FORESCOUT

Visibilidad de dispositivos: la clave para reducir el riesgo y mejorar su nivel de seguridad

Seis formas de mejorar la seguridad con el 100 % de visibilidad de sus dispositivos

La protección de la infraestructura de la red es cada día más compleja. Esta complejidad se debe al crecimiento extraordinario de dispositivos IoT, la diversidad de plataformas, la adopción de la nube y la convergencia de IT y OT. La gran mayoría de los dispositivos nuevos que se incorporan a las redes no están diseñados para incluir agentes de administración, lo que genera una brecha importante de visibilidad y graves riesgos. Y esta brecha es aún mayor a medida que la computación en la nube llega al último rincón de la red distribuida.

Está claro: lo que no se ve, puede ser letal. Hace falta algún modo de detectar los dispositivos, tengan agentes o no, sean físicos o virtuales y estén donde estén. También es preciso contar con supervisión continua en tiempo real y con la capacidad de identificar y clasificar los dispositivos en el momento mismo en que se conectan a la red. Cerrar esta brecha de visibilidad es el modo más eficaz de lograr un efecto positivo en la seguridad de la red y las iniciativas de reducción de riesgos. Aquí le presentamos seis maneras de alcanzar precisamente ese objetivo con visibilidad absoluta:

1 Obtenga visibilidad sin agentes de todos sus sistemas, incluidos los dispositivos BYOD, IoT y OT

Lo que no se ve no se puede proteger. Por lo tanto, no hay vuelta de hoja: para que una solución sea viable, debe ofrecer en tiempo real una imagen precisa de todos los endpoints de la red.

Las soluciones de seguridad convencionales de control de acceso a la red (NAC) solo pueden detectar los dispositivos que están equipados con agentes. Pero no es posible cargar agentes en todos los dispositivos BYOD y no tradicionales que entran en la red: smartphones, tablets y wearables de los empleados, así como dispositivos IoT, OT y ordenadores portátiles de los contratistas, por no mencionar los dispositivos no autorizados de quién sabe dónde. Todos suponen un riesgo para su empresa.

Para evitarlo, necesita visibilidad sin agentes desde el instante en que cualquier dispositivo se conecta a su red. No basta con detectar una dirección IP o MAC: necesita información detallada de todos los dispositivos para determinar su finalidad, su propietario y su estado de seguridad.

2 Unifique la visibilidad y el control en todos los entornos, ya sea el centro de datos, el campus o la nube

No hace mucho, solo era necesario proteger el centro de datos pero, como bien sabe, el mundo se ha vuelto bastante más complejo. En muchos casos, los centros de datos únicos se han transformado en centros múltiples distribuidos en varios campus repartidos por todo el mundo. Y luego está la nube.

Ahora no basta con limitarse a controlar el perímetro, si es que actualmente existe tal cosa. Hace falta acceso instantáneo en tiempo real a todos los endpoints, ya estén en el centro de datos, en campus o en la nube. Ya no es factible intentar gestionar y proteger los dispositivos y las cargas de trabajo con herramientas e interfaces dispares y aisladas. **Una solución viable debe facilitar una imagen consolidada de los sistemas tradicionales, móviles e IoT, así como de las máquinas virtuales y las instancias en la nube, independientemente de dónde se encuentren**. Pero además, la solución empleada debe adaptarse más que nunca a las necesidades crecientes de la red.

Este nuevo paradigma, independiente de la tecnología y la ubicación, exige una nueva forma de concebir la interoperabilidad de soluciones (y menos tolerancia a depender de un solo proveedor). Hoy, el valor de la tecnología aumenta cuando los sistemas comparten visibilidad a través de paneles y mecanismos de control comunes. El nuevo paradigma exige flexibilidad para desplegar arquitecturas tanto centralizadas como distribuidas en función de las necesidades cambiantes de la empresa.

3 Satisfaga los requisitos de cumplimiento de las normas y de conformidad de los dispositivos

Rotundo suspenso: es lo habitual hoy en día cuando se efectúan pruebas de penetración o auditorías de cumplimiento normativo, y se debe a la falta de detección de dispositivos IoT y a la segmentación incorrecta de otras amenazas. Una estrategia de seguridad eficaz comienza por ofrecer una visibilidad continua de los dispositivos y disponer de inventarios de dispositivos completos. De lo contrario, la empresa corre graves riesgos legales y económicos.

Las imprecisiones en los datos de gestión de activos de IT (ITAM) a veces dan lugar al incumplimiento de normas tales como el RGPD, la HIPAA, PCI, FISMA y otras, incumplimiento que puede comportar fuertes multas para su empresa.

Sea cual sea la naturaleza de los activos que protege —económicos, médicos, industriales u "otros"—, el primer paso para gestionar bien los riesgos y el cumplimiento es contar con una visibilidad absoluta. Es imprescindible poder *ver, clasificar y después automatizar el control de los dispositivos y limitar el acceso* a las áreas de la red según el nivel de autorización, las directivas de seguridad corporativas y los requisitos de las normas.

Dado que muchas de las normativas vigentes, ya sean nacionales, federales o internacionales, exigen notificar las violaciones de la seguridad a las pocas horas del incidente, es fundamental que las plataformas de seguridad trabajen conjuntamente para reaccionar y resolverlas con rapidez y eficacia.

4 Automatice el inventario y la gestión de los dispositivos

Para gestionar y proteger con eficacia los activos de su empresa, necesita un inventario preciso que incluya todos los dispositivos de la red. Recuerde: basta con que falte un dispositivo en su inventario o que los datos de uno solo estén obsoletos o sean inexactos para que los ciberdelincuentes aprovechen la oportunidad y entren en su red. Puede ser difícil detectar dispositivos con métodos tradicionales. Según Gartner, "en 2020, el 30 % de los activos de las empresas serán indetectables sin detección activa".

Cuando la detección de recursos es manual, la base de datos de administración de configuración (CMDB) puede estar incompleta y ser inexacta, lo que neutraliza las iniciativas de administración de la seguridad. El seguimiento del inventario con hojas de cálculo Excel y otros métodos manuales produce errores y falta de vigencia en sus datos. Si el inventario de dispositivos está actualizado, la respuesta de los equipos de asistencia puede ser más ágil. Además, *para los equipos de operaciones de seguridad que tienen que responder a los ataques dirigidos a determinados sistemas operativos o dispositivos IoT es fundamental acceder de inmediato a datos exactos sobre todos los dispositivos.*

Y a menos que la empresa lleve un seguimiento preciso del software, corre el riesgo de sobreutilizar e incumplir los acuerdos de licencia e incurrir en cuantiosas multas.

Al automatizar el inventario y su gestión, puede compartir datos contextuales con herramientas ITAM como ServiceNow® para tener siempre la CMDB actualizada en tiempo real. Un inventario actualizado también le permite gestionar con eficacia el ciclo de vida de los dispositivos y le ayuda a presupuestar la inversión en activos.

5 Segmente la red teniendo en cuenta el contexto

Los profesionales de red y los expertos en seguridad suelen coincidir en que la segmentación de la red debe ser la máxima prioridad a la hora de proteger una red. La evaluación y la segmentación de dispositivos permite automatizar la asignación y la implementación de listas de control de acceso y VLAN de acuerdo con las directivas, así como asignar los dispositivos de forma dinámica a segmentos determinados para aplicar el control de acceso con eficacia y limitar el acceso a los recursos autorizados para esos segmentos. Es una estrategia efectiva para impedir que los empleados entren en zonas de la red que no les corresponden y limitar la propagación de un ataque de malware.

Cuando a la asignación de segmento se añade el contexto de los dispositivos en tiempo real, la seguridad mejora drásticamente de varias formas. Por ejemplo, si una solución ofrece esta posibilidad, puede comprobar el estado de cumplimiento de un dispositivo antes de asignarlo a un segmento. Además, puede supervisar continuamente su comportamiento y nivel de seguridad y reasignarlo rápidamente al segmento adecuado o a una VLAN restringida, según resulte necesario, si deja de estar conforme o autorizado (por ejemplo, si una impresora intenta acceder a una base de datos de RR. HH. o una cámara de vigilancia intenta acceder a cualquier otro dispositivo que no sea una videograbadora digital). *Este nuevo método de segmentación inteligente y dinámica también simplifica radicalmente las modificaciones de la red y admite más flexibilidad arquitectónica, ya que posibilita el intercambio de contextos y la coordinación con los firewalls de próxima generación.*

Para que su empresa alcance este nivel de segmentación, necesita una solución NAC que se integre fácilmente en conmutadores, redes privadas virtuales (VPN), sistemas de gestión basados en la nube y firewalls de próxima generación.

6 Reduzca su exposición con una respuesta coordinada ante incidentes

Como media, un equipo de seguridad de red maneja hasta 15 herramientas, lo que significa que las empresas invierten mucho dinero —y tiempo— en comprar, aprender y coordinar el uso de todas ellas. Además, la mayoría de las soluciones de seguridad funcionan perfectamente para enviar alertas, pero son incapaces de aplicar las medidas correspondientes. Como resultado, los equipos de seguridad se ven desbordados con el volumen de alertas que tienen que valorar y resolver manualmente.

Para agilizar la respuesta ante incidentes, las herramientas deben reaccionar a las alertas con un grado muy elevado de automatización, responder automáticamente a situaciones conocidas y, cuando surgen nuevas amenazas, facilitar a los analistas de seguridad información organizada por prioridades.

Para sacar el máximo partido de estas herramientas, se necesita una interoperabilidad instantánea entre los flujos de trabajo y también capacidad para realizar procesos automatizados de detección y clasificación. Además, las soluciones elegidas deben conectarse sin problemas a las herramientas de red existentes para coordinar el intercambio de datos en tiempo real, el envío de alertas y la respuesta con otras herramientas ITAM y de seguridad.

Todas las herramientas nuevas deben ser también compatibles con las redes de múltiples proveedores, ya contengan activos físicos o virtuales y estén en entornos en campus, centros de datos o la nube.

La solución de Forescout

La plataforma Device Visibility and Control de Forescout le ayuda a dar estos seis pasos y a mucho más. Detecta continuamente todos los dispositivos conectados por IP —sin necesidad de agentes— en el instante en que se conectan a la red. Ofrece una visibilidad profunda de esos dispositivos utilizando una combinación de técnicas activas y pasivas de detección, identificación de perfiles y clasificación. Y proporciona una escalabilidad líder del sector, ya que llega a admitir hasta dos millones de dispositivos en un solo appliance Forescout eyeManage.

Nuestro exclusivo enfoque sin agentes ofrece visibilidad de una amplia gama de dispositivos —gestionados y no gestionados, corporativos y personales, cableados e inalámbricos—, incluidos dispositivos BYOD propios, servidores, conmutadores, hardware no autorizado y dispositivos IoT.

Forescout ha elevado la visibilidad y el control de dispositivos a nuevas cotas para mitigar los riesgos, reducir la superficie de ataque y automatizar la respuesta a incidentes en toda la red de la empresa, ***su*** red.

Más información en ***Forescout.com***

Glosario de acrónimos

BYOD: bring your own device (trae tu propio dispositivo)

CMDB: configuration management database (base de datos de la gestión de configuración)

FISMA: Federal Information System Management Act (Acto de Estabilidad Financiera, Servicios Financieros y Unión de los Mercados de Capitales)

HIPAA: Health Insurance Portability and Accountability Act (La Ley de Transferencia y Responsabilidad de Seguro Médico)

IoT: Internet of Things (Internet de las Cosas)

IP: Internet Protocol (Protocolo de Internet)

IT: information technology (tecnologías de la información)

ITAM: information technology asset management (gestión de activos en las tecnologías de la información)

MAC: Media Access Control (control de acceso al medio)

NAC: network access control (control de acceso a la red)

OT: operational technology (Tecnologías Operacionales)

PCI: Payment Card Industry (Industria de tarjetas de pago)

RGPD: Reglamento General de Protección de Datos

VLAN: virtual local area network (red de área local virtual)

VPN: virtual private network (red privada virtual)

Forescout Technologies, Inc.
190 West Tasman Drive
San José, CA 95134 EE. UU.

C. e.: info-espana@forescout.com
Tel. (internacional) +1-408-213-3191
Asistencia técnica +1-708-237-6591