4 Formas Prácticas de

Simplificar

Su Seguridad

WatchGuard®

Índice

Introducción

A medida que aumenta la sofisticación y complejidad de las amenazas cibernéticas, es lógico que las empresas busquen defensas cibernéticas más poderosas y complejas. ¿Cuál es el problema de aumentar la seguridad incrementando su complejidad? Los recursos con los que cuenta, principalmente el tiempo y el personal, no aumentan a la par de manera automática.

Una caja de herramientas bien equipada no sirve de mucho sin alguien que sepa manejar el martillo; del mismo modo, hasta la infraestructura de seguridad más sólida requiere de alguien que la administre. Lamentablemente, la escasez de personal de TI implica un desafío para toda la industria y no hay indicios de que vaya a disminuir. **Asombra saber que el 53% de los profesionales de TI del mundo lucha contra una insuficiencia crítica de personal capacitado en seguridad cibernética dentro de sus empresas[1].** Los roles que están cubiertos de manera adecuada dentro del departamento son escasos y tienen dificultades para cumplir con las responsabilidades diarias mientras hacen malabares con constantes alertas e incidencias de soporte técnico.

Si esto le resulta muy familiar y siente que la seguridad simplificada es inalcanzable para su organización, continúe leyendo para informarse sobre cuatro formas prácticas de simplificar su seguridad cibernética.

Complicado

Administración de diferentes soluciones centralizadas:

Es temprano un lunes por la mañana y recibe un incidente de soporte técnico de Marketing: "No es posible acceder a un documento crítico para la empresa almacenado en el sitio de hospedaje de archivos. SE REQUIERE SOLUCIÓN LO ANTES POSIBLE". Suspira, toma un sorbo de café, (luego otro) y se prepara para pasar la siguiente media hora navegando por la configuración, lidiando con cinco diferentes pantallas para poder agregar una simple excepción de URL. Al haber cada vez más colecciones de configuraciones, comandos y herramientas diversas que administrar, este escenario es cada vez más frecuente para muchos administradores de redes, y consume gran parte de su valioso tiempo.

Piénselo así: si tiene alrededor de tres cuentas de correo electrónico (una laboral, una personal y, quizás, una dedicada al correo no deseado) es probable que sea bastante fácil mantener su bandeja de entrada y rescatar mensajes importantes (como la invitación al cumpleaños de 80 de la abuela o una nota del CEO) del correo no deseado. Ahora imagine que tiene 100 cuentas que supervisar, y en todas ellas podría recibir comunicaciones de gran importancia en cualquier momento. Ya no sería tan fácil.

¿Sabía esto?

Desde el 2012 con RapidDeploy WatchGuard ha ayudado a sus clientes a ahorrarse más de **16 años de trabajo**

Simple

Administración Centralizada:

Invierta en productos fáciles de configurar, implementar y administrar

La solución: Ya tiene suficiente de que ocuparse sin sumar alertas constantes que administrar y un pequeño ejército de pantallas que supervisar. Busque productos de seguridad de red que le permitan una administración sin interrupciones desde una única interfaz de usuario intuitiva. Los dispositivos de WatchGuard Firebox no solo son fáciles de configurar e implementar, sino que también cuentan con un diseño basado en la administración centralizada desde una consola, y esto simplifica la administración sin interrupciones de redes y políticas.

Fácil de configurar: Realice actualizaciones de configuración o firmware en un solo paso en todos los dispositivos administrados de WatchGuard para ahorrar tiempo y asegúrese de que las políticas estén sincronizadas a través de la empresa distribuida. Cree plantillas de políticas desde cualquier lugar e introdúzcalas rápidamente en múltiples dispositivos a través de inquilinos basados en roles.

Fácil de implementar: WatchGuard RapidDeploy es una poderosa herramienta de implementación y configuración basada en la nube que viene con los dispositivos Firebox de WatchGuard. Lo único que debe hacer es encender el dispositivo y conectarlo a Internet, el resto se puede administrar de manera remota desde cualquier lugar.

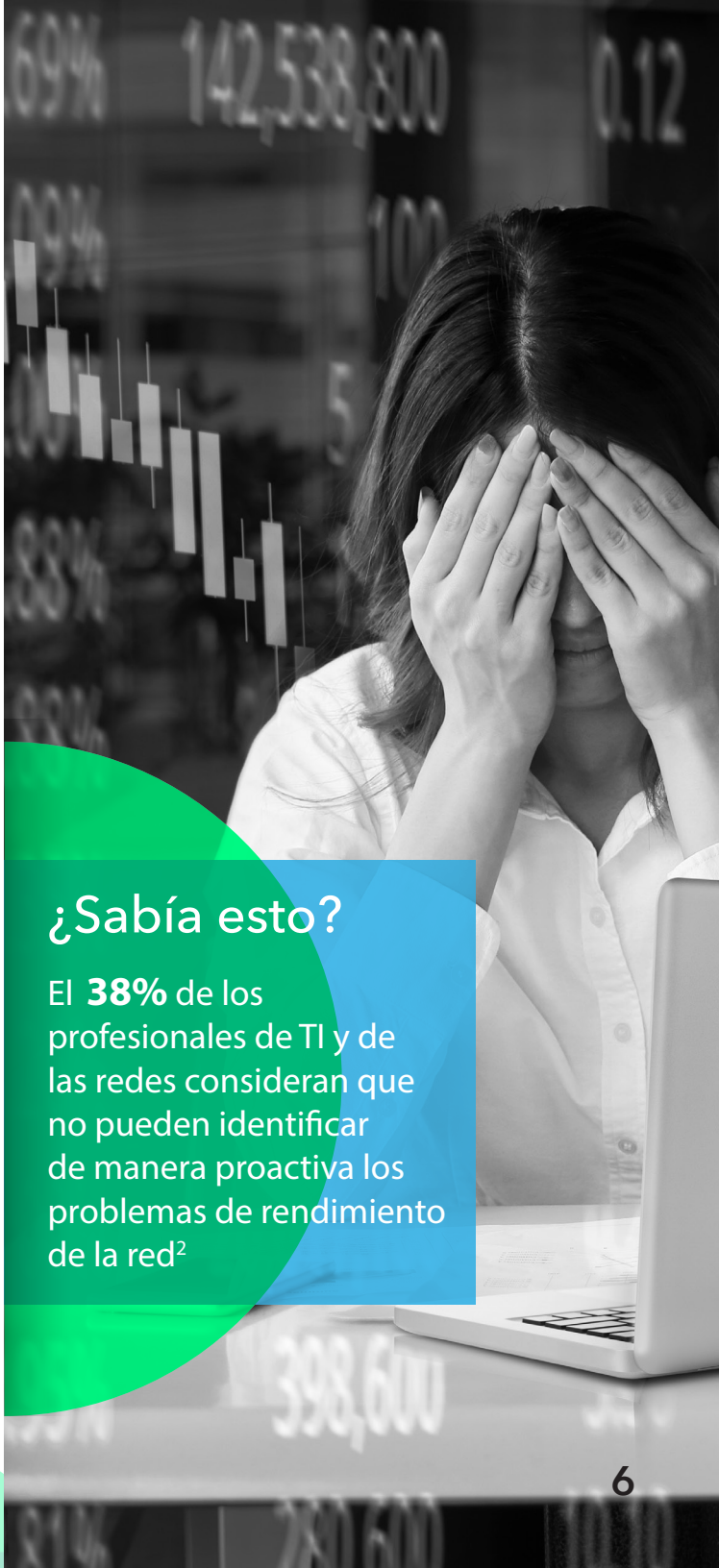
Fácil de administrar: Administre un dispositivo Firebox o cientos de dispositivos desde una consola fácil de usar, maximice la eficiencia y simplifique la administración de la red. Con una interfaz visual clara y mensajes de registros en lenguaje sencillo se elimina la incertidumbre sobre la creación y el mantenimiento de una seguridad sólida y se logra el cumplimiento.

Complicado

Análisis manual de enormes cantidades de datos

A medida que nuestras infraestructuras de TI crecen en tamaño y complejidad, la visibilidad granular de la actividad en la red es fundamental, ya que permite a los equipos de TI reconocer patrones, amenazas y brechas de seguridad, y responder antes de que se produzca un daño. Estos datos son muy valiosos, sin embargo, no son útiles si su equipo de seguridad no puede acceder con facilidad a los insights clave y realizar las acciones necesarias.

Muchas soluciones de visibilidad de red del mercado actual ofrecen grandes volúmenes de datos, pero sin tener demasiado en cuenta la clasificación de prioridades. Este enfoque es agobiante para la mayoría de los equipos de seguridad, que tienen colas de alertas de seguridad constantes que parecen no tener fin y que simplemente no se pueden investigar ni priorizar en su totalidad. Un producto con verdadera visibilidad efectiva reconoce las limitaciones de ancho de banda inherentes a muchos equipos de TI y destaca con efectividad los eventos más importantes para poder mantener el estado de la red.



¿Sabía esto?

El **38%** de los profesionales de TI y de las redes consideran que no pueden identificar de manera proactiva los problemas de rendimiento de la red[2]

Simple

Datos Prácticos:

Utilice soluciones automatizadas de visibilidad y generación de reportes

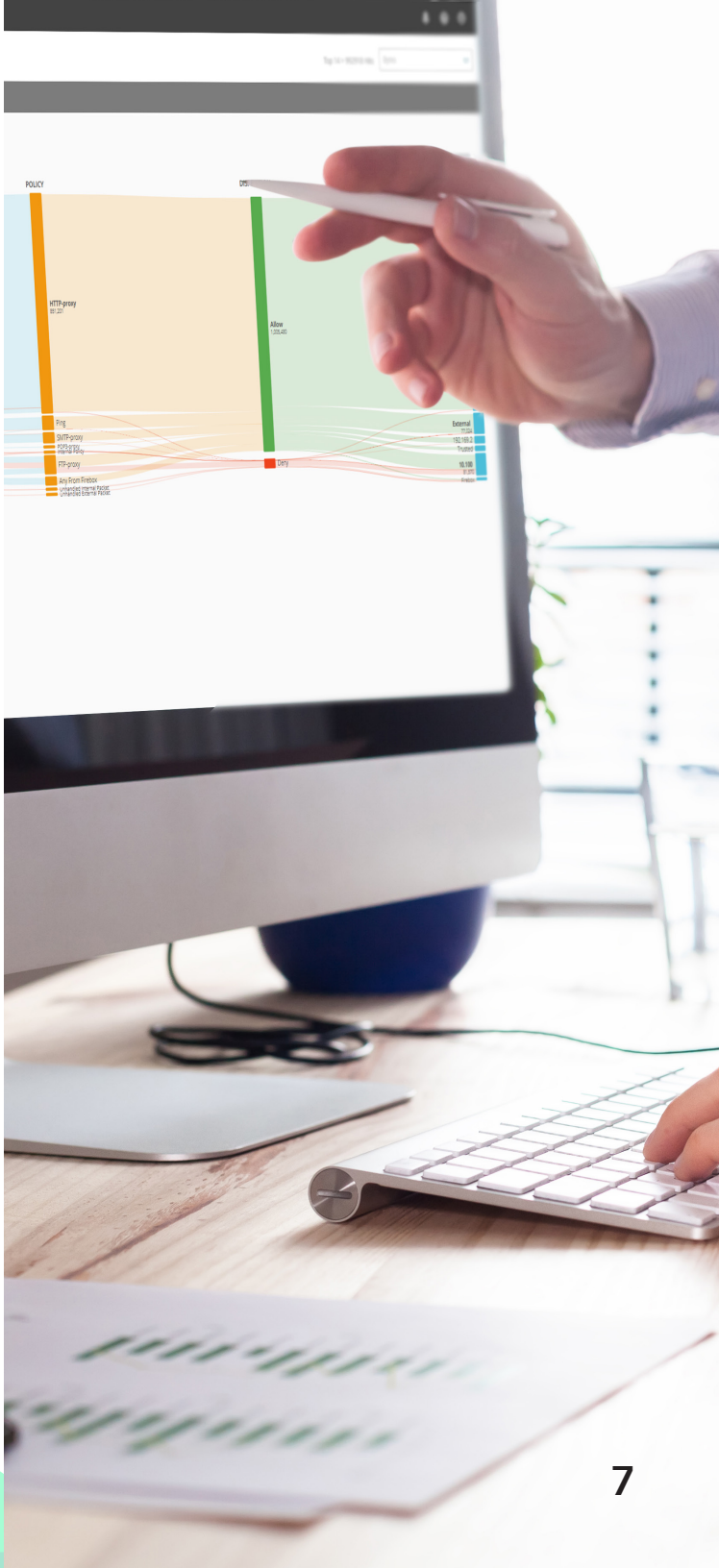
¿Cuál es la solución? Un panel de control de generación de reportes automatizado e intuitivo lo ayudará a evitar que su equipo de TI pierda tiempo y desaproveche recursos en eventos de bajo riesgo. WatchGuard Cloud Visibility ofrece insights rápidos, confiables y prácticos para que los equipos de TI puedan detectar con gran velocidad los patrones y tomar decisiones inteligentes. Con los paneles de control y las funcionalidades de generación de reportes integrados puede recopilar rápidamente información sobre eventos de seguridad, auditorías de cumplimiento y patrones de la red. Al ser una plataforma en la nube, le permite supervisar y obtener insights críticos sobre su seguridad de red en tiempo real, desde cualquier lugar y en cualquier momento. Y la mejor parte es que no requiere de infraestructura de hardware. ¿Qué tan sencillo es eso?

WatchGuard Cloud Visibility ofrece insights de nivel ejecutivo en su red, como los siguientes:

- Principales usuarios
- Principales destinos
- Principales aplicaciones
- Principales dominios

Vea su más reciente información de seguridad de Firebox, por ejemplo:

- Principales sitios de botnets bloqueados
- Principales clientes y destinos bloqueados
- Principales ataques de malware avanzado bloqueados
- Prevenciones de intrusiones



Complicado

Wi-Fi inseguro, de bajo rendimiento

Si bien el acceso a Wi-Fi ofrece gran eficiencia a las empresas modernas, como los programas BYOD (Bring Your Own Device) a el personal móvil, también genera grandes preocupaciones de seguridad en la red corporativa. La web ahora ofrece una gran variedad de recursos de ataques informáticos de Wi-Fi, incluidos videos informativos paso a paso en YouTube, lo que fortalece hasta al más inexperto de los criminales cibernéticos y ayuda a propagar las seis categorías conocidas de amenazas de Wi-Fi.

Punto de acceso "gemelo malvado"

Cliente no auto-rizado

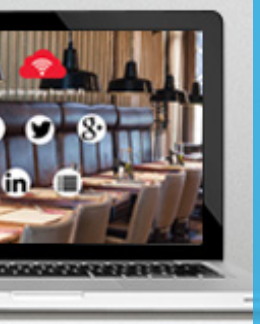
Punto de acceso configurado erróneamente

Punto de acceso vecino

Punto de acceso no autorizado

Red ad-hoc

A pesar de que muchos equipos de TI ya dedican una gran cantidad de recursos a problemas relacionados con Wi-Fi (como las contraseñas olvidadas en aplicaciones móviles, la sincronización de correos electrónicos y la dificultad para acceder a redes inalámbricas), la mayoría no cuenta con el ancho de banda necesario para implementar varias soluciones y brindar protección contra cada una de las seis categorías de amenazas de Wi-Fi, y muchos menos para mantenerlas. Necesita una única solución que sea fácil de implementar y administrar, y que no solo respalde los requisitos de rendimiento de su entorno único, sino que lo proteja en forma simultánea contra todas las categorías de amenazas de Wi-Fi.



¿Sabía esto?

El usuario promedio de BYOD (Bring Your Own Device) global ahorra 37 minutos en el trabajo por semana gracias al uso de su dispositivo móvil.[3]

Simple

Wi-Fi Más Fuerte y Más Seguro:
Ofrezca un Entorno Inalámbrico de Confianza

La solución: La conectividad de Wi-Fi segura y eficiente no tiene que ser complicada. WatchGuard es la única empresa que ofrece un framework verificado por Miercom para crear una red de Wi-Fi completa, de alto rendimiento, simple de administrar y con protección garantizada contra las seis categorías conocidas de amenazas de Wi-Fi. Mejor aún, los entornos administrados por WatchGuard Secure Cloud Wi-Fi, obtienen los beneficios de WatchGuard Discover, una aplicación dentro de Wi-Fi Cloud que ofrece un valioso insight del rendimiento y el estado de la red. Discover incluye un conjunto completo de funcionalidades prácticas de visibilidad, resolución de problemas y estado de la red, entre ellas:

Recorrido del cliente: una instantánea en vivo en todas sus ubicaciones para ver rápidamente los clientes que experimentan fallas de asociación, autenticación o de red no relacionadas con Wi-Fi pero que afectan su experiencia en la red.

Línea de base de la red: se realiza una supervisión del rendimiento, la conectividad y la experiencia de las aplicaciones en todos los clientes y puntos de acceso dentro del rango de sus redes para establecer qué es normal y qué es anormal. Cuando se detecta una anomalía, Discover ofrece visibilidad completa para identificar la causa principal y le brinda recomendaciones para resolver los problemas de red, incluso aquellos no relacionaos con Wi-Fi.

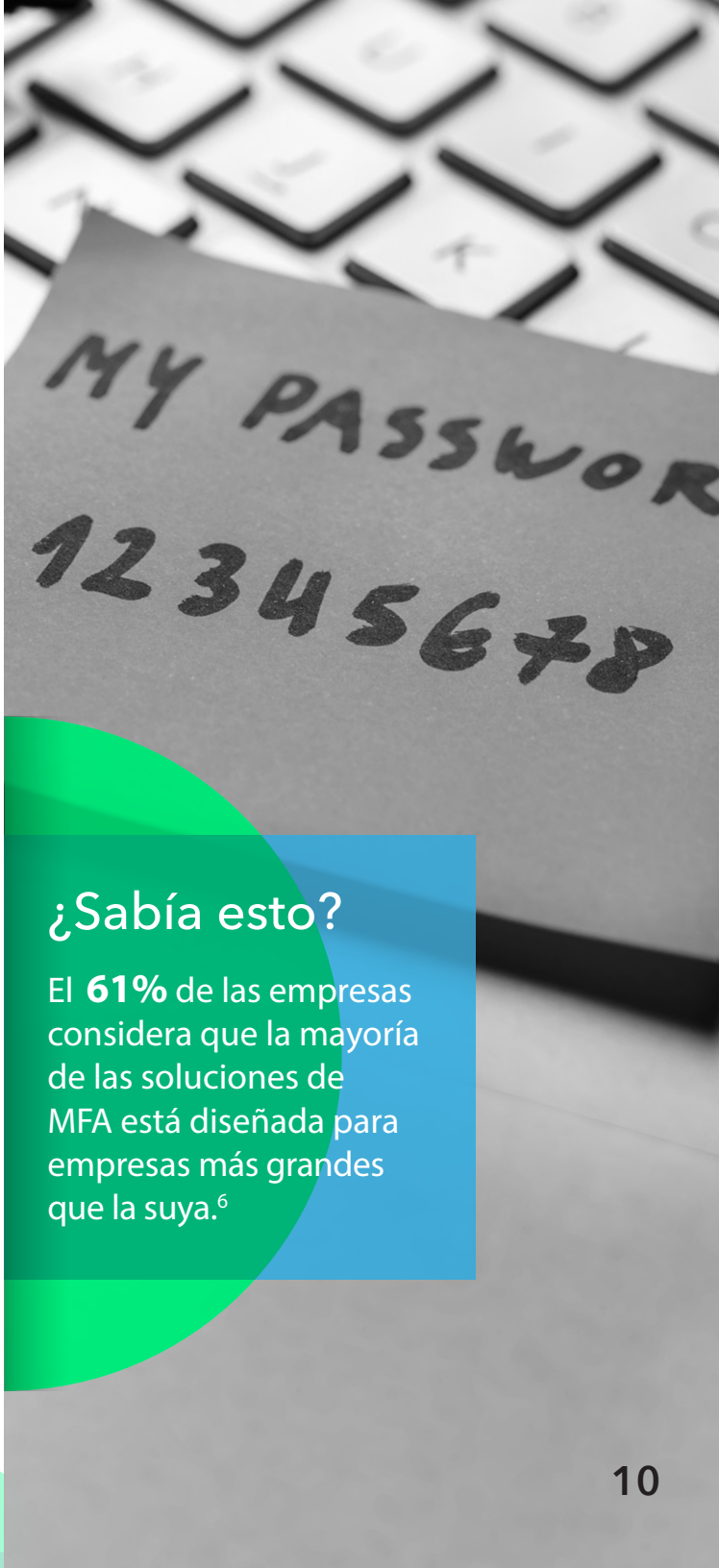
Alertas: mantener los acuerdos de nivel de servicio (SLA) es muy sencillo gracias a la funcionalidad de Alertas que incluye Discover. Consiga que sus recursos de red de Wi-Fi, inalámbricos y de aplicaciones funcionen sin problemas.

Complicado

Implementaciones de autenticación multifactor con uso intensivo de recursos

La seguridad de las contraseñas es uno de los mayores desafíos que enfrentan las organizaciones hoy. Sorprendentemente **el 81% de las violaciones de datos fue provocado por contraseñas poco seguras o robadas**[4]. Por lo tanto, las empresas evalúan los productos de autenticación multifactor (MFA) en busca de capas adicionales de seguridad relacionadas con el acceso a recursos corporativos.

Lamentablemente, muchos productos de MFA han resultado difíciles de administrar para los equipos de TI. Las implementaciones tradicionales de MFA basadas en hardware consumen tiempo y recursos, lo que dificulta lograr un equilibrio entre la implementación y las prioridades existentes (sin mencionar las solicitudes de servicio entrantes). Además, muchas implementaciones de MFA requieren de compromisos de entrenamiento importantes por parte de su equipo de TI y personal dedicado a tareas similares, ya que una de las quejas más frecuentes respecto a las soluciones tradicionales es la facilidad de uso (o la falta de esta). **De hecho, el 24% de las empresas que no utiliza una solución de MFA destaca que las dificultades de implementación, mantenimiento y soporte son los factores que limitan la adopción**[5].



¿Sabía esto?

El **61%** de las empresas considera que la mayoría de las soluciones de MFA está diseñada para empresas más grandes que la suya.[6]

Simple

MFA basada en la nube:

Disfrute de una verificación de identidad fácil de usar y libre de hardware

¿Cuál es la solución? Una autenticación multifactor que no solo se implementa de manera sencilla y rentable, sino que es intuitiva y fácil de usar para todos los empleados, sin importar sus conocimientos técnicos. AuthPoint de WatchGuard ofrece autenticación multifactor (MFA) en una plataforma fácil de usar y basada en la nube. Debido a que está basada en la nube, no hay ningún hardware que implementar y el acceso se puede administrar desde cualquier lugar. La aplicación móvil permite que cada intento de inicio de sesión sea visible y sencillo para que los usuarios lo aprueben o rechacen. AuthPoint también ofrece numerosas integraciones con terceros, incluidas conocidas aplicaciones en la nube, servicios web, VPN y redes.

Simple

Delegación:

Asóciese con un MSSP (Proveedor de Servicios de Seguridad Administrada)

Todos los productos de WatchGuard están diseñados teniendo en mente la simplicidad para ayudarlo a recuperar tiempo del día. Sin embargo, si la administración de la seguridad de su empresa simplemente no es un tema para el que tiene espacio en su lista de tareas pendientes, trabajar con uno de nuestros proveedores de soluciones de TI puede quitarle por completo ese peso de encima. Un proveedor de soluciones de WatchGuard puede funcionar como una extensión de su empresa para cubrir cualquier brecha de seguridad del equipo de TI mediante sus ofertas de servicios administrados, como la implementación, el mantenimiento continuo y la generación de reportes, entre otras.

Conectarse con un MSSP no podría ser más fácil con la herramienta Buscador de partners de WatchGuard, disponible en el sitio web watchguard.com/findapartner. Busque por ubicación y, luego, filtre los resultados por distancia o especialización para encontrar el partner certificado por WatchGuard que mejor se ajuste a las necesidades de su empresa.

Conclusión

Si no cuenta con tiempo ni recursos, administrar la seguridad de TI de su organización puede parecer un objetivo inalcanzable. Por suerte, el diseño de las soluciones de WatchGuard se basa en la simplicidad, es decir, en la configuración, la implementación y administración continua. Su red es de por sí bastante compleja, su seguridad no tiene por qué serlo.

Seguridad de Red

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

Wi-Fi Seguro

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 adecuada para eliminar la brecha de seguridad basada en contraseñas que deja a las empresas vulnerables a los accesos no autorizados. Proporciona autenticación multifactor en una plataforma en la nube fácil de usar. Nuestro enfoque exclusivo 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.

Encuentre un Partner >

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. Casi 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, el Pacífico y Latinoamérica. Para obtener más información, visite WatchGuard.com.

[1] StationX, "Predicciones para 2019: Mayor escasez de personal capacitado en seguridad cibernética", enero de 2019
[2] APM Digest, "Esta es la razón por la que los equipos de TI invierten demasiado tiempo en la resolución de problemas de red", marzo de 2019
[3] Information Age, "La relación entre la cultura de Wi-Fi y BYOD", abril de 2017
[4] CSO, "Las contraseñas robadas provocan el 81% de las vulneraciones de datos", mayo de 2017
[5] WatchGuard, "Las contraseñas fallaron, ¿qué es lo que sigue?", mayo de 2018
[6] WatchGuard, "Las contraseñas fallaron, ¿qué es lo que sigue?", mayo de 2018

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