SOPHOS

Guía para la adquisición de servicios de detección y respuesta gestionadas (MDR)

Pocas empresas cuentan con las herramientas, las personas y los procesos adecuados para gestionar eficazmente su programa de seguridad las 24 horas, a la vez que se protegen de forma proactiva contra las amenazas nuevas y emergentes. Como consecuencia, las empresas miran cada vez más hacia los servicios de detección y respuesta gestionadas (MDR) para ejecutar su programa de operaciones de seguridad.

Según Gartner[1], para el 2025, el 50 % de las empresas utilizará servicios de MDR (en 2019, la cifra era inferior al 5 %).

Sin embargo, el mercado de los servicios de seguridad es relativamente nuevo para muchos, y puede estar lleno de afirmaciones falsas y de una jerga técnica confusa. Tomar una decisión informada para su empresa resulta cada vez más difícil. Esta guía le brindará claridad sobre las consideraciones clave y le servirá como guía a la hora de elegir un servicio de MDR. También le permitirá descubrir las diferencias entre los proveedores de MDR, lo que le ayudará a tomar una decisión fundada.

Las operaciones de seguridad requieren profesionales cualificados

La industria de la ciberseguridad está experimentando una grave carencia de talento y experiencia. Como consecuencia, las empresas tienen dificultades para diseñar programas de operaciones de seguridad (SecOps) efectivos a fin de detectar, investigar y responder a amenazas antes de que se produzcan daños.

Si bien las herramientas como EDR están concebidas para buscar amenazas y responder a incidentes, siguen requiriendo un técnico especializado para beneficiarse de todas sus capacidades. En una encuesta realizada en 2019 a 2300 profesionales de TI y de seguridad[2], el 54 % de los encuestados afirmaron que "no lograban sacar el máximo partido a su solución EDR" debido a la falta de personal experto.

Este problema está tan extendido entre las empresas que, según la firma de analistas de investigación ESG[3], "el 34 % afirma que su mayor reto es que carecen de recursos cualificados para investigar un incidente de ciberseguridad que afecte a un endpoint a fin de determinar la causa raíz y la cadena de ataque".

Si las amenazas de seguridad no paran de crecer tanto en volumen como en sofisticación, ¿cómo se espera que las empresas puedan seguirles el ritmo sin ampliar drásticamente sus equipos de operaciones de seguridad? Este dilema ha dado paso a una nueva alternativa: los servicios de seguridad gestionados y, en concreto, los servicios de detección y respuesta gestionadas (MDR).

Definición de servicio de detección y respuesta gestionadas (MDR)

Los servicios de detección y respuesta gestionadas (MDR) son operaciones de seguridad externalizadas prestadas por un equipo de especialistas. Los servicios de MDR actúan como una extensión del equipo de seguridad de los clientes, combinando las investigaciones realizadas por seres humanos, la búsqueda de amenazas, la supervisión en tiempo real y la respuesta a incidentes con una pila tecnológica para recopilar y analizar información.

Los proveedores de MDR suelen utilizar una combinación de tecnologías de nivel de host y de red, así como análisis avanzados, información sobre amenazas, datos forenses y experiencia humana, para identificar y neutralizar rápidamente las amenazas. El objetivo de la MDR es detectar y responder a las amenazas que hayan eludido los controles de seguridad preventivos en los entornos del cliente. Estos controles preventivos —como los firewalls, los antivirus y el filtrado de contenido— son eficaces para detener las amenazas genéricas conocidas, pero pueden fracasar a la hora de defenderse con éxito contra los ciberataques nuevos y sofisticados. Los proveedores de MDR han asumido el reto de cubrir el vacío dejado por estas herramientas en cuanto a la detección y respuesta a amenazas.

Razones por las que las empresas eligen un servicio de MDR

Entre los principales factores para contratar un servicio de MDR se incluyen:

- **Capacidades de operaciones de seguridad limitadas a nivel interno:** muchas empresas tienen dificultades para ir más allá de una estrategia de seguridad centrada en la prevención y no tienen la capacidad de poner en marcha y mantener su propio programa de operaciones de seguridad.
- **Les cuesta obtener el máximo partido de las herramientas EDR:** algunas empresas adquieren soluciones EDR, ya sea como tecnología reactiva en caso de un incidente, o con la esperanza de utilizarlas para buscar y responder a amenazas de forma proactiva. Sin embargo, no logran desarrollar plenamente su propio programa de operaciones de seguridad y necesitan recurrir a expertos externos.
- **Ampliar un equipo de operaciones de seguridad existente:** incluso las empresas que cuentan con un equipo de analistas de seguridad cualificados tienen lagunas en cuanto a la cobertura (como noches, fines de semana o vacaciones) y a las funciones especializadas (como analista de malware o especialista en respuesta a incidentes). Del mismo modo, algunos equipos de seguridad necesitan la cobertura adicional de un SOC subcontratado para poder centrarse en tareas de TI y de seguridad más generales que les cuesta mantener al día.
- **Asegurarse de que al equipo no se le escapa nada:** incluso los centros de operaciones de seguridad consolidados a menudo quieren que un segundo par de ojos supervise su entorno para asegurarse de que nada se cuela entre las rendijas.

Ventajas de los servicios de MDR

Equipo de expertos 24/7/365

Los servicios de MDR también deben tener la experiencia necesaria para detectar y responder a cualquier tipo de ataque. No solo cuentan con profesionales que son notoriamente difíciles de contratar, formar y retener, sino que un servicio de MDR dotado del personal adecuado también debe ofrecer una cobertura continua. Esto significa que supervisan constantemente su entorno y pueden responder a cualquier amenaza potencial en cualquier momento. Esto incluye fines de semana, vacaciones y en mitad de la noche. Es como tener un gran equipo de operaciones de seguridad que nunca hace vacaciones, nunca enferma y nunca duerme.

Los servicios son un elemento facilitador

A la mayoría de empresas ya les cuesta llevar a cabo su propia búsqueda de amenazas, respuesta a incidentes y comprobaciones del estado de seguridad. Al externalizar las operaciones de detección y respuesta, los servicios de seguridad permiten a los miembros del equipo centrarse en las tareas que corresponden a sus habilidades. Para las empresas más avanzadas, la adición de un servicio de MDR también permite a los equipos priorizar los "momentos heroicos" al tiempo que se deshacen de gran parte de las tareas cotidianas de las operaciones de seguridad.

Ahorro de costes

Las empresas que buscan crear su propio programa de operaciones de seguridad rápidamente se darán cuenta de la dificultad y el coste de construir un auténtico centro de operaciones de seguridad (SOC) a nivel interno. Incluso una empresa de tamaño medio necesitaría como mínimo cuatro analistas de ciberseguridad para mantener una cobertura de 24 horas al día, 7 días a la semana y 365 días al año. Las empresas más grandes necesitarían unos cuantos más miembros del equipo altamente remunerados. Las empresas deben tener en cuenta el coste de los jefes e ingenieros del equipo para personalizar y mantener las herramientas del mismo. Y esto es solo el coste de contratar a los miembros del equipo; el presupuesto también tendría que prever las herramientas que el equipo necesitaría, como la protección de los endpoints, la protección de la red, la detección y respuesta para endpoints (EDR), la solución SIEM, el procesamiento de los flujos de trabajo (SOAR), las fuentes de información, etc.

Tranquilidad

Con un servicio de MDR adecuado, usted y su empresa tendrán la tranquilidad de saber que hay un equipo de expertos cualificados que supervisan constantemente su empresa, buscan amenazas, investigan actividades sospechosas y responden a posibles incidentes. Con el panorama de amenazas a la ciberseguridad en permanente evolución, trabajar con un equipo cuyo único objetivo es la ciberseguridad aporta tranquilidad.

Evaluación de proveedores de MDR: las principales preguntas que hacer

Criterios generales

¿Cuántos clientes tiene el servicio de MDR?

Parte de lo que distingue a los proveedores de MDR es la experiencia que tienen en la detección y respuesta a incidentes. El recuento actual de clientes no solo le dará una idea del número de empresas que confían en el proveedor de servicios, sino también de su capacidad para responder a una amplia gama de actividades sospechosas. Asegúrese además de que el proveedor tenga experiencia trabajando con empresas de perfil similar (tamaño, vertical, retos de seguridad) al suyo.

¿Cuál es el alcance del servicio? ¿Se incluye la respuesta a amenazas?

No todos los servicios de MDR están diseñados igual. Un requisito cada vez más importante de los servicios de MDR para los clientes —y uno que todavía muy pocos proveedores ofrecen— es la capacidad de tomar medidas específicas para neutralizar las amenazas en nombre del cliente y no simplemente informarle de amenazas potenciales o inminentes. Aunque la sigla MDR incluye la letra "R" correspondiente a "respuesta", la mayoría de proveedores se centran principal o exclusivamente en identificar y notificar las amenazas, dejando en manos del cliente la gestión de todos los esfuerzos de respuesta y remediación. Para que los servicios de MDR sean eficaces es necesario que los analistas realicen investigaciones metódicas para determinar la validez y el alcance de las posibles amenazas, minimizar los falsos positivos, neutralizar las amenazas confirmadas y proporcionar un contexto adicional y recomendaciones a fin de mejorar la posición general de seguridad de la empresa.

¿Es el servicio 24/7/365? Si surge un problema un domingo a las 2 de la madrugada, ¿quién responderá?

Asegúrese de que el servicio de MDR lleva a cabo una monitorización real de su entorno y es capaz de responder a cualquier hora del día o de la noche.

¿Qué tecnologías utiliza el servicio? ¿Están incluidas en el precio?

Al evaluar un servicio de MDR es importante saber si la tecnología que utilizan los operadores está incluida en el precio del servicio. Algunos proveedores requerirán que compre sus propias herramientas (como la protección para endpoints y la EDR) por separado. Otros ofrecerán la pila tecnológica completa además del componente de servicios.

¿El servicio que se presta es proactivo o reactivo?

La MDR es una disciplina intrínsecamente proactiva. A diferencia de los servicios forenses digitales (DF) y de respuesta a incidentes (IR) basados en un anticipo que suelen ofrecerse para ayudar a los clientes a hacer frente a una crisis que ya se ha producido (como un incidente o una infracción de seguridad), la MDR ofrece un servicio permanente y proactivo que supervisa los entornos de los clientes para detectar actividades de adversarios y, a medida que surgen amenazas, orienta, ayuda o lleva a cabo la neutralización de estas en tiempo real.

¿Cómo interactuará con el equipo de MDR?

Es importante entender cuál es el proceso para comunicarse con su proveedor de servicios. ¿Se dispone de soporte telefónico directo? ¿Podrá comunicarse por correo electrónico? ¿Podrá hablar directamente con los analistas del SOC o la comunicación se gestiona a través de un intermediario (por ejemplo, un gestor de éxito del cliente)? En algunos casos, la diferencia entre los proveedores de MDR puede ser tan marcada como comunicarse con una persona o hacerlo con un portal. Independientemente de cómo se lleve a cabo la comunicación, los proveedores de MDR siempre deben incluir resúmenes de las actividades de los casos para asegurarse de que su equipo sepa qué amenazas se han detectado y qué seguimiento debe realizarse.

Metodología y criterios de eficacia

¿Cuál es la metodología de detección y respuesta a amenazas (TDR) de las operaciones de seguridad?

Es importante que los proveedores de MDR tengan una metodología de TDR bien definida. En caso contrario, es probable que tengan dificultades para adaptarse a medida que crezca su negocio y es más probable que pasen por alto importantes indicadores de actividad sospechosa.

¿Cómo es de rápido el servicio?

En seguridad, los segundos importan. Los proveedores de MDR deben poder estimar lo siguiente:

- Tiempo medio de detección
- Tiempo medio de respuesta
- Tiempo medio de resolución

¿Qué tipos de medidas de remediación pueden adoptar los operadores de MDR? ¿Pueden tomar medidas activas de respuesta en su nombre?

Los proveedores de MDR deben poder explicar lo que sucede cuando el servicio detecta una actividad sospechosa. Como se ha indicado anteriormente, muchos simplemente supervisarán el entorno y le notificarán si ocurre algo sospechoso. El operador de MDR debe poder tomar medidas en su nombre; es decir, debe haber una persona que dé una respuesta proactiva, no solo una herramienta que bloquee las amenazas automáticamente.

¿La búsqueda de amenazas se realiza a partir de pistas (respondiendo a alertas), sin pistas (buscando nuevos indicadores de ataque sin una alerta) o ambas cosas?

No toda búsqueda de amenazas es igual. Aunque la búsqueda de amenazas es, por definición, una actividad llevada a cabo por una persona, hay proveedores que la definen como la generación automatizada de alertas (y no lo es). También es importante comprender si los operadores de MDR buscarán de forma proactiva para detectar a los adversarios que acechan en su entorno, independientemente de que se haya detectado o no un indicador claro de actividad o peligro. Pregunte qué tipo de actividad iniciaría la investigación de una amenaza.

¿Qué fuentes de datos se utilizan para proporcionar visibilidad? ¿El servicio es solo "EDR gestionada"?

Si bien los datos de los endpoints son absolutamente críticos para un programa de operaciones de seguridad, algunos proveedores de MDR no tienen ninguna visibilidad adicional más allá del endpoint. Estos no son verdaderos proveedores de MDR y se asemejan más a una solución "EDR gestionada" que tiene una visibilidad limitada de las amenazas que pueden estar presentes en su entorno.

¿Tiene el proveedor de MDR acceso a información sobre amenazas y a investigadores de amenazas?

Los proveedores de MDR deben tener un nivel de especialización que vaya más allá de lo que la mayoría de empresas pueden construir por sí mismas. Esto incluiría, evidentemente, analistas de seguridad cualificados. Sin embargo, el proveedor también debe tener acceso a información exclusiva sobre amenazas y colaborar con investigadores de amenazas cuando se detecte algo novedoso.

Comparación de proveedores

Los proveedores de detección y respuesta gestionadas (MDR) suelen dividirse en tres categorías:

- **Solo supervisión:** se centran en priorizar y notificar a los clientes cuando se genera una alerta automatizada en el producto. No ofrecen opciones de remediación más que el asesoramiento sobre lo que el cliente necesita hacer. Además, solo se sirven de la búsqueda de amenazas "automatizada", y no investigan ni buscan amenazas proactivamente en nombre del cliente.
- **Respuesta limitada ("r" minúscula):** incluyen acciones de respuesta parcial, pero se limitan a acciones automatizadas. La búsqueda de amenazas se lleva a cabo pero solo cuando una alerta desencadena la investigación.
- **Respuesta completa ("R" mayúscula)**: incluyen capacidades de respuesta completa. Toman medidas de forma proactiva en nombre del cliente con una respuesta manual realizada por un ser humano. La búsqueda de amenazas no solo se realiza a partir de pistas, sino que el equipo de MDR buscará de forma sistemática amenazas aunque no haya un indicador de ataque visible.

Funciones clave	Solo supervisión	Respuesta limitada ("r" minúscula)	Respuesta completa ("R" mayúscula)
Monitorización 24/7	✓	✓	✓
Notificación y priorización	✓	✓	✓
Guía de remediación	✓	✓	✓
Informes de actividades	✓	✓	✓
Búsqueda de amenazas "automatizada"	✓	✓	✓
Respuesta automatizada		✓	✓
Búsqueda de amenazas a partir de pistas		✓	✓
Búsqueda de amenazas sin pistas			✓
Respuesta realizada por seres humanos			✓

Proveedores representativos[4]		
Solo supervisión	Respuesta limitada ("r" minúscula)	Respuesta completa ("R" mayúscula)
Carbon Black Managed Detection	Arctic Wolf	Sophos MTR Standard
CrowdStrike Falcon OverWatch	eSentire	Sophos MTR Advanced
Huntress	Expel	CrowdStrike Falcon Complete
Perch	Rapid7	
	Red Canary	
	SentinelOne Vigilance Respond	

Servicio Sophos Managed Threat Response (MTR)

Sophos Managed Threat Response (MTR) es un servicio totalmente administrado prestado por un equipo de expertos que ofrece funciones de búsqueda, detección y respuesta a amenazas las 24 horas. Más allá de la simple notificación de ataques o comportamientos sospechosos, el equipo de Sophos MTR adopta medidas específicas en su nombre para neutralizar incluso las amenazas más sofisticadas y complejas.

El equipo de Sophos MTR de cazadores de amenazas y expertos en respuesta se dedican a:

- Buscar y validar de forma proactiva posibles amenazas e incidentes.
- Utilizar toda la información disponible para determinar el alcance y la gravedad de las amenazas.
- Aplicar el contexto empresarial adecuado para las amenazas reales.
- Iniciar acciones para interrumpir, contener y neutralizar amenazas de forma remota.
- Brindar asesoramiento práctico para abordar la causa raíz de los incidentes recurrentes.

Funciones clave de Sophos MTR

Sophos MTR: Standard

24/7 Lead-Driven Threat Hunting

Las actividades o artefactos maliciosos confirmados (indicios sólidos) se bloquean o detienen automáticamente, lo que libera la carga de trabajo de los analistas de amenazas para que puedan realizar búsquedas a partir de pistas. Este tipo de búsqueda de amenazas implica agregar e investigar eventos causales y adyacentes (indicios débiles) para descubrir nuevos indicadores de ataque y de peligro que antes no podían detectarse.

Comprobación del estado de seguridad

Mantenga el máximo rendimiento de sus productos de Sophos Central, empezando por Intercept X Advanced with EDR, con exámenes proactivos de sus condiciones operativas y mejoras de configuración recomendadas.

Informes de actividades

Los resúmenes de las actividades de los casos facilitan la priorización y comunicación para que su equipo sepa qué amenazas se han detectado y qué acciones de respuesta se han llevado a cabo dentro de cada periodo del informe.

Detección de adversarios

La mayoría de los ataques eficaces dependen de la ejecución de un proceso que puede parecer legítimo para las herramientas de supervisión. Mediante técnicas de investigación patentadas, nuestro equipo determina la diferencia entre un comportamiento legítimo y las tácticas, técnicas y procedimientos utilizados por los atacantes.

Sophos MTR: Avanzada

Búsqueda de amenazas sin pistas las 24 horas

Aplicando data science, la información sobre amenazas y la intuición de experimentados detectores de amenazas, combinamos el perfil de su empresa, sus activos de alto valor y usuarios de alto riesgo para anticiparnos al comportamiento de los atacantes e identificar nuevos indicadores de amenazas.

Telemetría optimizada

Las investigaciones de amenazas se complementan con la telemetría de otros productos de Sophos Central que van más allá del endpoint para ofrecer una imagen completa de las actividades del adversario.

Mejora proactiva de la posición de seguridad

Mejore de forma proactiva su posición de seguridad y refuerce sus defensas con una guía prescriptiva para corregir las carencias de configuración y arquitectura que merman sus capacidades generales en materia seguridad.

Responsable de respuesta ante amenazas dedicado

Cuando se confirma un incidente, se le asigna un responsable de respuesta ante amenazas dedicado para que colabore directamente con sus recursos locales (equipo interno o partner externo) hasta que se neutralice la amenaza activa.

Soporte telefónico directo

Su equipo tiene acceso telefónico directo a nuestro centro de operaciones de seguridad (SOC). Nuestro equipo de operaciones de MTR está disponible las 24 horas y cuenta con el apoyo de equipos de soporte en 26 lugares de todo el mundo.

Detección de recursos

Desde datos sobre recursos que incluyen versiones de sistemas operativos, aplicaciones y vulnerabilidades hasta la identificación de activos gestionados y no gestionados, proporcionamos información valiosa durante las evaluaciones de impacto, las búsquedas de amenazas y como parte de las recomendaciones para la mejora proactiva de la posición de seguridad.

Sophos Managed Threat Response (MTR): Protection, EDR y MDR			
Funciones clave	Sophos Intercept X Advanced with EDR (solo la tecnología)	Sophos MTR Standard (tecnología + servicio gestionado)	Sophos MTR Advanced (tecnología + servicio gestionado)
Protección para endpoints	✓	✓	✓
Detección y respuesta para endpoints (EDR) para las operaciones de TI	✓	✓	✓
Detección y respuesta para endpoints (EDR) para la búsqueda de amenazas	✓	✓	✓
Servicio gestionado: Supervisión y respuesta las 24 horas		✓	✓
Servicio gestionado: respuesta manual proactiva		✓	✓
Servicio gestionado: Búsqueda de amenazas a partir de pistas		✓	✓
Servicio gestionado: Búsqueda de amenazas avanzada sin pistas			✓
Servicio gestionado: responsable de respuesta dedicado			✓

Factores clave que distinguen a Sophos MTR

Sophos toma medidas en su nombre: a diferencia de Sophos MTR, otros servicios solo supervisan y notifican cuando se detectan actividades sospechosas. El equipo de Sophos MTR actúa. Iniciamos acciones de forma remota para interrumpir, contener y neutralizar incluso las amenazas más sofisticadas.

Experiencia de alto nivel: con más de 2000 clientes, Sophos lo ha visto y detenido todo. Nuestro equipo altamente cualificado de detectores de amenazas, ingenieros y hackers éticos cubre las 24 horas, investigando comportamientos anómalos y tomando medidas contra las amenazas.

Búsqueda de amenazas robusta: Sophos lleva a cabo búsquedas de amenazas con y sin pistas para descubrir nuevos indicadores de ataque y de peligro que antes no podían detectarse.

Detecciones de alta fidelidad: más allá de las detecciones tradicionales, Sophos combina modelos de Machine Learning y determinísticos para detectar comportamientos peligrosos, así como las tácticas, las técnicas y los procedimientos utilizados por los adversarios más avanzados.

Respuesta humana precisa: el servicio Sophos MTR incluye Intercept X Advanced with EDR, la mejor protección para endpoints del mundo. Esto significa que detiene automáticamente las amenazas que otros dejan pasar. Dado que el servicio tiene una prevención mejor y más proactiva, el equipo puede centrarse en detectar, responder y tomar medidas sobre los incidentes más desafiantes.

Transparencia y control: con Sophos, usted toma las decisiones y controla cómo y cuándo se derivan los incidentes potenciales, qué acciones de respuesta desea que tomemos (si corresponde) y quién debe incluirse en las comunicaciones. Las empresas pueden beneficiarse de cualquiera de los tres modos de respuesta (Notificar, Colaborar o Autorizar) para adaptarse a sus necesidades específicas.

Outcome-Focused Security™: cada acción de búsqueda, investigación y respuesta se traduce en datos para la toma de decisiones que sirven para mejorar las configuraciones y las funciones de detección automatizadas.

Estadísticas clave de Sophos MTR

Servicio Sophos Rapid Response

El servicio Sophos Rapid Response, prestado por un equipo de expertos en respuesta a incidentes, ofrece asistencia ultrarrápida a la hora de identificar y neutralizar amenazas activas contra una empresa. El servicio Rapid Response está dirigido a las empresas que están siendo atacadas. Los clientes de Sophos MTR no necesitarían el servicio Rapid Response, ya que la respuesta a incidentes forma parte del servicio Sophos MTR.

El servicio Rapid Response ofrece una acción inmediata para los incidentes activos. La incorporación empieza en cuestión de horas, y la mayoría de clientes son evaluados en 48 horas.

El equipo de Sophos Rapid Response, disponible 24/7, está compuesto por gestores de respuesta a incidentes, analistas de amenazas y cazadores de amenazas que:

- Toman medidas rápidamente para clasificar, contener y neutralizar las amenazas activas
- Expulsan a los adversarios de su entorno para evitar más daños a sus recursos
- Realizan una supervisión y respuesta 24/7 para mejorar su protección
- Recomiendan acciones preventivas en tiempo real para abordar la causa raíz
- Proporcionan un resumen detallado de la amenaza posterior al incidente que describe nuestra investigación

El servicio Sophos Rapid Response está disponible tanto para los actuales clientes de Sophos como para los que no lo son.

Para obtener más información sobre el servicio Sophos Managed Threat Response (MTR), visite nuestro sitio web o póngase en contacto con un representante de Sophos.

Si prefiere realizar sus propias búsquedas de amenazas, Sophos EDR le ofrece las herramientas necesarias para la búsqueda de amenazas avanzadas y la higiene de las operaciones de seguridad. Empiece una evaluación gratuita de 30 días sin compromiso hoy mismo.

Fuente:

1 Gartner, Guía de mercado de servicios de detección y respuesta gestionados, 26 de agosto de 2020; Analistas: Toby Bussa, Kelly Kavanagh, Pete Shoard, John Collins, Craig Lawson y Mitchell Schneider

2 Encuesta a 3100 directores de TI de 2019 https://secure2.sophos.com/es-es/security-news-trends/whitepapers/gated-wp/uncomfortable-truths-of-endpoint-security.aspx

3 https://www.esg-global.com/blog/soapa-discussion-on-edr-and-xdr-with-jon-oltsik-and-dave-gruber-video-part-1

4 Este documento comparativo e informativo se basa en la interpretación de Sophos de los datos disponibles públicamente a la fecha de preparación de esta comparativa. Este documento ha sido elaborado por Sophos y no por los otros proveedores que se mencionan. Las funciones o características de los productos que se comparan, que pueden repercutir directamente en la precisión y/o validez de esta comparativa, pueden sufrir cambios. La información que incluye esta comparativa tiene como finalidad ofrecer un conocimiento y una comprensión generales de la información objetiva de varios productos y podría no ser exhaustiva. Cualquiera que utilice este documento debe tomar su propia decisión en función de sus requisitos, además de consultar las fuentes de información originales y no basarse solo en esta comparativa a la hora de seleccionar un producto.

Para obtener más información sobre
Sophos Managed Threat Response (MTR)

visite es.sophos.com/mtr

Ventas en España
Teléfono: (+34) 913 756 756
Correo electrónico: comercialES@sophos.com

Ventas en América Latina
Correo electrónico: Latamsales@sophos.com

2021-02-25 BG-ES (PC)

SOPHOS