Cytomic es ahora WatchGuard for SOCs

FAQs para clientes, partners y prospects de WatchGuard Cytomic

Q. ¿Qué significa que WatchGuard Cytomic es ahora WatchGuard for SOCs?
R. Cuando WatchGuard adquirió Panda Security en junio de 2020, esta comercializaba y vendía productos y servicios de ciberseguridad para endpoint con la marca Cytomic.
Estas soluciones ofrecen características y capacidades específicas para las empresas con un centro de operaciones de seguridad (SOC), tanto para dar servicio interno como para dar servicio a sus clientes. Tras la compra, se aplicó una marca conjunta, WatchGuard Cytomic, y un equipo de ventas dedicado sigue apoyando a estos clientes y partners especializados.

Ahora, que el porfolio completo de Panda Security y sus servicios de seguridad se encuentra integrado en el porfolio unificado y bajo la Plataforma Unificada de WatchGuard (USP, Unified Security Platform™), el siguiente paso, ya en ejecución, es extender las capacidades avanzadas de detección y respuesta que aporta las soluciones de WatchGuard Cytomic, al resto del porfolio y Plataforma Unificada de WatchGuard.

P. ¿Qué significa desde el punto de vista de productos y servicios?
R. Con esta unificación, las soluciones anteriormente comercializadas bajo la marca WatchGuard Cytomic pasan a ser soluciones WatchGuard, e integrarse en el porfolio de **soluciones endpoints para SOC** de la siguiente forma:

- **WatchGuard Orion** (anteriormente comercializado con el nombre Cytomic Orion) - Plataforma en la nube multi-tenant e integral de hunting, detección y respuesta de ciber amenazas desconocidas y sofisticadas. Permite a los profesionales del SOC, mediante visibilidad 365 días de la actividad en los endpoints, analítica de comportamiento automatizado, y numerosas herramientas especializadas, descubrir, investigar y remediar eficientemente las amenazas ocultas en los endpoints que han conseguido evadir otros controles de seguridad.
- **WatchGuard Advanced EDR/EPDR** (anteriormente comercializado con el nombre Cytomic EDR/EPDR) - Productos de detección y respuesta endpoint que, además del Servicio Zero-Trust Application y el Servicio de Threat Hunting, se incluyen capacidades avanzadas de seguridad sobre los productos WatchGuard EDR/EPDR. Estas capacidades permiten a los analistas buscar indicadores de compromiso (IoCs y reglas YARA) y políticas de seguridad avanzadas para reducir la superficie de ataque en los endpoints.
- **Los módulos**: Patch, Encryption, Insights, SIEM Connect y Data Watch se renombran a sus correspondientes Módulos de Seguridad de Endpoint de WatchGuard.
- **Premium Threat Hunting Service** (anteriormente comercializado con el nombre Bronze Threat Hunting Service) - un servicio creado para que los partners puedan proactivamente identificar, parar y responder a amenazas que han podido evadir otros controles de seguridad, pero sin la problemática de contratar perfiles especializados y escasos, como threat hunters. Con el Servicio Premium Threat Hunting, el partner delega las actividades de hunting de amenazas al equipo de hunters de WatchGuard.

Q. ¿Qué implicaciones tiene para mí que los productos y servicios Cytomic sean ahora WatchGuard for SOCs?
R. En primer lugar, estos cambios no afectan en el corto plazo a los clientes y a los partners de productos y servicios de WatchGuard Cytomic. Se trata de un cambio de nombre de productos para ser consistentes con el porfolio y la plataforma unifica de WatchGuard, sin implicaciones funcionales, de seguridad o de cualquier otra índole.

Para el medio plazo, hay planes ambiciosos para hacer evolucionar la plataforma de Unificada de Seguridad de WatchGuard integrando las capacidades avanzadas de detección y respuesta de los productos y servicios anteriormente comercializados como WatchGuard Cytomic. Lo cual permitirá a los clientes y partners acceder inmediatamente a todas las capacidades de seguridad y gestión unificada que la plataforma de WatchGuard USP ofrece y al amplío porfolio de WatchGuard, gestionando desde la única consola de gestión en la nube, WatchGuard Cloud.

La marca en los productos irá cambiando a lo largo de los lanzamientos durante 2022 y 2023. Mientras tanto, es posible que vea la marca WatchGuard en los materiales de marketing y seguir viendo la marca Cytomic en ciertas áreas de los productos hasta que completemos la integración en los sistemas WatchGuard.

Esto no supondrá ningún cambio negativo para los clientes y partners, sino todo lo contrario, estos se irán beneficiando de numerosas funciones y capacidades avanzadas al integrarse en la Plataforma Unificada de WatchGuard.

De hecho, dado que los SOC desempeñan un papel fundamental en la protección de las organizaciones contra la evolución de las amenazas y la extensión de la superficie de ataque que vivimos en estos momento y que se verá potenciada en el futuro, el portfolio unificado y la Plataforma Unified Security Platform de WatchGuard acelerarán la modernización, la automatización y la optimización de la operación de seguridad en la red, los endpoints, las identidades y otros entornos y controles de seguridad, anticipando amenazas desconocidas y sofisticadas antes de que se produzcan daños en los clientes.

P. ¿Qué es WatchGuard Unified Security Platform?
R. WatchGuard Unified Security Platform eleva la práctica de los servicios de seguridad modernos al ofrecer una cartera completa de productos de autenticación multifactorial, punto final, Wi-Fi seguro y seguridad de red en una plataforma de seguridad completamente integrada.

Permite la implementación, administración y automatización de un verdadero enfoque de seguridad de confianza cero y servicios de seguridad basados en XDR para acelerar la detección y reparación de amenazas desconocidas y sofisticadas a escala. Si bien aumenta la eficiencia operativa para dedicar más tiempo a los asuntos más importantes, brinda más valor a sus clientes.
La plataforma de seguridad unificada de WatchGuard proporciona:

- S**eguridad integral**: una cartera completa de seguridad de red de nivel empresarial, seguridad avanzada de punto final, autenticación de múltiples factores y servicios Wi-Fi seguros que se escalan para satisfacer las necesidades de cualquier organización, independientemente de su tamaño.
- **Claridad y control:** WatchGuard Cloud™ permite la entrega y administración de hardware, software y servicios de ciberseguridad de suscripción mediante una interfaz intuitiva para una administración, visibilidad e informes consolidados.
- **Alineación operativa**: eliminamos la complejidad de las operaciones comerciales al ofrecer acceso directo a la API, un rico ecosistema de integraciones listas para usar y herramientas para una implementación rápida y eficiente.
- **Conocimiento compartido**: nuestra plataforma completamente integrada facilita la adopción de una verdadera postura de seguridad de confianza cero. Identity Framework y el motor de correlación ThreatSync™ de WatchGuard permiten un enfoque basado en XDR para acelerar la detección y corrección de amenazas.

- **Automatización**: un motor compartido a través de toda la plataforma, el Automation Core de WatchGuard proporciona simplicidad y escalabilidad a todos los aspectos de la seguridad desde la entrega, uso y gestión de esta.

Q. ¿Dónde encuentro información de WatchGuard Endpoint for SOC en la web de WatchGuard?
R. La información de los productos y servicios de WatchGuard Endpoint for SOCs (anteriormente comercializados bajo la marca WatchGuard Cytomic o Cytomic) se encuentra en la web corporativa de WatchGuard desde el 21 de abril de 2022, en la URL: https://www.watchguard.com/wgrd-products/security-operations-center-soc.

Q. ¿En qué se diferencian WatchGuard Orion y el Servicio Premium Threat Hunting de los productos y módulos actuales de WatchGuard Endpoint Security?
R. WatchGuard Endpoint for SOC ofrece soluciones con funcionalidad específica para mejorar las capacidades de los centros de operaciones de seguridad (SOC dedicados in-house, virtual SOC o SOC-as-a-service delegado a nuestros partner y SOC híbridos cliente/partner) que cuentan con personal para buscar, detectar, investigar y responder a amenazas sofisticadas desconocidas lo antes posible para mitigar el daño. Estas amenazas avanzadas pueden evadir otros controles de seguridad y acechan a la organización desde los endpoints.

WatchGuard Orion proporciona herramientas especializadas para hunters de amenazas y analistas de ciberseguridad que les permiten detectar, investigar y responder a amenazas avanzadas, aprovechando una visibilidad completa de la actividad en los endpoints durante 365 días, análisis de comportamiento automatizado y herramientas para la gestión de casos de incidentes para acelerar el análisis de la causa raíz y las acciones de respuesta a esas amenazas.

El servicio **Premium Threat Hunting** amplía el Servicio de Threat Hunting proporcionado con WatchGuard EDR/EPDR. El personal cualificado de WatchGuard monitoriza continuamente la actividad en los endpoints de cada cliente y ofreciendo información y recomendación de acciones, en caso de incidente.

Q. ¿Cuál es la diferencia entre WatchGuard EDR/EPDR y WatchGuard Advanced EDR/EPDR?
R. WatchGuard Advanced EDR/EPDR permite importar indicadores de compromiso (IoCs) de terceros en formato STIX 2.0 (hash, nombres de archivo, ruta, dominio, direcciones IP y reglas YARA) e implementar un conjunto de políticas de seguridad más avanzadas y proactivas requeridas por clientes con un programa de ciberseguridad más maduros.

Q. ¿Tiene WatchGuard algún plan para ampliar el servicio Premium de Threat Hunting de una cobertura de 8/5 a 24/7?
R. Sí, WatchGuard está trabajando activamente para disponer del servicio a clientes y partners con cobertura completa las 24 horas del día, los 7 días de la semana, en los próximos meses para