Las 6 Categorías de Amenazas Conocidas de Wi-Fi que Apuntan a su Empresa y Cómo Defenderse de Ellas

WatchGuard

Índice

El Crecimiento del Wi-Fi

El acceso a Wi-Fi se ha convertido en una forma de vida. Desde los dispositivos móviles y las computadoras portátiles hasta los sistemas de videojuegos y los electrodomésticos, casi todo requiere de una conexión inalámbrica para funcionar. De hecho, según Gartner, se espera que el número de dispositivos conectados supere los 20.400 millones para el 2020.

También hemos observado un enorme crecimiento en la cantidad de personas que utilizan teléfonos inteligentes, que aumentó en forma abrupta de un 35% en 2011 a un 77% en 2018[1]. Como sus clientes y empleados usan sus teléfonos inteligentes y otros dispositivos inalámbricos mientras circulan, es necesario proporcionarles un acceso a Wi-Fi robusto. ¿Qué sucede entonces con los riesgos de seguridad inherentes asociados con el Wi-Fi? ¿Ha pensado en las amenazas que acechan a su alrededor en cada esquina esperando a que alguien se conecte para poder robarle su información?

Analicemos algunos de los ataques más grandes a redes inalámbricas que han afectado a empresas como la suya en los últimos años.

Según Gartner, está previsto que el número de **dispositivos conectados supere los 20.400 millones** para el **2020**.

1. https://www.securedgenetworks.com/blog/wi-fi-planning-preparing-for-growth-in-a-mobile-first-world

Hacks famosos de Wi-Fi

En julio de 2005, **TJ Maxx** sufrió una violación de seguridad como consecuencia de una red inalámbrica insegura. El hacker se ubicó fuera de la tienda de St. Paul, Minnesota, con una computadora portátil y una antena con forma de telescopio, y descargó al menos 45,7 millones de números de tarjetas de crédito y débito, aunque es muy probable que haya tenido acceso a unos 200 millones de números de tarjetas en total.[2]

En un informe de CNBC de diciembre de 2017, **Starbucks** había tomado las medidas necesarias para impedir que las computadoras portátiles de los clientes se utilizaran para generar criptomonedas. La conexión de Wi-Fi de una de sus sucursales en Buenos Aires había sido atacada y modificada con un código inusual. Una vez que el usuario se conectaba, el proveedor de conexión de Wi-Fi podía utilizar la potencia de procesamiento del cliente para extraer bitcoins[3].

En marzo de 2018, varias autoridades municipales de Atlanta sufrieron un ataque de ransomware SamSam que cifraba archivos en sus dispositivos. Para evitar que el ransomware se diseminara a sus conexiones de Wi-Fi, el Aeropuerto Internacional Hartsfield-Jackson se vio obligado a cerrar el acceso a sus servicios de Wi-Fi. La rápida decisión del equipo de seguridad de Atlanta posiblemente permitió que sus pasajeros no fueran infectados[4].

¿Entonces cuáles son las amenazas que podrían atacar a su empresa y debe tener en cuenta?

2. https://www.zdnet.com/article/tjxs-failure-to-secure-wi-fi-could-cost-1b/

3. https://www.cnbc.com/2017/12/12/starbucks-customer-laptops-hacked-to-mine-cryptocurrency.html

4. https://www.secplicity.org/2018/03/23/the-worlds-busiest-airport-shuts-off-wi-fi-amid-a-ransomware-attack/

Las 6 Categorías de Amenazas Conocidas de Wi-Fi que Apuntan a su Empresa

A pesar de que la lista de posibles amenazas de Wi-Fi podría ser interminable, existen 6 categorías de amenazas conocidas de Wi-Fi contra las cuales debe proteger a su empresa. En la siguiente sección, trataremos cada una de estas categorías, cómo son, cómo funcionan y un ejemplo de la vida real que podría estar ocurriendo en su empresa ahora mismo.

Punto de Acceso "Gemelo Malvado"

QUÉ

Un PA "gemelo malvado" imita a un PA legítimo, a través de la falsificación de sus SSID y de su dirección de MAC única. Los atacantes pueden así interceptar el tráfico e insertarse en el intercambio de datos entre la víctima y los servidores a los que accede la víctima mientras está conectada al punto de acceso "gemelo malvado".

CÓMO

Una vez que la víctima está conectada, el atacante puede robar sus credenciales, insertar código malicioso en sus exploradores, redirigirla a un sitio de malware y mucho más.

EJEMPLO

En su hora de almuerzo usted decide que finalmente llegó el momento de actualizar el guardarropa. No hay nada de malo en eso. Sin embargo, un hacker está utilizando un punto de acceso "gemelo malvado" y usted sin sospecharlo, se encuentra ahora conectado a la copia que el hacker ha hecho de su SSID de Wi-Fi. En el momento en que efectúa la compra e introduce la información de su tarjeta de crédito para encargar su nuevo vestido, el hacker obtiene su información y está listo para venderla en la dark web.

Punto de Acceso Mal Configurado

QUÉ

En redes con mucho tráfico en las que se están implementando los nuevos PA, es fácil que los administradores de redes accidentalmente cometan un error de configuración, como dejar que un SSID privado quede abierto y sin cifrado, y aumente la posibilidad de exponer la información confidencial para que sea interceptada en el aire.

CÓMO

Esto puede suceder cada vez que un punto de acceso no se configure de manera apropiada (como por ejemplo, al dejar la configuración predeterminada sin cambios).

EJEMPLO

La empresa envía a su nueva oficina un punto de acceso, y Charles, el recepcionista, se ofrece a configurarlo. Charles sigue las instrucciones e instala el punto de acceso que ahora emite un SSID abierto, lo cual genera una gran filtración de datos privados. No es su culpa, ya que no es un profesional de TI, pero aun así, queda un punto de acceso configurado erróneamente que podría ser un riesgo grave para su empresa.

Punto de Acceso No Autorizado

QUÉ

Un PA no autorizado es un PA inalámbrico que se ha instalado en una red segura sin autorización explícita de un administrador.

CÓMO

Los PA no autorizados se conectan a la red autorizada, por lo general con un SSID abierto, que permite a los atacantes eludir la seguridad perimetral. Esto podría suceder con un PA físico o con uno creado en el software de una computadora que logra acceder a una red autorizada.

EJEMPLO

Usted es propietario de una tienda minorista en la que entran y salen clientes todo el día. Cuando la tienda está concurrida, es imposible estar atento a todas las personas cada segundo del día. No sería raro que alguien se metiera de pronto en el armario de cables, conectara el PA más económico que pudiera conseguir y obtuviera así acceso a la red segura y privada de la empresa. Así podría apropiarse de sistemas de punto de ventas para divulgar números de tarjetas de crédito y mucho más.

Cliente No Autorizado

QUÉ

Se considera cliente no autorizado a cualquier cliente previamente conectado a un PA no autorizado o a otro PA malicioso dentro del rango de una red privada.

CÓMO

Por lo general, se clasifica a un cliente como no autorizado si se ha conectado a cualquier PA no autorizado, PA "gemelo malvado" u otro PA malicioso mientras se está dentro del rango de una red WLAN privada. Este cliente podría haber sido víctima de una gran variedad de ataques de tipo "man-in-the-middle" (MitM), incluida la carga de ransomworms, malware o puertas traseras en el cliente.

EJEMPLO

Usted se detiene en la misma tienda de café en su camino al trabajo todos los días. Como se ha conectado a esa red Wi-Fi con anterioridad, su teléfono se conecta de forma automática apenas pone un pie allí. Lamentablemente, ese día, alguien había configurado un PA "gemelo malvado", engañó a su teléfono y lo infectó con ransomware mientras estaba dentro del rango de su red local inalámbrica (WLAN) privada y consiguió así que regresara a su oficina infectado. Tan pronto como vuelve a su escritorio, su teléfono se conecta a la red de Wi-Fi corporativa y el ransomware comienza a diseminarse rápidamente.

Punto de Acceso Vecino

QUÉ

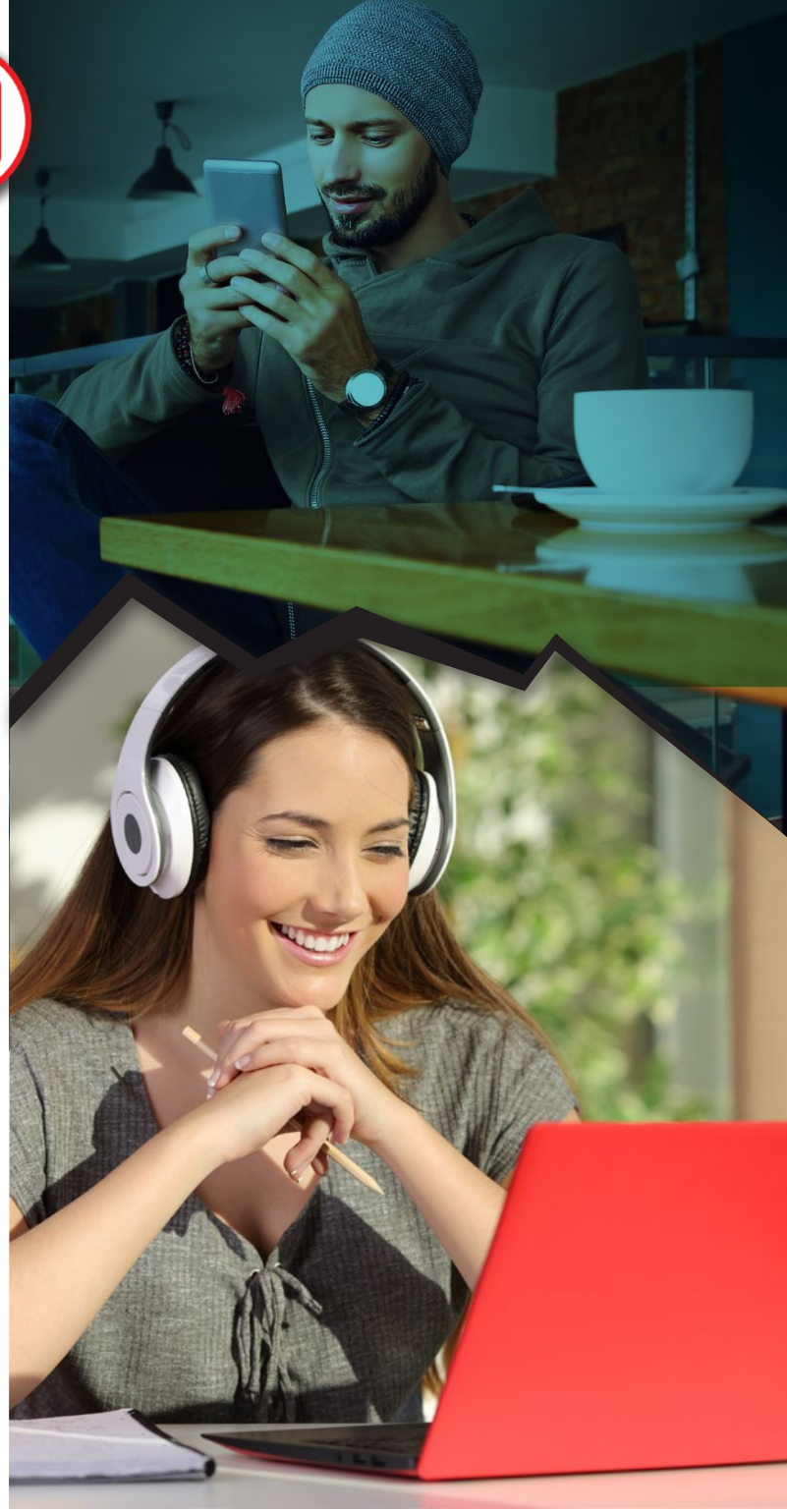
Cuando un cliente autorizado se conecta a un PA vecino, invitado o externo, elude la seguridad perimetral de la empresa y evita las restricciones de seguridad establecidas por el firewall.

CÓMO

No existe un truco súper secreto del hacker para esto. Cualquiera de sus empleados podría estar (y probablemente esté) haciendo esto ahora mismo. Al elegir conectar sus dispositivos a la red para invitados o la red de la tienda de café que está en el piso de abajo, sus empleados están eludiendo de manera sencilla la seguridad que usted ha creado para su red.

EJEMPLO

Janice del departamento de Marketing no puede pasar ni una sola mañana sin escuchar su nueva banda sonora favorita. Su teléfono ya casi no tiene batería, de modo que quiere usar la computadora que le proporciona la empresa para conectarse al sitio de transmisión. El firewall de su empresa restringe el acceso para la transmisión de música, pero eso no tiene a Janice preocupada. Ella piensa simplemente conectarse a la red de Wi-Fi insegura de la tienda de café que está en el piso de abajo y escuchar lo que desea. Lo que le juega en contra a su empresa es que un hacker está tomando su primera taza de café, esperando el momento justo en que ella se conecte para ponerse a trabajar con el objetivo de acceder a su red.



Red Ad-Hoc

QUÉ

Una conexión de Wi-Fi de punto a punto entre clientes que permite la comunicación entre dos o más dispositivos en forma directa, que elude sus políticas de seguridad de red y logra que el tráfico sea completamente invisible.

CÓMO

Con unos pocos cambios en la configuración, cualquiera de sus empleados podría rápidamente crear una red ad-hoc entre los dispositivos de sus colegas. Esto puede generar consecuencias legales y de seguridad que podrían afectar en última instancia a su empresa.

EJEMPLO

Minutos antes de empezar una reunión, el jefe de Carl sigue esperando un archivo que él le prometió entregar esta mañana. Le llevaría demasiado tiempo utilizar el uso compartido de archivos a través de la red segura aprobada por la empresa, de modo que decide configurar una red ad-hoc para enviarlo en forma directa de una computadora portátil a otra. Lamentablemente, esto abre la puerta a posibles consecuencias legales y de seguridad para su empresa.

Cómo Defenderse de las Amenazas de Wi-Fi con un Entorno Inalámbrico de Confianza

En un mundo con un número mayor de redes Wi-Fi abiertas, los hackers de Wi-Fi no solo pueden robar información, sino que también pueden propagar malware a las computadoras de la red, lo que podría implicar un costo millonario para sus empresas. Necesita un framework que le permita proporcionar alto rendimiento y, a su vez, acceso a Wi-Fi seguro para sus clientes y empleados.

Un framework de **Entorno Inalámbrico de Confianza** que se concentra en los tres principales pilares para permitir el rendimiento robusto que desea con la seguridad que necesita. Estos pilares son:

1. **Rendimiento Líder en el Mercado**
2. **Administración Escalable**
3. **Seguridad Completa Verificada**

Analicemos en mayor detalle cada uno de estos pilares y lo que significan para su empresa.

Rendimiento Líder en el Mercado 1

Nunca debe sentirse forzado a poner en riesgo la seguridad para lograr los niveles de rendimiento necesarios que le proporcionen a su entorno de Wi-Fi la velocidad, las conexiones y la densidad de clientes que necesita. Como hemos visto, un rendimiento lento de la red de Wi-Fi corporativa puede ser una excusa cómoda para que un empleado desvíe su conexión a una fuente de Wi-Fi menos segura, pero más rápida.

Una red inalámbrica de alto rendimiento no solamente garantiza la conexión de los empleados a redes seguras, sino que además les permite trabajar con un nivel máximo de eficiencia. Los momentos sin conectividad mientras esperan que algo se cargue es una oportunidad que provocará una distracción, los llevará a consultar datos en sus teléfonos o a aprovechar ese momento para dar una vuelta por la oficina.

Y en función de lo que su empresa decida, ofrecer una red de Wi-Fi de alto rendimiento podría ser la diferencia entre un gran experiencia del cliente y una mala reseña en Yelp. Para organizaciones como restaurantes, hoteles e incluso consultorios médicos, los clientes que tienen en mente invertir una cantidad significativa de tiempo (y a menudo dinero) deben saber que pueden contar con que no habrá ninguna dificultad con el rendimiento de Wi-Fi. Una conexión lenta o irregular podría ser el factor que los impulse a salir en busca de un competidor, sin importar cuánto les guste su producto.

Una red inalámbrica de alto rendimiento no solamente garantiza la **conexión** de los empleados **a redes seguras**, sino que además les permite **trabajar con un nivel máximo de eficiencia**.

¿Por Qué WatchGuard? 1

Poder confiar en el rendimiento de su conexión inalámbrica no debería ser algo que le quite el sueño. Debe ser algo en lo que sabe que puede contar todos los días.

La plataforma de administración y los puntos de acceso de vanguardia del Wi-Fi Seguro con Administración en la Nube de WatchGuard ofrecen el rendimiento que necesita para respaldar a su empresa. Nuestros modelos de punto de acceso están diseñados específicamente para permitir entornos de densidad media, como escuelas, espacios de oficina distribuidos, tiendas minoristas, salas de reuniones, restaurantes y centros de atención médica y, también, entornos de alta densidad, incluidos grandes predios escolares, centros de conferencias y centros comerciales.

Además, nuestros puntos de acceso con MIMO multiusuario (MU-MIMO) permiten que el punto de acceso preste servicio a varios dispositivos de clientes en cadena en forma simultánea. Esto disminuirá el tiempo que debe esperar cada dispositivo para una transmisión desde el punto de acceso, y aumentará la velocidad su red.

Lo mejor de todo es que ofrece este acceso inalámbrico de alto rendimiento a sus empleados y clientes sin tener que desactivar ninguna de sus configuraciones de seguridad. Ejecute la red Wi-Fi de manera absolutamente segura sin disminuir la velocidad del rendimiento. Ahora eso sí es una red Wi-Fi gana - gana.

La plataforma y los puntos de acceso de vanguardia del Wi-Fi Seguro con Administración en la Nube de WatchGuard ofrecen el **rendimiento que necesita para respaldar a su empresa**.

Administración Escalable 2

Disponer de una gran solución de Wi-Fi que es difícil de administrar no lo ayuda a obtener una mejor seguridad y rendimiento de la conectividad inalámbrica para su empresa. Necesita una solución que sea fácil de configurar y administrar, que le dé el control sobre toda la red inalámbrica, sin importar el tamaño, desde una única interfaz y que le permita a su vez ejecutar procesos clave para proteger el entorno y a sus usuarios.

A medida que su empresa crece, la implementación de Wi-Fi debe crecer de modo sencillo a la par. La centralización de la administración de Wi-Fi le permite llevar a su empresa desde un punto de acceso inalámbrico hasta un número ilimitado en múltiples ubicaciones, sin una infraestructura de controlador.

En este mundo conectado a Wi-Fi, sabemos que necesita además visibilidad de información crucial, como cobertura de intensidad de señal, consumo de ancho de banda de cliente inalámbrico, uso de punto de acceso, visibilidad de aplicaciones y distribución de clientes para asegurarse de tener siempre la imagen completa de lo que está sucediendo en su empresa. La posibilidad de ver estos datos de manera sencilla, así como de generar informes personalizables sobre estos datos, significa que puede saber lo que está pasando dentro de su empresa sin pasar horas mirando un panel de control.

Centralizar la administración del Wi-Fi le permite llevar a su empresa desde un punto de acceso hasta un número ilimitado de puntos de acceso en múltiples ubicaciones sin una infraestructura de controladores.

¿Por Qué WatchGuard? 2

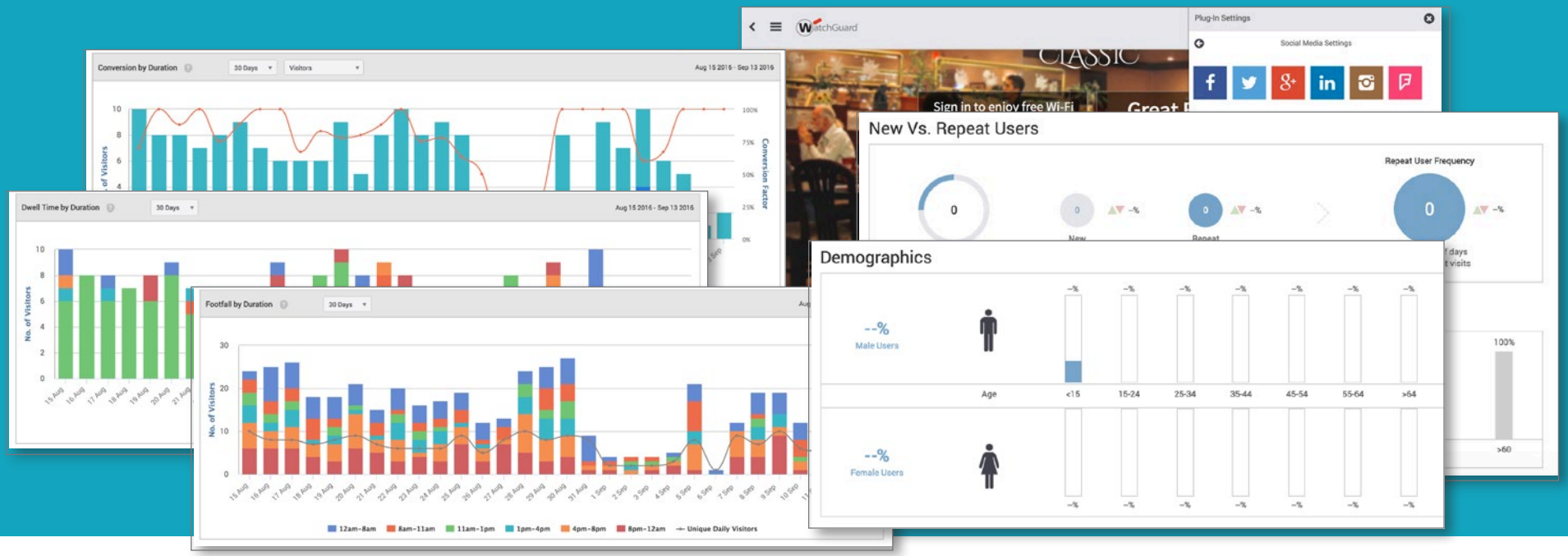
Wi-Fi Cloud es fácil de configurar y administrar, y le permite controlar toda la red inalámbrica desde una única interfaz, y a su vez agrupar puntos de acceso del modo que crea más sencillo incluidos ubicación, edificio, planta o hasta cliente, en caso de que usted sea un proveedor de servicios administrados.

Los informes, los widget de panel de control, las plantillas de configuración y una variada información de análisis están disponibles en todo WatchGuard Wi-Fi Cloud. Los administradores pueden crear una cantidad ilimitada de carpetas anidadas para representar edificios, plantas o cualquier grupo, y ofrecer visibilidad completa de la carpeta o permitirle ver solo los análisis para un nivel específico.

También puede obtener visibilidad de las aplicaciones que funcionan en la red Wi-Fi. Puede supervisar y generar informes de más de 1.300 aplicaciones de Capa 2 y superiores (como Facebook, YouTube, Instagram, etc.) para exigir políticas de uso justo y minimizar la congestión de la red.

Por último, manténgase actualizado en su entorno de Wi-Fi con plantillas predefinidas y personalizables para informes automatizados de amenazas de Wi-Fi, uso del Wi-Fi, inventario de clientes, estado de cumplimiento y rendimiento. El potente motor de informes de Wi-Fi Cloud le permite programar los informes para que se envíen de forma automática a los destinatarios de los correos electrónicos que usted elija.

Los informes, los widgets de panel de control, las plantillas de configuración y una **variada información de análisis** están **disponibles** en todo **WatchGuard Wi-Fi Cloud.**



Seguridad Completa Verificada

3

Muchos de los proveedores de Wi-Fi de la actualidad se basan en la ambigüedad cuando se trata de brindar Wi-Fi "seguro". Como con cualquier otra medida de seguridad para su empresa, necesita garantizar que la solución protegerá a su empresa de los ataques de Wi-Fi.

Una verdadera solución de seguridad completa debe ofrecer los tres siguientes beneficios clave:

- Ofrecer protección automática contra las 6 categorías de amenazas conocidas de Wi-Fi que se vieron anteriormente
- Permitir que puntos de acceso externo legítimos funcionen en el mismo espacio aéreo
- Impedir a los usuarios conectarse a puntos de acceso a Wi-Fi no autorizados

Ha sido un desafío encontrar este tipo de datos de seguridad en la mayoría de los proveedores más importantes de Wi-Fi, ya que, sinceramente, nunca se ha realizado una prueba de eficacia de la seguridad en soluciones de Wi-Fi. Hasta ahora.

En una reciente serie de pruebas nunca antes realizadas, Miercom, una empresa líder de la industria experta en generación de informes, expuso a algunos de los puntos de acceso principales al desafío de admitir aplicaciones en tiempo real y, en forma simultánea, detectar y evitar las amenazas de seguridad inalámbrica. Las pruebas incluían las 6 categorías de amenazas conocidas de Wi-Fi, y Miercom registró el tiempo que tomó la tarea de detección y prevención de cada una de las amenazas.

	WatchGuard AP420		Aruba IAP335		Cisco Meraki MR53		Ruckus R710	
Prueba	Detección	Prevención	Detección	Prevención	Detección	Prevención	Detección	Prevención
PA no autorizado	A	A	R	N/C	R	AA	R	N/C
Cliente no autorizado	A	A	R	N/C	R	AA	N/C	AA
PA vecino	A	A	A	A	R	N/C	R	N/C
Red ad-hoc	A	A	R	N/C	R	N/C	A	N/C
PA "gemelo malvado"	A	A	A	R	A	AA	A	R
PA mal configurado	A	A	A	N/C	N/C	N/C	N/C	N/C
Amenazas concurrentes	A	A	R	R	R	R	R	R

A = Aprobado
R = Reprobado
AA = Apenas Aprobado
N/C = Característica No Compatible

Vea el informe completo de Miercom: **www.watchguard.com/wifi-security-report**

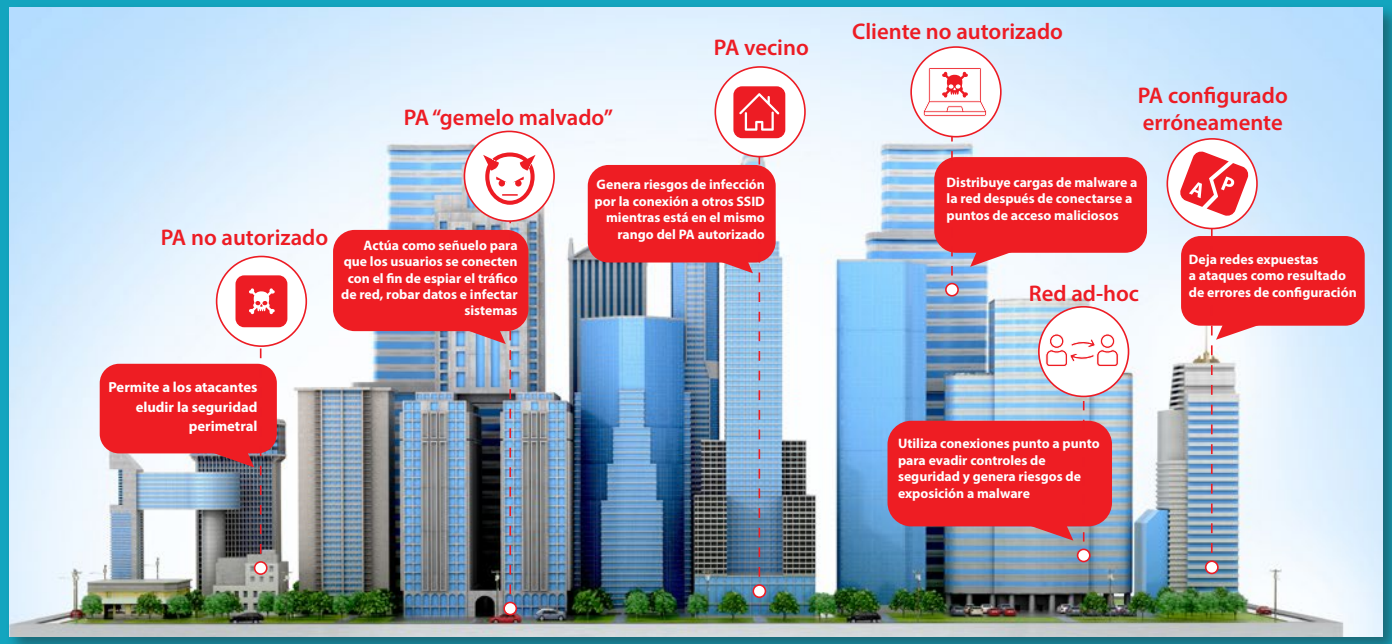
¿Por Qué WatchGuard? 3

WatchGuard es el ÚNICO proveedor que no solo detecta, sino que además evita de manera automática las 6 categorías de amenazas conocidas de Wi-Fi. Con la solución de Wi-Fi, WatchGuard fue además el único proveedor capaz de detectar y evitar todas las amenazas en forma simultánea en menos de 20 segundos.

Nuestro Sistema de Prevención de Intrusiones Inalámbricas (WIPS) patentado es diferente de cualquier otra solución de seguridad de Wi-Fi del mercado, ya que le garantiza que tendrá protección de Wi-Fi real, precisa y automatizada para su empresa. Mientras otros proveedores utilizan firmas y dependen en gran medida de las reglas de correlación de direcciones de MAC que pueden llevar a un alto volumen de falsos positivos, nuestra tecnología de marcadores de paquetes le garantiza que su espacio aéreo tenga pocos o ningún falso positivo.

El WIPS de WatchGuard es la única solución del mercado que analiza todos los puntos de acceso y dispositivos de cliente en el área y los clasifica como autorizados, externos o no autorizados. A través de una diferenciación rápida y confiable de los puntos de acceso y de los clientes, puede asegurarse de que los PA y los clientes autorizados tengan el acceso que necesitan, que los PA externos queden aislados y que los PA y clientes no autorizados no tengan posibilidad de conectarse.

WatchGuard es el **ÚNICO proveedor** que no solo **detecta,** sino **que además evita de manera automática las 6 categorías de amenazas conocidas** de Wi-Fi.



La ÚNICA Opción para su Entorno Inalámbrico de Confianza

WatchGuard es la única empresa que le ofrece la tecnología y las soluciones que puede utilizar para crear un Entorno Inalámbrico de Confianza, y que cumple con cada uno de los tres principales pilares: rendimiento líder en el mercado, administración escalable y seguridad completa verificada para proporcionar protección contra las 6 categorías de amenazas conocidas de Wi-Fi.
En todas las categorías, en cada prueba, WatchGuard es la única opción.

Los hallazgos clave del informe de Miercom determinaron que WatchGuard es el ÚNICO proveedor que:

- Detecta y evita de manera automática las 6 categorías de amenazas conocidas de Wi-Fi en forma simultánea y mantiene el rendimiento
- Soporta la detección y prevención automática de PA y clientes no autorizados
- Detecta e impide automáticamente que los endpoints puedan comunicarse a través de una conexión de Wi-Fi ad-hoc
- Impide automáticamente conexiones con PA "gemelo malvado" y conexiones peligrosas a PA configurados erróneamente como SSID privados sin cifrado

Obtenga más información sobre cómo crear su Entorno Inalámbrico de Confianza con WatchGuard hoy mismo

Watchguard.com/trustedwirelessenvironment

EL PORTAFOLIO DE SEGURIDAD DE WATCHGUARD

Seguridad de Red

Además de ofrecer seguridad de nivel empresarial, nuestra plataforma está diseñada desde el inicio para centrarse en la facilidad de implementación, uso y administración continua, lo que convierte a WatchGuard en la solución ideal para empresas pequeñas, medianas y distribuidas en todo el mundo.

Secure Wi-Fi

La solución Secure Wi-Fi de WatchGuard, una verdadera innovación en el mercado actual, está diseñada para proporcionar un espacio aéreo seguro y protegido para los entornos de Wi-Fi, a la vez que elimina los problemas administrativos y reduce los costos en gran medida. Cuenta con herramientas de interacción amplias y visibilidad de análisis empresariales, y proporciona la ventaja competitiva que su empresa necesita para triunfar.

Autenticación Multifactor

WatchGuard AuthPoint™ es la solución correcta para abordar la brecha de seguridad con la autenticación multifactor en una plataforma de nube fácil de usar. El enfoque exclusivo de WatchGuard agrega el "ADN del teléfono móvil" como factor de identificación para garantizar que solo las personas correctas tengan acceso a las redes confidenciales y a las aplicaciones en la nube.

Descúbralo

Para conocer más detalles, comuníquese con su revendedor autorizado de WatchGuard o visite el sitio web **www.trustedwirelessenvironment.com**

Acerca de WatchGuard

WatchGuard® Technologies, Inc. es un líder mundial en seguridad de red, Wi-Fi seguro, autenticación multifactor y servicios de inteligencia de red. Cerca de 10.000 revendedores de seguridad y proveedores de servicios confían en los productos y los servicios premiados de la empresa para proteger a más de 80.000 clientes. La misión de WatchGuard es lograr que compañías de todos los tipos y tamaños tengan acceso a seguridad de calidad empresarial a través de la simplicidad. Por ello, WatchGuard es una solución ideal para pequeñas y medianas empresas y también para empresas distribuidas. La empresa tiene sede central en Seattle, Washington, y posee oficinas en Norteamérica, Europa, Asia-Pacífico y Latinoamérica. Para obtener más información, visite WatchGuard.com.

Ventas en América del Norte: 1.800.734.9905 • Ventas Internacionales: 1.206.613.0895 • Sitio web: www.watchguard.com/wifi