GESTIÓN DE PUNTOS FINALES

datto
A Kaseya COMPANY

Datto RMM

Una solución que prioriza la seguridad

eBook

Seguridad integral, seguridad no compleja

Alrededor del 77% de las PYMES cree que sus entornos de TI se han vuelto más complejos en los últimos dos años, y el 52% de las PYMES cree que esta complejidad está impulsando un cambio rápido en el panorama de la ciberseguridad[1].

Proteger los puntos finales, monitorear nuevos dispositivos y gestionar parches son solo algunas de las tareas continuas que los equipos de TI realizan para mantener sus organizaciones seguras en medio de un panorama de amenazas cibernéticas en constante evolución.

Abordar desafíos complejos de seguridad a escala exige un enfoque integral que se base en fundamentos sólidos de seguridad y reúna marcos y procesos escalables. Datto RMM crea un ecosistema de seguridad sólido pero fácil de gestionar, con el objetivo de enfrentar estos desafíos de frente.

[1] Sharp - The Vulnerable State of SMB Cybersecurity and How Managed Service Providers Can Help

Un enfoque multifacético para la gestión segura de puntos finales

Datto RMM está diseñado para maximizar la protección contra múltiples vectores de amenazas en toda la superficie del ataque cibernético. Como parte de nuestro enfoque integral de seguridad, Datto RMM trabaja para lograr tres objetivos clave:

- **Proteger Datto RMM**: En Datto, la seguridad comienza con nosotros y hacemos todo lo posible para proteger nuestra infraestructura y aplicaciones a través de una combinación de procesos avanzados, marcos y cultura de productos.
- **Proteger su negocio**: Con una herramienta tan crítica y poderosa como la gestión de puntos finales, la seguridad de la plataforma es primordial. Datto RMM está diseñado para prevenir cualquier intento de hacer daño a través de la plataforma.
- **Permitir que TI proteja el negocio**: Datto RMM brinda una visibilidad profunda de los puntos finales, lo que les permite tomar medidas de seguridad proactivas y sólidas y mantenerse a la vanguardia de los desafíos de seguridad.

Proteger Datto RMM

Basada en nuestra cultura de seguridad, Datto RMM aprovecha los procesos de desarrollo seguros y las rigurosas evaluaciones periódicas de seguridad de la información. Otras medidas proactivas incluyen:

- **Nube desde el día uno**: Las versiones locales de la gestión de puntos finales han sido vulnerables a las violaciones de seguridad en los últimos años, especialmente cuando los entornos de TI se están volviendo cada vez más complejos y diversos. Datto RMM siempre ha sido una solución basada en la nube, lo que la convierte en una opción más segura con una superficie de ataque reducida.

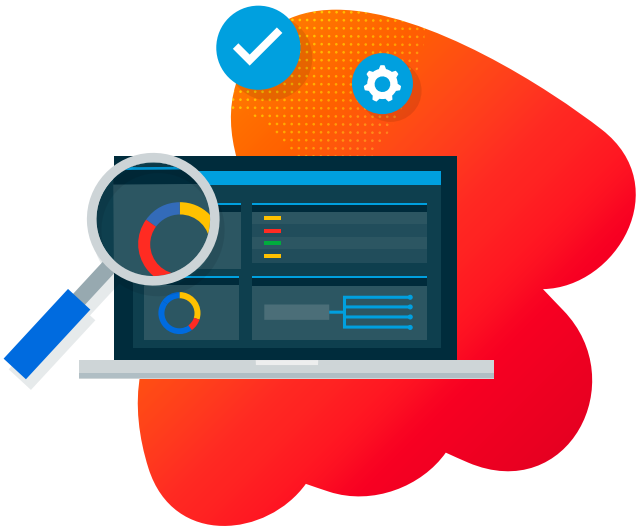
¿Sabía que...?

Datto RMM se ubicó en el 20% superior de todas las empresas que se sometieron a su evaluación del Modelo de seguridad en la consolidación de edificios (Building Security In Maturity Model, BSIMM), una evaluación independiente de seguridad de terceros de aplicaciones de software basada en un modelo de consolidación ampliamente aceptado. Datto RMM es la única solución de gestión de puntos finales de canal evaluada hasta la fecha. En el futuro, todos los participantes nuevos se compararán con Datto y una lista de empresas conocidas.

- El **equipo de desarrollo de productos altamente experimentado** de Datto RMM analiza el panorama tecnológico de manera constante para encontrar nuevas formas de mejorar la seguridad del producto.
- El **código fuente de Datto RMM se conserva en repositorios seguros y separados** a los que solo se puede acceder a través de la red interna de Datto con su propia autenticación multifactor (multifactor authentication, MFA), necesaria para acceder a él.
- Contamos con **un estricto proceso de revisión de códigos,** donde cualquier nuevo envío de código se revisa mediante un mínimo de dos desarrolladores adicionales.
- **Múltiples pases de aseguramiento de calidad (Quality Assurance, QA)** a lo largo del ciclo de vida del desarrollo del producto, desde entornos aislados hasta entornos de mantenimiento, pruebas y entornos de preparación. Después de cada actualización, el entorno de producción de software tiene una aprobación de QA muy estricta, incluidas pruebas de seguridad y simulaciones de ataques.
- Realizamos **revisiones de códigos y escaneado de dependencias** para garantizar que nuestra aplicación y sus dependencias sean seguras.
- Datto RMM ha sido **certificado por auditores independientes para cumplir con los requisitos SOC II Tipo II** de los criterios de servicios de fideicomiso de seguridad y disponibilidad. Estas auditorías se realizan todos los años para garantizar que cumplamos con los requisitos.

Proteger negocios

Cuando se trata de proteger su infraestructura, los equipos de TI tienen mucho en juego. Deben evaluar la postura de seguridad de su proveedor de gestión de puntos finales para garantizar que prioricen la seguridad. Datto RMM cuenta con varias medidas de seguridad integradas que están diseñadas para evitar que los perpetradores intenten armar la plataforma de gestión de puntos finales contra los negocios.



- Datto RMM opera en **múltiples plataformas de escalamiento resilientes y de alta disponibilidad** alojadas dentro de Amazon Web Services (AWS).
- Nuestro RMM está alojado en la **nube privada virtual de AWS**, aislado del entorno de la nube pública y en diferentes regiones a nivel mundial. Cada instancia en la nube se replica e incluso se equilibra la carga en un mínimo de dos centros de datos.
- **El acceso avanzado al entorno de producción está disponible solo para unos pocos empleados autorizados** y debe ser aprobado por otro empleado en cada instancia. El acceso a la instancia de RMM debe ser aprobado por ellos.
- Datto RMM tiene **revisiones regulares con AWS** para agudizar nuestras medidas de seguridad de alojamiento y minimizar el riesgo de un incidente de seguridad.
- **Todos los datos transferidos entre Datto RMM, los usuarios y los puntos finales están cifrados.** Los centros de datos están protegidos con firewalls. El producto se somete regularmente a pruebas de penetración por parte de profesionales fuera de la empresa y, en el caso de un descubrimiento, se prepara una solución y generalmente se libera fuera de los períodos de lanzamiento programados.
- **El acceso remoto SSH y RDP a la infraestructura de Datto RMM está desactivado** para mejorar aún más la seguridad del back-end.

- **El acceso a las instancias de AWS se controla a través de grupos de seguridad independientes**, grupos de firewall para front-end, back-end y repositorios de datos, etc.
- Datto RMM emplea un **firewall de aplicaciones web (web application firewall, WAF)** en todos nuestros servicios.
- Utilizamos una **solución de detección y respuesta gestionadas (managed detection and response, MDR) en toda la infraestructura de Datto RMM** para buscar comportamientos sospechosos o no conformes.
- Los **componentes de ComStore de Datto RMM se gestionan y prueban cuidadosamente** con el equipo de RMM, con solo un grupo de personal seleccionado y auditado con acceso para gestionar los componentes de ComStore. Los componentes no se actualizan automáticamente en los inquilinos de nuestros socios; permitimos que los socios vean y aprueben las actualizaciones de los componentes de ComStore individualmente, y el contenido puede inspeccionarse copiando el componente.

¿Sabía que...?

Los productos de gestión de puntos finales de la competencia a menudo se han enfocado en las operaciones locales, lo que coloca una carga de trabajo significativa en el personal de TI para garantizar que los sistemas estén funcionando y ejecutando las últimas versiones de aplicaciones, complementos de integración, certificados de seguridad, etc. En el pasado, se han informado incidentes de seguridad en productos de gestión de puntos finales locales que involucran complementos obsoletos que causan violaciones y certificados de seguridad vencidos que causan un funcionamiento incorrecto del software.

Por el contrario, Datto RMM es una solución puramente basada en la nube, con toda la configuración y los datos que se mantienen seguros en los centros de datos de AWS. Datto gestiona certificados de seguridad; de manera similar, no hay complementos ni extensiones de los que preocuparse, ya que todo es gestionado por los servidores en la nube que ejecutan el producto de Datto RMM. En caso de un problema de seguridad, se puede utilizar un parche en el producto instantáneamente.

Permitir que TI proteja el negocio

Datto recomienda una estrategia de seguridad integral que utilice las múltiples vías de seguridad de puntos finales y TI que ofrece Datto RMM, incluyendo:

- **Varios controles para proteger los puntos finales gestionados, proporcionados por Datto**. Estos controles también se describen en nuestro artículo Mejores prácticas de seguridad.
- **La seguridad del dispositivo/agente** garantiza que cualquier dispositivo nuevo requerirá la aprobación del administrador para ejecutar trabajos, descargar componentes e implementar políticas del dispositivo.
- **Cifrado del agente entre el dispositivo y la consola principal:** Se asigna una clave de cifrado única a cada instalación del agente para autenticar la comunicación entre el agente y la plataforma, evitando cualquier intento de hacerse pasar por el agente.
- **Restricción de dirección IP**: Controle quién utiliza el navegador del agente y la interfaz de usuario al permitir que solo direcciones IP seleccionadas accedan a estas interfaces.
- **Estados de actualización de Windows (gestión de parches):** Datto RMM trabaja con Windows para informar los problemas de inmediato mediante el servicio Windows Update. Además, el sólido núcleo de gestión de parches de Datto RMM es totalmente compatible con Windows 10 y Windows 11 e informará cualquier problema de instalación de actualizaciones utilizando la misma interfaz.
- **Las actualizaciones y el estado del software de terceros** garantizan que las aplicaciones críticas conectadas a Internet instaladas en los puntos finales se mantengan actualizadas sin problemas.
- **Auditoría de seguridad**: Datto RMM brinda un componente llamado "Auditoría de seguridad [WIN]" que ayuda a los negocios a identificar la política de seguridad adecuada para su red y cuántos dispositivos se desvían de esta política. La auditoría evalúa los dispositivos en función de diversos criterios en diferentes categorías, como sistemas operativos, cuentas de usuario, seguridad de redes y dispositivos.

¿Sabía que...?

La detección de ransomware de Datto RMM supervisa la existencia de ransomware de cifrado en puntos finales mediante el análisis conductual de archivos patentado, y genera una alerta cuando un dispositivo está infectado. Una vez detectado, Datto RMM puede aislar el dispositivo e intentar detener los procesos sospechosos de ransomware para evitar que el ransomware se propague.

- Para ayudarlo a responder estas preguntas, Datto RMM brinda un **componente de auditoría de seguridad y un conjunto de políticas de monitoreo** destinados a identificar inquietudes de seguridad comunes en dispositivos Windows. Estas inquietudes se plantean en el StdOut desde la ejecución del componente y dentro del registro de eventos de Windows. La política de monitoreo puede capturar y filtrar esta información. Si se está vinculando a una solución de PSA, las reglas del flujo de trabajo también se pueden aplicar a los tickets.
- **Las políticas del agente** se pueden utilizar para configurar cuánto control se otorga a los usuarios de Datto RMM sobre los puntos finales. Los negocios pueden configurar cuánto control reciben los usuarios que se conectan de forma remota a un dispositivo, si los dispositivos pueden recibir trabajos y otras funciones. Esto puede ser particularmente útil para dispositivos que nunca deben ejecutar trabajos automatizados o recibir soporte remoto.
- Datto RMM cuenta con varias **medidas de seguridad a nivel administrativo**, como:
  - **Autenticación de dos factores (2FA) obligatoria:** Datto RMM aplica 2FA en todas las cuentas para habilitar un segundo nivel de autenticación además de las credenciales de inicio de sesión. Ambos factores de autenticación se deben usar e ingresar correctamente para establecer la identidad del usuario sin duda.
  - **Restricción de dirección IP:** Considere bloquear la interfaz de usuario, al igual que con el navegador de agentes, solo para permitir inicios de sesión desde direcciones IP dentro de un rango aceptado.
  - **Niveles de seguridad granulares:** Los niveles de seguridad especifican y limitan el acceso de los usuarios cuando inician sesión en la interfaz web de Datto RMM, el explorador de agentes o una sesión remota web. Se pueden configurar, guardar y asignar diferentes niveles con control granular sobre los campos de acceso a diferentes usuarios. Si un grupo de usuarios necesita privilegios de seguridad idénticos, estos niveles se pueden aplicar a una lista de usuarios.
  - **Registro de actividad del usuario:** La nueva interfaz de usuario de Datto RMM combina el inicio de sesión de usuario y dispositivo en una interfaz unificada donde es posible consultar todas las acciones realizadas por un usuario y profundizar en su actividad relacionada con uno o más dispositivos. Esto permite a los administradores de RMM analizar y marcar cualquier actividad no deseada del usuario fácilmente.

Administración de Microsoft 365 para Datto RMM

En el panorama digital en rápida evolución actual, la gestión efectiva de TI es más que un lujo: es una necesidad. A medida que el lugar de trabajo continúa su transformación moderna, sus herramientas deben mantenerse a la vanguardia, garantizando eficiencia, seguridad y operaciones optimizadas. Teniendo esto en cuenta, presentamos la última función de Datto RMM: la **Administración de Microsoft 365**.

Conectar a su inquilino de Microsoft 365 a su herramienta de monitoreo y administración remota preferida no debe ser una tarea. La función de Administración de Microsoft 365 de Datto RMM le permite integrar ambas plataformas sin esfuerzo. Con solo unos pocos clics, obtendrá una descripción general integral de sus inquilinos, usuarios y dispositivos asociados.

Históricamente, los RMM a menudo se encasillaban como soluciones de gestión de criterios de puntos finales. Sin embargo, el panorama de TI moderno requiere una perspectiva más amplia. Con el universo en expansión de Microsoft 365, las complejidades están en aumento. La nueva función de Datto RMM está diseñada con este desafío exacto en mente, lo que garantiza que los profesionales de TI puedan mantenerse enfocados sin la molestia adicional de navegar constantemente por los numerosos portales de Microsoft.

A medida que las herramientas de gestión de TI evolucionan continuamente, los negocios que integran simplicidad, eficiencia y seguridad establecerán el estándar de la industria. La función de Administración de Microsoft 365 de Datto RMM no es solo una adición, es el futuro de la gestión de TI, un elemento de cambio.

Descargar eBook: Guía para el Éxito del Negocio de TI