TECNOVA | WatchGuard

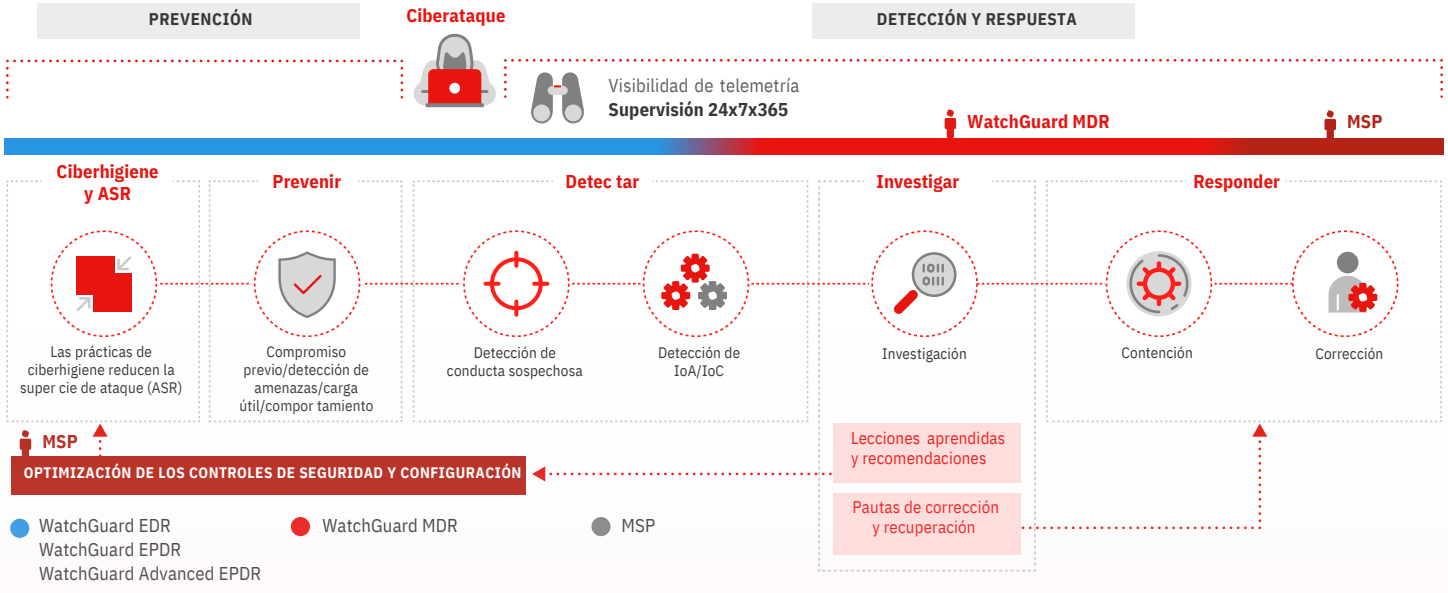
WatchGuard MDR

Detección y Respuesta 24/7 Sin Gastos Adicionales.

Mientras el panorama de las ciberamenazas continúa expandiéndose y se vuelve más sofisticado, las empresas luchan con serios riesgos de seguridad, una administración ineficiente de la ciberseguridad y la escasez de personal calificado. Por lo tanto, buscan delegar su protección a proveedores de servicios administrados (MSP) que cuentan con la tecnología, el personal y la experiencia para enfrentar estos desafíos.

Sin embargo, la administración de los complejos desafíos de seguridad y la creciente superficie de amenazas a la que se enfrentan la mayoría de las empresas en la actualidad requiere personas capacitadas y mucha inversión, de modo que para los MSP no es sencillo ofrecer servicios de detección y respuesta administradas (MDR) de manera efectiva y económica. Por este motivo, WatchGuard presentó WatchGuard MDR, un servicio administrado que ayuda a los proveedores de servicios de seguridad a superar estos problemas. Al incluir nuestro completo servicio de detección y respuesta en su oferta, los MSP pueden satisfacer las necesidades de los clientes sin los gastos adicionales que implica construir y mantener su propio centro de operaciones de seguridad (SOC) interno las 24 horas, los 7 días de la semana.

WatchGuard MDR proporciona servicios de ciberseguridad 24/7/365 a nuestros partners y sus clientes. Estos servicios ofrecen supervisión de seguridad de endpoints, búsqueda y detección de amenazas, investigación y contención de ataques, con recomendaciones guiadas para hacer correcciones. La oferta está administrada por un equipo de élite de expertos en ciberseguridad y cuenta con tecnología de IA. No requiere inversión en una infraestructura de SOC tradicional, en tecnologías avanzadas ni en escasos expertos en seguridad, de modo que se evitan las presiones globales relacionadas con estos problemas.



Modelo de MDR y Casos de Uso

1. MDR de un Centro de Operaciones de Seguridad (SOC) Interno:

Un SOC interno es una instalación y un equipo dedicados de un MSP responsable de administrar y responder a los problemas de ciberseguridad en el entorno de sus clientes.

- **Control:** control total de todos los procesos, herramientas y datos.
- **Costo:** alto; implica invertir en tecnología y personal calificado.
- **Escalabilidad:** requiere inversiones adicionales en personal y tecnología.
- **Administración:** la administración y las operaciones se manejan internamente.

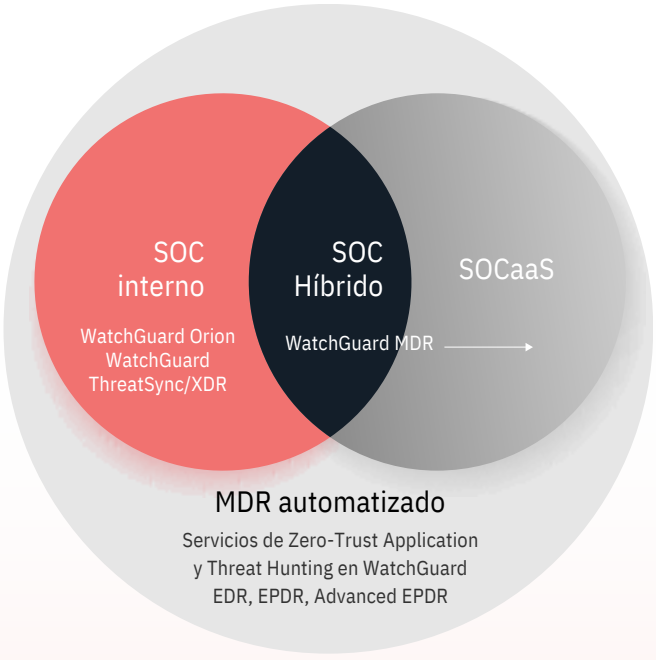
★ **Caso de uso:** ideal para grandes organizaciones con presupuestos de ciberseguridad importantes y requisitos de seguridad estrictos.

2. MDR de un SOC Como Servicio (SOCaaS):

SOCaaS es un servicio que proporciona supervisión, detección, investigación y respuesta de ciberseguridad subcontratada de un MDR de terceros.

- **Control:** control limitado, ya que el proveedor de MDR se encarga de los procesos.
- **Costo:** menor; gasto operativo en lugar de una inversión de capital.
- **Escalabilidad:** puede ser escalable, según el servicio elegido.
- **Administración**: administrado por profesionales de ciberseguridad ex ternos.

★ Caso de uso: apto para pequeñas y medianas empresas u organizaciones con presupuestos y personal de ciberseguridad limitados.



3. MDR de un SOC Híbrido:

un modelo de SOC híbrido combina funcionalidades de SOC interno y externo para equilibrar las capacidades de ciberseguridad internas y externas.

- **Control:** control moderado. Se administra internamente, pero aprovecha los recursos externos.
- **Costo:** se puede optimizar de acuerdo con el equilibrio de funciones internas y externas.
- **Escalabilidad:** mayor, ya que los esfuerzos internos se pueden aumentar con capacidades externas.
- **Administración:** incluye tanto a la administración interna como a la administración de terceros.

★ Caso de uso: ideal para organizaciones que buscan aumentar sus capacidades de SOC existentes sin inversiones sustanciales.

4. MDR Automatizado (Servicios)

En el contexto de un servicio de MDR automatizado, la tecnología tiene un rol fundamental en el refuerzo de la defensa de la ciberseguridad, ya que agiliza y, a menudo, procesa automáticamente varias funciones para mejorar la eficacia y la capacidad de respuesta.

- **Control:** las actividades de detección y respuesta están automatizadas. Esto permite a los equipos de TI centrarse en preocupaciones estratégicas, complejas o escaladas.
- **Costo:** no se necesitan gastos adicionales, ya que todas las tecnologías, incluida la IA en la nube, el personal calificado, las herramientas y la inteligencia de amenazas, están incluidas en el costo del producto.
- **Escalabilidad:** facilita la fácil adaptación a la escala y complejidad cambiantes de los entornos organizacionales.
- **Administración:** ofrece un enfoque sistemático para la detección y respuesta de amenazas, lo que minimiza el esfuerzo de gestión.

★ Caso de uso: los servicios de MDR automatizados son fundamentales para las empresas con personal o presupuesto de ciberseguridad limitados, ya que proporcionan una defensa sólida y económica.

Contáctenos

+506 4055 - 7700

+502 2229-6218

info@tecnovasoluciones.com

www.tecnovasoluciones.com