LIBRO VIRTUAL

8 PRINCIPALES DESAFÍOS DE LA SEGURIDAD DE ENDPOINTS

Introducción

En el clima empresarial de hoy en día, la gestión y la seguridad de los endpoints son críticas. Con usuarios finales que inician y cierran sesión en la red desde dispositivos con vulnerabilidades que no cuentan con los correspondientes parches de seguridad, y con amenazas cifradas que llegan a los endpoints sin ser comprobadas, los dispositivos deben protegerse para garantizar la seguridad tanto de los propios endpoints como de la red en su conjunto. Mientras que el ransomware y el robo de credenciales cada vez están más extendidos, los endpoints se han convertido en el campo de batalla del panorama actual de las amenazas.

A pesar de la gran cantidad de soluciones disponibles actualmente en el mercado, los administradores aún tienen dificultades con la visibilidad y la gestión de su sistema de seguridad. Además, se enfrentan al reto de tener que garantizar la seguridad coherente del cliente, y al mismo tiempo proporcionar funciones de inteligencia e informes accionables y fáciles de usar. A continuación, presentamos algunos de los desafíos con los que se puede encontrar a la hora de formular su estrategia de protección de endpoints.

Soluciones de seguridad anticuadas

Los administradores deben asegurarse de que los endpoints gestionados ejecuten la versión correcta de los componentes de software de seguridad instalados, tal y como dictan las políticas de cumplimiento. Este problema se ve agravado cuando se utilizan soluciones antivirus tradicionales basadas en una base de datos de definiciones actualizada para ofrecer protección contra las últimas amenazas. Las soluciones de Protección avanzada de endpoints (AEP) que examinan el comportamiento (heurística) del sistema son más efectivas contra estos ataques y además pueden bloquear scripts maliciosos, como los observados en ataques sin archivos.

"El 85% de las bases de código contenían dependencias de código abierto anticuadas de hace más de cuatro años."

Sinopsis del Informe OSSRA (Open Source Security and Risk Analysis) 2021

SONICWALL®

Refuerzo de políticas y cumplimiento Web

Los administradores tienen dificultades para mitigar los riesgos cuando los empleados usan dispositivos desde casa, en cafeterías, hoteles o aeropuertos a través de redes ajenas. Al mismo tiempo, se enfrentan a retos a la hora de reforzar la política de uso Web de la empresa cuando los empleados trabajan fuera de la oficina. Fuera del lugar de trabajo, los empleados tienden más a acceder a sitios Web maliciosos y a visitar sitios Web improductivos. Además, si los usuarios pasan todos sus datos por el centro de datos corporativo vía VPN, es posible que sea necesario restringir el contenido con un alto consumo de ancho de banda, como el vídeo. Durante los inicios de la pandemia, los administradores de red se quejaban de que sus redes estaban siendo inundadas por tráfico de TikTok, YouTube, Netflix, etc. procedente de servicios de streaming — problema que continuará creciendo a medida que aumente la calidad de la imagen y el uso de estas aplicaciones con fines de entretenimiento.

"Entre el 30 y el 40 por ciento de la actividad de los empleados en Internet no está relacionada con el trabajo"

Fuente: Estudios de IDC

Obtención de informes y gestión del acceso

En algunos casos, es posible que los administradores gestionen múltiples tenants a través de firewalls, aunque sus usuarios estén configurados en un único grupo. Esto hace que, a la hora de intentar gestionar políticas de clientes, obtener un inicio de sesión único (SSO) de un administrador de firewall o de consolas de gestión de la seguridad se convierta en un reto. Al mismo tiempo, la normativa a menudo dicta que todos los roles de administrador deben adherirse al principio de mínimo privilegio, de modo que una suite de gestión unificada de clientes que no pueda gestionar los controles del acceso basado en roles dará muchos problemas. Por ejemplo, alguien puede estar limitado a dos roles, uno de ellos con acceso de lectura y escritura y el otro solo de lectura.

Amenazas que llegan a través de canales cifrados

Puesto que cada vez más aplicaciones Web se protegen mediante canales cifrados, como HTTPS, y los autores de malware también están recurriendo al cifrado a fin de eludir la inspección basada en la red, la Inspección profunda de paquetes del tráfico SSL/TLS (DPI-SSL) se ha convertido en una práctica absolutamente necesaria. No obstante, si se quiere evitar un deterioro de la experiencia de usuario y la seguridad, por regla general, esto solamente puede conseguirse implementando de forma masiva certificados SSL/TLS fiables en todos los endpoints.

Entender las alertas y los pasos de resolución

Normalmente, los usuarios finales son menos conscientes de los riesgos de seguridad que los profesionales de seguridad. En consecuencia, no entienden las alertas de la mayoría de los clientes de seguridad de endpoints. Además, la mayoría de los clientes no incluyen información de autoayuda, por lo que los usuarios o bien ignoran el problema o recurren al departamento de TI. Por ejemplo, en el caso de que el dispositivo de un usuario incumpla las políticas y el usuario sea puesto en cuarentena, dicho usuario no sabrá cuáles son las acciones requeridas para volver a cumplir las normas.

Gestión de licencias

Un problema de backend del software de seguridad de endpoints consiste en que los administradores, en especial los MSSPs, no pueden asegurar que su software cuente con las licencias oportunas. Si la información sobre las licencias de los clientes no se monitoriza y almacena de forma centralizada, podrían producirse caídas o brechas de seguridad. Además, los administradores pueden tener dificultades para elaborar regularmente informes de cumplimiento normativo de todas las licencias de terceros implementadas para pagar a sus partners.

Detener las amenazas avanzadas, como el ransomware

A veces, los enfoques tradicionales de seguridad de endpoints pueden dejar brechas en el cumplimiento de los requisitos administrativos. Las tecnologías antivirus tradicionales utilizan un enfoque anticuado basado en definiciones que no ha sido capaz de seguir el ritmo del malware emergente ni de las nuevas técnicas de evasión. Muchas soluciones antiguas no son capaces de ofrecer detección de amenazas avanzadas ni de soportar una estrategia de defensa multicapa en los endpoints, incluida la integración con un entorno de sandboxing.

Asimismo, sin una capa adicional de detección y respuesta para endpoints, los ataques avanzados y sofisticados pueden burlar su protección de endpoints u otras medidas de seguridad.

"Al final del 3er trimestre de 2020, el ransomware había aumentado en un 40% con respecto al mismo periodo de 2019."

Fuente: Datos de amenazas del 3er trimestre de SonicWall

SONICWALL®

¿Dónde están las vulnerabilidades críticas?

Con el gran aumento de las aplicaciones de negocio, la amenaza de las vulnerabilidades de las aplicaciones ha crecido de forma exponencial, causando dolores de cabeza a los administradores de TI y brechas de seguridad. Muchas organizaciones todavía no cuentan con un método para identificar la cantidad y el tipo de las vulnerabilidades, lo cual dificulta la creación de un plan, ya sea para proporcionar un parche o para desinstalar las aplicaciones peligrosas.

Además de las vulnerabilidades que no cuentan con los correspondientes parches de seguridad, es posible que los equipos de TI no dispongan de los recursos necesarios para detectar de forma proactiva amenazas ocultas que esperan pacientemente para atacar en el momento oportuno (Caza de amenazas).

"Tan solo en 2019, los CNAs asignaron puntuaciones CVSS críticas de 9.0+ a más de 16.000 vulnerabilidades."

Fuente: NIST National Vulnerability Database

Conclusión

Si bien la gran cantidad de posibles desafíos puede dificultar la elaboración de un plan de protección de endpoints hasta el punto de que parezca una tarea imposible, hay disponibles numerosos recursos para simplificar el proceso. Si desea identificar la solución más adecuada para su organización, lea nuestro resumen ejecutivo, "Qué deben buscar los administradores a la hora de comprar una solución de seguridad de endpoints."

LEER RESUMEN EJECUTIVO

Acerca de SonicWall

SonicWall proporciona una Ciberseguridad sin límites, sin perímetro, para la era hiperdistribuida y una realidad laboral caracterizada por la movilidad, el teletrabajo y la inseguridad. Al detectar amenazas desconocidas, proporcionar visibilidad en tiempo real y ofrecer una alta rentabilidad, SonicWall cierra la brecha de la seguridad cibernética para empresas, gobiernos y pymes en todo el mundo. Si desea obtener más información, visite www.sonicwall.com.

Si tiene alguna duda sobre el posible uso de este material, póngase en contacto con nosotros:

SonicWall Inc.
1033 McCarthy Boulevard
Milpitas, CA 95035

Para más información, consulte nuestra página Web.
www.sonicwall.com