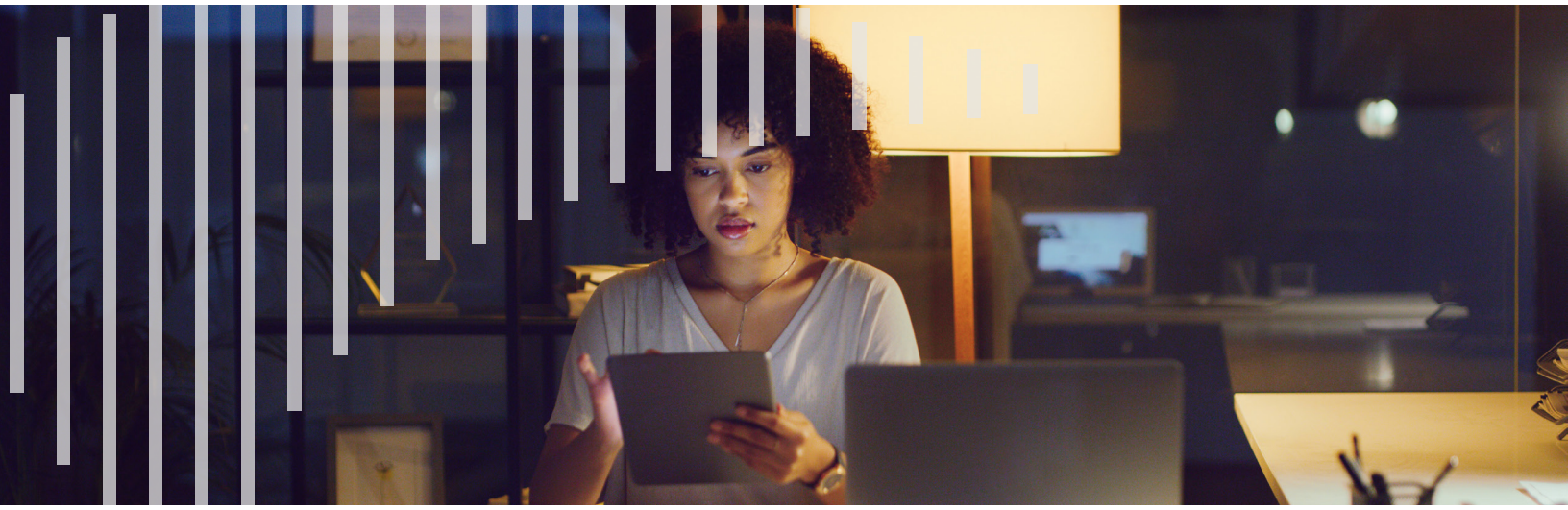

RESUMEN EJECUTIVO

Qué deben buscar los administradores a la hora de comprar una solución de seguridad de endpoints

Una nueva perspectiva de los retos que plantea la protección de endpoints

Resumen

Los administradores se enfrentan a una serie de retos planteados por los productos de seguridad de endpoints. Este resumen examina varios de estos retos persistentes, como son los siguientes:

- Mantenimiento y refuerzo de la seguridad
- Amenazas cifradas y avanzadas
- Gestión de alertas y de la resolución
- Creación y mantenimiento de políticas
- Visibilidad del estado de los tenants
- Vulnerabilidades que no cuentan con los correspondientes parches de seguridad

En el actual entorno del crimen cibernético, que se halla en continua evolución, la gestión y la seguridad de los endpoints resultan críticas. Los usuarios finales continuamente entran y salen de la red con sus dispositivos terminales. Al mismo tiempo, estos endpoints constituyen el campo de batalla del panorama actual de las amenazas. Cada vez son más las amenazas cifradas que llegan a los endpoints de forma desapercibida. Además, el ransomware va en aumento y el robo de credenciales persiste en segundo plano. La creciente amenaza del ransomware y de los demás ataques maliciosos basados en malware ha demostrado que las soluciones de protección de clientes no pueden medirse únicamente por el cumplimiento normativo de los endpoints.

Estos retos se ven agravados cuando se deben gestionar múltiples tenants, ya sea en una única organización o para múltiples clientes. Esto a menudo requiere diferentes políticas y configuraciones en base al grupo de usuarios, el dispositivo y la ubicación.

Los retos de la protección de endpoints

Aunque los productos de seguridad de endpoints llevan años en el mercado, los administradores siguen enfrentándose a retos importantes, como:

- Mantener los productos de seguridad al día
- Reforzar las políticas y el cumplimiento Web
- Obtener informes y gestionar el acceso
- Detectar las amenazas que llegan a través de canales cifrados
- Entender las alertas y los pasos de resolución
- Gestionar las licencias
- Detener las amenazas avanzadas, como el ransomware
- Saber dónde están las vulnerabilidades críticas
- Conocer el estado de los tenants y mantener las políticas globales

Mantener los productos de seguridad al día

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.

Con el fin de frustrar los ataques emergentes, los administradores de seguridad de red necesitan endpoints gestionados para evaluar el estado de seguridad y emitir informes de forma regular.

Algunos administradores necesitan detener el tráfico que circula en sus centros de datos en dirección este-oeste, lo cual a menudo supone la mayoría del tráfico que circula por sus switches. Necesitan la opción de poner en cuarentena un dispositivo

de forma local en el caso de que incumpla las normas o sea infectado. En estos casos, el firewall debe bloquear el acceso de dicho dispositivo a Internet y a la LAN, restringiendo las rutas a las mismas ubicaciones de cuarentena designadas por el firewall.

A fin de garantizar la integridad de los datos, los administradores de seguridad deben asegurar además que los datos que se intercambian entre la consola de gestión unificada de clientes y la de gestión centralizada no puedan ser manipulados mientras están en tránsito.

Reforzar las políticas y el cumplimiento Web

Si los endpoints incumplen las políticas, los administradores deben poder evitar que el dispositivo terminal utilice servicios UTM para hacer pasar el tráfico por el firewall. Los usuarios finales también desempeñan un papel importante en la seguridad de los endpoints. Trabajan desde portátiles corporativos y otros endpoints. Los usuarios necesitan saber inmediatamente si se ha detectado algún software o comportamiento malicioso, para poder tomar medidas o iniciar un ticket en caso necesario.

Si tiene empleados que trabajan desde fuera de la oficina, puede reforzar las políticas de uso Web de su organización con un filtro Web o de contenido embebido en su solución de seguridad. Es vital bloquear además el acceso a sitios maliciosos conocidos, y algunos también consideran importante bloquear los sitios Web improductivos y el material adulto. Si los usuarios acceden a datos de vídeo a través de servidores locales vía VPN, también debería considerarse restringir los sitios Web con un alto consumo de datos.

Obtención de informes y gestión del acceso

En algunos casos, es posible que los administradores gestionen múltiples firewalls, aunque sus usuarios estén configurados en un único grupo. Necesitan poder obtener un inicio de sesión único (SSO) desde cualquier consola de administración de firewall o de gestión de la seguridad para gestionar las políticas de los clientes. Al mismo tiempo, la normativa a menudo dicta que todos los roles de administrador deben adherirse al principio de mínimo privilegio, de modo que la gestión unificada de clientes debería tener un control del acceso basado en roles suficiente para el acceso privilegiado. Por ejemplo, puede estar limitado a dos roles, uno de ellos con acceso de lectura y escritura y el otro solo de lectura.

Las amenazas ocultas 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, sin la implementación masiva de certificados SSL/TLS fiables en todos los endpoints, no es fácil aplicarlo sin deteriorar la experiencia de usuario y la seguridad. Se requiere un mecanismo que permita distribuir y gestionar los certificados y el modo en que los navegadores deben confiar en ellos.

Entender las alertas y los pasos de resolución

Los usuarios finales suelen ser menos conscientes de los riesgos de seguridad que los profesionales de seguridad. En consecuencia, sería importante que su plataforma de protección de endpoints les avisara sobre los cambios del perfil de riesgo cuando viajan con sus portátiles entre diferentes ubicaciones, y les diera consejos sobre cómo mantenerse a salvo.

Para resolver rápidamente cualquier problema de incumplimiento de políticas corporativas, puede resultar beneficioso tanto para el equipo de TI como para los usuarios finales tener acceso a información de autoayuda. En el caso de que el dispositivo de un usuario incumpla las políticas y el usuario sea puesto en cuarentena, el usuario también necesita orientación en cuanto a las acciones requeridas para volver a cumplir las normas.

La gestión de licencias

Los administradores necesitan asegurar que cualquier software de seguridad de endpoints adquirido se actualice automáticamente en su interfaz de gestión, a fin de que puedan mantener los endpoints equipados con las licencias correctas. Por ejemplo, debería monitorizarse y almacenarse de forma centralizada toda la información de las licencias de un cliente. En caso de que se adquiera una nueva licencia, debería enviarse una señal a la gestión unificada de clientes y a la gestión centralizada para alertar de la nueva adquisición y comenzar a tramitar los derechos de software.

Algunos administradores deben 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 pueden dejar brechas en el cumplimiento de los requisitos administrativos. El enfoque basado en definiciones de las tecnologías antivirus tradicionales, que lleva tiempo causando problemas, no ha sido capaz de seguir el ritmo al que aparecen nuevas variantes de malware y técnicas de evasión. Esto ha hecho necesario un enfoque diferente para la protección de los endpoints. Se requiere un enfoque que no solo proporcione motores de detección de amenazas avanzadas, sino que además soporte una estrategia de defensa multicapa en los endpoints, incluida la integración con un entorno de sandboxing.

Una limitación importante de las soluciones puntuales existentes hoy en día (conocidas como clientes AV reforzados) es que suelen desarrollarse específicamente para un tercer proveedor e integrarse en sus soluciones. Los administradores necesitan un modelo más abierto, que permita implementar de forma relativamente rápida módulos de seguridad adicionales si el negocio o la industria lo requieren.

¿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. Tan solo en 2019, se asignaron numerosas puntuaciones CVSS críticas de 9.0+ a vulnerabilidades, causando dolores de cabeza a los administradores de TI y brechas de seguridad. Las organizaciones necesitan un método para identificar la cantidad y el tipo de las vulnerabilidades con el fin de crear un plan, ya sea para proporcionar un parche o para desinstalar las aplicaciones peligrosas.

Conocer el estado de los tenants y mantener las políticas globales

A menudo, las empresas grandes tienen que gestionar gran cantidad de endpoints; o garantizar la seguridad de los endpoints en diferentes regiones, grupos de usuarios o tipos de dispositivos: o ambas cosas. Esto sólo es posible si disponen de los medios adecuados para crear nuevos tenants con rapidez y si cuentan con un dashboard global que les permita ver el estado de los tenants. En estas situaciones, los administradores deben enmendar rápidamente una política global que se aplique a los tenants y grupos. Los MSSPs y MSPs también necesitan tener libertad para crear políticas personalizadas para los tenants que no se vean afectados por los cambios de la política global. La función de gestión debería proporcionarles estadísticas de alto nivel sobre las infecciones y vulnerabilidades sin necesidad de desglosar la información de cada tenant.

Conclusión

Puesto que los endpoints se usan cada vez más como vectores de ciberataques, los profesionales de la seguridad deben tomar medidas para proteger los dispositivos terminales. Además, con la proliferación del teletrabajo, surge la acuciante necesidad de proporcionar una protección coherente para cualquier cliente, independientemente de dónde se encuentre.

Los administradores de seguridad deben evaluar las soluciones de endpoints teniendo en cuenta los requisitos reales.

Obtenga más información. Lea nuestro resumen de la solución "Seguridad de endpoints adaptada a su organización" o visite www.sonicwall.com/capture-client.

Acerca de SonicWall

SonicWall proporciona una Ciberseguridad sin límites, sin perímetro, para la era hiperdistribuida y una realidad laboral caracterizada por la movilidad, el trabajo remoto 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.

SonicWall, Inc.
1033 McCarthy Boulevard | Milpitas, CA 95035
Para más información, consulte nuestra página Web.
www.sonicwall.com

ExecBrief-WhatAdminNeed-A4-VG-3575