KEEPER®
CONNECTION MANAGER

Ficha de datos: acceso remoto para equipos de TI y DevOps

Acceda al instante a su infraestructura remota con una seguridad de confianza cero

Keeper Connection Manager ofrece a los equipos de TI y DevOps un acceso sin esfuerzos a los puntos finales de RDP, SSH y Kubernetes a través de un navegador web.

Acceder de forma fácil y segura a toda la infraestructura interna siempre ha sido un reto. Otorgar acceso a un sistema es normalmente una acción del tipo “configurar y olvidar”. Con el tiempo, esto se acumula y puede llegar a tener un número desconocido de personas con acceso a estos sistemas críticos.

Realizar cambios o auditar la autorización es un reto. Si algo sale mal, a menudo es imposible saber lo que se hizo en un sistema tras el hecho.

Algunas soluciones tratan de resolver esto con agentes, clientes, servidores bastión distribuidos o una combinación de ellos. Estos enfoques aumentan la complejidad del sistema, reducen la seguridad y dificultan su adopción a gran escala.

Keeper Connection Manager resuelve este dilema de complejidad y seguridad con una solución sin agentes moderna que ofrece la seguridad, la facilidad de uso y la velocidad requeridas en los actuales entornos de trabajo remotos y distribuidos.

¿Por qué elegir Keeper Connection Manager para los equipos de TI y DevOps?

- Integración inmediata con Keeper Secrets Manager. Gestione las credenciales de las conexiones a sistemas con privilegios en el almacén de Keeper.
- Compatible con la autenticación sin contraseñas para los servidores remotos a través de todas las soluciones de autenticación conocidas con o sin solución IdP.
- Acceso instantáneo a la sesión de consola de sus sistemas con privilegios. No es necesario el acceso físico al dispositivo, lo que reduce los costes de asistencia.
- Para conseguir y mantener la conformidad con la SOX, la HIPAA, el RGPD, la FINRA y otros reglamentos específicos del sector, los administradores pueden grabar las sesiones con privilegios y mantener registros detallados.
- Las funciones avanzadas de última generación permiten el acceso multiusuario, el uso compartido de varias sesiones, la apertura de varias sesiones y el cambio rápido de sesión.
- El acceso a los sistemas críticos se puede bloquear al completo para asegurar que no existe ningún punto de entrada desconocido o no autorizado.
- Mitigue y reduzca el riesgo para los proveedores y contratistas de terceros con un acceso seguro, temporal y supervisado a los dispositivos y equipos autorizados.

KEEPER
CONNECTION MANAGER

Ficha de datos
Acceso remoto para equipos de TI y DevOps

Una conexión rápida, simple y segura a su infraestructura remota. Con el respaldo de la seguridad de confianza y conocimiento cero y asistencia de primera categoría.

¿Qué hace que Keeper Connection Manager sea mucho más seguro que las soluciones de escritorios remotos tradicionales?

- Todo el tráfico pasa a través de una puerta de enlace autenticada y segura. La sesión remota nunca se expone al internet público.
- Siguiendo los principios de la confianza cero, solo se permiten las conexiones autenticadas y autorizadas.
- ATodas las funciones remotas se ejecutan tras el firewall corporativo. Los usuarios remotos disfrutan de la misma protección que tendrían si trabajaran en una oficina de la red corporativa.
- Se pueden aplicar certificados de cliente y la autenticación de varios factores para una seguridad incluso más fuerte.
- Keeper Connection Manager se ha diseñado para operar según el principio de mínimo privilegio. Los derechos de acceso se delegan cuidadosamente a través de usuarios y grupos, que son creados automáticamente por los paquetes de Keeper Connection Manager a través de estrictos permisos de archivos.
- Los usuarios finales se comunican con los escritorios remotos a través de una sesión segura desde sus navegadores. Es una forma sencilla y efectiva de cifrar el tráfico entre los usuarios finales y la puerta de enlace sin entorpecer el rendimiento.
- El acceso a los sistemas con privilegios se puede garantizar sin exponer las credenciales de acceso al usuario final.
- Funciona con los puntos finales de MySQL, RDP, SSH, VNC y K8s.

Casos de uso	Keeper Connection Manager
Acceso basado en la web	✓
Autenticación con múltiples factores	✓
Acceso sin agentes	✓
Varios almacenes de datos	✓
Seguridad de conocimiento cero	✓
Marco de confianza cero	✓
Grabación de sesiones	✓
Autenticación sin contraseñas	✓
Asistencia multiprotocolo	✓
Integración con Keeper Secrets Manager	✓

Información sobre Keeper Security, Inc

Keeper Security, Inc. (Keeper) es la plataforma líder en el sector y la mejor valorada para evitar las ciberamenazas y las filtraciones de datos relacionadas con las contraseñas. Millones de personas y miles de negocios de todo el mundo ya confían en el software de cifrado y seguridad de conocimiento y confianza cero de Keeper. Keeper ha sido nombrado por PC Magazine como el mejor gestor de contraseñas del año y seleccionado por sus editores. También ha sido seleccionado por los editores de PCWorld y ha ganado varios premios de G2 al mejor software. Keeper tiene los certificados SOC-2 e ISO 27001 y también está listado para su uso por el gobierno federal estadounidense a través de su System for Award Management (SAM). Descubra más en **https://keepersecurity.com**.