TeamViewer
Remote Management

Tu plataforma de gestión de TI profesional

Gestiona la TI de forma proactiva con TeamViewer Remote Management

Toma el control de tu infraestructura de TI

Aumenta la eficiencia de los procesos de TI con TeamViewer Remote Management.

Adopta un enfoque proactivo para la TI y nunca más dejes que surjan fallas repentinas del sistema que interrumpan tu negocio. TeamViewer Remote Management te ofrece los servicios que necesitas para que puedas automatizar tu TI.

Juntos es mejor: TeamViewer Remote Management está totalmente integrado en TeamViewer.

TeamViewer Remote Management está totalmente integrado en tu consola de TeamViewer y te informa de los riesgos existentes y potenciales detectados en tu infraestructura de TI, para que tengas la oportunidad de intervenir de forma remota y evitar que los inconvenientes se transformen en problemas graves.

Monitorea y protege tu TI desde la consola de TeamViewer.

Obtén los servicios correctos para la gestión de tu TI

Device and Network Monitoring

Monitorea los aspectos críticos de tus dispositivos.

TeamViewer Monitoring te permite reconocer problemas en tu infraestructura de TI de manera temprana y te notifica de inmediato.

Define políticas de monitoreo individuales para obtener información sobre el estado del disco, el uso de la CPU, el estado en línea de tus computadoras, el nivel de tinta de tus impresoras y mucho más.

Administra tu TI de forma proactiva para evitar los apagones y la pérdida de datos que te hacen perder tiempo y dinero con TeamViewer Monitoring.

Tiempo de reacción más rápido

Define límites individuales y recibe notificaciones cuando se alcance esos límites.

Menos periodos de inactividad

Reduce la cantidad de periodos de inactividad imprevistos realizando mantenimiento preventivo cuando recibas notificaciones de que se alcanzaron los límites establecidos.

Reducción de costos

Si realizas las tareas de mantenimiento de tus sistemas de manera proactiva, reducirás la frecuencia de los costosos apagones y evitarás las pérdidas de datos potenciales.

Administrador de tareas remotas

Optimiza tu servicio de asistencia: ofréceles a tus clientes una experiencia más rápida, más fluida y menos intrusiva.

Visualiza y gestiona todos tus procesos y servicios en curso de tus dispositivos de forma remota desde una página principal centralizada con el administrador de tareas remotas integrado.

Inicia y detén procesos y servicios de forma remota sin tener que establecer una conexión remota primero.

Scripting remoto

Automatiza las tareas complejas en un solo dispositivo o en todos ellos.

Ejecuta scripts al instante o en un horario que sea conveniente para ti y tus usuarios.

Además, puedes ejecutar scripts proactivos cuando se detecten ciertos eventos o se alcancen los límites establecidos.

Identifica problemas de manera temprana y actúa de inmediato con las notificaciones instantáneas

TeamViewer Monitoring realiza un seguimiento continuo de los aspectos críticos de tus dispositivos con Windows, macOS, Linux o de red, como impresoras o enrutadores, y te notifica de inmediato para que puedas actuar rápida y eficientemente.

Estado en línea

Cuando los dispositivos ya no estén en línea, recibe alertas basadas en reglas para que te notifiquen sobre la duración de estado fuera de línea.

Uso de la CPU

Fija un límite y recibe alertas cuando se supere el límite por un periodo de tiempo más largo del establecido.

Actualización del sistema

Mantente al tanto de todas las actualizaciones disponibles y mira si los usuarios han desactivado las actualizaciones automáticas de Windows.

Procesos

Recibe alertas solo cuando se inicien procesos, cuando se terminen o para ambos casos.

Estado del disco

Recibe alertas tan pronto como tu dispositivo informe un error S.M.A.R.T. para actuar rápidamente y evitar pérdidas de datos.

Espacio del disco

Recibe una notificación cuando el espacio del disco de tus dispositivos caiga por debajo de un límite en específico.

Servicios de Windows

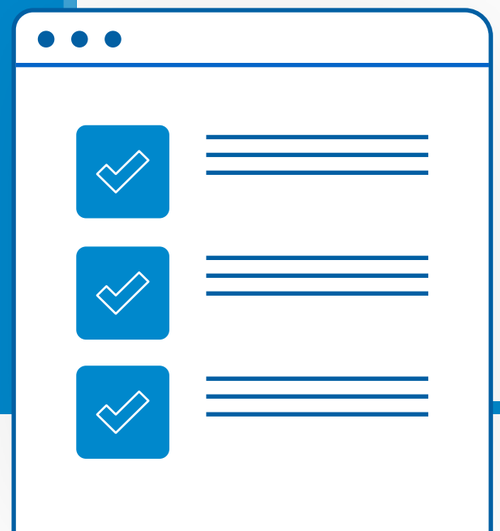
Recibe una notificación cuando se detengan ciertos servicios de Windows o luego de varios intentos consecutivos.

Registro de actividad

Recibe una notificación cuando se reconozcan ciertos eventos en el registro de actividades de tus dispositivos.

Cortafuegos

Un cortafuegos desactivado representa uno de los mayores riesgos para la seguridad de tu TI. Cuando se desactive el cortafuegos, recibirás una notificación de inmediato.



Estado del antivirus

Recibe alertas si se detecta que tu antivirus está desactivado o desactualizado.

Tráfico del adaptador de red

Fija límites mínimos y máximos para el tráfico entrante y saliente y recibe una notificación si el tráfico no se encuentra dentro de esos límites.

Uso de la memoria

Trabaja en un entorno que esté libre de los inconvenientes y los apagones causados por llevar la memoria al límite.

Descubre más sobre

Remote Device Monitoring

Network Device Monitoring

Asset Management

Logra visualizar tus sistemas de TI con mayor detalle creando un inventario y realizando un seguimiento de tu hardware y los programas informáticos instalados de forma automática.

TeamViewer Asset Management te ofrece resúmenes sobre el hardware y los programas informáticos operativos utilizados en tu empresa.

Con tan solo un par de clics, recibirás toda la información esencial sobre tu inventario en una página principal centralizada, integrada por completo en TeamViewer.

Control de inventario

Desde el número de teclados en uso hasta un resumen general de las versiones específicas de los programas informáticos que tienes instalados, con TeamViewer Asset Management, siempre estarás al tanto sobre todos los detalles de tu inventario de TI.

Hardware

Genera un informe de inventario detallado con todo el hardware operativo en segundos.

- Tipo
- Nombre
- Detalles
- Fabricante

Software

Verifica si se instalaron programas informáticos inadecuados en tu infraestructura o si tus licencias condicen con el uso real de los programas.

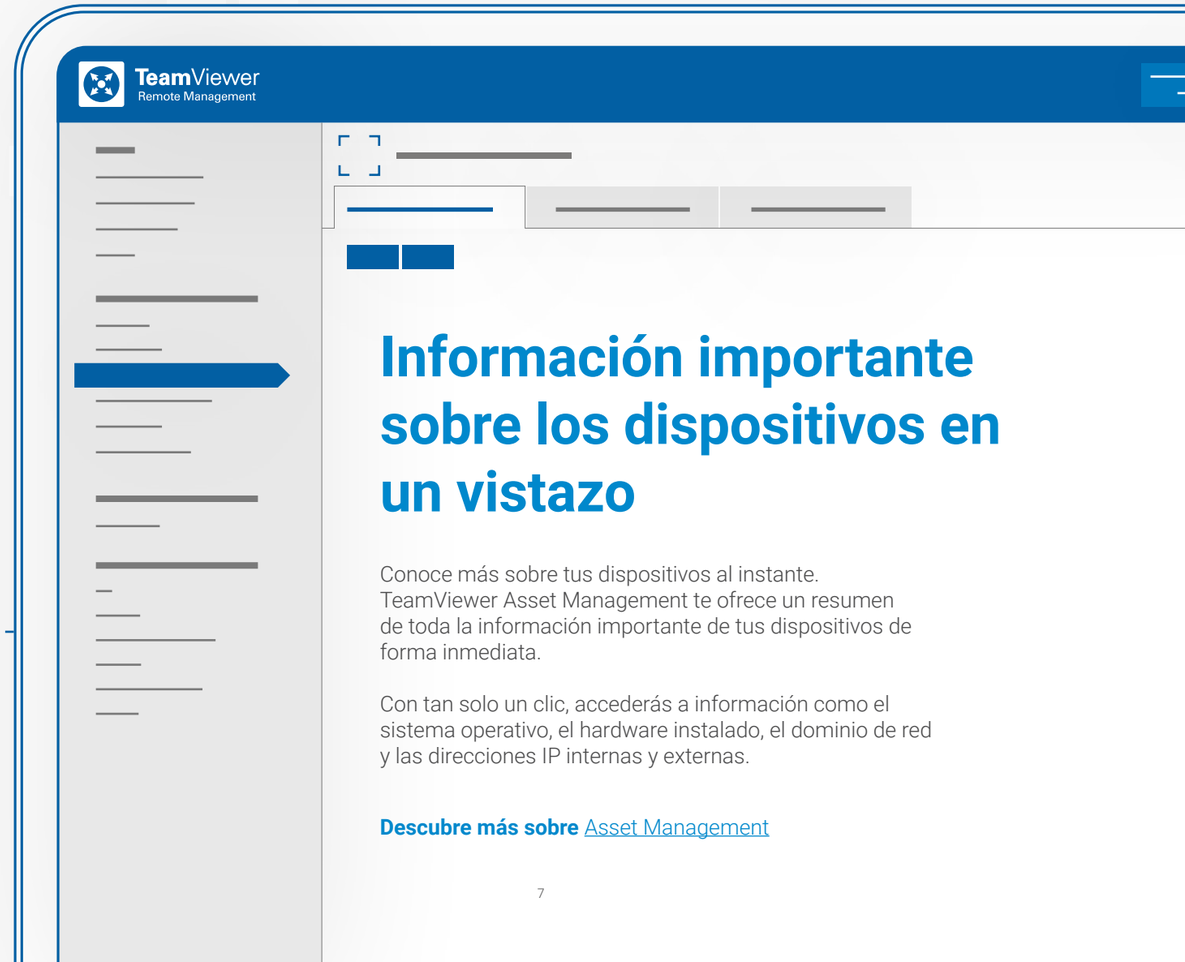
- Versión
- Fecha de modificación

Genera informes detallados donde puedas visualizar la configuración de todos tus dispositivos.

Informes de inventario

Con TeamViewer Asset Management, puedes generar informes detallados sobre tu hardware y tus programas informáticos. En segundos, tendrás un informe completo o uno que hayas creado con contenido específico.

También puedes exportar la información a un archivo CSV para que puedas utilizarlo en otras aplicaciones.



Información importante sobre los dispositivos en un vistazo

Conoce más sobre tus dispositivos al instante. TeamViewer Asset Management te ofrece un resumen de toda la información importante de tus dispositivos de forma inmediata.

Con tan solo un clic, accederás a información como el sistema operativo, el hardware instalado, el dominio de red y las direcciones IP internas y externas.

Descubre más sobre Asset Management

Patch Management

Protege tus dispositivos con la instalación automática y oportuna de parches en Windows y en aplicaciones de terceros.

Muchos incidentes de seguridad pueden deberse a una estrategia de parcheo inadecuada. Ahorra tiempo y mantén tus sistemas operativos y aplicaciones actualizados.

Un solo punto final sin parchar puede poner en riesgo toda tu infraestructura de TI. Patch Management, de TeamViewer Remote Management (incluido en la licencia de TeamViewer Monitoring y Asset Management), detecta vulnerabilidades en los programas informáticos y las aplicaciones de terceros de forma automática. Los parches también se instalan de forma automática desde la principal base de datos de parches del mundo.

Datos más seguros

Mantén tus dispositivos actualizados y protegidos, para reducir así los riesgos de violaciones de datos debido a los programas maliciosos o al secuestro de datos que les cuestan a las empresas millones de dólares cada año.

Mayor productividad

Con el parcheo automatizado, evitarás interrumpir a los usuarios durante el día y al mismo tiempo lograrás parchar los dispositivos de forma oportuna.

Una TI más eficiente

Usa el tiempo que normalmente le dedicas al parcheo manual a otros proyectos de mayor valor.

Mayor cumplimiento

Prueba fácilmente que se cumplen las políticas de seguridad de datos y otros requisitos regulatorios.

Un sistema de parcheo que se adapta a tus necesidades

TeamViewer Patch Management te da la capacidad y la flexibilidad para parchar como y cuando quieras, mientras visualizas todo el proceso.

Parcha Windows

Actualiza Windows desde una ubicación central.

Parcha aplicaciones de terceros

Parcha aplicaciones vulnerables con la principal base de datos de parches del mundo.

Totalmente integrado

Instala parches desde la misma consola de TeamViewer que ya conoces.

Conveniente

Entérate del estado de los parches de cada dispositivo al instante en una página principal centralizada.

Automatización

Identifica e instala parches de forma automática de acuerdo con tus horarios.

Políticas personalizadas

Define políticas individuales para cubrir las necesidades de tus usuarios.

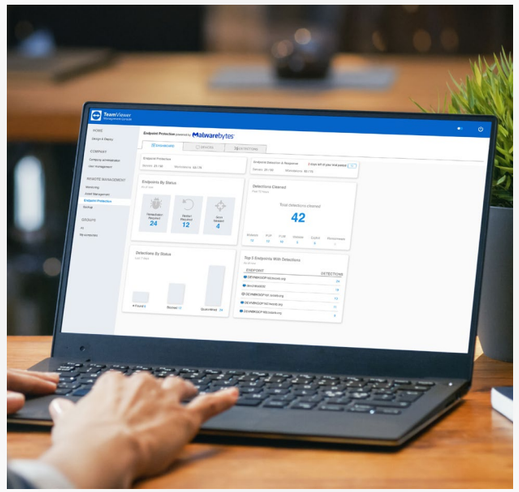
Mira qué fácil es instalar parches

1. **Desde la página principal centralizada, mira si hay parches disponibles, su prioridad y qué dispositivos los necesitan.**
2. **Define políticas individuales y configura los parches para que se instalen de forma automática en un horario que sea cómodo para ti y tus usuarios.**
3. **Como Patch Management está totalmente integrado en TeamViewer, puedes utilizar Remote Access para acceder de forma remota a los dispositivos y brindar asistencia para resolver problemas.**
4. **Realiza todas estas tareas desde cualquier lugar.**

Descubre más sobre Patch Management

Endpoint Protection

Protección cibernética avanzada para empresas con visión de futuro con Malwarebytes, que está totalmente integrado en TeamViewer.



Detección predictiva y bloqueo proactivo de amenazas contra virus, troyanos y el secuestro de datos para prevenir ataques de día cero.

Hoy más que nunca, es necesario adoptar un enfoque unificado y holístico para la protección de puntos finales que sea lo suficientemente potente como para bloquear los ataques avanzados y también lo suficientemente ágil como para adaptarse al panorama de amenazas cibernéticas que se encuentra en constante cambio.

Malwarebytes Endpoint Protection, que está basado en la nube, ofrece protección y reparación contra los programas informáticos maliciosos con detección predictiva de amenazas, bloqueo de ataques de día cero y protección integrada de extremo a extremo.

Soluciones proactivas contra amenazas cibernéticas

Prevención de amenazas de día cero

Logra prevenir los ataques de día cero por medio del análisis de carga útil sin firma y la detección de anomalías.

Reparación en un solo paso

Elimina de forma profunda y permanente tanto la infección como cualquier artefacto para lograr una reparación en un solo paso.

Bloqueo proactivo basado en el comportamiento

Con el análisis basado en el comportamiento, logra una identificación casi en tiempo real de comportamientos maliciosos y bloquea amenazas de forma automática, que es una de las funciones de seguridad más proactivas del mercado actual.

Detección unificada de amenazas

El monitoreo del comportamiento y el aprendizaje automatizado generan tasas de detección de amenazas más “inteligentes” con menos falsos positivos trazando el perfil de las amenazas en todas las capas: en la web, la memoria, las aplicaciones y los archivos.

Escaneos y reparación centralizados

Automatiza los escaneos y las reparaciones en un solo departamento o para miles de dispositivos a la vez con tan solo un par de clics, todo dentro de una consola centralizada en la nube.

Protección inteligente

Obtención más rápida de datos

Obtención de información de forma más rápida con el análisis con automatizado de amenazas y la evaluación del impacto potencial; así logramos que los directores de seguridad de la información ahorren tiempo y alerten los equipos de liderazgo ejecutivo sobre los riegos potenciales, lo suficientemente rápido como para mitigar los problemas y evitar que se agraven los incidentes.

Fácil escalabilidad

Nuestra solución basada en la nube escala para respaldar a empresas de todos los tamaños, con una rápida implementación remota a través de TeamViewer. Puedes personalizarla para cubrir las necesidades de departamentos individuales, lo que te permite detectar amenazas complejas de forma eficiente y brindar una respuesta rápida y consistente.

Simplicidad sin scripts

Combate los programas maliciosos por medio de tan solo un par de clics, no scripts, con funciones integrales y automatizadas de protección de puntos finales.

Cómo logra Endpoint Detection & Response detener ataques de fuerza bruta

1

Un delincuente intenta iniciar sesión varias veces con una herramienta automatizada.

2

Malwarebytes Endpoint Detection & Response (EDR) detecta los ataques de fuerza bruta como actividades sospechosas.

3

Los puntos finales en riesgo se aíslan del resto de la red para evitar que la actividad maliciosa se propague.

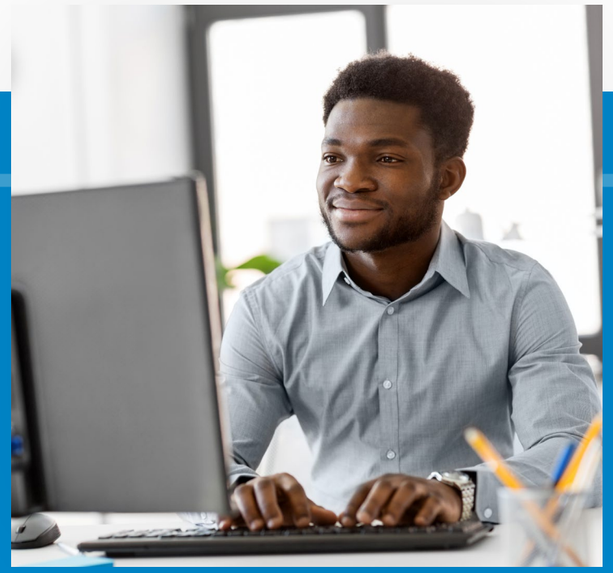
4

Luego, EDR investiga y mitiga el problema y aun así puedes acceder al dispositivo con TeamViewer Remote Access sin poner en riesgo a tu red.

Descubre más sobre Malwarebytes Endpoint Protection

Backup

Accede a tus copias de seguridad desde cualquier lugar, en cualquier momento.



Integrado por completo en TeamViewer, TeamViewer Backup te ofrece protección para los datos de tus puntos finales por medio de copias de seguridad.

Puedes instalarlo y activarlo de forma remota en segundos y tus datos y los de tus usuarios se guardarán de forma segura en la nube. Así, podrás tener la tranquilidad de saber que tus datos se mantendrán seguros y de que podrás recuperarlos de forma remota en caso de que suceda un desastre.

Copias de seguridad de puntos finales

Haz copias de seguridad de archivos y carpetas almacenados de forma local en tus dispositivos.

La nube

Almacena tus datos de forma segura en la nube y accede a ellos cuando lo necesites.

Instalación remota

Inicia una copia de seguridad en menos de un minuto con tan solo un par de clics.

Recuperación remota

Recupera tus archivos desde cualquier lugar, en cualquier momento, ya sea en el dispositivo original o en uno nuevo.

Puntos finales ilimitados

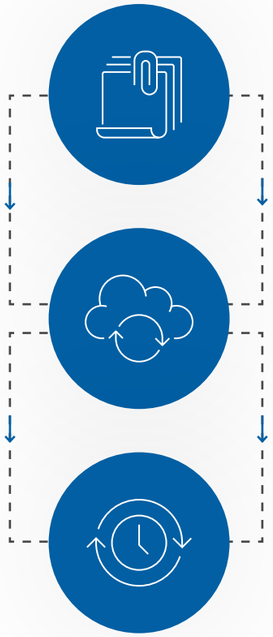
El almacenamiento disponible se distribuirá entre los dispositivos de forma automática.

Escalabilidad

Compra más espacio de almacenamiento en cualquier momento.

Políticas individuales para copias de seguridad

Ya sea que debas gestionar un solo dispositivo, departamentos enteros o diferentes clientes, ofrece un plan de copias de seguridad que mejor se adapte a cada caso particular.



Selección y exclusión de archivos

Especifica qué tipo de archivos deseas incluir o excluir de tus copias de seguridad.

Ciclos y programación de copias de seguridad

Configura las copias de seguridad para que se realicen de forma automática o en momentos específicos.

Limitación del ancho de banda

Limita la cantidad de tráfico que se envía a los servidores de copias de seguridad durante periodos determinados.

Haz tus copias de seguridad con los estándares de seguridad más estrictos

Nos tomamos muy en serio la seguridad de tus datos almacenados. Por eso nuestra principal prioridad es aplicar los estándares de seguridad más estrictos.

- **Encriptación AES de 256 bits** y de nivel militar del lado del cliente, antes de transferir los datos.
- Transferencia de datos de extremo a extremo con encriptación SSL.
- Datos almacenados **en servidores Amazon AWS S3 con encriptación AES de 256 bits.**
- Ubicación de los centros de datos:
  - Europa, Oriente Medio y África: Fráncfort, París, Londres, Dublín, Estocolmo.
  - América: Virginia (EE.UU.), Montreal (Canadá).
- Asia-Pacífico: Sídney, Tokio, Bombay, Seúl, Singapur.
- **Con certificación ISO/IEC 27001:2005** para los sistemas de gestión de la seguridad de la información.
- Almacenamiento de datos redundantes.

Descubre más sobre Endpoint Backup

Web Monitoring

Asegúrate de que el rendimiento de tu sitio web esté optimizado para cada visitante, en todo momento.

Se supone que tu sitio web debe atraer a los visitantes para que interactúen con tu negocio, pero también puede espantarlos y hacer que opten por visitar a la competencia. Además de cómo se ve y lo que dice, el funcionamiento de tu sitio web tiene mucho que ver con cuán exitoso es tu negocio.

Para garantizar el correcto funcionamiento de un sitio web, debe probarse de forma regular. Pero las pruebas manuales regulares pueden ser costosas y complicadas. Cuando utilizas TeamViewer Web Monitoring, se prueba la disponibilidad y la velocidad de tu sitio web de forma automática a intervalos personalizados desde docenas de ubicaciones en todo el mundo. Si surge un problema, recibirás una notificación para solucionarlo antes de que un apagón derive en una pérdida de ingresos.

Evita la pérdida de ingresos

Ofrece la mejor experiencia de usuario posible para cada visitante, cliente o comprador potencial.

Identifica ataques más rápido

Recibe una alerta si la disponibilidad se ve amenazada por un ataque externo.

Mejora el rendimiento de tu sitio web

Identifica cuellos de botella y componentes que no estén debidamente optimizados.

Logra posicionarte más alto en los motores de búsqueda

Evita sanciones por el rendimiento pobre de tu sitio web y mejora tu posicionamiento SEO y tu presencia en los resultados de los motores de búsqueda (SERP, por sus siglas en inglés).

Monitoreo web simplificado

TeamViewer Web Monitoring te ayuda a que tu sitio web se mantenga estable y rápido, en cualquier lugar.

Uptime monitoring

Los sitios web pueden dejar de funcionar por diferentes motivos, como los siguientes:

- Sobrecarga del servidor.
- Ataques de hackers.
- Problemas en el centro de datos.
- Problemas con el código del sitio web.
- Problemas con los proveedores de servicios de Internet.

Uptime Monitoring te alerta en el momento que tu sitio web deja de estar disponible en cualquier lugar del mundo para revertir la situación lo antes posible.

Page Load Monitoring

Como el 40 % de los consumidores abandonan los sitios web que tardan más de 3 segundos en cargar, cada segundo cuenta si no quieres perder clientes potenciales.

Con Page Load Monitoring, recibe alertas si tu sitio web excede un límite de tiempo de carga, que se monitorea constantemente desde 30 ubicaciones en todo el mundo. Detecta los elementos individuales y los cuellos de botella que ralentizan tu sitio web.

Transaction Monitoring

El monitoreo automatizado de las transacciones te puede ayudar a evitar que pierdas ganancias por errores en la tienda en línea, los inicios de sesión y otras transacciones.¿Cómo? Dándote la posibilidad de visualizar los siguientes elementos:

1. Si las transacciones están funcionando o no.
2. Si existen fallas o elementos que ralenticen tu sitio web.
3. La rentabilidad del rendimiento de tu sitio web.
4. El estado operativo de los componentes de terceros.

Descubra más sobre Web Monitoring

La principal prioridad de TeamViewer es **la protección de tus datos**

Como una empresa alemana, nos dedicamos a cumplir los estándares y los requisitos de cumplimiento de seguridad europeos. Nuestras soluciones cuentan con capas de protocolos de seguridad predefinidos para que tus datos se mantengan seguros y privados. Si bien TeamViewer ofrece seguridad de fondo a través de la encriptación, la firma de código, la verificación en dos pasos y más, también te brindamos otras funciones útiles para que puedas trabajar de forma segura en el día a día.

TeamViewer **Security**

La ID de TeamViewer

Cada dispositivo cuenta con una ID de TeamViewer única, que se genera y se verifica de forma automática antes de cada sesión.

Los estándares de seguridad más altos del mundo

Nuestros principales centros de datos cumplen los estándares industriales de seguridad de la ISO 27001.

Protección contra los ataques de fuerza bruta

Con TeamViewer, el tiempo entre los intentos fallidos de inicio de sesión aumenta exponencialmente y solo se resetea cuando se ingresa la contraseña correcta. Los dispositivos de acceso remoto y los compañeros de conexión también cuentan con protección contra otros ataques.

La contraseña de TeamViewer

TeamViewer automáticamente genera una nueva contraseña dinámica de sesión luego de que cada servicio de TeamViewer se vuelva a iniciar. También existe una configuración opcional que permite establecer una contraseña de manera dinámica luego de cada sesión. Esta contraseña es alfanumérica, como el estándar, y consta de 6 caracteres, lo que significa que existen más de 2,1 mil millones de combinaciones posibles.

Contraseña remota segura (SRP)

TeamViewer utiliza el protocolo SRP para la verificación y la encriptación de la contraseña, para que nunca se envíe por Internet ni la cifren. Por lo tanto, cuenta con una protección óptima contra los accesos externos. Las contraseñas también cuentan con encriptación de backend.

Encriptación

Todas las interacciones a través de TeamViewer, incluidas las transferencias, las VPN, los chats, etc., cuentan con protección por medio del cifrado de extremo de extremo con un intercambio de claves públicas y privadas RSA de 4096 bits.

Acceso condicional*

Con el acceso condicional, puedes reforzar las reglas de acceso remoto para prevenir las actividades sin autorización y ajustar las políticas de seguridad.

Verificación en dos pasos

En este caso, el inicio de sesión se realiza a través de un código nuevo y único, que se genera cada vez con un algoritmo desde un dispositivo móvil.

*Disponible con TeamViewer Tensor™. Se aplican términos y condiciones.

Sesiones de TeamViewer

Configuración de las sesiones y conexión

Cuando se establece una sesión, TeamViewer selecciona el mejor tipo de conexión. En el 70 % de los casos, luego del apretón de manos a través de nuestro servidor maestro (incluso detrás de portales estándar, enrutadores NAT y cortafuegos), la conexión de los datos se realiza por medio del protocolo UDP o TCP. Las otras conexiones se establecen a través de una red de enrutadores de alta redundancia por medio del protocolo TCP o un túnel HTTP. Eso significa que no debes abrir ningún puerto para poder trabajar con TeamViewer.

Encriptación y verificación

Las conexiones de TeamViewer se establecen a través de canales de datos totalmente protegidos con el intercambio de claves públicas y privadas RSA 4096 y el cifrado de las sesiones con encriptación AES de 256 bits. Esta tecnología se utiliza de la misma forma para HTTPS/TLS y se considera que es complemente segura de acuerdo con los estándares actuales. Como la clave privada nunca abandona la computadora del cliente, se garantiza que las computadoras interconectadas, incluidos los servidores de enrutamiento de TeamViewer, no puedan descifrar la transmisión de datos. Como operador del principal centro de datos, ni siquiera TeamViewer puede leer el tráfico de datos encriptados.

Cumplimiento y protección de datos

Dispositivos confiables

La función de dispositivos confiables garantiza que se solicite la verificación cada vez que un nuevo dispositivo intente iniciar sesión en un cuenta existente de TeamViewer.

Integridad de datos

La función de integridad de datos te protege de los delincuentes cibernéticos: el sistema verifica constantemente si se realiza alguna actividad inusual en una cuenta de usuario y genera un restablecimiento de contraseña automático en caso de detectar un comportamiento sospechoso.

Lista de contactos permitidos y bloqueados

La lista de contactos permitidos provee protección especial, sobre todo cuando se instala TeamViewer en computadoras para brindarles mantenimiento sin supervisión. Con la lista de contactos permitidos, puedes decidir qué clientes pueden obtener acceso. La lista de contactos bloqueados se utiliza para decidir qué ID y qué cuentas de TeamViewer se bloquearán o tendrán acceso denegado.

ISO/IEC 27001

Nuestro principal centro de datos cuenta con certificación ISO/IEC 27001, que es el estándar internacional para la gestión y el control de la seguridad.

ISO 9001:2015

TeamViewer también cuenta con certificación ISO 9001:2015 para los sistemas de gestión de la calidad (QMS, por sus siglas en inglés).

General Data Protection Regulation (GDPR)

El 25 de mayo del 2018, se hizo efectivo el General Data Protection Regulation (GDPR), que pone de relieve la importancia de la protección de los datos en un mundo que se digitaliza cada día más. TeamViewer es una empresa mundial y, para nosotros, resulta vital que la información personal de nuestros clientes y nuestra gente se gestione de acuerdo con el GDPR. Para saber más sobre cómo nos comprometemos a proteger tus datos de acuerdo con el GDPR, visita nuestro Trust Center.

Certificado HIPAA, HITECH y SOC2

A-LIGN, un proveedor de seguridad y cumplimiento a nivel nacional de Estados Unidos de América, le otorgó a TeamViewer la certificación HIPAA, HITECH y SOC2. HIPPA y HITECH son cruciales para las organizaciones del cuidado de la salud para garantizar la confidencialidad y la seguridad de los datos personales y la información de salud protegida (PHI), mientras que SOC2 es un marco de generación de informes esencial para las organizaciones proveedoras de servicios para establecer un medio para informar sobre los controles internos de índole no financiera, para que los clientes puedan entender cómo se cumplen los principios de servicios confiables (TSP, por sus siglas en inglés).