TeamViewer
Remote Management

DOCUMENTO TÉCNICO

4 claves para gestionar la TI de forma remota

Contenidos

Introducción:
Ventajas de la gestión remota de la TI

La TI es más valiosa cuando maximiza la efectividad, la seguridad y la eficiencia de la infraestructura de la TI, lo que hace que las organizaciones mantengan los máximos niveles de productividad posibles. Para alcanzar el objetivo, es necesario reemplazar el proceso reactivo tradicional de "se rompe/se arregla" adoptando un enfoque proactivo diseñado para mantener a los sistemas funcionando correctamente en vez de esperar a que fallen.

El cambio del paradigma de ser reactivo a proactivo cobra mayor notoriedad con el número creciente de contratistas de TI antiguos que se convirtieron en proveedores de servicios gestionados (MSP, por sus siglas en inglés). En tan solo seis años, del 2018 al 2023, se espera que el crecimiento del mercado global de los proveedores de servicios gestionados aumente de USD 173,4 mil millones a USD 296,38 mil millones.[1] Su objetivo es identificar problemas potenciales y solucionarlos antes de que causen periodos de inactividad y costosas reparaciones.

Cuando cada instalación, actualización o reparación requiere de una llamada de servicio en persona, resulta difícil adoptar un enfoque proactivo para la TI porque siempre se está reaccionando frente a incidentes específicos. Las empresas deben decidir por sí mismas cuándo es que su infraestructura de TI ya no depende de un servicio 100 % en persona. Una vez que la TI puede ofrecer sus servicios a una red con cinco o más dispositivos y hay algunas personas trabajando de forma remota, es hora de comparar los costos actuales de la asistencia de TI (incluidos los costos de los periodos de inactividad imprevistos) con los costos estimados de una gestión de TI remota y proactiva.

Las ventajas de una solución de gestión remota de TI bien diseñada se vuelven indispensables una que vez que permiten que los MSP y los departamentos de TI realicen todo lo siguiente de forma remota:

- Gestionar y realizar tareas de mantenimiento de la infraestructura de TI a fin de reducir los tiempos de respuesta para los tickets de manera significativa.
- Realizar tareas de mantenimiento fuera del horario de trabajo para evitar interrumpir a los empleados.
- Ser proactivo en vez de proactivo manteniendo a los programas actualizados y protegidos contra ataques cibernéticos, así como garantizar que los puntos finales se encuentren seguros y que toda la información de los dispositivos cuente con copia de seguridad.
- Obtener detalles en tiempo real sobre la infraestructura de TI y compartirlos con los accionistas de la empresa para evaluar su condición actual, tomar decisiones oportunas y proyectar necesidades futuras.
- Aumentar la eficiencia operativa, reducir costos monitoreando los dispositivos y solucionar los inconvenientes antes de que se conviertan en problemas graves.

Con la creciente popularidad de la gestión remota de la TI, el número de los servicios de TI que se pueden brindar de forma remota también ha aumentado y ahora incluyen el monitoreo de red, el monitoreo de dispositivos, el parcheo, el monitoreo web, la protección de puntos finales, las copias de seguridad de los puntos finales, entre otros. Estos servicios se agrupan y se ofrecen como soluciones de monitoreo y gestión remotos (RMM, por sus siglas en inglés).

De acuerdo con Smarter MSP[2], un experimentado responsable del área de marketing de producto de MSP indicó que las soluciones de RMM traen las siguientes ventajas clave para los MSP:

1

Aumentan la eficiencia por poder visualizar todos los activos y prestar servicios de manera rápida y sin contratiempos.

2

Garantizan el máximo periodo de funcionamiento monitoreando las redes y los dispositivos, por lo que los MSP pueden actuar rápido cuando reciben alertas por problemas potenciales antes de que sean graves.

3

Reducen los gastos eliminando la necesidad de realizar traslados cada vez que se requiera de asistencia.

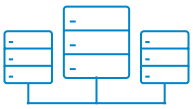
Estos beneficios no solo aplican para los MSP, sino también para los departamentos de TI internos, especialmente las fuerzas de trabajo remotas.

Muchas soluciones de RMM se pueden ajustar a los requisitos de la TI, así que obtienes solo las opciones y los servicios que tu empresa necesita. En este documento técnico, hablaremos sobre las cuatro claves a la hora de gestionar la TI de forma remota, así como las opciones disponibles que debes considerar para poder elegir tu solución de RMM.

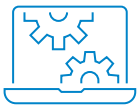
Cuatro claves para gestionar la TI de forma remota

1 Conoce lo que quieres que la TI monitoree y gestione de forma remota

No todas las soluciones de RMM son iguales. La mayoría de ellas te ayudan a monitorear y gestionar algunos o la totalidad de estos elementos.



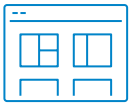
Centros de datos



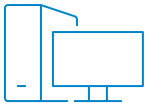
Sistemas operativos

Servidores

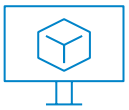
Aplicaciones



Sitios web



Puntos finales



Máquinas virtuales

Dispositivos periféricos

2 Cuenta con las herramientas correctas para realizar el trabajo

Prioriza. Crea una lista de desafíos y problemas que tu organización debe enfrentar. ¿Cuáles son los inconvenientes que requieren de atención inmediata? Una vez que definas los principales desafíos, puedes priorizar cuáles serán las herramientas absolutamente esenciales. A partir de esa información, decide qué herramientas necesitarías en el futuro cercano y cuáles son irrelevantes.

Este es un resumen de las herramientas y servicios de RMM disponibles. ¿Cuáles son críticos para tu negocio?

Monitoreo de red y de dispositivos en tiempo real, 24/7

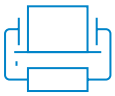
Monitorea servidores y puntos finales 24/7 y recibe alertas en tiempo real de problemas potenciales, para que puedas solucionarlos antes de que sean graves.

Gestión de activos

Con plena visibilidad gracias a una consola de gestión de activos, puedes ver, monitorear y gestionar cada dispositivo de tu infraestructura de TI en una sola pantalla.

Gestión de parches

El parcheo masivo oportuno y automatizado de los sistemas operativos y de los programas informáticos de terceros ofrece protección contra los ataques cibernéticos que se aprovechan de las vulnerabilidades de los programas informáticos.



Gestión de los dispositivos de red

Monitorea y gestiona la disponibilidad de los dispositivos periféricos de red, como impresoras, enrutadores, cortafuegos, interruptores, USB y más.

Protección de puntos finales

La protección contra programas maliciosos centralizada y automatizada para computadoras de escritorio, computadoras portátiles, tabletas y smartphones reduce de forma dramática el riesgo de ataques de virus, secuestro de datos, programas espía y más.

Copias de seguridad

Gestionar copias de seguridad de forma remota garantiza que este elemento crítico de cada plan de recuperación corporativa se ejecute de manera exhaustiva y de acuerdo al calendario programado.

Monitoreo web

Monitorea tu sitio web desde múltiples ubicaciones y recibe alertas si se está cargando demasiado lento, no se puede acceder a él o tiene problemas funcionales (por ejemplo, errores con la página de pago de la tienda en línea o fallas con los inicios de sesión de los clientes).

Aplicación móvil

Permite que los técnicos de TI operen el RMM desde sus dispositivos móviles con Android o iOS, para que puedan identificar y solucionar problemas desde cualquier lugar, 24/7.

Informes

Genera automáticamente informes detallados y personalizados sobre los indicadores clave de rendimiento que especifiques, como el tiempo de funcionamiento del servidor, las detecciones de programas maliciosos, el tiempo de resolución de problemas y mucho más.

Auditorías

Realiza un seguimiento del cumplimiento de licencia de los programas informáticos de terceros, para siempre estar al tanto de cuántas licencias para cada aplicación están en uso y cuántas están disponibles.

Escaneo de red

Verifica cuántos dispositivos nuevos se han agregado a tu red para poder configurarlos y gestionarlos de forma remota adecuadamente.

Gestión de dispositivos móviles

Monitorea y gestiona computadoras portátiles y de escritorio, smartphones y tabletas.

Sistemas de tickets integrado

Organiza y gestiona todos los tickets de asistencia en tu RMM, ya sea que se hayan enviado por teléfono, por e-mail o por un formulario en línea de atención al cliente.

Interfaz de programación de aplicaciones (API, por sus siglas en inglés)

Te permite analizar los datos recolectados y asentados en los informes de la solución de RMM en los programas informáticos de terceros, para que puedas compartirlos con unidades que no tienen acceso al RMM.

Instalación de programas informáticos

Instala nuevos programas en docenas, cientos o miles de dispositivos en segundo plano sin interrumpir a los empleados.

Scripting y automatización

Ejecuta scripts para tareas rutinarias: programa la ejecución de procesos repetitivos de forma automática (por ejemplo, la creación de puntos de recuperación del sistema o la eliminación de archivos temporales con una frecuencia determinada).

Automatización de servicios profesionales (PSA, por sus siglas en inglés)

La automatización de servicios profesionales puede funcionar con o ser parte de la solución de RMM para gestionar los negocios de los MSP integrando el sistema de tickets, brindando información sobre el negocio, programando periodos de mantenimiento técnico y optimizando la facturación.

Analiza tus opciones junto a vendedores de RMM que ofrezcan herramientas que necesitas y que te permitan personalizar tu solución, para que no termines pagando por herramientas o servicios que no utilizarás.

3 Gestiona de manera segura

De acuerdo con Statista, el costo medio de un ciberataque para los negocios de Europa o Norteamérica de 50 o menos empleados en 2020 fue de USD 24 000; USD 133 000 para otras empresas de 250 a 300 empleados; y USD 504 000 para las empresas de alrededor de 1000 empleados.[3]

Debido a los altos costos que deben afrontar las empresas por la pérdida de datos, los programas maliciosos, los ataques de día cero, el robo de datos, el secuestro de datos y más, contar una solución de RMM segura con herramientas que te permitan proteger tu red y tus dispositivos es vital.

Si bien tu RMM facilita la gestión de la seguridad de tu infraestructura de TI, también es importante tener en cuenta la seguridad de la solución de RMM en sí misma, porque esta se conecta a cada sección de tu infraestructura. Algunas soluciones de RMM también se conectan con programas informáticos de terceros. Si existen vulnerabilidades en esas conexiones, tu empresa podría estar en riesgo. Un investigador especializado en seguridad publicó información sobre esa vulnerabilidad en una herramienta popular de RMM en el 2017. Dos años después, un MSP que no había parchado la vulnerabilidad vio cómo se paralizaba toda su base de clientes debido a esa vulnerabilidad.[4]

Tres herramientas de RMM (la gestión de parches, las copias de seguridad y la protección de puntos finales) lidian con desafíos comunes de seguridad de TI. Las soluciones de RMM integradas te permiten realizar tareas relacionadas con la seguridad sin tener que alternar aplicaciones. El RMM también te permite obtener y ver información al instante sobre tus dispositivos, con detalles como los siguientes:

- Qué dispositivos necesitan parches para sus sistemas operativos y aplicaciones de terceros.
- Si las copias de seguridad de los dispositivos se realizaron correctamente.
- Cuál es el estado actual de la protección de los puntos finales.

La protección de los puntos finales te notifica si alguien intentó atacar un dispositivo, para que puedas tomar medidas de respuesta de forma remota y al instante. Con el RMM, los técnicos de TI no tienen que solucionar los problemas que presenten los dispositivos en persona para poder tomar las medidas correspondientes. Pueden resolver problemas urgentes en cualquier lugar y desde cualquier lugar donde estén.

Para garantizar que ningún tercero o intermediario descifre transmisiones hacia o desde tu RMM, cada sesión remota que tienes con los servidores y los puntos finales debe cifrarse con encriptación de extremo a extremo. Otras funciones de seguridad críticas de RMM incluyen lo siguiente:

- La garantía de los socios de RMM potenciales de que parcharán las vulnerabilidades apenas tengan conocimiento de ellas.
- La capacidad administrativa de eliminar y denegar el acceso a los antiguos empleados de forma permanente.
- La protección contra el keylogger (registro de pulsación de teclas) y los ataques de fuerza bruta.

Con la solución de RMM correcta, la plataforma en sí misma debe ser segura y debe tener integradas herramientas de RMM para que la gestión de la seguridad de la TI sea más fácil.

4 Simplifica tu kit de tecnología

Ya sea que seas un administrador de TI o un operador MSP, la eficiencia debe ser tu principal prioridad. Con la velocidad de los negocios de hoy en día, la ineficiencia conlleva al caos, los riesgos de seguridad, las malas experiencias de usuario, entre otras.

Probablemente puedas encontrar un vendedor diferente para cada una de las herramientas que utilizas para gestionar la TI de forma remota, pero uno de los mayores beneficios que ofrece una solución de RMM es la capacidad de consolidar tu kit tecnológico obteniendo todas las herramientas de un solo proveedor. Contar con una plataforma de RMM centralizada con todas las herramientas de gestión remotas te trae tres ventajas principales:

1. **Mayor eficiencia**

   Monitorea y gestiona cada dispositivo desde una sola pantalla. Esto significa que los técnicos de TI no tendrán que alternar plataformas cada vez que se agrega un nuevo dispositivo al sistema y cada vez que necesiten acceder a una herramienta de RMM diferente.

2. **Completa tranquilidad**

   Despreocúpate eliminando toda posibilidad de incompatibilidad de soluciones, ya que todas las herramientas y servicios están integrados en una sola plataforma.

3. **Solución conveniente todo en uno**

   Adquirir la solución de RMM de un solo vendedor significa una sola persona de ventas, un solo número de asistencia, una sola dirección de e-mail y una sola factura para pagar. En cambio, adquirir las herramientas de gestión remota de dos o más vendedores agrega complejidad y más tareas administrativas para los accionistas y los departamentos involucrados.

El RMM va de la mano con el acceso y la asistencia remotos. ¿Cómo? Cuando se identifica problemas con el RMM, puedes utilizar el acceso remoto para conectarte al dispositivo y resolver problemas de manera inmediata, todo desde una sola plataforma integrada.

Puedes optimizar tu kit tecnológico de la TI con RMM y asistencia remota, que está disponible en la misma plataforma integrada de TeamViewer.

La solución TeamViewer RMM

TeamViewer Remote Management es una solución robusta para la gestión remota de TI que ofrece Remote Device Monitoring (monitoreo de dispositivos remotos), Network Device Monitoring (monitoreo de dispositivos de red), Asset Management (gestión de activos), Patch Management (gestión de parches), Endpoint Protection (protección de puntos finales), Backup (copias de seguridad) y Web Monitoring (monitoreo web). Si bien TeamViewer Remote Management está disponible como una solución todo en uno, también funciona perfectamente con TeamViewer Remote Access y Support (acceso y asistencia remotos), para que tus herramientas de gestión remotas siempre sean confiables, rápidas y seguras. Para los usuarios de TeamViewer Remote Access y Support, TeamViewer Remote Management es una extensión integrada y, por tanto, conveniente.

Conclusión

La gestión remota de TI proactiva es mucho más eficiente que el antiguo enfoque de "se rompe/se arregla" que requiere que los técnicos y los dispositivos estén en el mismo lugar. La variedad de funciones y dispositivos que pueden gestionarse de forma remota continúa aumentando. El RMM ha hecho que la gestión remota de la TI sea incluso más eficiente agrupando herramientas personalizadas en una sola plataforma, lo que les permite a las empresas consolidar sus kits de tecnologías y utilizar todas las funciones de gestión de TI remota desde una sola plataforma.

Cuando se complementa TeamViewer RMM con TeamViewer Remote Access y Support, las organizaciones de TI y los MSP trabajan con mayor rapidez y seguridad y son más productivos que nunca. Teniendo en cuenta las cuatro claves para gestionar la TI de forma remota, puedes elegir la solución de RMM más adecuada para tu empresa.

Próximo paso

¿Quieres evaluar TeamViewer RMM en tu empresa? Prueba todas las funciones y los servicios con una versión de prueba gratis de 14 días.

Quiero mi versión de prueba gratis

Sin compromiso y sin ingresar los datos de tu tarjeta de crédito.

TeamViewer

Recursos

Descubre más sobre TeamViewer RMM

Solicita una demostración gratis de TeamViewer RMM

Referencias

1. Impact (2020, June): Why the Break/Fix Model for IT Services Is Dying. Retrieved from https://www.impactmybiz.com/blog/why-the-break-fix-model-for-it-services-is-dying/

2. smartermsp.com (2020, July): Ask an MSP Expert: How can an RMM tool help my MSP business? Retrieved from https://smartermsp.com/ask-an-msp-expert-how-can-an-rmm-tool-help-my-msp-business/

3. Statista (2020, November): Average cost of cyberattack to European and North American firms 2020, by size. Retrieved from https://www.statista.com/statistics/1008112/european-north-american-firms-cyberattack-cost/

4. securityboulevard.com (2019, February): Ransomware attack on MSPs exploits popular PSA/RMM Tool. Retrieved from https://securityboulevard.com/2019/02/ransomware-attack-on-msps-exploits-popular-psa-rmm-tool/

Acerca de TeamViewer

Como una plataforma líder mundial en conectividad remota, TeamViewer permite que los usuarios se conecten con cualquier persona, con cualquier cosa, en cualquier lugar y en cualquier momento. TeamViewer ofrece capacidades seguras y remotas de acceso, asistencia, control y colaboración para puntos finales en línea de todo tipo y ayuda a las empresas de todos los tamaños a alcanzar su máximo potencial digital. Se ha activado TeamViewer en alrededor de 2,5 mil millones de dispositivos; cerca de 45 millones de dispositivos se encuentran en línea al mismo tiempo.

Fundada en el 2005 en Göppingen, Alemania, TeamViewer es una empresa de capital abierto que cotiza en la Bolsa de Fráncfort y que cuenta con alrededor de 1350 empleados en sus oficinas de Europa, Estados Unidos y la región de Asia-Pacífico.

Mantente conectado

www.teamviewer.com

TVRM-WP-ES-MX-032021-1