SONICWALL

QUÉ DEBEN BUSCAR LOS ADMINISTRADORES CUANDO COMPRAN UNA SOLUCIÓN DE SEGURIDAD DE LOS ENDPOINTS

Una perspectiva fresca de los desafíos de la protección en los endpoints

Resumen

Los administradores luchan con los desafíos de los productos de seguridad de los endpoints. En este informe se examinan varios de estos desafíos recurrentes, entre ellos:

- El mantenimiento y la ejecución de la seguridad
- Amenazas cifradas y avanzadas
- Gestión de alertas y correcciones
- Creación y mantenimiento de políticas
- Visibilidad en la condición del tenant
- Vulnerabilidades sin parches

Introducción

La administración y la seguridad de los endpoints es fundamental en el entorno actual del cibercrimen en evolución. Los usuarios finales se conectan continuamente dentro y fuera de la red con sus dispositivos endpoint. Al mismo tiempo, estos endpoints son el campo de batalla del actual panorama de amenazas. Las amenazas cifradas llegan cada vez más a los endpoints no controlados, el ransomware está en aumento y el robo de credenciales persiste silenciosamente. Sin embargo, la amenaza cada vez mayor del ransomware y otros ataques maliciosos basados en malware ha demostrado que las soluciones de protección de clientes no pueden medirse únicamente en función del cumplimiento de los endpoints.

Además, estos desafíos solo se agravan cuando se debe gestionar múltiples tenants, ya sea dentro de una sola organización o para múltiples clientes. Esto a menudo requiere diferentes políticas y configuraciones basadas en el grupo de usuarios, el dispositivo y la ubicación.

Los desafíos de protección en los endpoints

Los productos de seguridad de los endpoints han estado en el mercado durante años, pero los administradores tienen estas dificultades:

- Mantener los productos de seguridad actualizados
- Ejecutar las políticas y el cumplimiento
- Obtener informes
- Amenazas que llegan a través de canales cifrados
- Comprender las alertas y las medidas de corrección
- Administración de licencias
- Detener las amenazas avanzadas como el ransomware
- Crear y actualizar políticas en todo el mundo
- Comprender la condición de cada tenant
- No saber dónde se encuentran las vulnerabilidades fundamentales

Mantener los productos de seguridad actualizados

Los administradores deben asegurarse de que los endpoints administrados ejecuten la versión correcta de los componentes de software de seguridad instalados, tal como lo exige la política de cumplimiento.

Para frustrar los ataques emergentes, los administradores de seguridad en red necesitan endpoints administrados para evaluar la situación de seguridad e informar de su estado de forma continua.

Algunos administradores necesitan detener el tráfico este-oeste a través de sus centros de datos, que a menudo puede representar la mayor parte del tráfico a través de sus switches. Necesitan la opción de poner un dispositivo en cuarentena localmente en caso de que no cumpla con las normas o se infecte. En estos casos, el firewall debe bloquear el acceso a Internet y bloquear el dispositivo de la LAN, restringiendo así las rutas de la red a las mismas ubicaciones de cuarentena que el firewall está aplicando.

Todos los administradores de empresas grandes y pequeñas necesitan visibilidad de las vulnerabilidades de las aplicaciones presentes en los endpoints protegidos. Conocer la escala de una vulnerabilidad fundamental ayudará a la organización a desarrollar un plan para parchar estas aplicaciones para evitar mejor una violación.

Además, los administradores de seguridad deben garantizar que todos los datos entre el cliente unificado y la consola de administración centralizada no puedan ser manipulados mientras estén en tránsito, para asegurar la integridad de los datos.

Ejecutar las políticas y el cumplimiento

Si los endpoints están en un estado no regulado por la política, los administradores deben poder evitar que el dispositivo endpoint utilice los servicios de administración unificada de amenazas (UTM) para atravesar el tráfico a través del firewall. Los usuarios finales también tienen un papel importante que desempeñar en la seguridad de los endpoints. Trabajan con las laptops empresariales y con otros endpoints. Los usuarios deben saber inmediatamente si se detecta algún software o comportamiento malicioso, para que puedan tomar medidas o presentar un aviso si es necesario.

En el caso de los administradores de empresas con múltiples tenants y proveedores de servicios administrados de seguridad (MSSP), los administradores deben poder modificar las políticas para los tenants nuevos y enmendar las políticas existentes para cuando se detecte una nueva amenaza, o una nueva propiedad web esté acaparando el ancho de banda o afectando a la productividad, por ejemplo.

Obtener informes

En algunos casos, los administradores pueden administrar múltiples firewalls, pero sus usuarios están configurados en un solo bloque. Necesitan poder obtener un inicio de sesión único (SSO) de cualquier administrador de firewalls o consolas de administración de seguridad para administrar las políticas de los clientes. Al mismo tiempo, las reglamentaciones de cumplimiento suelen exigir que todas las funciones de administración se atengan al principio del menor privilegio, de modo que la administración unificada de clientes tenga suficiente control de acceso basado en funciones para el acceso privilegiado. Por ejemplo, esto puede limitarse a dos funciones: una que tenga acceso de lectura/escritura y otra que sea de sólo lectura.

También deben tener una instantánea global de la condición de sus tenants dentro de una visión global. Quieren ver la condición de cada tenant. Esto podría determinarse por la cantidad de infecciones, las vulnerabilidades presentes, la versión de seguridad de los endpoints instalada o también qué dispositivos están en línea y en funcionamiento. Además. podrían querer ver qué y quién está generando más alertas por el contenido de la web.

Amenazas que llegan a través de canales cifrados

Con más aplicaciones web aseguradas a través de canales cifrados como HTTPS, y el malware que también recurre al cifrado para eludir la inspección basada en la red, se ha vuelto imprescindible habilitar la inspección profunda de paquetes de tráfico SSL/TLS (DPI-SSL). Sin embargo, esto no es fácil de implementar sin la implementación masiva de certificados SSL/TLS de confianza en todos los endpoints para evitar la experiencia del usuario y los problemas de seguridad. Esto requiere un mecanismo subyacente para distribuir y administrar los certificados y la forma en que los navegadores confían en ellos.

Comprender las alertas y las medidas de corrección

Los usuarios finales suelen ser menos conscientes de los riesgos de seguridad que los profesionales de la seguridad y, por ello, necesitarían que su plataforma de protección de los endpoints les alerte sobre el cambiante perfil de riesgo cuando viajan con su laptop entre diferentes lugares, y les aconseje sobre cómo mantenerse seguros.

Por ejemplo, se podría generar una alerta a partir de un cliente unificado o de un software de terceros, o proporcionar una redirección a una fuente externa, como una página web.

Para remediar rápidamente cualquier problema de cumplimiento de la política de la empresa, puede ser beneficioso tanto para los usuarios finales como para la TI que los usuarios finales tengan acceso a información para ayudarse de forma autónoma. Si el dispositivo de un usuario no cumple la política y el usuario entra en cuarentena, los usuarios también necesitan orientación sobre las medidas necesarias para volver a cumplirla.

Administración de licencias

Los administradores deben asegurarse de que todo el software de seguridad de los endpoints adquirido se actualice automáticamente en su interfaz de administración, para poder mantener las licencias de los endpoints correctamente. Por ejemplo, toda la información de licencias relacionada con un cliente se debe supervisar y almacenar de forma centralizada. En caso de que se adquiera una nueva licencia, debe enviarse una señal a la administración unificada centralizada de clientes para alertar y comenzar la habilitación del software.

De forma periódica, algunos administradores deben ejecutar informes de cumplimiento de todas las licencias de terceros implementadas para pagar a sus partners.

Detener las amenazas avanzadas como el ransomware

Los enfoques tradicionales pueden a veces dejar vacíos en el cumplimiento de los requisitos administrativos. El enfoque basado en las firmas de las tecnologías antivirus tradicionales, que lleva mucho tiempo en vigor, ha fracasado frente al ritmo de desarrollo de nuevos malware y sus técnicas de evasión, lo que hace necesario un enfoque diferente en materia de protección de clientes. Esto no solo debe ofrecer motores avanzados de detección de amenazas, sino también apoyar una estrategia de defensa por capas en los endpoints, incluida la integración con un entorno aislado.

Una limitación importante de las soluciones existentes para points hoy en día (conocidas como clientes de AV ejecutados) es que el desarrollo es específico para un tercero determinado, y se ha incorporado a las ofertas de ese tercero. Los administradores necesitan un modelo más abierto, que permita una adición relativamente rápida de módulos de seguridad adicionales si el negocio o la industria lo demanda.

Conclusión

Debido al aumento del uso de los endpoints como vectores de ciberataques, los profesionales de la seguridad deben tomar medidas para proteger los dispositivos endpoint. Además, con la proliferación del teletrabajo, la movilidad y el traer su propio dispositivo (BYOD), hay una necesidad imperiosa de ofrecer protección sistemática para todos los clientes, en todas partes.

Los administradores de seguridad deben evaluar las soluciones de los endpoints teniendo en cuenta los requisitos del mundo real.

Obtenga más información. Lea nuestro informe de soluciones, "Fitting endpoint security to your organization" (Cómo adaptar la seguridad de los endpoints a su empresa) o visite www.sonicwall.com/capture-client.

Acerca de nosotros

SonicWall ofrece una ciberseguridad sin límites para la era de la hiperdistribución y una realidad laboral en la que todo el mundo es remoto, móvil y poco seguro. Al conocer lo desconocido, proporcionar visibilidad en tiempo real y permitir un gran avance económico, SonicWall cierra la brecha del negocio de la ciberseguridad para empresas, gobiernos y pequeñas y medianas empresas (SMB) de todo el mundo. Para obtener más información, visite www.sonicwall.com.

Si tiene alguna pregunta sobre el posible uso de este material, comuníquese con:

SonicWall Inc.
1033 McCarthy Boulevard
Milpitas, CA 95035 (Estados Unidos)

Encontrará más información en nuestro sitio web.
www.sonicwall.com