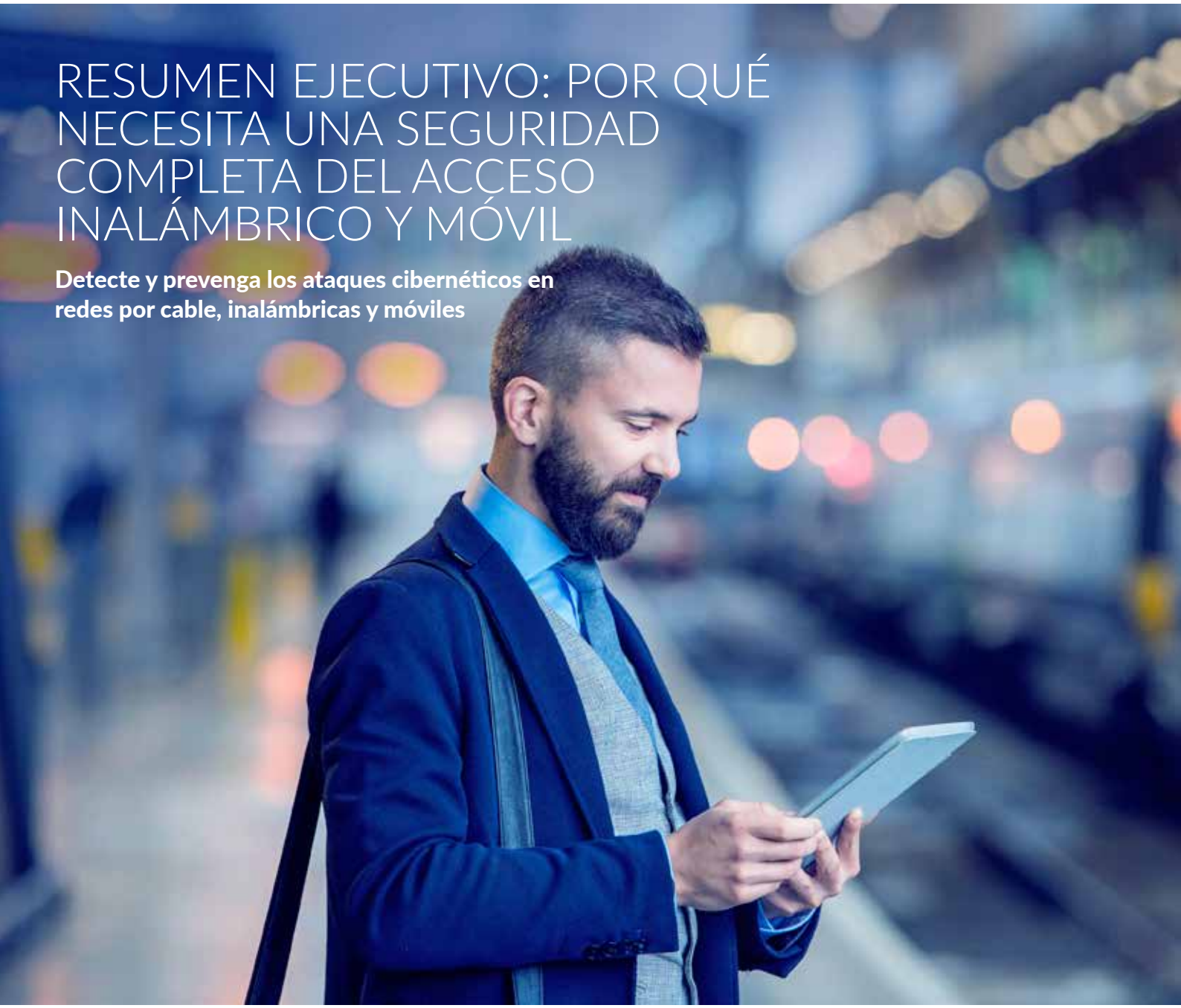
SONICWALL

RESUMEN EJECUTIVO: POR QUÉ NECESITA UNA SEGURIDAD COMPLETA DEL ACCESO INALÁMBRICO Y MÓVIL

Detecte y prevenga los ataques cibernéticos en redes por cable, inalámbricas y móviles



Resumen

Hoy en día, las organizaciones necesitan proporcionar a los trabajadores acceso de alta velocidad a los recursos, ya sea en redes por cable, inalámbricas o móviles.
El problema es que los cibercriminales están aprovechando todos estos vectores para perpetrar ataques avanzados, con amenazas cifradas y ataques de día cero. Además, las organizaciones pueden perder el control sobre los datos en entornos con equipos remotos que utilizan redes inalámbricas y móviles y se conectan a servicios en la nube. Las interrupciones del acceso provocan pérdidas de productividad, fomentan la informática en la sombra y crean lagunas en la seguridad de las organizaciones.

Acceso a los recursos desde cualquier lugar

Hoy en día, los trabajadores se desplazan constantemente. Necesitan acceso las 24 horas a los recursos corporativos desde cualquier lugar y utilizando el dispositivo que deseen. Por otra parte, las organizaciones están adoptando iniciativas basadas en políticas BYOD, el IoT, la movilidad y la nube. Para mantener un alto nivel de competitividad, las organizaciones deben proporcionar un acceso fluido a los recursos en redes por cable, inalámbricas y móviles. Las redes por cable están evolucionando a 2,5G, 5G y 10G. Pero no solo se conectan a las redes dispositivos por cable. Los puntos terminales varían desde equipos de escritorio hasta portátiles, tablets y teléfonos inteligentes. Asimismo, debido al creciente número de puntos terminales BYOD y del Internet de

> Las organizaciones no solo han de proporcionar acceso en cualquier momento y desde cualquier lugar y dispositivo, sino que además dicho acceso debe ser rápido y seguro.

las cosas (IoT), actualmente se conectan a la red corporativa más dispositivos que nunca.

Cada vez es más frecuente que las organizaciones utilicen conectividad inalámbrica de alta velocidad en sus entornos. Los trabajadores móviles y remotos, por su parte, se conectan a través de VPNs desde sus casas, sucursales, oficinas de trabajo compartido, aeropuertos, hoteles o cafés. Como resultado, ahora los empleados esperan la misma experiencia de usuario y el mismo acceso de alto rendimiento en las conexiones inalámbricas y móviles que en las redes por cable. Cuando los empleados están de viaje, necesitan acceder a las mismas aplicaciones de negocio que cuando están conectados a redes por cable en la oficina.

Los ataques cibernéticos utilizan redes por cable, inalámbricas y móviles

Al igual que el acceso y la conectividad de alta velocidad desde cualquier lugar es importante tanto para los usuarios como para las organizaciones, también lo es la seguridad de los datos que viajan por la red. Al fin y al cabo, las organizaciones necesitan ampliar las funciones completas de detección y prevención de brechas de seguridad de forma fluida a todas sus redes por cable, inalámbricas y móviles.

En cualquier plataforma de red, un reto muy importante a la hora de combatir los ataques cibernéticos es que hoy en día la mayoría de las amenazas están cifradas. La tendencia hacia el cifrado TLS/SSL lleva varios años en aumento. A medida que ha crecido el tráfico Web, también lo ha hecho el cifrado: de 5,3 billones de conexiones Web en 2015 a 7,3 billones en 2016, según la red Capture Threat Network de SonicWall. La mayoría de las sesiones Web detectadas por la red Capture Threat Network de SonicWall en todo el año estaban cifradas mediante TLS/SSL, representando este tipo de datos el 62% del tráfico Web. Esta cifra continuará aumentando, dado que cada vez más páginas Web recurren al cifrado para proteger las conexiones entrantes.

Además, las amenazas avanzadas, como los exploits de día cero y el malware personalizado, van en aumento. Las organizaciones de todos los tamaños están en el punto de mira de los cibercriminales, quienes buscan, encuentran y explotan constantemente vulnerabilidades de software. Su objetivo es acceder a las redes, a los sistemas y a los datos, a menudo causando daños graves en cuestión de minutos. Para poder detectar estas amenazas desconocidas con mayor eficacia, los profesionales de seguridad están implementando tecnologías de detección de amenazas avanzadas, como sandboxes virtuales, que analizan el comportamiento de los archivos sospechosos y descubren amenazas de malware ocultas. El problema es que las amenazas se están volviendo cada vez más inteligentes. Actualmente, el malware se está diseñando para detectar la presencia de sandboxes virtuales y evadirlos. Los entornos de sandbox de hoy en día deben ser tan completos y dinámicos como las amenazas que pretenden prevenir. En la actualidad, resulta imprescindible poder descifrar y escanear todo el tráfico y aislar los archivos sospechosos en sandboxes ya sea en redes por cable, inalámbricas o móviles.

Colaboración en grupo remota

Además, las organizaciones pueden perder el control sobre los datos en entornos con equipos remotos que utilizan redes inalámbricas y móviles y se conectan a servicios en la nube. Muchas organizaciones tienen equipos remotos que necesitan utilizar herramientas de colaboración, como SharePoint o Dropbox, para compartir archivos y trabajar de forma colectiva. En la colaboración en proyectos también suelen verse involucrados interesados externos, como contratistas o partners. Por ejemplo, tanto las instituciones de educación básica como las de educación superior proporcionan a los alumnos y al profesorado acceso inalámbrico a Internet para conectarse y colaborar con otros usuarios de forma local y en todo el mundo.

Como resultado, se cargan o comparten archivos constantemente utilizando portátiles y teléfonos inteligentes personales (no gestionados) a través de redes móviles e inalámbricas. Siempre que se ofrezca la posibilidad de compartir archivos, existe el riesgo de que se cargue malware. Sin embargo, cuando los departamentos de TI toman medidas drásticas e implementan políticas de uso compartido de archivos restrictivas por motivos de seguridad, los usuarios finales tienden a utilizar cuentas personales de uso compartido de archivos, como Google Drive, para transferir archivos y colaborar. Estos archivos eluden los firewalls de la red cuando los usuarios remotos acceden a la red corporativa utilizando acceso VPN. Además, las organizaciones pierden el control de los datos cuando éstos abandonan el perímetro de seguridad mediante servicios de nube públicos, como Google Drive, correo electrónico o USB. Para las organizaciones, esto supone un elevado riesgo de seguridad y de cumplimiento normativo.

Rendimiento de la red y productividad del personal

No solo debe proporcionarse acceso en cualquier momento y desde cualquier lugar y dispositivo, sino que además dicho acceso debe ser rápido y seguro. La tecnología de seguridad requerida para ofrecer protección contra las amenazas cibernéticas modernas puede tener consecuencias negativas para las organizaciones, como la reducción de la productividad del personal, el incremento de los gastos de TI y, en definitiva, el aumento del coste total de propiedad.

El creciente volumen de tráfico por sí solo afecta al ancho de banda disponible y al rendimiento de la red. El número de dispositivos con tecnología Wi-Fi, tanto personales como gestionados por el departamento de TI, continúa creciendo a medida que el uso y la importancia de la movilidad van en aumento. Según Gartner, en 2016 se vendieron casi 1.500 millones de teléfonos inteligentes.[1] Al final de ese mismo año, la Wi-Fi Alliance esperaba que las ventas de productos Wi-Fi sobrepasaran los 15.000 millones de unidades.[2] Además, con el aumento de dispositivos Wi-Fi, también crece el uso de aplicaciones con gran consumo de ancho de banda, como las aplicaciones multimedia HD y las aplicaciones móviles y en la nube.

El crecimiento del IoT ha provocado un aumento del número de dispositivos inalámbricos que pueden ejecutar aplicaciones con gran consumo de ancho de banda. El uso de aplicaciones de vídeo y de colaboración, como Microsoft Lync, SharePoint y WebEx, requiere la disponibilidad de un gran volumen de ancho de banda para poder disfrutar de un rendimiento óptimo. Además, la computación en la nube puede implicar la transferencia de archivos de datos de gran tamaño por la red inalámbrica, que se traduce en el consumo de ancho de banda valioso.

Asimismo, el incremento de la cantidad de dispositivos ha creado un entorno en el que las señales inalámbricas a menudo interfieren entre ellas debido al elevado número de dispositivos que comparten la misma red. Entre estos dispositivos se incluyen desde portátiles, teléfonos inteligentes, tablets y puntos de acceso hasta dispositivos de microondas, Bluetooth, etc. El consecuente bajo rendimiento se percibe en diversos sectores, como la Sanidad, la Educación, aeropuertos y centros comerciales. Otro servicio que los usuarios ya dan por supuesto es la conectividad inalámbrica en estadios, campus, obras, parques industriales y otros lugares al aire libre, donde la señal puede verse afectada por el entorno físico, como p.ej. por árboles y otros edificios.

Los propios servicios de seguridad también afectan al rendimiento de la red. La capacidad de descifrar y escanear el tráfico cifrado en busca de amenazas con poca o ninguna latencia es vital, puesto que cualquier retraso ralentiza la circulación de los datos a través de la red. El descifrado y escaneado de posiblemente miles de conexiones Web cifradas en busca de amenazas de forma simultánea puede suponer un elevado consumo de recursos informáticos. Los firewalls antiguos posiblemente sean capaces de descifrar el tráfico y proporcionar algún tipo de funciones de detección, pero no de prevención. Incluso es posible que ofrezcan todas las funciones necesarias – aunque a una velocidad muy reducida, debido a su bajo rendimiento. Algunas organizaciones incluso desactivan sus servicios de firewall clave con el fin de mantener el nivel de rendimiento.

Todo esto está provocando que las organizaciones tengan que proporcionar a sus clientes, empleados y alumnos una experiencia mejorada en todas sus plataformas. La última tecnología inalámbrica de alta velocidad, 802.11ac Wave 2, ofrece un rendimiento inalámbrico multi-gigabit. No obstante, para poder disfrutar de este rendimiento, tanto los puntos de acceso como los dispositivos que se conectan deben soportar el estándar inalámbrico 802.11ac Wave 2. Además, para permitir el nivel requerido de rendimiento inalámbrico, la mayoría de los firewalls deben utilizar un puerto con retrocompatibilidad para 5 GbE o 10 GbE, lo cual supone una capacidad muy superior a la requerida, o bien añadir un switch, con el consecuente incremento de los costes.

Para mayor complicación del rendimiento y de la seguridad, la mayoría de las organizaciones crean un entorno de TI híbrido mezclando aplicaciones locales y en la nube. Los departamentos de TI deben mantener múltiples directorios de usuarios para las aplicaciones implementadas en sus centros de datos locales o en las aplicaciones SaaS en la nube de terceros. Estos directorios deben actualizarse constantemente para asegurarse de que las personas adecuadas tengan el acceso apropiado a las aplicaciones correctas en el momento oportuno. Los usuarios deben mantener y recordar múltiples URLs y contraseñas, lo cual induce a malas prácticas de seguridad. Cualquier interrupción del acceso provoca pérdidas de productividad, fomenta la informática en la sombra y crea lagunas en la seguridad de las organizaciones.

Conclusión

Obtenga más información. Descubra cómo proporcionar funciones de detección y prevención de brechas en sus redes por cable, inalámbricas y móviles. Lea nuestro Resumen de la solución, Best practices for wireless and mobile access security (Mejores prácticas para la seguridad del acceso inalámbrico y móvil), y visite nuestra página Web Wireless and Mobility (Tecnología inalámbrica y movilidad).

[1] *http://www.gartner.com/newsroom/id/3609817*
[2] *http://www.wi-fi.org/news-events/newsroom/wi-fi-device-shipments-to-surpass-15-billion-by-end-of-2016*

Acerca de nosotros

Durante sus 25 años de historia, SonicWall ha sido el partner de seguridad de confianza del sector. Desde la seguridad de red, pasando por la seguridad de acceso, hasta la seguridad del correo electrónico, SonicWall ha desarrollado continuamente su cartera de productos para ayudar a las organizaciones a innovar, a acelerar y a crecer. Con más de un millón de dispositivos de seguridad en casi 200 países y territorios en todo el mundo, SonicWall permite a sus clientes decir "Sí" al futuro con confianza.

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

SonicWall Inc.
5455 Great America Parkway
Santa Clara, CA 95054

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

ExecBrief-NS-WhyYouNeed-US-IMAG-29144

SONICWALL®