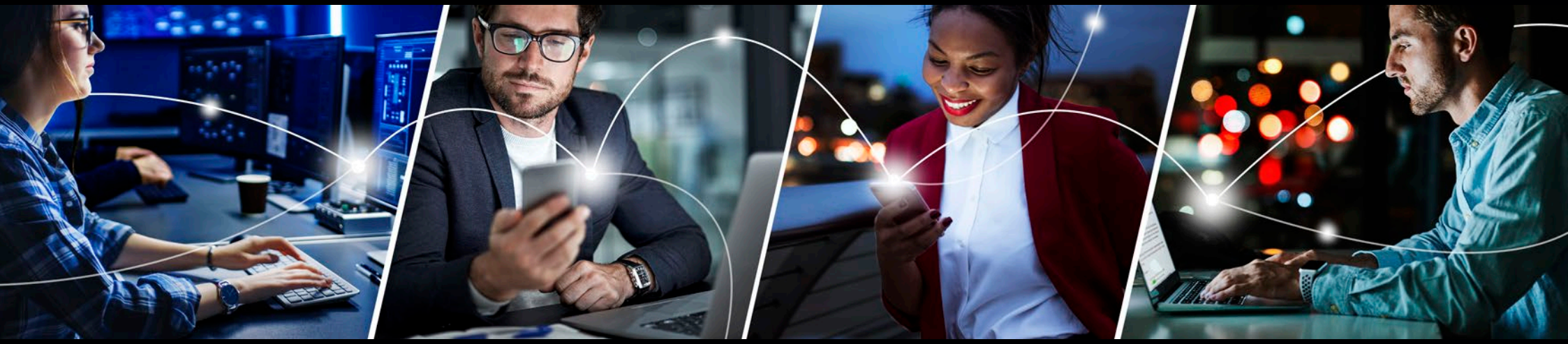
Seguridad Unificada para un mundo en **RECONEXIÓN**



Es hora de reconectarse

WatchGuard®

CUANDO LOS USUARIOS ESTÁN A UNA RED DE DISTANCIA, LAS AMENAZAS ESTÁN MÁS CERCA QUE NUNCA

Durante el distanciamiento social, nos adaptamos para buscar nuevas maneras de trabajar, colaborar y jugar. Tuvimos que reemplazar las charlas y las bromas de oficina por las comunicaciones digitales. En el proceso, nos distrajimos más a nivel digital.

Brindar acceso remoto a los recursos y datos corporativos para mantener la experiencia del usuario "en el sitio" es fundamental para la continuidad del negocio, pero hacerlo de manera segura puede ser una tarea abrumadora. Hay mucho en juego; un clic erróneo puede hacer que su empresa se detenga por completo.

Más que nunca, las empresas están repensando cómo los usuarios mantienen la conexión, la productividad Y la seguridad en el mundo remoto.

Desafíos para la continuidad del negocio:

- Las oficinas híbridas y el trabajo remoto son la nueva normalidad
- Se normalizó el uso de dispositivos personales para trabajar
- Las aplicaciones en la nube de acceso directo eluden las protecciones de red tradicionales

La seguridad cibernética es el principal desafío para la movilidad de los empleados.

PULSE

Los Desafíos de Proteger una Fuerza Laboral Distribuida

Distracción Digital

Un oficinista promedio recibe alrededor de 121 correos electrónicos por día[1], y las llamadas y reuniones que tiene por semana aumentaron un 55%[2]. La facilidad de trabajar desde casa también significa que es más probable que los empleados se conecten fuera del horario laboral. Según Pulse, alrededor del 60% de los líderes de TI afirman que desconectarse después del trabajo es el área que más dificultades presenta para los usuarios que trabajan de forma remota.

Equipos de TI Abrumados por la Nueva Realidad

La mayoría de los equipos de tecnología afirman que las solicitudes de soporte técnico aumentaron el 39% como resultado del trabajo remoto, con problemas con la VPN, las videoconferencias y el restablecimiento de contraseñas como la principal causa de dolores de cabeza.

Marcas en la Balanza

Las consecuencias de las vulnerabilidades de seguridad pueden causar un caos devastador en el buen nombre de una empresa, y es muy probable que algunas empresas nunca se recuperen. Un ataque exitoso puede bloquear sus sistemas, detener su empresa y evitar que brinde el nivel de servicio que sus clientes esperan.

Presupuestos de Seguridad Bajos

A pesar de ser una de las principales prioridades para los líderes de TI, más del 70% de las empresas invierten menos del 2% de las ganancias en seguridad cibernética[3]. Incluso con más personas que nunca trabajando de forma remota, más de la mitad de las empresas gastan menos de USD 1.000 por empleado en seguridad cibernética.

Expertos en Escasez

La falta de habilidades internas en seguridad cibernética es un gran problema, en especial, para las organizaciones pequeñas. Más del 76% de las empresas carecen del personal suficiente para cubrir las necesidades de seguridad cibernética. En promedio, una persona del equipo de TI solo permanece en la empresa durante tres años o menos, por lo que necesita que su equipo pueda progresar rápidamente para administrar la seguridad de manera efectiva.

Soluciones de Punto Desconectadas

Una empresa mediana promedio utiliza cuatro o más herramientas para la administración de vulnerabilidades, y el 79% de los líderes de TI admiten que se necesitan más de 48 horas para cerrar una vulnerabilidad[4]. Las soluciones de múltiples puntos sin integraciones no comparten contexto ni análisis para identificar indicadores de peligro. Cada producto de seguridad requiere su propia administración, entrenamiento, soporte y proceso operativo, los cuales administran equipos diferentes. Y, lo que es peor aún: el 41% de los líderes de TI indican que nunca o casi nunca tienen tiempo para mirar los registros de seguridad.

74% de todos los ataques de malware son incidentes de día cero

Más de **280%** de aumento en los ataques de suplantación de identidad contra los usuarios

76% de las empresas carecen del personal suficiente para satisfacer las necesidades de seguridad cibernética

41% de los líderes de TI sugieren que nunca o casi nunca tienen tiempo para mirar los registros de seguridad

79% de los líderes de TI admiten que se necesitan más de 48 horas para cerrar una vulnerabilidad.

[1] https://www.mckinsey.com/~/media/mckinsey/industries/technology%20media%20and%20telecommunications/high%20tech/our%20insights/the%20social%20economy/mgi_the_social_economy_full_report.pdf
[2] https://www.microsoft.com/en-us/microsoft-365/blog/2020/09/22/pulse-employees-wellbeing-six-months-pandemic/
[3] Pulse
[4] Pulse

Redefinición de la Conexión con Seguridad Centrada en el Usuario

Gracias al predominio del trabajo remoto, su empresa pasó de tener algunas oficinas con muchos empleados a tener casi la misma cantidad de oficinas que de empleados. Simplemente permitir el acceso con total libertad desde las redes del hogar a aplicaciones comerciales en la nube es un no rotundo a nivel de seguridad.

A continuación, se mencionan algunas de los vectores de ataque inicial más comunes a los que probablemente se enfrentará su empresa:

Vectores de Amenaza Inicial	Descripción de la Amenaza	Probabilidad de Ocurrencia	Impacto Potencial
Credenciales en peligro	Las credenciales se pueden robar, comprar, adivinar o encontrar en la dark web, en especial, si los hábitos de contraseñas de los usuarios son deficientes.	ALTA	MEDIANA
Suplantación de identidad e ingeniería social	A través de correos electrónicos, mensajes directos o incluso llamadas telefónicas, estos ataques apuntan a usuarios distraídos para extraer sus credenciales.	ALTA	ALTA
Vulnerabilidad en software de terceros	Los software sin parches de seguridad son un punto de entrada frecuente para los ataques cibernéticos que buscan aprovechar vulnerabilidades conocidas.	MEDIANA	ALTA
Correo electrónico empresarial en peligro	Los hackers intentarán apoderarse de todas las cuentas de correo electrónico para intensificar su ataque y dirigirse a otros objetivos.	BAJA	ALTA
Dispositivo perdido o robado	Cuando sus usuarios son remotos o itinerantes, sus dispositivos dejan de contar con la protección física que brinda la oficina. Un dispositivo de la empresa que se pierda puede funcionar como un gateway para los hackers que intentan ingresar a su red.	BAJA	MEDIANA

Según IBM, una vulneración en la que el trabajo remoto fue un factor cuesta USD 1,07 millones adicionales.

Reporte de 2021 sobre el Costo de la Vulneración de Datos de IBM

WatchGuard®

Reconectándose a la Red con Aceso Zero Trust

Las redes privadas virtuales (VPN), de forma aislada, asumen que todo lo que se conecta a través de su gateway de red es de confianza. Si bien este enfoque brinda una conexión segura y agrega una capa de seguridad a los protocolos y servicios menos seguros, también expone a la empresa a ataques que aprovechan a los usuarios remotos y sus dispositivos. Solo se necesita una contraseña en peligro o un dispositivo de endpoint para que esa conexión VPN se convierta en un punto de acceso para malhechores.

Con el modelo de "zero-trust ", término acuñado por primera vez en el 2010, se elimina este riesgo al adoptar el enfoque de "nunca confiar, siempre verificar" para dar acceso a los usuarios. El acceso a la red Zero-Trust establece políticas para el acceso de los usuarios en función del rol del empleado y el estado de seguridad del endpoint en base a los siguientes tres principios:

1

Siempre sepa quién y qué se conecta a la red empresarial.

Los criminales cibernéticos utilizan diferentes técnicas para robar nombres de usuarios y contraseñas. La suplantación de identidad, la suplantación dirigida de identidad y la ingeniería social son habituales. Las credenciales robadas se venden en la dark web. Las contraseñas ya no son suficientes. Si algo se debe proteger, necesita una autenticación multifactor.

2

Limite el acceso a sistemas críticos para la empresa en función de permisos bien definidos.

Con el modelo de Zero-Trust puede administrar de manera central el acceso a todos los sistemas comunes de TI y, a la vez, limitarlos a determinados usuarios, dispositivos o aplicaciones. Las decisiones de acceso suceden en tiempo real y se basan en las políticas que define la empresa y el contexto de la solicitud de acceso.

3

Supervise el estado y la posición de seguridad de la red y de todos los endpoints administrados.

Al estar en casa, es muy probable que los empleados utilicen las computadoras portátiles de la empresa para navegación personal en la Web y para revisar su correo electrónico. Hacer un seguimiento de las amenazas requiere de una seguridad continua y avanzada que va más allá del antivirus de endpoints tradicional.

Las contraseñas ya no son suficientes. Si algo se debe proteger, necesita **una autenticación multifactor.**

La Microsegmentación y el Zero-Trust

Las políticas de Zero-Trust abarcan la verificación y el cumplimiento de dispositivos, aplicaciones e identidades. Esto permite a los equipos de TI aplicar microsegmentación para limitar la oportunidad de amenazas internas, infiltraciones en la red y movimiento lateral. Al definir microsegmentos e implementar políticas personalizadas según las necesidades de seguridad de su empresa, se crea una jerarquía de protección para su entorno. Esto comienza con la identificación del usuario que tendrá acceso a las aplicaciones y los servicios.

Un microsegmento se puede construir en torno a una aplicación basada en la nube, como una solución de administración de las relaciones con el cliente (CMR). Los diferentes equipos de su empresa requieren diferentes niveles de acceso. Es probable que los equipos de ventas y de soporte técnico necesiten acceso a la CMR, pero ¿qué sucede con el equipo de ingeniería? Probablemente no lo necesiten.

Al utilizar este enfoque, puede aplicar controles granulares para limitar un mayor acceso. Para los equipos de soporte técnico ubicados en el centro, tiene sentido restringir el acceso a la CRM solo durante sus horas de trabajo o evitar que accedan al sistema cuando se conectan desde una nueva ubicación.

Evolución de la Red con SD-WAN

Antes de la pandemia, los equipos de tecnología desarrollaron redes para adaptarse a un uso más significativo de aplicaciones y entornos en la nube. Las soluciones de SD-WAN ayudaron a mejorar la productividad y la eficiencia de sus trabajadores con acceso rápido y directo a las aplicaciones en la nube, y priorizaron el rendimiento de la red para soportar la utilización de video y VoIP de alta calidad. Con la pandemia, los líderes de tecnología se vieron obligados a redefinir qué era importante al conectar a la empresa con los usuarios.

Si bien las aplicaciones en la nube continúan creciendo, las empresas de hoy lidian con cómo diseñar redes con el predominio de su fuerza de trabajo remota. Muchas arquitecturas basadas en la nube se diseñaron para que todo atraviese el perímetro de la red y, luego, lo abandone. Los usuarios, sin importar quiénes sean, deben interactuar con la red empresarial para salir al mundo exterior, a veces, con tecnología poco eficiente. Esto crea grandes desafíos en cuanto a la disponibilidad del servicio, el rendimiento y la productividad de los usuarios.

La experiencia del usuario debe ser una consideración primordial al permitir el trabajo remoto. Los usuarios deben poder acceder a sus aplicaciones sin experimentar demoras excesivas ni problemas de rendimiento. La SD-WAN controla sus conexiones WAN y utiliza estos datos para tomar decisiones de enrutamiento. Si una conexión de WAN se satura, distribuye el tráfico de red de manera automática según las políticas que usted defina. La SD-WAN también permite localizar la seguridad en las sucursales, por lo que el tráfico se inspecciona en línea, lo que mejora la eficiencia y ahorra un costoso ancho de banda.

Alcance de su Seguridad

Si solo lee los títulos, parecería que defender su empresa contra ataques requiere herramientas de seguridad costosas y de vanguardia que solo son sostenibles para equipos de seguridad cibernética muy capacitados y con muchos recursos. Si hace un análisis más profundo, verá que muchas de las vulneraciones que lee las noticias comenzaron con vulneraciones simples de usuarios, dispositivos y redes que se pueden prevenir con herramientas de seguridad estándar, siempre y cuando se implementen de manera adecuada.

Desde el perímetro al endpoint, diferentes herramientas abordan posibles debilidades y detectan vulnerabilidades. Los enfoques prácticos del modelo de Zero-Trust combinan autenticación, protección de endpoints y seguridad de red para limitar el daño potencial de un ataque contra un usuario.

En este libro electrónico, describimos cuatro niveles de implementación de seguridad centrada en el usuario de extremo a extremo que pueden ayudar a reducir de manera drástica la superficie de amenazas de empresas como la suya.

NIVEL 1

Bloquee amenazas conocidas y evite accesos no autorizados.

NIVEL 2

Controle el tráfico de la web, simplifique la autenticación y bloquee los intentos de suplantación de identidad.

NIVEL 3

Limite la exposición según el riesgo, responda a las amenazas avanzadas y examine el tráfico cifrado.

NIVEL 4

Adopte el enfoque de seguridad "nunca confiar, siempre verificar".

Muchas de las vulneraciones comienzan con el simple aprovechamiento de usuarios, dispositivos y redes que se puede evitar con herramientas de seguridad estándar.

Nivel 1: Bueno

Bloquee amenazas conocidas y evite accesos no autorizados.

Autenticación multifactor

Cuando un hacker puede utilizar una sola contraseña en peligro para eludir incluso la seguridad más sofisticada, las empresas deben hacer todo lo posible para mantener seguras las credenciales de los usuarios. Al requerir factores adicionales de autenticación, la autenticación multifactor disminuye la amenaza de las credenciales robadas y, al mismo tiempo, reduce los problemas de red y las vulneraciones de datos.

La autenticación multifactor mejora la autenticación del usuario al solicitar lo siguiente:

- Un dato (contraseña, PIN)
- Una posesión (token, teléfono móvil)
- Una parte del cuerpo (huella digital, rostro)

Protección de endpoint para empresas

Es probable que su empresa utilice una amplia gama de computadoras de escritorio, computadoras portátiles, dispositivos móviles y servidores que necesitan protección contra una serie de amenazas conocidas. La infección por malware en tan solo uno de estos endpoints puede causar grandes problemas y momentos sin conectividad en su empresa. Si bien las soluciones antivirus para los consumidores pueden brindar cierta protección, las organizaciones que se toman en serio su seguridad necesitan una solución de nivel empresarial.

Qué buscar:

- Una solución para todos sus dispositivos Windows, Linux, macOS y Android
- Protección y generación de reportes detallados y en tiempo real
- Un "congelador" de malware para aislar y recuperarse de malware si es necesario

Firewall de red, VPN y acceso remoto seguro

En el centro de su red, un firewall cumple una función fundamental en la seguridad general de su empresa. Con un firewall, puede analizar el tráfico de amenazas, facilitar las conexiones VPN y brindar acceso seguro a las aplicaciones web de terceros, a las aplicaciones internas y a los servicios de Microsoft Exchange, así como también proteger las sesiones de RDP y SSH para recursos locales.

Qué buscar:

- VPN
- SD-WAN
- Acceso Remoto

Las contraseñas robadas o adivinadas causaron el 89% de las vulnerabilidades en aplicaciones web en el 2020 y el 61% de todas las vulnerabilidades aprovecharon credenciales.

Reporte de 2021 sobre la Vulneración de Datos de Verizon

WatchGuard®

Nivel 2: Mejor

Controle el tráfico de la web, simplifique la autenticación y bloquee los intentos de suplantación de identidad.

Autenticación push

La autenticación multifactor ha recorrido un largo camino desde cuando se usaban los torpes tokens de contraseña de un solo uso. Las soluciones de autenticación push brindan un mejor equilibrio entre la seguridad y la experiencia del usuario, ya que eliminan la necesidad de un token de hardware, al tiempo que mejoran la seguridad y la visibilidad. Si todo el mundo tiene un teléfono inteligente, ¿por qué le pediría a sus usuarios que lleven un token de hardware? Los usuarios pueden solo presionar para aceptar o rechazar en el dispositivo que quieran.

Qué buscar:

- Muestra el contexto de la autenticación: a qué se accede y desde dónde
- Reduce las posibilidades de ingeniería social
- No es posible copiar o robar la contraseña de un solo uso (OTP) incrustada en la respuesta push

Protección contra la suplantación de identidad y filtrado de DNS

Los usuarios son un objetivo principal para la suplantación de identidad, en especial, cuando se conectan de forma remota. Las soluciones de detección de nivel de DNS identifican de forma proactiva las solicitudes de DNS maliciosas asociadas con los ataques de suplantación de identidad, lo que proporciona una capa adicional de seguridad para bloquear las conexiones con los malhechores. El filtrado de DNS también puede eliminar las conexiones de comando y control, lo que corta la línea de comunicación entre el atacante y su malware.

Qué buscar:

- Protege de forma automática a los usuarios finales de ataques de suplantación de identidad y conexiones C2
- Seguridad ligera y siempre activa; no se necesita VPN
- Habilidades de filtrado de contenido para limitar el acceso a áreas riesgosas de la Web

Filtrado de contenido y gateway antivirus

Los firewalls brindan una amplia protección contra intrusiones y malware para todos los dispositivos conectados a su red. También pueden aplicar la política de la web al utilizar herramientas de filtrado web para bloquear contenido inapropiado, conservar el ancho de banda de la red y preservar la productividad de los empleados.

Qué buscar:

- Identifica y bloquea spyware, virus, troyanos, gusanos informáticos, rogueware y amenazas combinadas conocidas
- Bloquea de manera automática sitios maliciosos conocidos en base a la política
- Varias fuentes en tiempo real para proteger contra botnets y sitios maliciosos


El 77% de las vulneraciones de datos de cuentas en la nube se deben a credenciales robadas o hackeadas.
Reporte de 2020 sobre las Investigaciones de Vulneración de Datos de Verizon
WatchGuard

Nivel 3: Sobresaliente

Limite la exposición según el riesgo, responda a las amenazas avanzadas y examine el tráfico cifrado.

Autenticación basada en riesgos

Si no cuenta con políticas de riesgos, la empresa deberá activar el método de autenticación más seguro para todos los usuarios en todo momento, lo que posiblemente ocasione el desacuerdo de los usuarios en algunas áreas. La autenticación de riesgos es una forma de modernizar su estrategia usando la cantidad precisa de seguridad con protección contra riesgos personalizada, lo que mejora la capacidad de detectar amenazas y responder a ellas.

Qué buscar:

- Reglas que se basan en la ubicación de la red: mejor experiencia para los usuarios en redes protegidas
- Reglas que se basan en la geolocalización: la ubicación en computadoras y teléfonos móviles puede ayudar a mitigar los problemas de privacidad y seguridad
- Reglas que se basan en el tiempo: la mayoría de los ataques se realizan cuando todos duermen

Detección y respuesta en endpoints

Lamentablemente, los ataques de día cero, el ransomware, el criptojacking y las amenazas avanzadas cada vez más tienen como objetivo empresas más pequeñas. Esta clase de ataques pueden eludir la mayoría de las soluciones antivirus tradicionales. Sin una visibilidad completa de los endpoints y los servidores, es posible que no detecte una amenaza activa. Las soluciones de detección y respuesta en endpoints controlan si los endpoints tienen actividad maliciosa y pueden detectar y responder de manera automática a ataques dirigidos y vulnerabilidades en la memoria.

Qué buscar:

- Seguridad contra amenazas avanzadas desconocidas: detecta y bloquea malware, troyanos, suplantación de identidad y ransomware
- Seguridad para todos los vectores de ataque: navegadores, correo electrónico, sistemas de archivos y dispositivos externos conectados a endpoints
- Protección para dispositivos Windows, Linux, macOS y Android

Inspección de tráfico cifrado y antimalware avanzado

Hoy es habitual que los hackers escondan amenazas en el tráfico cifrado. En la actualidad, el malware que llega a través de conexiones cifradas con TLS como HTTPS representa más del 40% de las detecciones generales en la red, y las intrusiones están en aumento. La capacidad de controlar este tráfico ahora es un requisito fundamental para cualquier firewall. Las herramientas avanzadas, como el sandboxing en la nube y el antimalware con tecnología de IA, pueden ayudar a exponer incluso las amenazas más avanzadas que se esconden en el tráfico cifrado.

Qué buscar:

- Inspección HTTPS de alto rendimiento con TODOS los servicios de seguridad activos
- Inspección completa del tráfico TLS 1.3
- Inteligencia artificial y aprendizaje automático que brindan protección predictiva contra amenazas


Más del 60% de los ataques cibernéticos
que se detectan actualmente en la red
se esconden en tráfico cifrado.
Reporte de 2021 sobre la Seguridad en Internet del Primer Trimestre de WatchGuard
WatchGuard

Nivel 4: Zero-Trust

Adopte el enfoque de seguridad “nunca confiar, siempre verificar”.

Autenticación de Zero-Trust

Si no cuenta con políticas de riesgos, la empresa deberá activar el método de autenticación más seguro para todos los usuarios en todo momento. Para algunos usuarios, esto es innecesariamente engorroso. La autenticación de riesgos es una forma de modernizar su estrategia usando la cantidad precisa de seguridad con protección contra riesgos personalizada, lo que mejora la capacidad de detectar amenazas y responder a ellas.

Qué buscar:

- Diferentes métodos de autenticación en base a las diferentes ubicaciones y redes
- Aplicaciones de geovalla/geofence, lo que reduce la exposición

Control de aplicaciones de Threat Hunting y denegación predeterminada

Las amenazas pueden durar cientos de días. Reducir el tiempo de detección es fundamental para minimizar el impacto de un ataque cibernético. El control continuo del comportamiento de los endpoints para los indicadores de ataque (IoA) ayuda a evitar malware avanzado, mantenerse al tanto del software oculto y descubrir hackers y amenazas internas. Además, es posible adoptar un enfoque de denegación predeterminada para la protección de endpoints al limitar la ejecución solo a las aplicaciones que se sabe que son seguras.

Qué buscar:

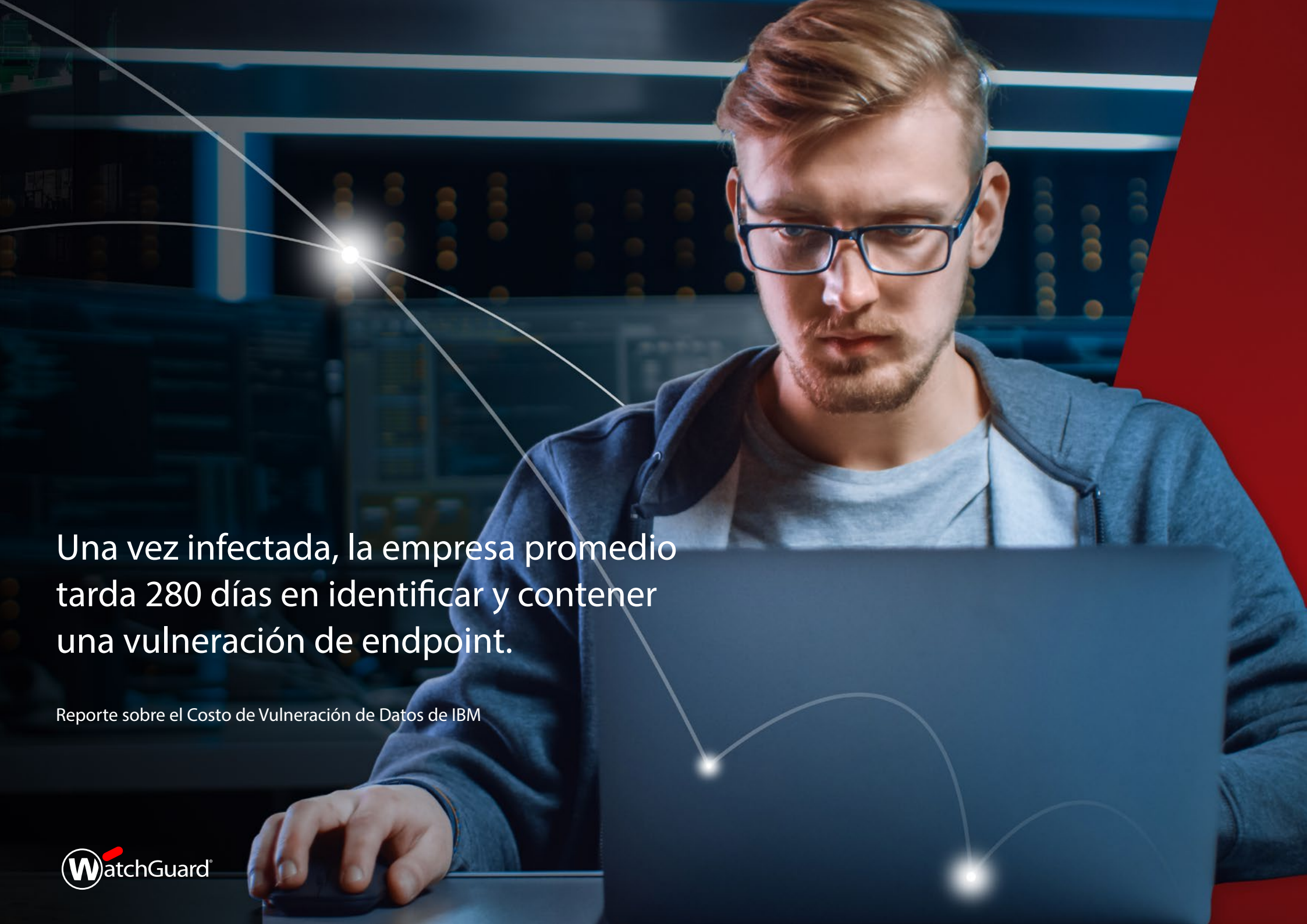
- Clasificación basada en IA de procesos de endpoints como malware o de confianza
- Investigación automática de indicadores de ataque para encontrar técnicas de evasión y compromiso
- Entrega rápida de nuevos IoA para proteger los endpoints contra más ataques

Secure Wi-Fi, correlación de amenazas y valoración universal

Los firewalls poseen las condiciones para brindar amplia protección contra intrusiones y malware para todos los dispositivos conectados a su red. También pueden aplicar la política de la web al utilizar herramientas de filtrado web para bloquear contenido inapropiado, conservar el ancho de banda de la red y preservar la productividad de los empleados.

Qué buscar:

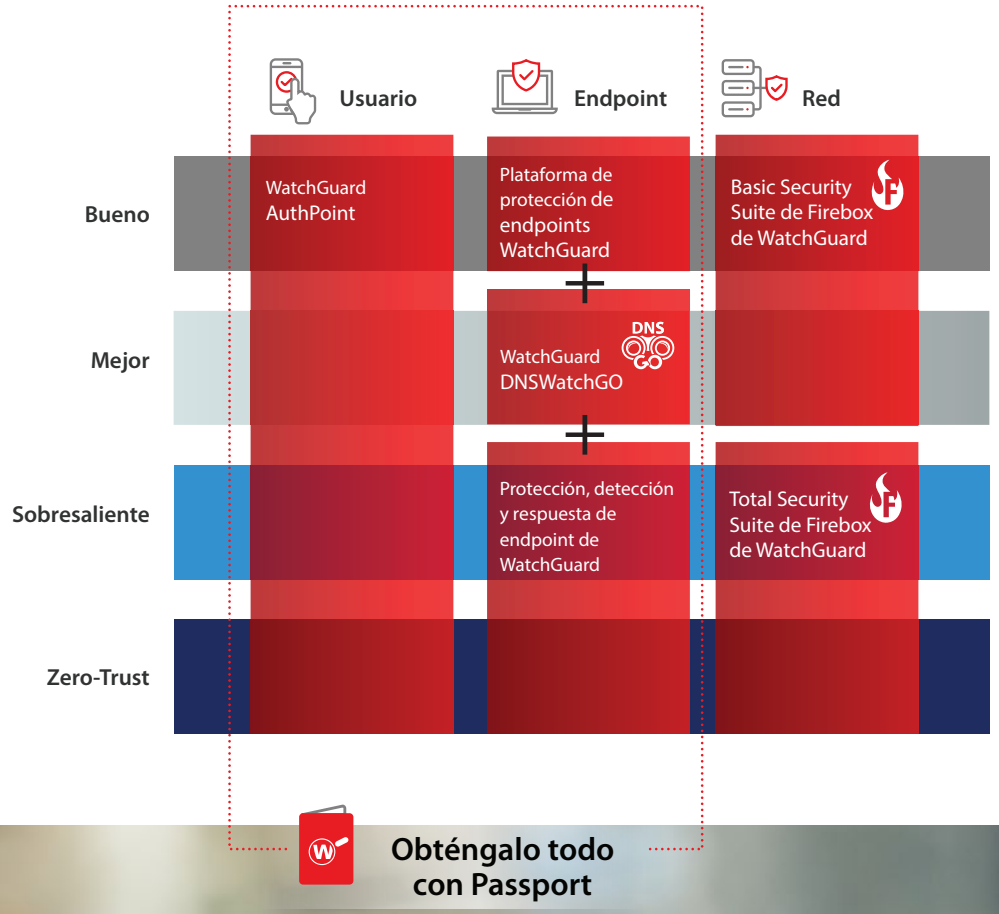
- Identifica y bloquea spyware, virus, troyanos, gusanos informáticos, rogueware y amenazas combinadas conocidas
- Bloqueo automático de sitios maliciosos conocidos en base a la política
- Varias fuentes en tiempo real para protegerse de botnets y sitios maliciosos


Una vez infectada, la empresa promedio tarda 280 días en identificar y contener una vulneración de endpoint.
Reporte sobre el Costo de Vulneración de Datos de IBM
WatchGuard

WatchGuard Tiene lo que Necesita

Durante más de 20 años, WatchGuard ha sido líder en tecnología de seguridad cibernética de avanzada y ofreció esa tecnología en soluciones fáciles de implementar y administrar. Con productos y servicios líderes en la industria de seguridad de redes y endpoint, Secure Wi-Fi, autenticación multifactor e inteligencia de red, WatchGuard permite que más de 250.000 empresas pequeñas y medianas de todo el mundo protejan sus activos más importantes. Hoy en día, WatchGuard protege miles de redes empresariales y más de 10 millones de usuarios confían en WatchGuard Technology para mantenerlos seguros mientras trabajan de forma remota.

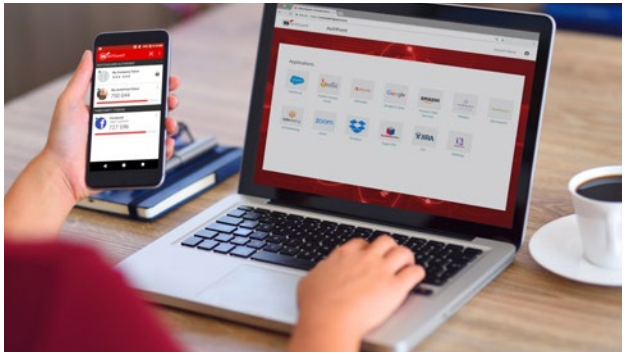
Nuestro portafolio de seguridad único y centrado en el usuario aborda las vulnerabilidades de seguridad críticas en redes, usuarios, endpoints y aplicaciones.



WatchGuard Tiene lo que Necesita

Proteja a sus usuarios

En WatchGuard, creemos que el panorama de amenazas requiere que todas las empresas implementen una autenticación multifactor (MFA) como una mejor práctica, y lo hacemos simple. AuthPoint de WatchGuard es una solución de MFA con todas las funciones que deja atrás la autenticación de 2 factores tradicional (2FA) gracias a la incorporación de maneras innovadoras de identificación de usuarios. AuthPoint se entrega por completo desde la nube para una configuración y administración sencillas. La autenticación basada en riesgos está integrada en la plataforma, lo que le permite crear reglas exclusivas para la estructura de seguridad existente en su organización.

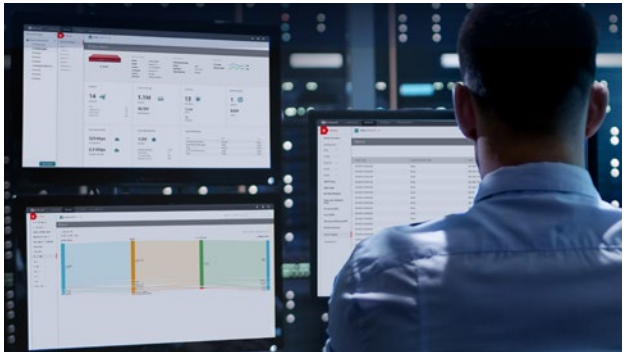


Proteja sus dispositivos

Con muchas vulnerabilidades para aprovechar y versiones de software obsoletas, a menudo, los dispositivos de endpoint están en Internet sin protección de la seguridad del perímetro empresarial, lo que los convierte en el objetivo favorito de los criminales cibernéticos. La plataforma de seguridad para endpoints de WatchGuard ofrece la máxima protección y una complejidad mínima con enfoques avanzados de plataforma de protección de terminales (EPP) y detección y respuesta de endpoints (EDR). Nuestra oferta única de Servicio de Zero-Trust de aplicaciones y Servicio de Threat Hunting (incluida en la EDR) permite detectar hackers y amenazas internas y evita que las aplicaciones maliciosas se ejecuten en un endpoint administrado.

Proteja sus entornos

WatchGuard ofrece un premiado portafolio de servicios de seguridad de red que incluye desde servicios de prevención de intrusiones, gateway antivirus, control de aplicaciones, bloqueo de correo no deseado y filtrado web hasta servicios más avanzados de protección contra malware avanzado, ransomware y robo de datos. WatchGuard Firebox es una plataforma de seguridad de red integral y avanzada que pone a los profesionales de seguridad de TI nuevamente a cargo de sus redes. Cada año, la plataforma WatchGuard Firebox promedio bloquea más de 1.300 ataques de malware y 250 intrusiones para clientes de WatchGuard.



Simplifique con Seguridad Unificada

Las soluciones dispares no solo son difíciles de administrar, sino que también hacen que la identificación de amenazas y vulnerabilidades sea casi imposible. Con Unified Security Platform™ de WatchGuard, las empresas mejoran y amplían su seguridad y, al mismo tiempo, reducen los gastos generales y simplifican la mitigación de riesgos con enfoques de seguridad centrados en el usuario.

No Solo *Consolidada*; Seguridad *Unificada*

Unified Security Platform es una verdadera fuerza multiplicadora para los equipos de TI. Esta plataforma hace posible la facilidad operativa, ya que integra tecnologías avanzadas por lo general desconectadas para permitir una seguridad integral de múltiples capas en la red, los usuarios, los hosts y las aplicaciones.

> La falta de una estrategia unificada de seguridad cibernética es la razón principal por la que las organizaciones son víctimas de ataques de ransomware.
>
> PULSE

Transparencia y Control

WatchGuard Cloud es la interfaz de visibilidad y reportes de administración centralizada para toda Unified Security Platform, lo que brinda a los equipos de tecnología un panel único para la administración de seguridad de extremo a extremo de toda la pila de seguridad de WatchGuard.

Seguridad Integral

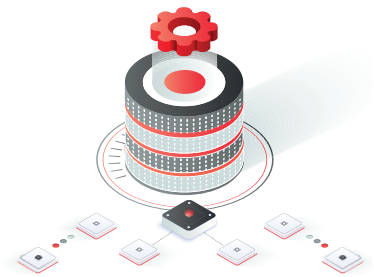
El portafolio integral de WatchGuard rompe la Cyber Kill Chain® en cada nivel. Detenga los intentos de encontrar y vulnerar sistemas desprotegidos, suplantación de identidad, ransomware, intrusiones, malware avanzado en todos sus usuarios, entornos y dispositivos.

Conocimiento Compartido

Sin importar cuán avanzada sea la tecnología, la implementación de capas de seguridad de forma aislada arriesga la posibilidad de no atrapar a un atacante. Con correlación y un framework de identidad sólido que se brinda desde una única plataforma, puede cerrar las brechas en la visibilidad y revelar los problemas de seguridad.

Armonización Operativa

Seguridad que funciona para su empresa con tres opciones de compra clave para partners, que incluyen prepago a plazo fijo, pago por uso a plazo fijo y pago por uso sin compromiso. Integre WatchGuard de manera sencilla a su ecosistema con API RESTful en toda la plataforma.



Automatización

La automatización es la clave de Unified Security Platform de WatchGuard, lo que acelera los procesos, elimina las amenazas y permite a los equipos de TI hacer más tareas en menos tiempo. El Núcleo de Automatización de WatchGuard crea un bucle de retroalimentación de seguridad sin intervención y acelera la administración de seguridad con fines empresariales.

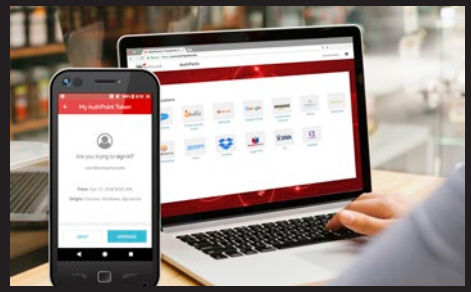
Portafolio de WatchGuard

Seguridad de Red

Las soluciones de Seguridad de Red de WatchGuard están diseñadas desde el inicio para ser fáciles de implementar, usar y administrar, además de brindar la mayor seguridad posible. Nuestra propuesta única para la seguridad de redes se concentra en brindar la mejor seguridad de tipo empresarial de su clase a cualquier organización, independientemente del tamaño o la capacidad técnica.

Secure Wi-Fi

La solución Secure Wi-Fi de WatchGuard, una verdadera innovación en el mercado actual, está diseñada para brindar 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 empresarial, y proporciona la ventaja competitiva que su empresa necesita para tener éxito.



Autenticación Multifactor

WatchGuard AuthPoint® es la solución correcta para abordar la brecha de seguridad basada en contraseñas 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.

Seguridad de Endpoints

La Seguridad de Endpoints de WatchGuard es un portafolio avanzado de seguridad de endpoints en la nube, que protege a las empresas contra cualquier tipo de ataque cibernético presente y futuro. Su principal solución, WatchGuard EPDR, impulsada por la inteligencia artificial, mejora de inmediato la posición de seguridad de las organizaciones. Combina las capacidades de protección de endpoints (EPP) y detección y respuesta de endpoints (EDR) con los servicios de aplicación de Zero-Trust y de búsqueda de amenazas.

Acerca de WatchGuard

WatchGuard® Technologies, Inc. es un líder mundial en seguridad de red, seguridad de endpoint, Wi-Fi seguro, autenticación multifactor y servicios de inteligencia de red. Más de 18.000 revendedores de seguridad y proveedores de servicios de todo el mundo confían en los productos y los premiados servicios de la empresa para proteger a más de 250.000 clientes. La misión de WatchGuard es lograr que empresas de todos los tipos y tamaños accedan de manera sencilla a una seguridad de calidad empresarial. Por ello, WatchGuard es una solución ideal para medianas empresas y también para empresas distribuidas. La empresa tiene su oficina central en Seattle, Washington, y posee oficinas en Norteamérica, Europa, Asia-Pacífico y Latinoamérica.

VENTAS EN NORTEAMÉRICA 1.800.734.9905 VENTAS INTERNACIONALES 1.206.613.0895 SITIO WEB www.watchguard.com

N.º de pieza WGCE67514_110421