WatchGuard

Las **conexiones wifi**
son **sencillas.**
Lo **difícil** es que **sean seguras.**

Índice

Las Conexiones Wifi Están **por Todas Partes**

Las organizaciones de todas las industrias se enfrentan a una presión más intensa por parte de los clientes, proveedores y empleados para ofrecer acceso inalámbrico. Si bien ofrecer este servicio proporciona ganancias, hay múltiples aspectos que el proveedor debe considerar, que incluyen los análisis y las interacciones móviles, los puntos de acceso, la Internet de las cosas (Internet of Things, IoT) y las deficiencias de capacidad para un espectro de celulares cada vez más amplio.

En este libro electrónico, exploraremos la demanda en aumento de wifi y, lo más importante, abordaremos las maneras en que puede proteger su red inalámbrica.

De todo el **tráfico de Internet** del mundo, el

63 %

será a través de una conexión **wifi** para el año **2019**[1]

Impulsores para la Adopción de Wifi

iPass predice que la cantidad de puntos de acceso crecerá de

23 millones en 2014 a casi **300 millones** en **2018**[2]

Productividad en el Lugar de Trabajo

Con el aumento de la capacidad de proceso de la conexión inalámbrica a una velocidad de 802.11ac, los trabajadores no están limitados por un cable Ethernet. Las organizaciones pueden ofrecer la flexibilidad de un lugar de trabajo móvil y, al mismo tiempo, evitan hacer sacrificios de productividad con cuellos de botella inalámbricos.

Mayor Rendimiento de la Inversión

Instalar una infraestructura cableada es costoso y resulta poco flexible. Las empresas que optan por ofrecer una conectividad cableada exclusivamente deben cubrir los costos de cables, enchufes de pared e interruptores, además del costo de la instalación y el mantenimiento. A medida que la organización crece y se agregan usuarios, las empresas incurren en costos adicionales. Ofrecer puntos de acceso inalámbricos es mucho más barato, proporciona mayor escalabilidad y brinda flexibilidad y eficiencia para que los usuarios se muevan por toda la instalación.

Satisfacción del Cliente y Repetición de Visitas

La conexión wifi para los invitados se ha convertido en una oferta común en diversos sectores empresariales. Las organizaciones que optan por brindar este servicio también deben adaptarse a las demandas de alta velocidad de la transmisión de videos de alta definición y de música. La industria hotelera depende especialmente de la oferta de wifi, ya que los viajeros califican el acceso wifi gratuito como su criterio principal a la hora de elegir un hotel.

Interacciones Móviles

Las interacciones móviles abarcan la gran variedad de técnicas que las empresas usan para comunicarse con sus clientes una vez que estos se han conectado a la red de wifi para invitados. Esto permite que las empresas extiendan sus estrategias de interacción más allá de la página de inicio y proporcionen una experiencia en línea aún más enriquecedora que informe a los clientes sobre los detalles relevantes precisamente cuando ellos más los necesitan.

Análisis de Clientes

Cantidades masivas de datos de clientes (recolectados por medio de análisis pasivos, análisis activos y conexiones del usuario dentro y alrededor de las redes de wifi de una empresa) pueden proporcionar a las empresas conocimientos valiosos sobre el comportamiento, la demografía y las tendencias de los invitados. Las empresas que aprovechan estos datos junto con el análisis de inicio de sesión en redes sociales, obtienen una potente visibilidad de la información demográfica, entre la que se incluye el sexo, la edad y las tendencias de compra de los clientes, que a su vez informa a los clientes sobre las estrategias de marketing aun después de haber abandonado la tienda.

Internet de las Cosas (IoT)

La cantidad de "cosas" conectadas a Internet aumenta rápidamente. El Centro Internacional de Datos (International Data Corporation, IDC) estima que la cantidad de equipos conectados a un extremo de IoT, como automóviles, refrigeradores y todo lo que esté en medio, se triplicará entre el año 2014 y el 2020. La firma predice que el mercado de IoT global crecerá un 150 % durante este período, de $655,8 mil millones a $1,7 millones de billones.

Deficiencia de Capacidad Celular Cada Vez más Amplia

Los proveedores de datos celulares están invirtiendo grandes sumas de dinero en los derechos para enviar señales por aire a través de radiofrecuencias, a menudo denominado espectro. La capacidad de cada espectro, con licencias otorgadas por reguladores gubernamentales, se ve sobrepasada por la demanda de los consumidores. Para poder resolver estas deficiencias de capacidad cada vez mayores, los proveedores de datos están pensando en satisfacer la demanda mediante wifi, específicamente mediante la banda industrial, científica y médica (ISM) de 5 GHz. No obstante, en comparación con los datos celulares, la conexión wifi tiene un alcance muy corto. Esto presenta un desafío que solo puede resolverse con una implementación masiva de puntos de acceso inalámbrico, al crear redes de wifi con nivel de operador.

Las Once Amenazas Principales a su Red Inalámbrica

1. Violación de la Contraseña de Wifi

Los puntos de acceso inalámbrico que aún utilizan protocolos de seguridad más antiguos, como WEP, resultan objetivos fáciles porque es notablemente sencillo violar las contraseñas.

2. Clientes y PA No Autorizados

Físicamente, no hay nada que prevenga que un criminal cibernético habilite un punto de acceso externo cerca de su punto de acceso con una SSID que coincida, la cual invita a los clientes desprevenidos a iniciar sesión. Los usuarios que son víctimas de un PA no autorizado son susceptibles de sufrir una inyección de código malicioso que a menudo pasa desapercibida.

3. Implantación de Malware

Los clientes que se unen a una red inalámbrica para invitados son susceptibles de que al desconectarse, lleven un malware no deseado sin saberlo, creado por usuarios vecinos mal intencionados. Una táctica frecuente que los hackers usan es implantar una puerta trasera en la red, la que les permite volver más tarde para robar información confidencial.

4. Interceptación

Los invitados corren el riesgo de que fisgones informáticos detecten sus comunicaciones privadas o revisen sus paquetes mientras se encuentren en redes inalámbricas no protegidas.

5. Robo de Datos

Unirse a una red inalámbrica pone a los usuarios en riesgo de perder sus documentos privados que puedan contener información altamente confidencial ante ladrones cibernéticos, quienes aprovechan la situación e interceptan los datos que se envían a través de la red.

6. Uso Indebido e Ilegal

Las empresas que ofrecen conexión wifi para invitados corren el riesgo de alojar una amplia variedad de comunicaciones ilegales y potencialmente dañinas. El contenido extremista o para adultos puede ser ofensivo para usuarios vecinos, y las descargas ilegales de medios protegidos hacen que las empresas puedan recibir demandas por vulneración de los derechos de propiedad intelectual.

7. Malos Vecinos

A medida que la cantidad de usuarios inalámbricos en la red crece, también crece el riesgo de que haya clientes previamente infectados que ingresen a la red. Ataques móviles, como Stagefright de Android, pueden diseminarse de invitado a invitado, aun cuando la víctima cero no sea consciente del brote.

8. Ataque de Tipo "Man in the Middle" (MiM)

La comunicación mundana a través de wifi puede dar como resultado una infracción cuando un actor malicioso secretamente intercepta y altera conversaciones legítimas.

9. DoS Inalámbrico

Los atacantes pueden provocar una paralización del acceso wifi cuando intencionalmente envían grandes cantidades de tráfico a puntos de acceso legítimos, y esto desactiva el dispositivo de un uso legítimo.

10. Ataques Enmascarados

Es común que los criminales cibernéticos abocados a infringir la seguridad de wifi intenten simular que sus equipos son legítimos o conocidos falsificando direcciones MAC.

11. PA Configurados erróneamente

La implementación de puntos de acceso sin seguir las mejores prácticas de seguridad de wifi puede dar como resultado malas configuraciones que pasan inadvertidas, que a menudo plantean riesgos de seguridad.

Problemas que Comparten las Industrias Principales

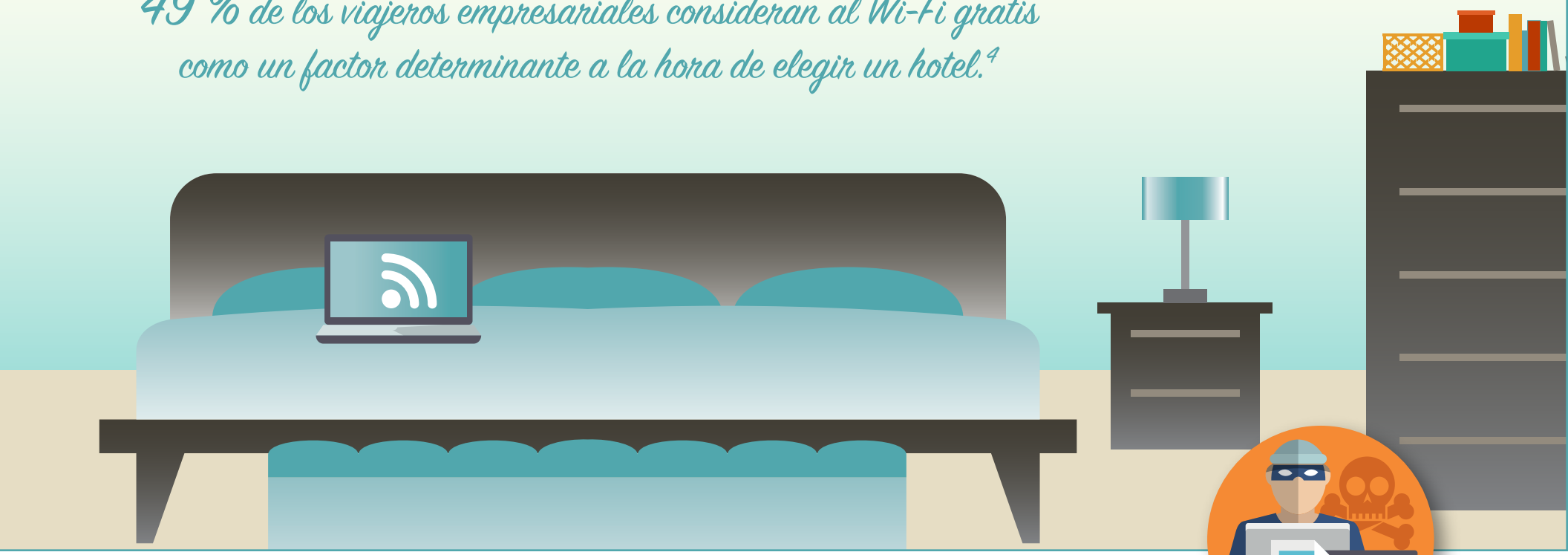
El 60 % de las pequeñas y medianas empresas (Small and Medium Businesses, SMB) que sufren la pérdida de datos, salen del mercado dentro **de los siguientes seis meses.**[3]

Preocupaciones de las Ventas al por Menor

Los sistemas de puntos de ventas (Point of Sale, POS) móviles son cada vez más comunes. Cualquier empresa que acepte tarjetas de crédito a través de una red inalámbrica o red cableada tiene la responsabilidad de proteger el almacenamiento y la transmisión de los datos del titular de la tarjeta. Un grupo de bancos desarrolló una norma por medio de la cual la información del pago debe protegerse y la llamó PCI DSS o Estándar de Seguridad de Datos de la Industria de Tarjetas de Pago. Este conjunto de pautas está diseñado para proteger a los minoristas y a los consumidores de robos. Las organizaciones se enfrentan a multas severas si no cumplen estas pautas a la hora de proteger sus puntos de acceso wifi.

Obtener visibilidad del acceso inalámbrico de invitados implica otro desafío significativo para las organizaciones del sector de ventas al por menor. Durante mucho tiempo, las empresas en línea han disfrutado de métodos confiables para mejorar el rendimiento de la inversión (Return on Investment, ROI) de marketing, las tasas de conversión de ventas y muchas otras métricas. Sin embargo, en el mundo físico, se ha abierto una inmensa brecha en las herramientas que tienen a disposición las empresas para alcanzar el valioso conocimiento que puede ser usado en la optimización de sus operaciones.

49 % de los viajeros empresariales consideran al Wi-Fi gratis como un factor determinante a la hora de elegir un hotel.[4]



Preocupaciones del Sector de Hotelería

Un sistema de gestión de propiedades (PMS) es una aplicación de software que utilizan los hoteles para automatizar y coordinar diversas funciones empresariales que incluyen desde operaciones de atención al cliente hasta operaciones administrativas, como la gestión de la información de las tarjetas de crédito de los huéspedes. Además, los sistemas PMS comúnmente se integran a los POS y a los sistemas de reservas, lo cual constituye un objetivo muy valioso para los criminales informáticos. Recientemente, muchas cadenas de hoteles importantes han sido víctimas del infiltraciones de los sistemas PMS o POS, lo cual les significó multas, demandas y daños a su reputación. Un gran desafío para las organizaciones de la industria hotelera es ofrecer una conexión wifi de alta velocidad, pero al mismo tiempo proteger tanto los recursos corporativos como los de los huéspedes.

Además, las organizaciones de la industria hotelera requieren plataformas en línea a través de las cuales puedan interactuar con los invitados. Estas herramientas deberían ofrecer una experiencia del cliente con contenido de marca e, idealmente, un medio para medir la satisfacción del cliente y la probabilidad de su regreso.

El sector de la atención médica representa el **42,5 %** de **toda la pérdida de datos** de los **últimos tres años**.[5]

Preocupaciones en la Atención Médica

La industria de atención médica se enfrenta a una serie de desafíos de seguridad inalámbrica únicos que surgen de la naturaleza altamente confidencial y valiosa de los datos que se intercambian en la red. La Ley de Portabilidad y Responsabilidad del Seguro Médico (HIPAA), junto con estándares globales similares, exige que las organizaciones que procesan datos de pacientes cumplan con una serie de estrictas prácticas de seguridad. Diversos tipos de tecnologías médicas han evolucionado para intercambiar datos de manera inalámbrica, lo cual optimiza procesos como el seguimiento de inventario de equipos, pero también abre una nueva ventana de vulnerabilidad. Esta tendencia, conocida como Internet de las cosas (IoT), ha revolucionado la atención médica con una eficiencia mejorada; sin embargo, estos equipos son los objetivos más comunes de ataques maliciosos.
Los equipos médicos generalmente ejecutan versiones anteriores de sistemas operativos, y es sabido que estas son vulnerables. Con frecuencia, los profesionales de la atención médica almacenan información médica protegida en equipos móviles y acceden a ella desde los equipos. El acceso a los datos de los clientes y pacientes desde equipos móviles ofrece grandes beneficios en relación con la eficiencia y, a la vez, aumenta la exposición, a menos que se pongan en práctica medidas estrictas de seguridad.

Preocupaciones en la Educación

Los equipos móviles están transformando la educación. Las escuelas entregan tabletas en todos los niveles de grado, y los estudiantes necesitan acceso inalámbrico de alta velocidad a una abundante cantidad de recursos educativos basados en la Web. No obstante, acceder a este caudal de conocimientos acarrea algunos riesgos. Las escuelas, especialmente primarias y secundarias, están obligadas a filtrar el contenido web no apropiado. Los estudiantes de la escuela primaria son particularmente vulnerables al malware porque no están tan familiarizados con las trampas comunes que los hackers establecen. Además de las amenazas externas, las redes de los estudiantes están separadas de la red del administrador, con el fin de que se minimicen los riesgos de realizar engaños, alteraciones y otras cuestiones de privacidad.

Cambios que se Deben Implementar **DE INMEDIATO**:

WPA2: implemente el protocolo de seguridad **más actual**.

Contraseña Segura: NO utilice las contraseñas predeterminadas. Cambie la contraseña con regularidad.

Conozca su Red: detecte **PA no autorizados** y **realice una lista de aprobación de direcciones de control de acceso al medio (MAC)** cuando sea posible.

Limite el Alcance la Conexión Wifi: **limite el alcance** a sus áreas de operación.

Mantenga el **Firmware Actualizado**.

Lleve su **Seguridad a un Nivel Empresarial**

Seguridad

Habilitar una Conexión Wifi Es Sencillo. Lo Difícil es que Sea Segura. Los profesionales de seguridad de primera categoría aseguran que todo el tráfico de una red inalámbrica se realiza mediante un conjunto completo de servicios de Gestión Unificada de Amenazas (UTM) que incluyen antivirus (AV), Servicios de Prevención de Intrusiones (IPS), filtrado web, bloqueo de correo no deseado, control de aplicaciones, búsqueda de reputaciones, bloqueador de amenazas avanzadas persistentes (APT) y prevención de pérdida de datos. Idealmente, los servicios deberían habilitarse sin sacrificar el rendimiento y en pos de la eficiencia, y todo debería gestionarse de manera centralizada desde una única interfaz. Además, solo deberían usarse los puntos de acceso habilitados con WIPS.

Un Sistema de Prevención de Intrusiones Inalámbricas, o **WIPS**, es una capa de protección esencial para las redes inalámbricas que almacenan o transmiten datos confidenciales que permite que los administradores de la red protejan su espacio aéreo contra equipos no autorizados, ataques de denegación de servicio, PA no autorizados y mucho más. El WIPS más confiable y eficaz clasifica automática y rápidamente los equipos inalámbricos detectados en el espacio aéreo como Autorizados, No autorizados y Externos. Así, elimina las falsas alarmas y les ahorra a los administradores de la seguridad el trabajo de definir reglas complejas para identificar equipos inalámbricos no autorizados o inspeccionar los equipos de manera manual.

Visibilidad

Las redes inalámbricas constituyen uno de los puntos ciegos de seguridad más ignorados en cualquier organización. Los profesionales de seguridad de TI exigen una solución que ofrezca **visibilidad** del tráfico de la red en tiempo real e histórico, que proporcione **informes automáticos** que brinden información a las partes interesadas sobre tendencias y patrones clave, y conocimientos sobre hacia dónde se dirigen los invitados en el entorno físico y que permita que TI **analice la cobertura inalámbrica** y detecte PA no autorizados.

Gestión

La incorrecta configuración de los equipos de la red es una de las causas más comunes de infracciones de seguridad de red. Al consolidar la gestión de redes cableadas e inalámbricas, el riesgo de realizar una configuración incorrectamente se reduce de manera significativa. Los modernos profesionales de TI están buscando la manera de obtener una **flexibilidad completa en las opciones de gestión**, por medio de la nube, Windows, la web y de sistemas basados en la interfaz de línea de comandos (CLI) para habilitar un **control de seguridad máximo**.

Tecnologías de Seguridad Inalámbrica de WatchGuard

Puntos de Acceso Inalámbricos Aptos para Funcionar en la Nube

Los clientes pueden mejorar o agregar conexiones inalámbricas a un firewall existente implementando puntos de acceso inalámbricos aptos para funcionar en la nube. El AP120 es ideal para redes inalámbricas más pequeñas, mientras que el AP320 es perfecto para entornos inalámbricos más grandes y complejos. Si le interesa que su empresa funcione en exteriores, el AP322 es la solución que busca. Los PA de WatchGuard proporcionan opciones flexibles de implementación, pero todos los PA de WatchGuard son aptos para funcionar en la nube y pueden administrarse desde la Nube Wifi.

Dispositivos de Seguridad de Red

Ejecute todo el tráfico de wifi a través de un dispositivo de seguridad de red de WatchGuard y habilite un nivel adicional de seguridad para proteger a sus clientes y su empresa.

WatchGuard Dimension™

Gracias a su integración completa con la Nube Wifi de WatchGuard, WatchGuard Dimension consolida el tráfico inalámbrico en tiempo real e histórico en una única fuente, completa con paneles de control e informes personalizables, lo cual permite que el personal de TI establezca las directrices, identifique tendencias y ponga fin a las actividades inalámbricas maliciosas antes de que se transformen en una mayor amenaza para la empresa.

WatchGuard Wi-Fi Cloud

La Nube Wifi de WatchGuard ofrece una visibilidad sin precedentes de cada rincón del entorno inalámbrico de su empresa y más allá. Los paneles de control y las alertas personalizables proporcionan una descripción general integral y la capacidad de explorar en profundidad para obtener una visión más detallada. Al aprovechar la tecnología innovadora de wifi, la Nube Wifi proporciona visibilidad de una valiosa fuente de datos de marketing, incluidos conocimientos sobre la concurrencia y la demografía de los clientes. Las organizaciones pueden monetizar estos conocimientos fácilmente al aprovechar las funcionalidades de Interacciones Móviles, lo cual permite una comunicación directa y personalizada con clientes individuales a través de SMS, MMS y su red social de preferencia.

Friendly Wi-Fi es la primera acreditación mundial que prueba que los servicios de wifi para jóvenes ofrecidos por un lugar son seguros y cuentan con filtros contra el contenido indebido e ilegal. Iniciada por el gobierno y organismos industriales como el primer estándar mundial para wifi público, con marcas clave que ya demuestran su apoyo y participan en la iniciativa de Friendly Wi-Fi. Recientemente, WatchGuard recibió la acreditación de Friendly Wi-Fi como el proveedor preferido de soluciones de wifi segura. En el caso de los lugares que usan las funcionalidades o puntos de acceso de la Gestión Unificada de Amenazas (Unified Threat Management, UTM) de WatchGuard administradas por la Nube Wifi, recibir la acreditación les permite exhibir el colorido símbolo 'Navegación Segura' (Safe Surf). Además, esos lugares pueden encontrarse en el sitio web de Friendly Wi-Fi.

Productos de Wifi Seguro de WatchGuard

1. *Cisco VNI Global IP Traffic and Service Adoption Forecast (Predicción del Tráfico de IP Global y la Adopción del Servicio de Cisco VNI), 2014-2019*
2. *http://www.marketwired.com/press-release/ipass-wi-fi-growth-map-shows-1-public-hotspot-for-every-20-people-on-earth-by-2018-nasdaq-ipas-1963515.htm*
3. *https://www.staysafeonline.org/stay-safe-online/resources/small-business-online-security-infographic*
4. *Hotels.com. "Free Wi-Fi Reigns but Wanes as Top Hotel Amenity" (La Conexión Wifi Gratuita Impera, pero Disminuye como Servicio Principal de los Hoteles), 6 de mayo de 2015*
5. *USA TODAY. "Another Health Care Data Breach" (Otra Infracción de Datos en la Atención Médica), 25 de julio de 2015*
6. *Websense Security Labs Blog. "Today's Lesson" (La Lección de Hoy), 7 de julio de 2015*

Todos los productos creados por WatchGuard están diseñados teniendo en cuenta el entorno inalámbrico seguro. Desde firewalls de red hasta puntos de acceso aptos para funcionar en la nube, WatchGuard sabe que su empresa confía en una Seguridad Inalámbrica rápida y confiable.

Al aprovechar la cartera de tecnologías de seguridad inalámbrica de WatchGuard, las organizaciones pueden configurar, implementar y gestionar con facilidad la seguridad de red constante y de nivel empresarial, y proteger la conexión inalámbrica en todas las ubicaciones remotas sin la necesidad de contar con conocimientos técnicos en cada ubicación con la tecnología innovadora RapidDeploy. Además de proporcionar una seguridad fácil de implementar y líder en el mundo, la solución de nube wifi de la empresa, WatchGuard Wi-Fi Cloud, combina la seguridad inalámbrica y la prevención de amenaza líderes en el mundo con un conjunto completo de herramientas de interacción participativa y análisis para brindar seguridad de nivel empresarial y funcionalidades inalámbricas principales a empresas pequeñas, medianas y distribuidas.

www.watchguard.com/wifi

© 2017 WatchGuard Technologies, Inc. Todos los derechos reservados. WGCE66886_061317