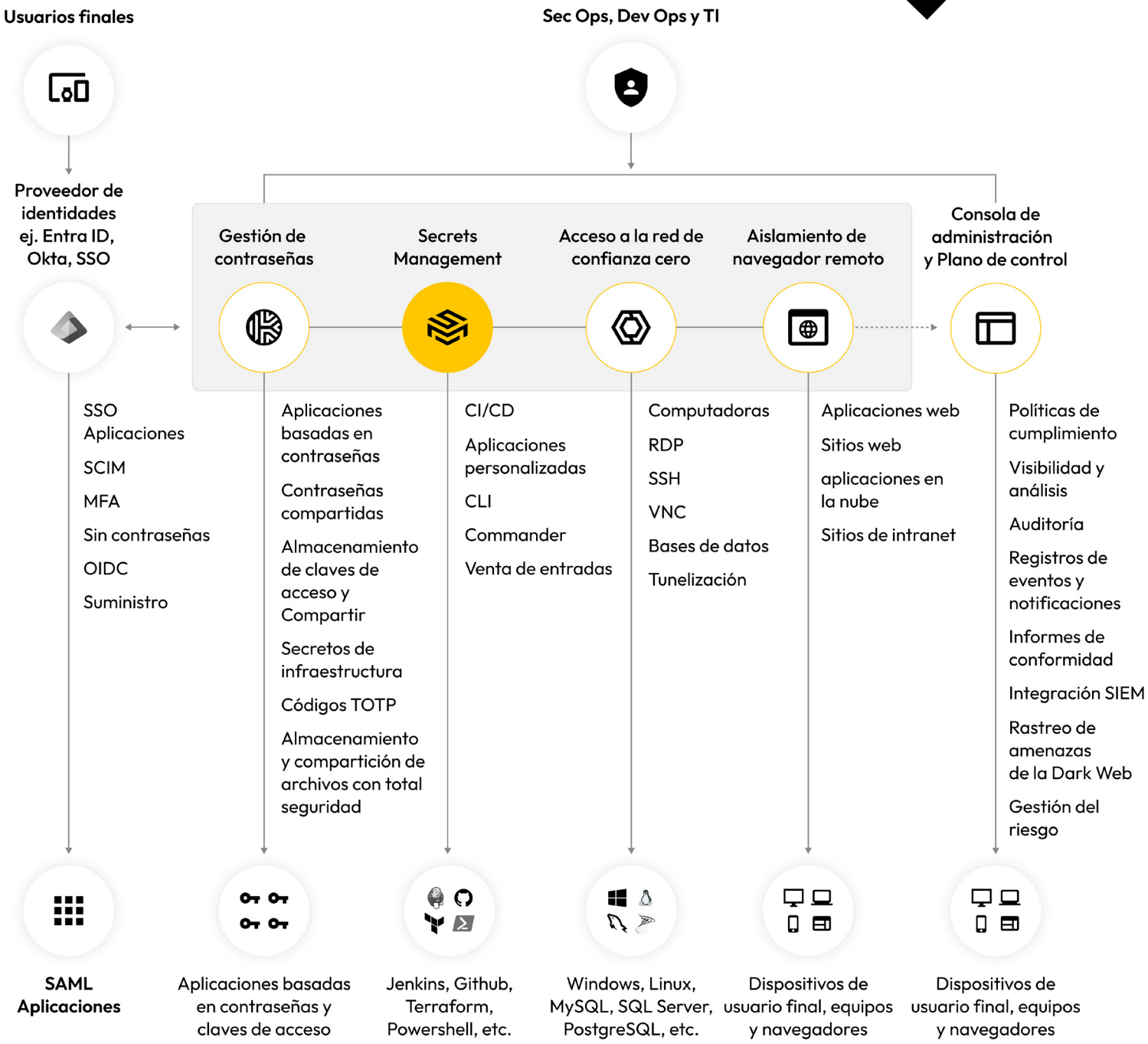
Solicitar un demo
keeper.io/ksm

Sobre nosotros

Keeper Security está transformando la ciberseguridad para personas y organizaciones alrededor del mundo. Las soluciones intuitivas de Keeper están diseñadas con cifrado de extremo a extremo para proteger a cada usuario, en cada dispositivo y en cualquier ubicación. Con la confianza de millones de individuos y miles de organizaciones, Keeper es el líder en gestión de contraseñas, claves de acceso y secretos, acceso privilegiado, acceso remoto seguro y mensajería cifrada.

KEEPER SECRETS MANAGER

Plataforma de gestión del acceso privilegiado de Keeper



Valor empresarial

Protege sus sistemas y datos con grandes privilegios
Consolide sus secretos en una plataforma unificada y elimine la proliferación de secretos eliminando las credenciales codificadas en el código fuente, los archivos de configuración y los sistemas CI/CD.

Integración flexible y rápida
Integración inmediata con todas las plataformas de CI/CD más populares, como Github Actions, Jenkins y Ansible.

Implementación y uso fáciles
Plataforma totalmente basada en la nube, de confianza cero y conocimiento cero que no requiere complejas configuraciones de red, almacenamiento o alta disponibilidad.

Capacidades clave

- Haga que roten automáticamente las credenciales de las cuentas de servicio y de administrador, las identidades de usuario, las cuentas de API basadas en REST, las cuentas de máquinas y de usuario en toda su infraestructura y en los entornos de varias nubes.
- Gestione los derechos de acceso y los permisos con controles de acceso basados en roles.
- Los dispositivos cliente descifran los secretos del bóveda de manera local tras la recuperación. Keeper no tiene capacidad para descifrar los datos almacenados en la bóveda.
- Keeper Secrets Manager es un servicio totalmente gestionado con capacidad de ampliación ilimitada.