KEEPER®
CONNECTION MANAGER

Ficha de datos: acceso a servidores y escritorios remotos

# Acceso seguro y sin esfuerzos a escritorios y equipos remotos sin una VPN

**Acceda de forma segura a sus sistemas desde cualquier lugar, en cualquier dispositivo y a través de cualquier navegador web.**

Para que el trabajo remoto tenga éxito a largo plazo, las organizaciones necesitan una forma segura, fiable y expansible de proporcionar a los empleados un acceso rápido a escritorios y aplicaciones.

Las redes privadas virtuales (VPN) son una opción común, pero se quedan cortas en varios ámbitos. Son caras y notoriamente difíciles de configurar y mantener para el personal de TI y de usar para los usuarios finales. Las VPN también tienen problemas de latencia, fiabilidad y disponibilidad.

Cuando se implementan de forma adecuada, los escritorios remotos son una alternativa convincente a las VPN.

- La carga administrativa que supone desplegar, respaldar y mantener un entorno estandarizado de escritorios remotos es significativamente menor que tener que asistir a los dispositivos físicos distribuidos que utilizan los usuarios finales.
- Siempre y cuando la solución de escritorio remoto no requiera un agente o puntos finales, los empleados pueden utilizar cualquier equipo para acceder, incluidos sus ordenadores portátiles o móviles personales.
- Rara vez es necesario acceder físicamente al dispositivo del usuario final, lo que reduce los costes generales de asistencia para los activos de la empresa.
- Los escritorios remotos refuerzan la seguridad de los trabajadores distribuidos al hacer posible la adopción de una arquitectura de confianza cero, algo que no es posible con la mayoría de las VPN.
- Las acciones que realizan los equipos distribuidos a través de escritorios remotos se ejecutan tras el firewall de la empresa. Como resultado, disfrutan de la misma protección de los sistemas de seguridad corporativos que tendrían si trabajaran en una oficina física.
- Los escritorios remotos animan a los usuarios a almacenar datos en la red de trabajo de la empresa en lugar de hacerlo en equipos locales. La protección es más fuerte dentro del firewall porque se pueden proteger los datos y hacerles copias de seguridad de forma adecuada. Además, es mucho menos probable que los datos se extravíen y es mucho más fácil compartirlos con otros.
- Los escritorios remotos son muy expansibles, sobre todo cuando no requieren un agente en los puntos finales. Las imágenes se pueden estandarizar fácilmente y las actualizaciones de los escritorios y aplicaciones se pueden automatizar, ya que no hay necesidad de acceder a dispositivos individuales.

## Historia de un cliente de Keeper Connection Manager: sector manufacturero

Keeper Connection Manager puede hacer mucho más que ofrecer escritorios remotos a las personas que trabajan desde casa. Como es tan expansible, seguro y fácil de usar, muchas organizaciones lo usan para proporcionar escritorios a laboratorios y entornos de formación.

Un importante fabricante de dispositivos de consumo creó laboratorios de formación en sus oficinas mundiales. Ofrecer un acceso directo a los escritorios fue difícil de mantener y confuso para los usuarios.

Keeper Connection Manager simplificó los sistemas internos para actualizar, proteger y proporcionar acceso a su equipo a fin de capacitarlo en escritorios remotos basados en laboratorios. La seguridad y la rapidez transformaron el entorno de formación del fabricante. Los alumnos solo necesitaban un navegador web, una URL y las credenciales de acceso.

KEEPER
CONNECTION MANAGER

**Ficha de datos**
**Acceso a servidores y escritorios remotos**

## Una experiencia de escritorio completamente remoto dondequiera que estén sus usuarios. Con el respaldo de la seguridad de confianza y conocimiento cero y asistencia de primera categoría.

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

- Todo el tráfico pasa a través de una puerta de enlace autenticada y segura. Los escritorios nunca se exponen al internet público. Siguiendo los principios de la confianza cero, solo se permiten las conexiones autenticadas y autorizadas.
- Todas las funciones de escritorio 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.
- Los certificados de cliente y la autenticación de varios factores se pueden aplicar para una seguridad aún mayor.
- 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**.