



Establezca sesiones privilegiadas tanto en la nube como en las instalaciones, cree túneles, impulse el acceso de confianza cero a la infraestructura y proteja el acceso remoto a las bases de datos sin necesidad de VPN.

## Desafíos

Organizaciones de todos los tamaños deben proporcionar un acceso seguro y fiable a la infraestructura de TI, las bases de datos y los sitios web back-end. Sin embargo, las soluciones de acceso remoto heredadas suelen dar lugar a una escalabilidad limitada, una elevada sobrecarga administrativa, la frustración del usuario final y graves lagunas de seguridad.

01

Las redes privadas virtuales (VPN) suelen proporcionar demasiado acceso, especialmente a contratistas, proveedores y empleados de uso ocasional.

02

Las VPN no protegen del seguimiento de las cookies, los virus u otros tipos de malware, por lo que las organizaciones siguen expuestas a riesgos cada vez mayores.

03

Las VPN son caras y notoriamente difíciles de configurar, mantener y utilizar, lo que frustra tanto a los administradores como a los usuarios.

04

Algunas soluciones se basan en combinaciones de agentes, clientes y servidores de bastión distribuidos, lo que aumenta la complejidad del sistema y ralentiza su adopción.

**Los empleados necesitan establecer conexiones remotas seguras, fiables y fáciles de usar desde cualquier lugar para minimizar el riesgo de acceso no autorizado a recursos sensibles.**

## Solución

Keeper Connection Manager resuelve el dilema de la complejidad y la seguridad con una solución sin agentes que ofrece la seguridad, la simplicidad y la velocidad necesarias para los entornos de trabajo actuales.

Keeper Connection Manager está diseñado para funcionar según el Principio de privilegios mínimos. Los derechos de acceso se delegan a través de usuarios y grupos, que se crean automáticamente con los paquetes de Keeper Connection Manager y mediante estrictos permisos de archivo.

Todo el tráfico pasa por una puerta de enlace segura y autenticada. Los equipos de escritorio nunca están expuestos a la Internet pública. Siguiendo los principios de confianza cero, solo se permiten las conexiones autorizadas y autenticadas.

## No se convierta en una víctima de los hackers.

Más información  
[keepersecurity.com](https://keepersecurity.com)

Pruébalo gratis  
[keeper.io/kcm](https://keeper.io/kcm)

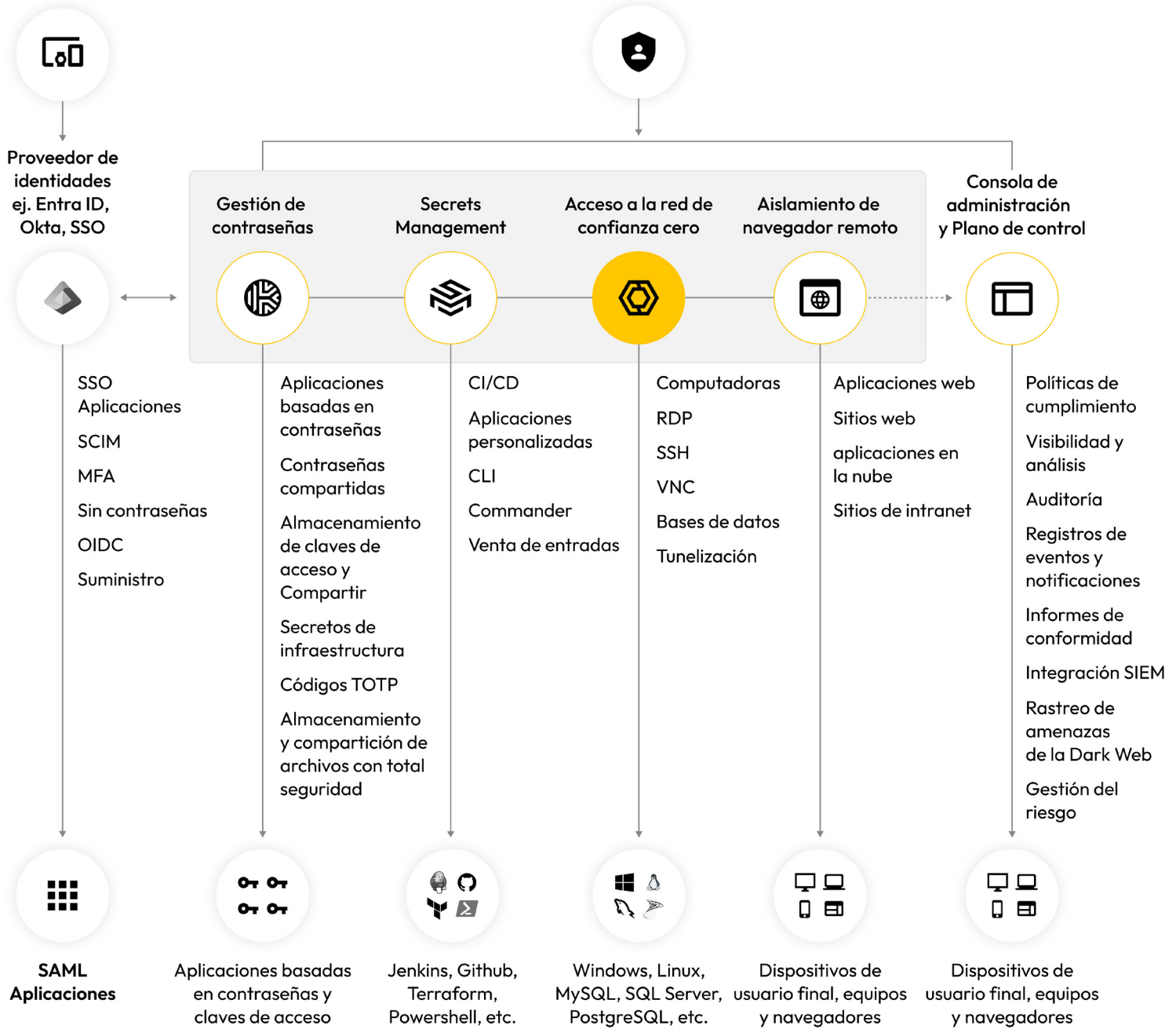


### Sobre nosotros

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.

Usuarios finales

Sec Ops, Dev Ops y TI



## Valor empresarial

### Aislamiento remoto del navegador

Mitigue las amenazas a la seguridad cibernética alojando sesiones de navegación en un entorno remoto y controlado.

### Acceso remoto a bases de datos

Proteja los datos confidenciales y la información de identificación personal con un acceso remoto seguro a las bases de datos.

### Acceso remoto seguro a la infraestructura

Establezca conexiones remotas seguras para cualquier usuario, ya sea interno o externo, desde cualquier lugar sin exponer sus credenciales.

### Gestión de sesiones de cuentas privilegiadas

Cumpla los requisitos de conformidad con las sesiones auditadas y grabadas.

## Capacidades clave

- Acceso basado en web con cifrado integral
- Autenticación multifactor
- Acceso sin agentes (no se requiere VPN)
- Seguridad de conocimiento cero
- Marco de confianza cero
- Motor de políticas de control de acceso basado en roles (RBAC)
- Supervisión de eventos y grabación de sesiones
- Compatibilidad con varios protocolos
- Aislamiento remoto del navegador
- Integración con Keeper Secrets Manager