



Descubre cómo las **soluciones de WatchGuard** pueden ayudarte a cumplir con las **normativas europeas** y proteger tu empresa y la de tus clientes

Para más información, ¡ponte en contacto con nosotros!

www.infinigate.com/es
technical-spain@infinigate.com

MDR

Potencie su Defensa con Protección las 24 Horas Contra las Amenazas en Constante Evolución

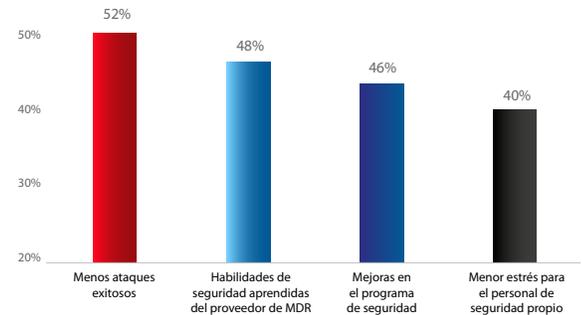


Aproveche el potencial de MDR

Las pymes se enfrentan a desafíos de ciberseguridad crecientes, desde ataques cada vez más sofisticados hasta la escasez de personal calificado y el aumento de la demanda de cumplimiento normativo y seguros cibernéticos. Sin una protección adecuada, corren el riesgo de sufrir costosos ciberataques y posibles multas por incumplimiento. Las organizaciones pequeñas y medianas experimentan mejoras sustanciales cuando abordan estos desafíos con MDR.

Nuestro servicio de MDR, desarrollado en sociedad con WatchGuard MDR, ofrece a los clientes una solución integral y administrada de ciberseguridad que combina capacidades de supervisión, detección y respuesta ante incidentes 24/7. Con el apoyo de los expertos en SOC de WatchGuard y nuestra experiencia, este servicio protege a las organizaciones contra amenazas sofisticadas y las ayuda a mantener la continuidad del negocio y mejorar la resiliencia contra los ciberataques.

Las medianas empresas (midmarket) reportan beneficios del MDR¹



Funcionalidades Clave del Servicio

Supervisión y detección continuas de amenazas 24/7

Nuestro servicio de MDR proporciona supervisión en tiempo real de los endpoints y de Office 365 durante todo el día para detectar amenazas avanzadas, como el ransomware y los ataques "Living Off the Land". Esta vigilancia constante permite la rápida identificación de actividades sospechosas y acciones proactivas para proteger a los clientes.

Investigación de incidentes y respuesta proactiva

En caso de un incidente, el equipo de MDR de WatchGuard realiza una investigación exhaustiva para comprender la naturaleza de la amenaza y, si es necesario, implementa la contención a través del aislamiento. Gracias a las pautas proporcionadas por WatchGuard, nuestro equipo puede responder activamente a los incidentes, conoce qué activos se vieron afectados y puede implementar la corrección lo más rápido posible y asegurar un rápido retorno a la normalidad.

Mejora de la posición de seguridad y prácticas de ciberhigiene

Nuestro servicio de MDR no solo incluye detección y corrección de amenazas, sino que también incorpora pasos proactivos para mejorar la posición de seguridad general de los clientes. Estos incluyen la implementación de prácticas de ciberhigiene, como la reducción de la exposición de los endpoints a los riesgos a través de evaluaciones periódicas de vulnerabilidad crítica. Al abordar las vulnerabilidades de alto riesgo, los clientes crean una defensa más resistente contra las posibles amenazas.

Soporte de cumplimiento y mejora continua

La adopción de un servicio de MDR proactivo ayuda a los clientes a cumplir con las regulaciones de seguridad (como NIST, NIS 2, DORA y PCI DSS), ya que se implementa una administración completa del ciclo de vida de las amenazas de extremo a extremo, se generan reportes exhaustivos y se proporciona orientación sobre las prácticas recomendadas de ciberseguridad. Este soporte incluye evaluaciones periódicas de la posición de seguridad y recomendaciones para reducir las vulnerabilidades, lo que garantiza que los clientes sigan el ritmo de los requisitos regulatorios.

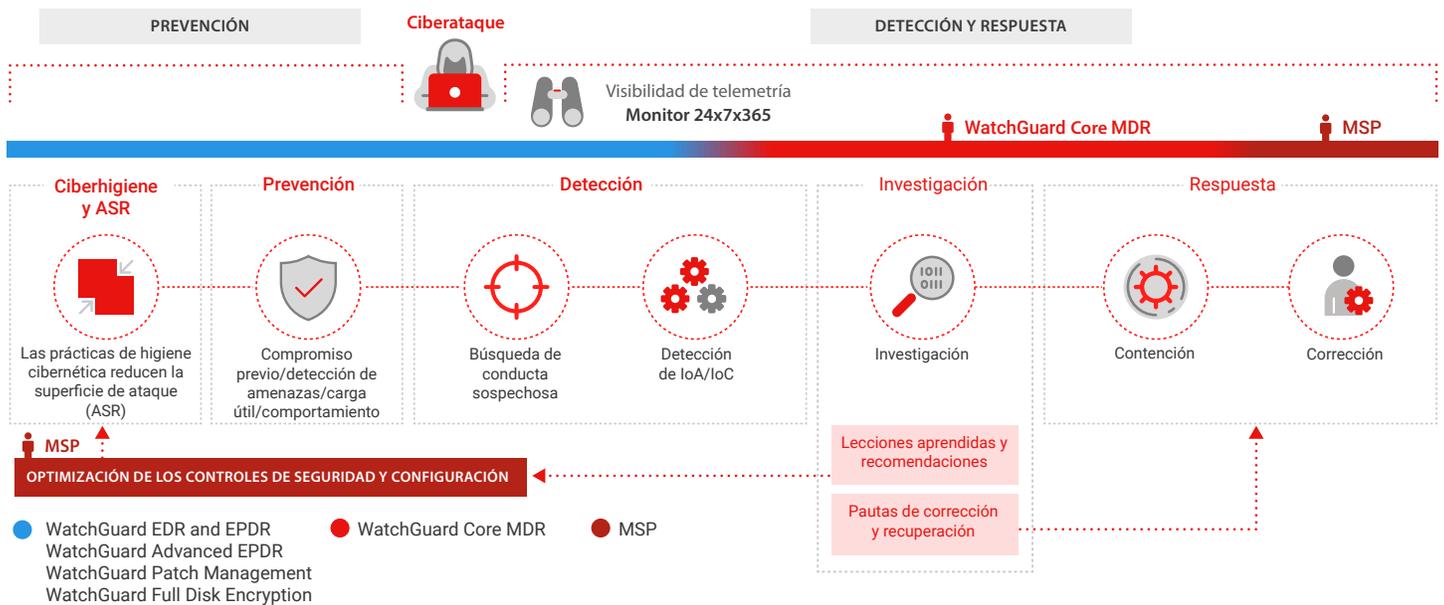
Reportes y planes de seguridad

Como parte del servicio, proporcionamos reportes detallados de incidentes y del estado de la seguridad de la infraestructura de los clientes. Además, se proporcionan informes semanales y mensuales de actividades de seguridad, que incluyen un análisis del estado actual y un plan de acción para la mejora continua de la seguridad.

Un servicio administrado que ofrece seguridad y confianza

Gracias a la combinación de la experiencia de WatchGuard y nuestro soporte personalizado, el servicio de detección y respuesta administradas que ofrecemos permite a nuestros clientes no solo mitigar las amenazas avanzadas, sino también mejorar continuamente su posición de seguridad. Con la tranquilidad que brindan los expertos en ciberseguridad y las soluciones avanzadas, las empresas pueden centrarse en el crecimiento sabiendo que están protegidas contra los ciberataques.

¹ Lo que los equipos de seguridad esperan de los proveedores de MDR ESG, mayo de 2023



Sus Beneficios



Protección contra amenazas sofisticadas

Nuestro servicio de MDR proporciona supervisión continua y respuesta de expertos a ataques avanzados, como el ransomware, lo que permite una rápida detección y mitigación para minimizar la interrupción comercial.



Acceso a especialistas en ciberseguridad

Muchas empresas carecen de recursos internos esenciales para hacer frente a la escasez de profesionales de ciberseguridad y las amenazas cada vez más complejas. Nuestro servicio de MDR otorga acceso a un equipo de especialistas, de modo que no es necesario crear un SOC y se garantiza un soporte confiable de expertos.



Asistencia para el cumplimiento normativo

Las regulaciones de ciberseguridad, como NIST, NIS 2 y DORA, son cada vez más estrictas, y se aplican multas severas por incumplimiento. Este servicio de MDR ayuda a los clientes a cumplir con estas normas, reducir el riesgo de sanciones y mejorar la confianza de los partners y clientes.



Reducción de los costos operativos

Los ciberataques pueden ser devastadores desde el punto de vista financiero, especialmente para las pymes, ya que la filtración de datos promedio cuesta USD 2.980.000. Al tercerizar la ciberseguridad con MDR, los clientes obtienen una protección rentable y evitan realizar grandes inversiones en personal y tecnología.



Respuesta rápida a incidentes

Una respuesta rápida es crucial para minimizar el impacto de los ciberataques. Nuestro servicio de MDR ofrece tiempos de respuesta inmediatos con contención automática, lo que garantiza que los incidentes se administren rápidamente y que los clientes puedan evitar las principales consecuencias no deseadas.



Acceso a seguro cibernético

Los proveedores de seguros cibernéticos exigen cada vez más que las empresas contraten servicios de MDR para mejorar la resiliencia cibernética, por lo que ofrecen importantes descuentos en las primas y una mayor protección financiera.



Tranquilidad y confianza en la seguridad

Gracias a la ayuda de un equipo de expertos que supervisa las amenazas y administra las respuestas, su organización puede centrarse en las operaciones sin preocuparse por los riesgos cibernéticos, beneficiándose del soporte continuo de su partner de seguridad de confianza y del SOC de WatchGuard, todo ello sin la necesidad de administrar múltiples proveedores de seguridad.



La Anatomía de Unified Security



En los últimos años, las organizaciones han experimentado una explosión sin precedentes en el volumen de entornos, usuarios, dispositivos y conexiones que necesitan administrar y proteger. Más del **60%** de las empresas informan que sus entornos de TI son más complejos ahora que hace dos años. En consecuencia, los MSP están tratando con clientes que sufren con una superficie de amenazas cada vez más compleja y amplia, y suelen contar con soluciones desconectadas e inconexas que son costosas y difíciles de administrar.

Muchos MSP se están alejando del antiguo enfoque fragmentario de la seguridad en favor de la consolidación de proveedores como una estrategia para proporcionar una mejor protección, al tiempo que generan

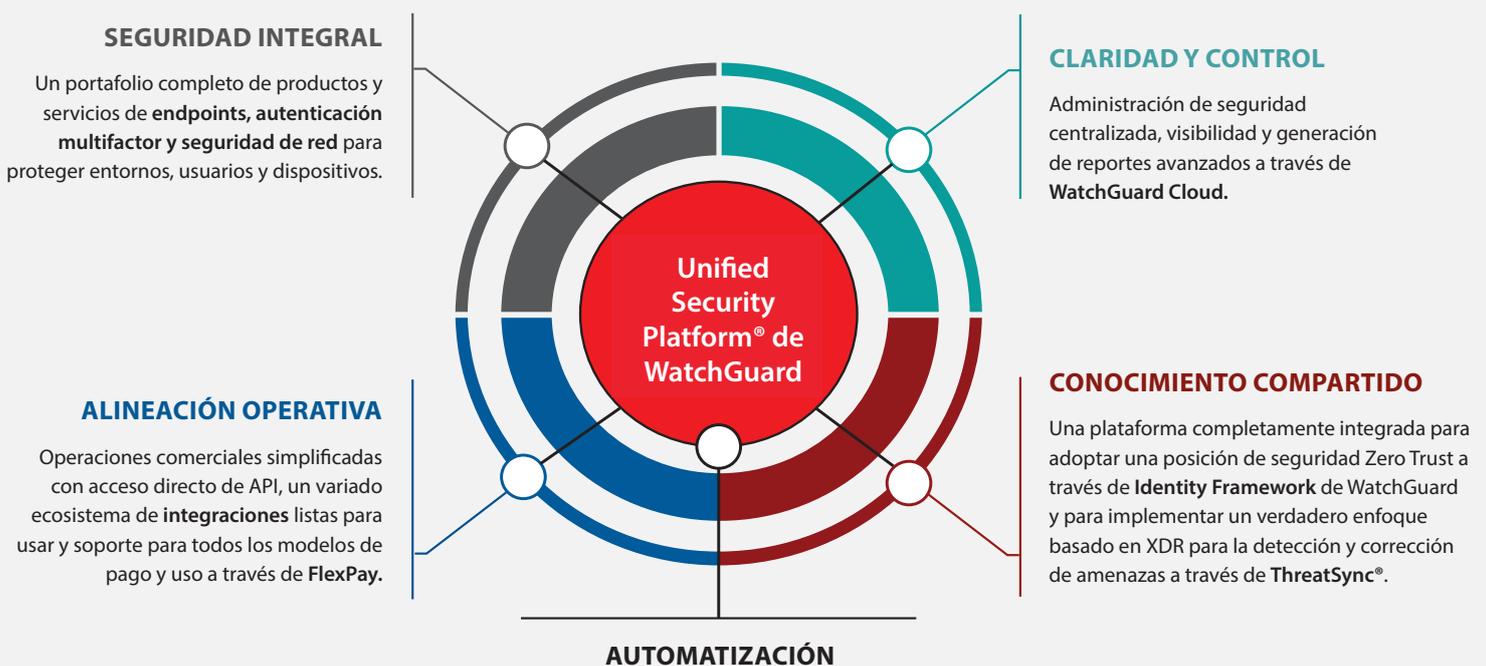
ahorros de CapEx y limitan la fricción operativa. Pero, en realidad, esto deja sin resolver muchos de los mismos problemas que surgen al alternar entre múltiples interfaces de administración de seguridad de forma diaria. La consolidación sin integración y visibilidad automatizadas y entre productos puede conducir a brechas de seguridad persistentes y a la frustración debido a las continuas cargas operativas, que hacen perder tiempo y recursos.

A fin de ofrecer la solución de seguridad rentable, escalable y eficaz que los clientes necesitan en el dinámico panorama de amenazas actual, los MSP deben mirar más allá de la consolidación para adoptar la seguridad *unificada*.

Implemente una Seguridad Poderosa y Simplificada con Unified Security Platform de WatchGuard

Unified Security Platform® de WatchGuard es una plataforma única que permite mejorar la seguridad moderna. Nuestro enfoque de plataforma lo ayuda a ofrecer servicios de seguridad poderosos para cada vector de amenazas con mayor escala y velocidad, a la vez que respalda eficiencias operativas y una mayor rentabilidad.

Una plataforma única y escalable para aumentar la entrega de seguridad moderna.



SEGURIDAD INTEGRAL

Un portafolio completo de productos y servicios de **endpoints**, **autenticación multifactor** y **seguridad de red** para proteger entornos, usuarios y dispositivos.

CLARIDAD Y CONTROL

Administración de seguridad centralizada, visibilidad y generación de reportes avanzados a través de WatchGuard Cloud.

ALINEACIÓN OPERATIVA

Operaciones comerciales simplificadas con acceso directo de API, un variado ecosistema de **integraciones** listas para usar y soporte para todos los modelos de pago y uso a través de FlexPay.

CONOCIMIENTO COMPARTIDO

Una plataforma completamente integrada para adoptar una posición de seguridad Zero Trust a través de **Identity Framework** de WatchGuard y para implementar un verdadero enfoque basado en XDR para la detección y corrección de amenazas a través de **ThreatSync**®.

AUTOMATIZACIÓN

WatchGuard Automation Core® ofrece simplificación y escala para todos los aspectos de uso, prestación de servicios y administración de seguridad.

Comprender la arquitectura de Unified Security Platform de WatchGuard

SEGURIDAD INTEGRAL

Para combatir el dinámico y siempre cambiante panorama de amenazas, y la escasez generalizada de tiempo, presupuesto y recursos para la ciberseguridad, nuestro enfoque unificado de seguridad ofrece múltiples productos y servicios poderosos que se integran de manera inteligente para cubrir toda la superficie de la amenaza. Las soluciones de seguridad de red, endpoints, MFA y Wi-Fi de WatchGuard se combinan para proporcionar la seguridad integral que usted necesita para proteger los entornos empresariales, los usuarios y los dispositivos de sus clientes.

CLARIDAD Y CONTROL

WatchGuard Cloud es la interfaz de administración centralizada para la creación, difusión y aplicación de políticas en toda la Unified Security Platform.

- Confíe en una arquitectura multi-tier, multi-tenant
- Habilite o inhabilite rápidamente los servicios de seguridad para los clientes
- Realice implementaciones sin intervención para soluciones de seguridad de red, MFA y endpoint
- Con la automatización, minimice la fatiga por alertas y manténgase siempre un paso adelante de las amenazas

WatchGuard Cloud proporciona una claridad superior, lo que lo ayuda a identificar fácilmente las tendencias de seguridad accionables, supervisar la eficacia del servicio de seguridad y generar reportes con impresionantes herramientas de visualización.

- Acceda a vistas resumidas de cada capa de seguridad a través del panel de control
- Identifique rápidamente problemas y explore en profundidad los servicios
- Acceda instantáneamente a hallazgos clave en varios terabytes de datos
- Comunique el valor con reportes personalizados y automatizados

CONOCIMIENTO COMPARTIDO

WatchGuard ThreatSync le permite ahorrar ciclos a su equipo de seguridad, acelera la detección y aumenta su precisión a través de la correlación automática de datos de amenazas relevantes de toda la plataforma WatchGuard Unified Security.

ThreatSync:

- Ofrece capacidades extendidas de detección y respuesta (XDR) en entornos, usuarios y dispositivos
- Recopila, correlaciona, analiza y responde a las amenazas en todas las capas de seguridad
- Ofrece una puntuación de amenazas fácil de entender para indicadores e incidentes
- Ofrece un panorama detallado, contextualizado y fácil de comprender de su superficie de amenazas

Con la capa Identity Framework de WatchGuard, nuestra arquitectura de Unified Security Platform utiliza políticas de autenticación sólidas para permitir el acceso seguro y respaldar la adopción de Zero Trust.

Nuestro Identity Framework:

- Desbloquea capacidades de confianza cero con un enfoque de seguridad que prioriza la identidad
- Se sincroniza con Microsoft Active Directory para habilitar MFA en todas las aplicaciones SaaS
- Simplifica la generación de reportes con definiciones de grupo y grupos de usuarios
- Facilita el acceso remoto seguro a través de Firebox sin necesidad de hardware RADIUS

ALINEACIÓN OPERATIVA

Con un sólido conjunto de API disponibles en múltiples capas de la Unified Security Platform, puede disfrutar de los beneficios operativos de la integración a escala. Haga crecer su negocio a través de la integración con:

- Más de 140 integraciones de terceros para respaldar las necesidades de los MSP y de los clientes
- Interoperabilidad superior con soluciones, herramientas para MSP y mercados líderes
- Implementaciones más fáciles con mayor confianza

Aproveche WatchGuard FlexPay para realizar transacciones con WatchGuard de una manera que se alinee con la forma en que vende a sus clientes y sea más útil para su negocio. Acceda a la agilidad empresarial acelerada y a la máxima flexibilidad entre el flujo de caja y el margen con:

- Opciones de modelo de negocio de prepago a plazo fijo, de pago por uso a plazo fijo y de compromiso cero de pago por uso
- Facturación basada en el uso
- Renovaciones automatizadas

AUTOMATIZACIÓN

WatchGuard Automation Core® respalda toda nuestra arquitectura de Unified Security Platform, y ofrece simplificación y escala para todos los aspectos de uso, prestación de servicios y administración de seguridad. Nuestra automatización de toda la plataforma agiliza los procesos de seguridad y los flujos de trabajo operativos para minimizar las tareas manuales frecuentes, que hacen un uso intensivo de los recursos y son propensas a errores. Por ejemplo, ofrece una protección continua e integrada, asegura el acceso del usuario a los recursos esenciales, bloquea las amenazas avanzadas que ingresan a su red, mantiene los endpoints libres de malware, optimiza el rendimiento de la red, al tiempo que ofrece la eficiencia operativa que su equipo necesita para hacer más con menos.



Para obtener más información sobre Unified Security Platform de WatchGuard, visite: <https://www.watchguard.com/es/wgrd-partners/unified-security-platform-partners>

XDR

La Respuesta a un Panorama de Amenazas Cada Vez Más Complejo

Las amenazas sofisticadas pueden venir de cualquier lugar, en cualquier momento y paralizar su negocio antes de que descubra cualquier indicio de vulneración. Las empresas se esfuerzan por hacer frente a una superficie de amenazas en rápida expansión y cada vez más compleja. En el mundo híbrido actual, los equipos de seguridad de TI operan en más entornos y dan soporte a más usuarios y dispositivos que nunca.

Cada uno de estos vectores de ataque implica un conjunto único de riesgos y vulnerabilidades que requieren soluciones de seguridad especializadas. Una colección fragmentada de productos de seguridad sencillamente no puede enfrentar estos desafíos de seguridad a escala. Además, las organizaciones carecen de tiempo y de recursos de ciberseguridad calificados para administrar las numerosas y diversas herramientas de seguridad o manejar el nivel de visibilidad, supervisión y corrección manual de amenazas que se requiere.

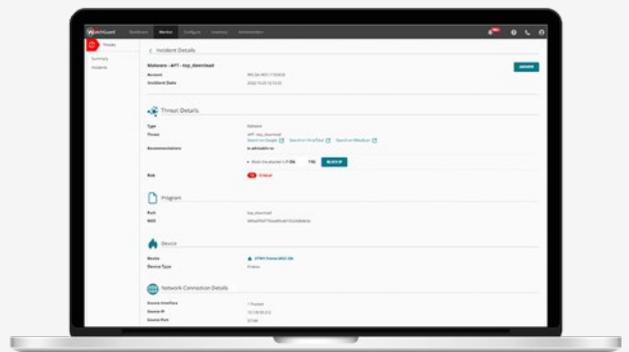
La detección y respuesta extendidas (XDR) es la respuesta. Las ofertas de XDR combinan la inteligencia de amenazas de una única plataforma de seguridad para ofrecer un sistema unificado de operaciones de seguridad capaz de detectar y responder a incidentes en todos los dominios y entornos. La clave de una verdadera solución de XDR es combinar datos de múltiples componentes de seguridad para ampliar la detección con capacidades centralizadas de respuesta a incidentes.

Con XDR, puede minimizar las brechas de visibilidad, la fatiga de alertas y los desafíos del personal y mejorar a la vez la productividad, los tiempos de detección y respuesta y, en definitiva, la solidez y eficacia generales de su posición de seguridad.

Descubra el Poder de XDR Hoy Mismo con WatchGuard ThreatSync

ThreatSync es una verdadera solución de XDR disponible dentro de la arquitectura Unified Security Platform® de WatchGuard. Ofrece un enfoque integrado basado en la nube para implementar capacidades de detección y respuesta extendidas en entornos, usuarios y dispositivos.

Con ThreatSync, obtendrá una imagen detallada, contextualizada y totalmente procesable de su superficie de amenazas. La solución recopila, analiza y correlaciona las amenazas en todo el paquete de seguridad de WatchGuard y permite brindar protección crítica de XDR de manera sencilla.



Cientos de miles de millones de eventos analizados



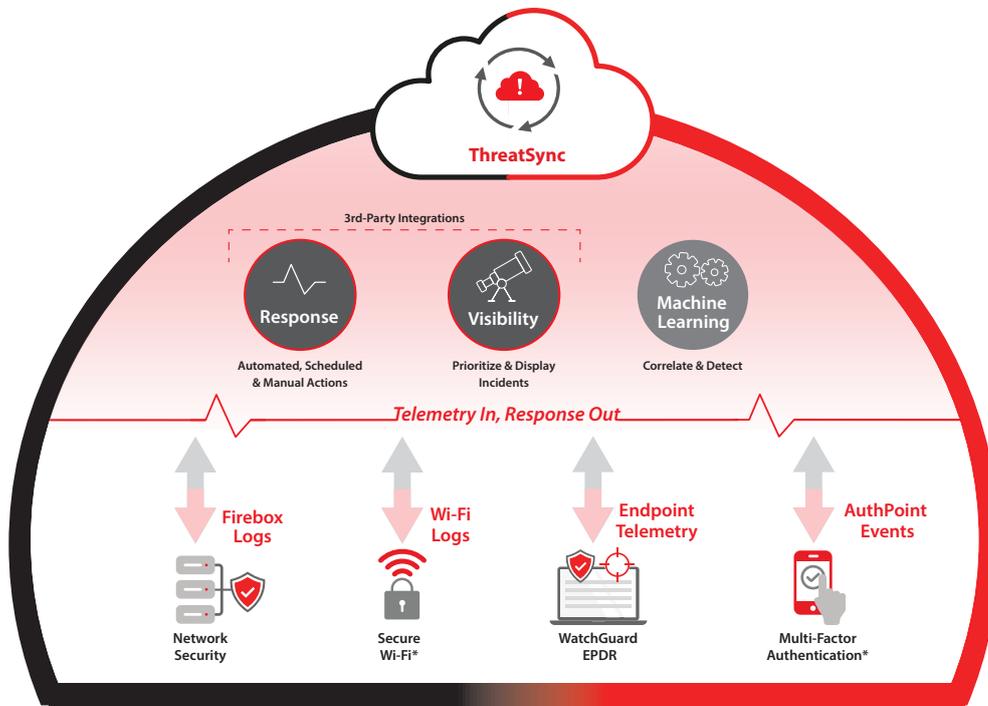
2.100 millones de binarios clasificados



Millones de movimientos de adversarios rastreados



Miles de malware de día cero bloqueados



* Secure Wi-Fi and AuthPoint will be available soon, integrated into ThreatSync.

Detección de Amenazas Entre Plataformas

La solución ofrece capacidades de detección extendidas a través del consumo y la correlación de indicadores de peligro (IoC) de todos los productos de seguridad de WatchGuard. Este contexto y correlación combinados entre dominios permite a ThreatSync detectar y calificar posibles actividades maliciosas relacionadas con entornos, usuarios y dispositivos específicos para reducir el tiempo promedio de detección (MTTD), mejorar la precisión y, en definitiva, lograr una corrección más rápida.

Orquestación de Seguridad Unificada y Respuesta a Amenazas

Cuando los administradores de seguridad y TI tienen una visión holística de su superficie de amenazas, es fácil hacer una evaluación y responder con rapidez y confianza. ThreatSync permite a los administradores de seguridad de TI trabajar con mayor eficiencia gracias a la valoración de alertas, las políticas de corrección automatizadas y las opciones de intervención manual según sea necesario. Este nivel de orquestación de respuesta a amenazas eleva tanto la escala como la precisión para los equipos de seguridad.

Simple de Implementar y Administrar

WatchGuard ThreatSync facilita la adopción de un enfoque XDR para un mercado con escasez de tiempo y habilidades ya que cuenta con las capacidades intuitivas de administración y automatización basadas en la nube. Al ser una poderosa capa de XDR dentro de la arquitectura Unified Security Platform® de WatchGuard, ThreatSync integra inteligencia entre productos para reducir los costos y las cargas de administración que implica la implementación de múltiples soluciones de punto para la detección y respuesta ante amenazas.

XDR es un principio esencial de la ciberseguridad moderna que debería estar al alcance de todas las empresas. Por ello, WatchGuard incluye ThreatSync como una capacidad entre productos disponible sin costo adicional.



¿ESTÁ LISTO PARA VER A XDR EN ACCIÓN?

Visite el sitio web de WatchGuard para obtener más información