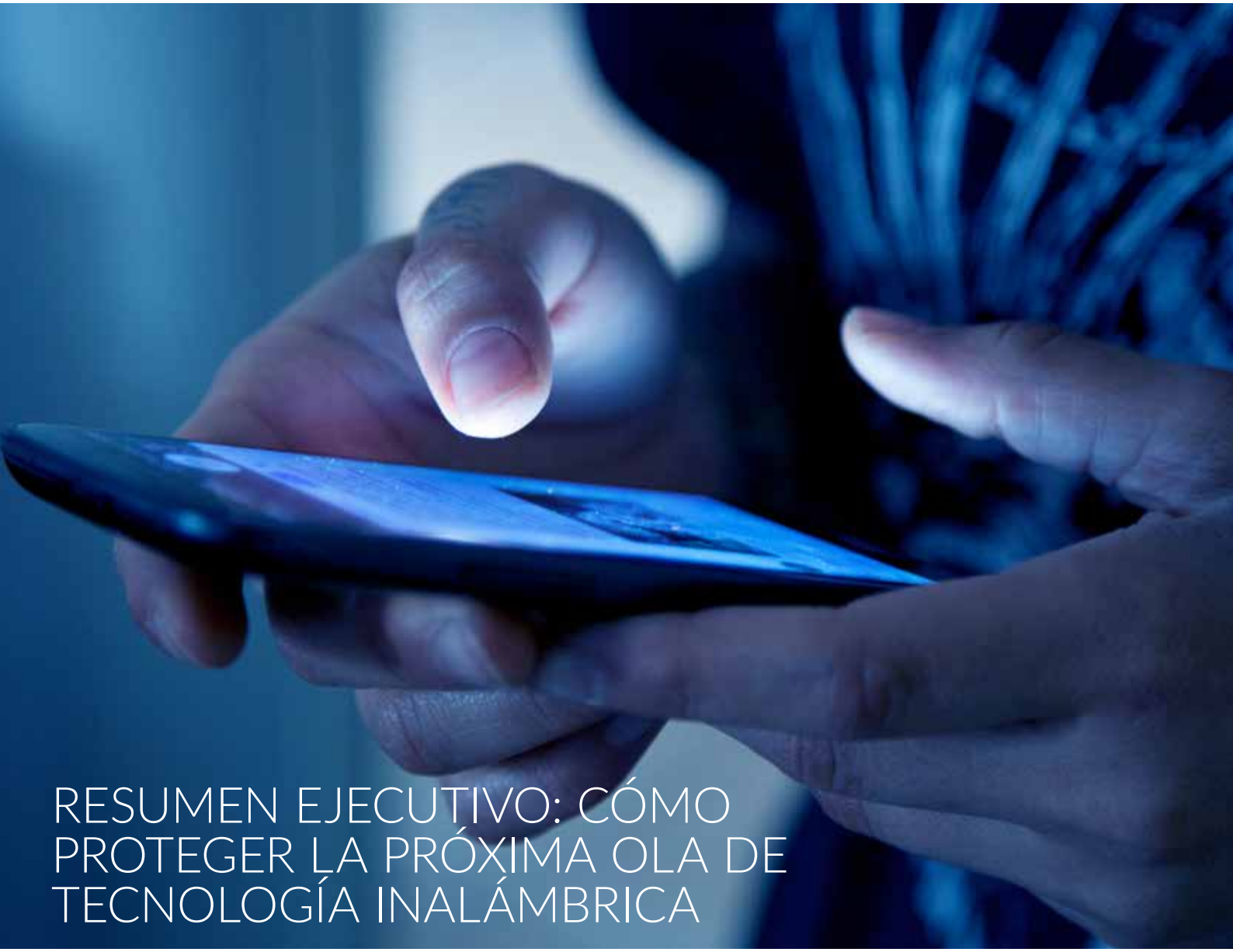
SONICWALL



# RESUMEN EJECUTIVO: CÓMO PROTEGER LA PRÓXIMA OLA DE TECNOLOGÍA INALÁMBRICA

## Resumen

En la economía móvil y global de hoy en día, la conectividad inalámbrica está en todas partes. Los dispositivos inalámbricos abarcan desde teléfonos inteligentes y ordenadores portátiles hasta cámaras de seguridad y auriculares de realidad virtual. Las empresas deben reconocer su necesidad de alta calidad, rendimiento y seguridad en sus redes inalámbricas y puntos terminales y actuar en consecuencia.

## La empresa actual se halla en un mundo inalámbrico

En el panorama actual de las redes, la conectividad inalámbrica de alta velocidad ya no es opcional. Se ha convertido en una necesidad, mientras las empresas intentan aumentar la rentabilidad para los clientes y mejorar la productividad de los empleados mediante iniciativas BYOD y el creciente uso de aplicaciones con un elevado consumo de ancho de banda. Otras organizaciones, como escuelas y universidades, utilizan tecnología inalámbrica para proporcionar a los alumnos un entorno educativo más conectado. Los usuarios, por su parte, esperan conectividad inalámbrica desde cualquier lugar o tipo de dispositivo. Es más, existe una creciente tendencia hacia el uso de dispositivos "exclusivamente inalámbricos" en el lugar de trabajo, en clase, en hospitales y en la vida diaria.

## IoT inalámbrico

Todo esto viene impulsado por diversos factores clave. En primer lugar, la proliferación continuada de los dispositivos con tecnología Wi-Fi, tanto personales como gestionados por el departamento de TI. Según ABI Research, se espera que se vendan más de 20.000 millones de conjuntos de chips Wi-Fi entre 2016 y 2021. Además, más del 95% de los dispositivos vendidos en 2021 soportarán 5GHz. En segundo lugar, también se ha extendido el Internet de las cosas (IoT). Muchos dispositivos que hasta el momento no eran conocidos por incluir funcionalidad inalámbrica, como coches, dispositivos de domótica (p.ej. neveras, cámaras de seguridad...) etc., ahora pueden conectarse a Internet mediante tecnología inalámbrica. Múltiples empresas analistas han pronosticado que en 2020 habrá 50.000 millones de dispositivos de IoT.

En tercer lugar, y en combinación con el aumento de los dispositivos con tecnología Wi-Fi, está el uso de aplicaciones con un elevado consumo de ancho de banda, como aplicaciones multimedia HD, de nube y móviles, que cada vez con más frecuencia se hospedan en la red. Y finalmente, el último estándar inalámbrico, 802.11ac Wave 2, se ha generalizado mientras los usuarios tratan de beneficiarse de la promesa de las velocidades inalámbricas multigigabit. Esta combinación obliga a las organizaciones a proporcionar a los clientes, empleados y alumnos una solución inalámbrica de alta velocidad que mejore considerablemente la experiencia de usuario.

## El hogar como parte de la empresa

Según Wi-Fi Alliance, el hogar se está convirtiendo en una red empresarial. Esto se debe principalmente a la gran cantidad de equipos y cosas cotidianas conectadas, los asistentes personales y los equipos de realidad virtual inalámbricos. Además, el impacto de la conectividad Wi-Fi puede apreciarse en las vidas diarias no solo de los usuarios, sino también de empresas como Amazon, Facebook, Netflix y las principales compañías aéreas. Dependen del Wi-Fi para realizar sus operaciones cotidianas, como el envío el mismo día, el acceso móvil a los medios sociales, servicios de medios streaming e incluso para la salida puntual de vuelos en el caso de las compañías aéreas. La introducción de nuevos estándares y protocolos obliga a la tecnología Wi-Fi a evolucionar y mejorar.

## Cómo asegurar la calidad del servicio de la conectividad inalámbrica

Mientras que la velocidad siempre es importante en cualquier entorno de red, en entornos de alta densidad, incluidas las ubicaciones exteriores, donde las condiciones pueden ser adversas, también lo es la calidad de la conexión inalámbrica. En muchos casos, múltiples dispositivos se conectan al mismo punto de acceso y compiten por el ancho de banda. Esta "congestión de dispositivos" provoca una interferencia que puede desembocar en una degradación de la señal y consecuentemente en un rendimiento pobre. Otros factores, como objetos físicos (p.ej. edificios, paredes, árboles) y otros dispositivos que comparten la misma frecuencia o el mismo canal (p.ej. microondas, teléfonos inalámbricos), pueden interferir con la señal inalámbrica al obstruir la ruta de transmisión de la radiofrecuencia. Todos ellos pueden tener un impacto sobre aplicaciones como el streaming de vídeo, que puede sufrir cuando los paquetes se retrasan y la calidad de la imagen es pobre o el vídeo se ralentiza como consecuencia del almacenamiento en búfer.

## Una amenaza creciente para la seguridad

Detrás de todo esto se encuentra la necesidad de proteger el tráfico inalámbrico contra las amenazas maliciosas y las vulnerabilidades de Internet. Actualmente, muchos productos para redes inalámbricas ofrecen protección contra actividades como los puntos de acceso no autorizados o el mapeo de puntos de acceso, para impedir que accedan intrusos a la red y por tanto a los recursos críticos. No obstante, a menudo no ofrecen la capacidad de escanear el tráfico cifrado de la LAN inalámbrica mediante inspección profunda de paquetes, poniendo en peligro a las organizaciones. Estos productos también carecen de prestaciones de seguridad adicionales, como la detección de puntos terminales no autorizados y la capacidad de segmentar el acceso de usuarios externos e internos. Además de los riesgos de seguridad, la implementación, monitorización y gestión de los productos pueden llevar mucho tiempo. Asimismo, es posible que carezcan de prestaciones de soporte para la autoconfiguración y la gestión centralizada, especialmente vitales a la hora de crear y mantener una infraestructura de red inalámbrica de gran tamaño.

## Conclusiones

Hoy en día, lo que las organizaciones necesitan de su red inalámbrica va más allá de una mayor velocidad de conectividad. Necesitan una solución que les proporcione un mayor nivel de rendimiento, una mejor calidad de señal y una experiencia de usuario mejorada desde una amplia variedad de clientes inalámbricos en entornos de alta densidad. Pero eso no es todo. También debe ofrecer funciones de escaneado que permitan detectar las amenazas en el tráfico inalámbrico, ya sea cifrado o no, y eliminarlas, con el fin de proteger la red, y al mismo tiempo simplificar la implementación y la gestión continuada.

**Obtenga más información.** Visite www.sonicwall.com/en-us/products/firewalls/wireless-security.

### Acerca de nosotros

SonicWall lleva más de 25 años combatiendo la industria del crimen cibernético, defendiendo a las empresas pequeñas, medianas y grandes de todo el mundo. Nuestra combinación de productos y partners nos ha permitido crear una solución de defensa cibernética en tiempo real adaptada a las necesidades específicas de más de 500.000 negocios en más de 150 países, para que usted pueda centrarse por completo en su negocio sin tener que preocuparse por las amenazas.

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**