datto
A Kaseya COMPANY

8 medidas de seguridad que las empresas de LATAM necesitan más allá del antivirus

América Latina (LATAM) enfrenta más ciberataques que cualquier otra región del mundo. En la primera mitad de 2025, las organizaciones de la región sufrieron un 39 % más de ataques semanales que el promedio global —una clara advertencia para que las empresas y los proveedores de TI refuercen sus defensas ahora mismo.

El panorama de amenazas ha evolucionado. Los atacantes están utilizando IA y kits avanzados para ejecutar ataques que superan fácilmente tanto la supervisión humana como las defensas tradicionales. El software antivirus básico ya no puede mantenerse al ritmo de estas tácticas, por lo que la protección por capas y las soluciones avanzadas para endpoints son esenciales.

Hemos creado esta lista de verificación de ocho puntos para ayudar a las organizaciones en LATAM a evaluar su preparación en materia de seguridad, cerrar brechas y construir una protección duradera para sus usuarios y clientes.

1. Obtén visibilidad total con un inventario completo de endpoints

Un inventario integral de endpoints es el punto de partida para una seguridad sólida. Mantener un registro actualizado de cada dispositivo conectado a tu red (servidores, laptops, teléfonos móviles y equipos IoT) garantiza una visibilidad y control completos. Incluso un solo dispositivo no rastreado o olvidado puede convertirse en un endpoint sombra, abriendo una brecha que los atacantes pueden aprovechar.

2. Elimina vulnerabilidades más rápido mediante parches automatizados

El software sin actualizar sigue siendo una de las formas más fáciles para que los atacantes obtengan acceso. Los retrasos en las actualizaciones dejan los sistemas expuestos a ransomware y otras amenazas que pueden apoderarse rápidamente de la red. La gestión automatizada de parches ayuda a los equipos de TI pequeños o sobrecargados a implementar actualizaciones en todos los endpoints de manera rápida y consistente, reduciendo el error humano y cerrando las brechas de seguridad antes de que sean explotadas.

3. Detecta y detén ataques avanzados con inteligencia EDR

Las soluciones antivirus tradicionales dependen de firmas de malware conocidas, lo que las vuelve ineficaces frente a amenazas nuevas o en evolución. Las soluciones de detección y respuesta en endpoints (EDR, por sus siglas en inglés) pueden identificar tanto amenazas conocidas como desconocidas. Estas monitorean continuamente la actividad de los endpoints en busca de comportamientos inusuales, aíslan los sistemas infectados y detienen las amenazas en tiempo real. Para las empresas de LATAM que enfrentan amenazas impulsadas por IA o ataques fileless, EDR ofrece la visibilidad y velocidad necesarias para mantenerse un paso adelante.

4. Asegura protección 24/7 con MDR o SOC como servicio

La detección y respuesta gestionada (Managed Detection and Response, MDR) o el modelo de SOC-as-a-Service combinan herramientas de seguridad avanzadas con un equipo de analistas que monitorean y responden a amenazas las 24 horas del día, los 7 días de la semana. Para los equipos de TI en LATAM con recursos limitados, MDR ofrece protección de nivel empresarial, una respuesta más rápida ante amenazas y una reducción del tiempo de inactividad, sin necesidad de construir un centro de operaciones de seguridad interno.

5. Bloquea el acceso no autorizado con MFA

La autenticación multifactor (Multi-Factor Authentication, MFA) añade una capa esencial de protección de identidad. Al requerir que los usuarios verifiquen su identidad mediante varios métodos, MFA evita el acceso no autorizado incluso si las contraseñas son robadas. En LATAM, donde el robo de credenciales es común, MFA es una de las defensas más simples y efectivas disponibles.

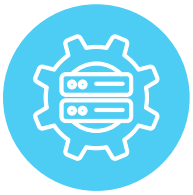
6. Protege a cada usuario y dispositivo en entornos remotos e híbridos

Con más empleados trabajando de forma remota o desde dispositivos personales, mantener controles de seguridad consistentes es fundamental. Aplica el uso obligatorio de VPN, estándares de configuración para los endpoints y políticas de acceso en todos los dispositivos. La supervisión centralizada ayuda a mantener la visibilidad y a prevenir la exposición de datos en entornos de trabajo distribuidos.

7. Minimiza el tiempo de inactividad con planes confiables de respaldo y recuperación

Incluso las mejores defensas pueden verse comprometidas. Realizar respaldos regulares y verificados, almacenados de forma separada de la red principal, garantiza que los datos puedan restaurarse rápidamente en caso de un incidente. Un plan de recuperación probado reduce el tiempo de inactividad y las pérdidas financieras, algo especialmente crucial para las empresas de LATAM, donde los recursos para recuperación suelen ser limitados.

8. Responde con confianza con un plan de respuesta a incidentes probado



Un plan claro de respuesta a incidentes garantiza una reacción rápida y coordinada cuando ocurre una brecha de seguridad. Las simulaciones regulares ayudan a que los equipos estén preparados y actúen de manera coordinada ante incidentes reales. Una buena preparación no solo reduce el impacto, sino que también fortalece la resiliencia a largo plazo.

Estos ocho elementos esenciales forman una base sólida para una mejor protección y una respuesta más rápida. A medida que las ciberamenazas en LATAM continúan creciendo en escala y sofisticación, actuar con información y preparación es más importante que nunca. Descarga el **Informe sobre el estado de la ciberseguridad en LATAM** para conocer referencias, datos regionales y orientación práctica que te ayuden a dar los próximos pasos.

Descubre cómo

datto
A Kaseya COMPANY