Implementación de Redes de Confianza Cero en la Era del COVID-19

WatchGuard®

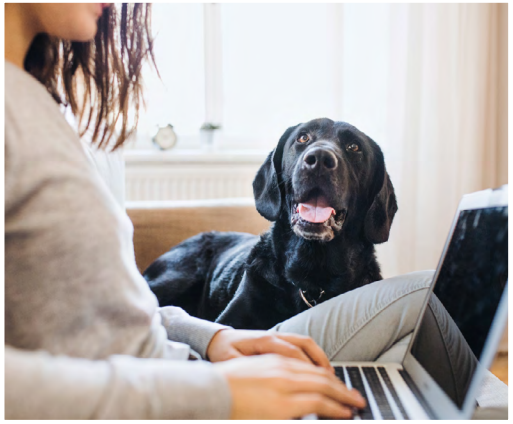
Índice

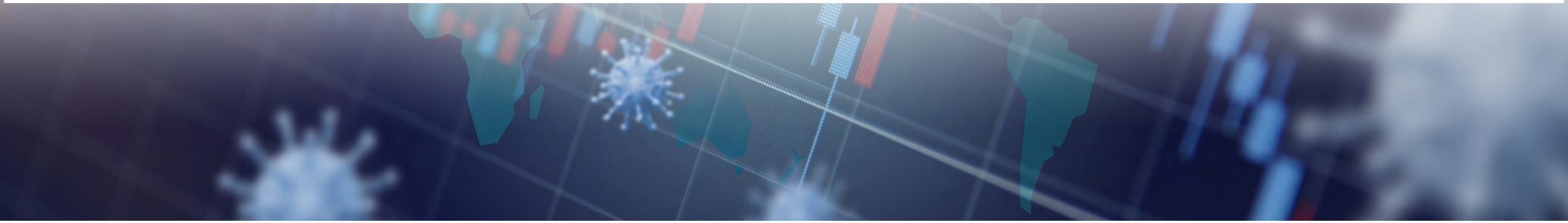
INTRODUCCIÓN

La pandemia de coronavirus ha puesto de manifiesto las deficiencias de la continuidad empresarial en muchas organizaciones y ha enfatizado la lentitud del progreso de la transformación digital. A medida que las aguas vuelven a su cauce, muchas empresas se encuentran en un período de intensa racionalización, trabajando para continuar con sus operaciones a corto o mediano plazo y luchando por evaluar qué camino deben seguir. Esto representa un desafío aún mayor, ya que deben considerar cómo proteger a sus empleados, sus datos y sus aplicaciones a distancia durante un período prolongado y, tal vez, para siempre.

Esta nueva realidad requiere una desviación del modelo de seguridad tradicional centrado en la red que asume que se debe confiar en todos los dispositivos y usuarios de la red. Con la mayor parte de los usuarios finales trabajando ahora de forma remota, la adopción de enfoques de seguridad de confianza cero se ha acelerado, especialmente en la empresa. Sin embargo, es comprensible que las empresas en crecimiento, que a menudo carecen de experiencia en seguridad interna, hayan tenido que hacer un gran esfuerzo para mantener el ritmo.

En este libro electrónico, exploraremos cómo la dinámica del COVID-19 ha tenido una incidencia en la seguridad, describiremos la importancia de un enfoque de confianza cero y discutiremos cómo WatchGuard puede ayudar a su empresa a brindar la seguridad que necesita durante estos tiempos difíciles.





EL TRABAJO REMOTO ESTÁ ACELERANDO LAS INFRACCIONES DE SEGURIDAD

Con todo lo que cambió como resultado del COVID-19, algunas cosas se mantuvieron igual, ya que la amenaza a las empresas que plantean los ciberataques continuó sin cesar. Lamentablemente, mientras algunas empresas se enfocaron en el modo "sobrevivir para prosperar", los ciberdelincuentes aprovecharon la oportunidad para identificar vulnerabilidades y objetivos principales:

- Se dispararon los ataques de suplantación de identidad a causa de decenas de dominios maliciosos que aparecen todos los días y se aprovechan de la ansiedad que causa el coronavirus. En el punto álgido de la crisis, Microsoft informó que se estaban produciendo 70.000 ataques temáticos a diario relacionados con el COVID-19 solo en EE. UU.[1] Muchas de estas campañas utilizaban kits de suplantación de identidad conocidos, simplemente readaptados para ese momento.[2]

- A medida que las plataformas de videoconferencia, como ZOOM, se dispararon de 10 millones de usuarios simultáneos a más de 200 millones, el programa CISA (Certified Information Systems Auditor, Auditor Certificado de Sistemas de Información) emitió una advertencia sobre los ciberactores malintencionados que buscaban sacar provecho del mayor uso de plataformas de comunicación populares enviando correos electrónicos de suplantación que incluían archivos maliciosos.[3]

- Tan solo durante las primeras semanas de la crisis, los investigadores de seguridad notaron un aumento del 41% en la cantidad de dispositivos que exponían el protocolo de escritorio remoto (RDP) a Internet utilizando el puerto altamente vulnerable TCP 3389 predeterminado de RDP.[4]

- Los sitios web falsos, que parecían ofrecer clientes VPN legítimos y prometían proteger a las personas, engañaron a los usuarios para que descargaran e instalaran malware en sus computadoras.[5]

- En un momento en el que los edificios están llenos de personas que trabajan desde su casa, los vecinos malintencionados podrían aprovechar el hecho de que el Wi-Fi representa casi el 50% de todo el tráfico IP.[6]

1 https://www.microsoft.com/security/blog/2020/06/16/exploiting-a-crisis-how-cybercriminals-behaved-during-the-outbreak/
2 https://threatpost.com/covid-19-scam-scramble-cybercrooks-recycle/154383/
3 https://us-cert.cisa.gov/ncas/alerts/aa20-099a
4 https://www.bankinfosecurity.com/covid-19-driving-surge-in-unsafe-remote-connectivity-a-14035
5 https://www.cybereason.com/blog/just-because-youre-home-doesnt-mean-youre-safe
6 https://www.rehmann.com/resources-insights/business-wisdom-2/item/2740-it-leadership-8-remote-workforce-tips-for-optimal-access-security-and-productivity

LA EXTENSIÓN DE LA PROTECCIÓN DE LA VPN NO ES SUFICIENTE

El uso de las VPN ha aumentado vertiginosamente, y los investigadores han observado un incremento del 50% en el tráfico de red en solo una semana. Solamente en Estados Unidos, se espera que el uso de VPN aumente un 150% en tan solo un mes. La migración repentina de los usuarios de la oficina al hogar ha hecho que muchas empresas deban ingeniárselas para ofrecer licencias de VPN a sus empleados. El riesgo es que, sin conectividad de VPN, los usuarios no tendrán acceso a los recursos que necesitan o utilizarán conexiones inseguras para acceder a ellos.

Estos usuarios no solo necesitan seguridad ahora que están fuera de la red, sino que además es importante que nos aseguremos de que no permitan el ingreso de malware y otras amenazas cuando se vuelvan a conectar a la red, ya sea a través de VPN o al volver a la oficina. Si bien extender las protecciones de la red a través de VPN puede proporcionar un alto grado de seguridad, la naturaleza del ciberdelito actual implica exigencias aún mayores.

Cuando se usa una VPN de forma aislada, se otorga una enorme cantidad de confianza al endpoint, lo que podría dar como resultado la propagación del malware a la red en general. Las empresas tienen que comprender que sus empleados son ahora la primera línea de defensa de facto contra las amenazas cibernéticas.

Por esta razón, los equipos de TI deben comenzar a tratar las redes domésticas de los empleados como si fueran la versión digital del salvaje Oeste, por los siguientes motivos:

- Solo se necesita un único endpoint comprometido o una credencial robada para infiltrarse en su entorno.
- Casi dos tercios de las amenazas se esconden en el tráfico cifrado.
- Algunos ataques son altamente dirigidos, mientras que otros afectan a objetivos de oportunidad. Es necesario tener protecciones contra ambos tipos de amenazas.
- Ahora, los usuarios son la primera línea de defensa y deben recibir ayuda para identificar, evitar y denunciar amenazas.

El uso de las VPN ha aumentado vertiginosamente, **con un incremento del 50% en el tráfico de red en solo una semana**. Solo en Estados Unidos, se espera que **aumente el uso de VPN un 150% en un mes.**

IMPLEMENTACIÓN DE REDES DE CONFIANZA CERO

¿Tiene un marco de seguridad que se enfoca en evitar vulneraciones eliminando la confianza indebida? Mientras una red tradicional se basa en la idea de la confianza inherente, un marco de confianza cero supone que cada dispositivo y cada usuario, dentro o fuera de la red, representan un riesgo de seguridad. Conceptualmente, la confianza cero se puede considerar como un enfoque de seguridad del tipo "nunca confiar, verificar siempre", que utiliza múltiples niveles de protección para prevenir amenazas, bloquear el movimiento lateral y hacer cumplir controles pormenorizados de acceso de usuarios.

El marco de confianza cero se basa en tres principios:

1. Identificación de usuarios y dispositivos: Sepa siempre quién y qué se conecta a la red empresarial.

Mientras las empresas luchan por conseguir que la mayor parte de su personal pueda trabajar de manera remota, garantizar el acceso a las herramientas internas es un enorme desafío. Al mismo tiempo, los ciberdelincuentes están utilizando una variedad de técnicas para adquirir nombres de usuario y contraseñas, como suplantación dirigida de identidad (spear phishing), ingeniería social y compra de credenciales robadas en la dark web, para obtener acceso a la red y luego robar datos valiosos de la empresa y los clientes. Los servicios de autenticación multifactor (MFA) basados en la nube ofrecen mitigación contra el robo de credenciales, el fraude y los ataques de suplantación de identidad.

2. Proporcionar acceso seguro: Limite los permisos de acceso de los dispositivos a los sistemas y aplicaciones críticos para la empresa.

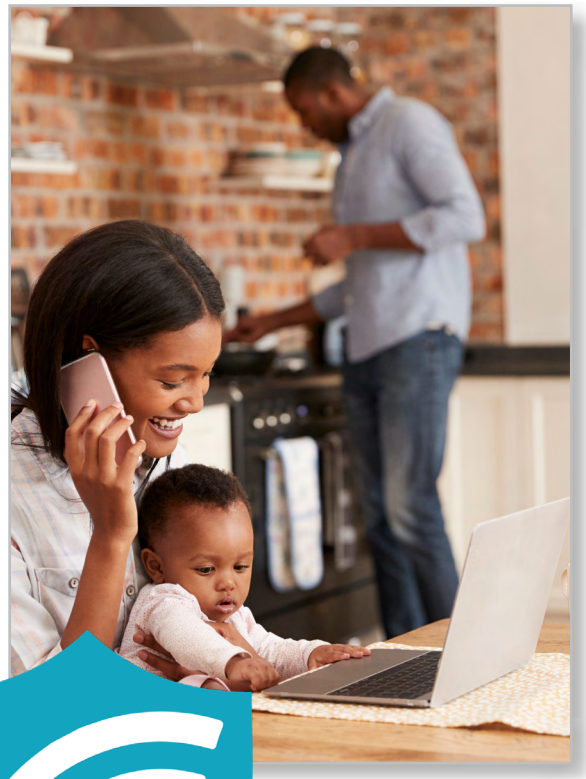
En el marco de confianza cero, el objetivo de la administración de acceso es proporcionar un medio para administrar de manera centralizada el acceso a todos los sistemas de TI comunes y, al mismo tiempo, limitar ese acceso solamente a usuarios, dispositivos o aplicaciones específicos. Las decisiones de acceso deben tomarse en tiempo real con base en las políticas definidas por la empresa y el contexto de la solicitud de acceso. Las tecnologías single sign-on (SSO), combinadas con la MFA, pueden mejorar la seguridad del acceso y minimizar la carga de contraseñas para los usuarios.

3. Supervisión continua: Supervise la situación de salud y seguridad de la red y todos los endpoints administrados.

Como resultado del coronavirus, las amenazas de malware y ransomware han aumentado significativamente. Además, el riesgo de infección nunca ha sido más alto, debido a que, al trabajar desde sus casas, los usuarios ya no cuentan con los beneficios de la protección de un firewall. Por si esto fuera poco, proteger a los usuarios cuando navegan por Internet es más difícil cuando se conectan fuera de su red.

Con los empleados encerrados en casa, lo más probable es que las computadoras portátiles de la empresa se utilicen en gran medida para navegación personal de la web y para ver el correo electrónico. Mantenerse al tanto de las amenazas requiere seguridad avanzada y persistente que va más allá de los antivirus tradicionales.

CÓMO CREAR UN ENTORNO INALÁMBRICO CONFIABLE (TWE)



El trabajo remoto puede generar preocupaciones de seguridad relacionadas con el Wi-Fi también. Mientras las ubicaciones de todo el mundo que fueron cerradas debido a la pandemia del COVID-19 consideran su plan de reapertura, los administradores de red se están preparando para una sobrecarga de trabajo a medida que las personas regresen a las oficinas. ¿Quién sabe qué ransomware podría haberse instalado en sus computadoras portátiles corporativas mientras usaban la red Wi-Fi de su hogar?

Con un entorno inalámbrico de confianza, usted puede:

- Automatizar la detección y el análisis de la causa raíz de fallas y anomalías.
- Detectar automáticamente y en tiempo real si los clientes de Wi-Fi no se conectan e identificar la causa raíz (ya sea que esté relacionada con el Wi-Fi, con el servicio de red o con un dispositivo o aplicación cliente).
- Importar fácilmente archivos de imágenes estándar de los planos de planta correspondientes a cada ubicación. Una vez agregados, con un clic con el botón derecho sobre el punto de acceso, se obtienen todas las funcionalidades de administración y resolución de problemas para cada PA. Los mapas de calor muestran la cobertura de punto de acceso, la velocidad de enlace y la cobertura de canal.

¿Vuelve a la Oficina? El Wi-Fi Puede Contribuir al Distanciamiento Social

Promueva un ambiente de trabajo seguro con monitoreo automatizado del distanciamiento social a través de la administración de Wi-Fi en la nube. Los puntos de acceso Wi-Fi pueden proporcionar mediciones en tiempo real de volúmenes de personas, alertas y notificaciones si se alcanzan o superan los límites de capacidad.

Con la supervisión de multitudes basada en Wi-Fi, las organizaciones pueden:

- Gestionar reuniones de empleados y flujos de reuniones.
- Analizar los visitantes que llegan y se van, incluido el movimiento.
- Certificar el cumplimiento de las restricciones sanitarias y de multitudes.
- Mejorar las operaciones comerciales, la planificación, el impacto económico y la valoración de activos con datos prácticos.

  Realizar las tareas de supervisión de manera totalmente anónima y privada, y en cumplimiento con el RGPD.

GUÍA DE CONFIANZA CERO DE SEGURIDAD DE WATCHGUARD

La adopción de una estrategia de confianza cero puede ayudar a su organización a desarrollar un enfoque más moderno de la ciberseguridad. La buena noticia es que no tiene que hacer esto solo. Ya sea que su Departamento de TI sea demasiado pequeño o que su empresa no tenga personal de TI, los proveedores de servicios administrados brindan el poder que las empresas necesitan para contar con una infraestructura sólida que permita a los usuarios móviles trabajar desde cualquier dispositivo y en cualquier lugar, y brinde acceso a servicios públicos en la nube garantizando al mismo tiempo la seguridad del negocio.

Cómo Ofrece WatchGuard Seguridad de Confianza Cero

1. Protección de la identidad del usuario y del dispositivo especialmente adecuada para entornos de confianza cero:

- **100% Administrado en la Nube.** WatchGuard Cloud le permite administrar y realizar informes de seguridad desde una única plataforma poderosa. Ya sea que desee reducir o eliminar los costos de infraestructura, acelerar su configuración, implementar sitios remotos a cualquier escala, simplificar sus herramientas de administración de seguridad u obtener una mayor visibilidad de su red, WatchGuard Cloud puede ayudarlo.
- **ADN Móvil.** Los agentes de amenazas sofisticados han demostrado tener la capacidad de clonar dispositivos móviles y utilizar el nuevo teléfono imitado para autenticarse en los sistemas como un medio para vulnerar la MFA. La característica de ADN Móvil, que es exclusiva de WatchGuard, toma una huella digital de las características particulares de cada dispositivo móvil. Cada vez que un usuario inicie sesión, la aplicación AuthPoint recreará este ADN móvil y lo incluirá en un cálculo de contraseña de un solo uso (OTP), asegurando que solo el dispositivo original pueda realizar la autenticación.
- **Integraciones de Terceros.** El ecosistema de WatchGuard incluye una gran cantidad de integraciones de terceros con AuthPoint. Esto permite a las empresas exigir que los usuarios se sometan al proceso de autenticación antes de acceder a aplicaciones sensibles en la nube, VPN y redes. Además, AuthPoint admite el estándar SAML, lo cual permite a los usuarios iniciar sesión una sola vez para acceder a una amplia variedad de aplicaciones y servicios.

2. Acceso seguro simplificado en todos los frentes:

- **Integración de AuthPoint con las Principales Plataformas de Identidad y Acceso (IAM).** Las empresas están implementando soluciones de administración de identidad y acceso para proporcionar a los usuarios control total y facilidad de acceso en todas las aplicaciones de sus organizaciones. WatchGuard AuthPoint se integra directamente con las principales plataformas de IAM del mercado, incluidas CyberArk, Akamai, Oracle y más.
- **WatchGuard Firebox y Portal de Acceso.** El Portal de Acceso es una solución de VPN sin cliente que viene de serie con cada Firebox y proporciona acceso remoto seguro a usuarios remotos. Con el Portal de Acceso, los usuarios solo necesitan un navegador web para conectarse a aplicaciones web de terceros, aplicaciones internas y servicios de Microsoft Exchange, y también para crear sesiones RDP y SSH en recursos locales.
- **Aplicación Segura de VPN y Aislamiento de Hosts**. Nuestra exclusiva plataforma Detección y Respuesta ante Amenazas (TDR) unifica la seguridad de red y las capacidades de seguridad de endpoint para evitar que las máquinas potencialmente infectadas introduzcan malware en la red en general. Con la TDR, usted puede requerir un sensor de host activo en cada dispositivo que intente conectarse a la red directamente o a través de VPN. Además, el sensor del host controlará activamente el estado del dispositivo y lo aislará si se convierte en un riesgo.

3. Las redes, los endpoints y los usuarios están seguros, sin importar dónde se conecten las personas:

- **Filtrado de DNS con DNSWatch y DNSWatchGO.** El filtrado de DNS basado en la nube permite bloquear conexiones y limitar el acceso a las áreas de riesgo de Internet sin enrutar el tráfico a través de su red. Los clics en enlaces maliciosos o los intentos de conectarse a dominios relacionados con la suplantación de identidad y el malware se bloquean automáticamente.

- **Detección y Respuesta de Endpoints AD360.** La detección de malware avanzado requiere técnicas avanzadas. AD360 combina varios métodos de detección, incluido el análisis de comportamiento, heurístico y de sandbox en una sola plataforma. Las capacidades de IA de AD360 permiten predecir y bloquear automáticamente las amenazas antes de que comience a producirse el daño, además de descubrir anomalías que el analista humano podría pasar por alto.

- **WatchGuard Firebox y Total Security Suite.** Implementado en el corazón de la red, un Firebox de WatchGuard proporciona seguridad multicapa de nivel empresarial que defiende contra las amenazas más recientes.

- **Detección y Respuesta ante Amenazas (TDR).** Con TDR, WatchGuard integra la telemetría de red y de endpoint en la nube, y correlaciona los datos de seguridad para detectar amenazas que, de otro modo, se perderían de forma aislada y responder a esas amenazas.

- **Núcleo de Automatización.** Las soluciones de WatchGuard están altamente automatizadas, lo que les permite ahorrar ciclos en procesos manuales y repetibles. La automatización agiliza todo, desde las actualizaciones de antivirus y la gestión de parches hasta la detección de anomalías y alertas. Además, los procesos de seguridad se pueden integrar sin problemas con las herramientas de automatización de servicios profesionales (PSA), y la estrecha integración con las herramientas de supervisión y administración remotas (RMM) permite una respuesta más rápida a las solicitudes de soporte.

COMIENCE A PLANIFICAR LA CONFIANZA CERO PARA SU EMPRESA

La respuesta al coronavirus no tiene precedentes y este experimento del "trabajo desde casa" lleva a muchas empresas a un territorio decididamente desconocido. Con la mayor parte de los usuarios finales trabajando ahora de forma remota, los enfoques de seguridad de confianza cero pueden ayudar a mantener la continuidad y la seguridad.

Los proveedores de servicios administrados pueden desempeñar un papel fundamental a la hora de brindar las habilidades y los recursos necesarios a su organización para implementar de manera efectiva redes de confianza cero. Al tercerizar la responsabilidad a un proveedor de soluciones, usted obtiene seguridad y tranquilidad totales para poder concentrarse en hacer crecer su negocio y mantenerse competitivo en su campo.

Visite https://watchguardsupport.secure.force.com/PartnerFinder/ para obtener más información sobre los socios de WatchGuard y su cartera de productos.

"Gracias a WatchGuard y nuestro MSP, Calvert Technologies, ahora tenemos tranquilidad en lo que respecta a nuestra seguridad de TI. En lugar de tener que preocuparnos por el riesgo de ser víctimas de un ataque cibernético o una violación de datos, podemos concentrar nuestra mente en brindar el mejor nivel de servicio posible a nuestros clientes".

- Carson Coz, gerente de TI, Mykra

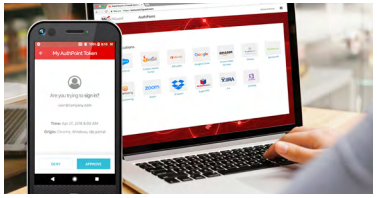
Plataforma de Seguridad Unificada de WatchGuard™

Seguridad de Red

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

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. Gracias a sus herramientas de interacción integrales y la visibilidad de análisis empresarial, proporciona la ventaja competitiva que su empresa necesita para triunfar.



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, nativo de la nube, que protege las empresas contra cualquier tipo de ataque cibernético presente y futuro. Su principal solución, Panda Adaptive Defense 360, impulsada por la inteligencia artificial, mejora de inmediato la posición de seguridad de las organizaciones. Combina las capacidades de protección de endpoints (EPP) y de detección y respuesta de endpoints (EDR) con los servicios de aplicaciones de confianza cero y de búsqueda de amenazas.

Ventas en Norteamérica: 1.800.734.9905 • Ventas internacionales: 1.206.613.0895 • Sitio web: www.watchguard.com