SOPHOS

Guía para la adquisición de detección y respuesta gestionadas

A medida que evolucionan las ciberamenazas, muchas organizaciones están recurriendo a los servicios de detección y respuesta gestionadas (MDR) para que les proporcionen capacidades de supervisión y respuesta a amenazas 24/7 a cargo de expertos, necesarias para detener a los sofisticados adversarios de hoy en día.

Sin embargo, ante el creciente número de competidores en el mercado de la MDR, la variedad de opciones de despliegue y los numerosos reclamos de marketing carentes de fundamento, seleccionar al Partner de servicios de MDR adecuado para su organización puede resultar todo un reto.

Esta guía le brindará claridad sobre los elementos clave que caracterizan a un servicio de MDR de primera clase y los resultados de seguridad y empresariales superiores que todo servicio de MDR debe ofrecer. Al disponer de todos estos datos, podrá tomar la decisión correcta para su organización.

Monográficos de Sophos. Marzo 2024

Crece la demanda de operaciones de seguridad

Los recientes cambios en el panorama de las amenazas han incrementado el desafío para los responsables de la seguridad y han acelerado la necesidad de contar con soporte dedicado para las operaciones de seguridad en organizaciones de todos los tamaños.

La evolución de la economía de la ciberdelincuencia

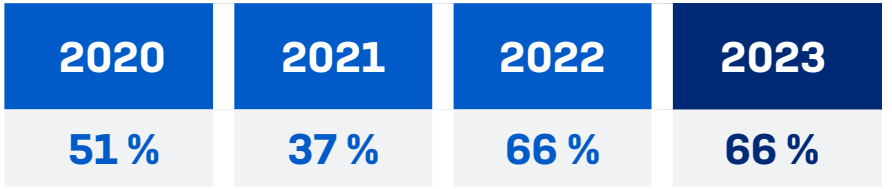
En los últimos años, uno de los cambios más significativos en el panorama de las amenazas ha sido la transformación de la economía de la ciberdelincuencia en una industria con una red de servicios de apoyo y enfoques operativos consolidados y profesionalizados.

A medida que las empresas tecnológicas se han ido decantando por las soluciones «como servicio», el ecosistema de los ciberdelitos ha hecho lo mismo. Esto ha rebajado la barrera de entrada para los ciberdelincuentes en potencia y les ha permitido multiplicar el volumen, la velocidad y el impacto de sus ataques. En consecuencia, los adversarios ahora pueden ejecutar una amplia variedad de ataques sofisticados a escala.

Para obtener más información, consulte El estado de la ciberseguridad 2023: el impacto de los adversarios en el negocio.

El ransomware sigue siendo una amenaza constante

Dos tercios (66 %) de las organizaciones afirman que sufrieron un ataque de ransomware en el último año.



En el último año, ¿se ha visto afectada su organización por el ransomware?
Sí. n=3000 (2023), 5600 (2022), 5400 (2021), 5000 (2020)

Mientras que el índice de ataques registrados en 2023 se ha mantenido al mismo nivel que en 2022, el cifrado de datos como consecuencia del ransomware se encuentra en su nivel más alto de los últimos cuatro años: los delincuentes logran cifrar los datos en más de tres cuartas partes de los ataques (76 %).

Para saber más al respecto, como la frecuencia, el coste y la causa raíz de los ataques, lea nuestro estudio anual El estado del ransomware.

El ransomware remoto es una amenaza que crece rápidamente y que puede tener un enorme impacto en las víctimas. Utilizado en cerca del 60 % de los ataques de ransomware perpetrados por humanos[1], consiste en utilizar un dispositivo comprometido para cifrar maliciosamente los datos de otros dispositivos de la misma red.

Con el ransomware remoto, un solo dispositivo no administrado o mal protegido puede dejar expuesta toda la red de una organización al cifrado remoto malicioso, aunque todos los demás dispositivos cuenten con un antivirus o una solución de seguridad para endpoints next-gen.

Los adversarios no se cuelan, sino que inician sesión

23 %
de las organizaciones sufrieron un ataque relacionado con un adversario activo en el último año

30 %
de los encuestados afirman que los adversarios activos son una de las ciberamenazas que más les preocupan para 2023

Las tecnologías de mitigación de ciberriesgos son una inversión necesaria para cualquier organización, pero ante un hacker decidido, ninguna tecnología es invencible por sí sola, por muy eficaz que sea.

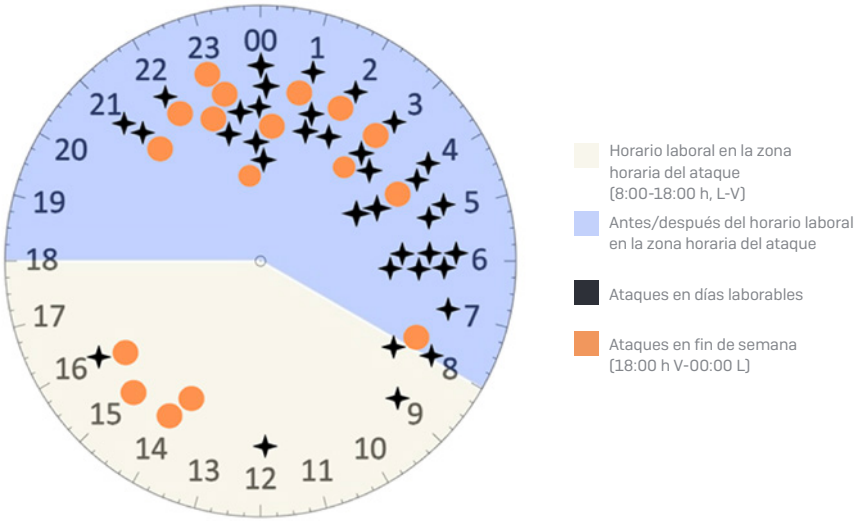
Los adversarios activos son ciberdelincuentes altamente cualificados, muchas veces con sofisticadas habilidades en materia de software y redes, que obtienen acceso a los sistemas de una organización, esquivan la detección y adaptan continuamente sus técnicas, sirviéndose de métodos manuales directos y asistidos por IA para eludir los controles de seguridad preventivos y ejecutar sus ataques.

Estos ataques, que a menudo desembocan en devastadores incidentes de ransomware y filtración de datos, son de los más difíciles de detener. También se han vuelto muy frecuentes, y es que el 23 % de las pequeñas y medianas empresas afirman que sufrieron un ataque perpetrado por un adversario activo en el último año[2].

Estos hábiles y perseverantes atacantes despliegan múltiples estrategias para lograr sus objetivos, entre ellas:

- **Explotar las deficiencias de seguridad** para penetrar en las organizaciones y moverse lateralmente una vez dentro de la red, incluyendo credenciales robadas, vulnerabilidades no parcheadas y errores de configuración de seguridad.
- **Usar indebidamente herramientas de TI legítimas** para evitar que se activen las detecciones, como PowerShell, PsExec y RDP.
- **Modificar sus ataques en tiempo real en respuesta a los controles de seguridad** pasando a nuevas técnicas (como el ransomware remoto) hasta lograr sus objetivos.
- **Hacerse pasar por usuarios autorizados y explotar los puntos débiles en las defensas de una organización** para evitar la activación de las tecnologías de detección automatizadas que tienen dificultades para diferenciar entre usuarios legítimos y atacantes.
- **Ejecutar ataques de varias fases**, desde el acceso inicial, al movimiento lateral, al aumento de privilegios, etc. Ante la naturaleza de estos ataques, es importante tener visibilidad e información en todas las superficies de ataque clave para identificar un ataque más rápido, ya que las tecnologías individuales (endpoint, firewall, identidad, etc.) puede que solo contengan una pieza del rompecabezas.
- **Atacar a las organizaciones cuando es menos probable que los detecten:** el 91 % de los ataques de ransomware resueltos por los expertos en respuesta a incidentes de Sophos se inician fuera de las horas de trabajo habituales en la zona horaria de la víctima (es decir, fuera del horario de 8:00 a 18:00 h de lunes a viernes)[3].

Hora del día en que se inician los ataques de ransomware[4]



Retos en la ejecución de las operaciones de seguridad

Los recientes cambios en el entorno empresarial agravan los retos que plantea el panorama de las amenazas. Los usuarios pueden estar en la oficina, trabajar a distancia o desplazarse continuamente. Al mismo tiempo, los datos de la empresa pueden guardarse localmente, en la nube y en los dispositivos de los empleados geográficamente dispersos.

Ante estas complejidades, no es de extrañar que más de la mitad de las organizaciones (52 %) afirmen que las ciberamenazas son demasiado avanzadas para que su organización las gestione por sí sola[5].

Entre los principales retos a los que se enfrentan los equipos de TI a la hora de ejecutar operaciones de seguridad con eficacia se incluyen:

Escasez de conocimientos especializados: según el 93 % de los equipos de TI, las operaciones de seguridad suponen un reto[6], y sigue siendo difícil contratar a empleados cualificados. La falta de experiencia significa que los miembros del equipo a menudo tienen dificultades para determinar si una alerta de seguridad es maliciosa o benigna, lo que crea un efecto dominó: se tarda más en investigar las alertas, lo que, a su vez, reduce la capacidad del equipo y aumenta la exposición al riesgo.

Falta de cobertura 24/7: a las organizaciones les cuesta supervisar y responder activamente a las alertas y a la actividad sospechosa fuera del horario de trabajo estándar (noches, fines de semana y festivos). Los analistas necesitan identificar, investigar y responder de forma activa a la actividad sospechosa en cuanto se produce.

Exceso de ruido: el 71 % de las organizaciones tienen problemas para identificar qué alertas deben investigar. El hecho de recibir demasiadas alertas de muchos sistemas diferentes abruma al personal de TI, que a menudo no sabe cómo priorizar qué señales o alertas investigar, con lo que puede pasar por alto indicadores de un ataque.

Datos aislados: las señales de amenazas se limitan a tecnologías específicas, lo que impide a los equipos de TI obtener una visión de conjunto, identificar los ataques de varias fases y remediar las alertas o incidentes maliciosos con prontitud.

Falta de integración: las herramientas de seguridad no se integran entre sí ni con la infraestructura de TI de la empresa, lo que aumenta la complejidad.

Procesos manuales: los equipos de TI dedican muchas horas a correlacionar eventos, registros e información para comprender lo que está ocurriendo. Este esfuerzo manual retrasa la identificación y la respuesta a los ataques.

Respuesta reactiva: muchos equipos de TI se encuentran a la zaga, respondiendo a las amenazas solo después de que hayan causado daños en lugar de detenerlas en una fase más temprana de la cadena de ataque.

Centrarse en los imprevistos: la labor diaria para detener las amenazas impide mejoras a largo plazo. Cuando los equipos de TI están apagando fuegos, a menudo no tienen la ocasión de identificar y atajar las causas raíz de los incidentes.

Las organizaciones recurren a los servicios de MDR

Como consecuencia de estas amenazas y estos retos operativos, las organizaciones acuden cada vez más a proveedores de servicios de MDR para complementar y ampliar sus capacidades de operaciones de seguridad a nivel interno. Gartner® prevé que, para el 2025, el 60 % de las organizaciones utilizarán proveedores de servicios de MDR, lo que supone un notable aumento con respecto al 30 % de 2023[7].

Aspectos básicos sobre MDR

Las soluciones MDR son servicios 24/7 totalmente gestionados prestados por expertos especializados en detectar y responder a los ciberataques que las soluciones tecnológicas por sí solas no pueden detener. Lo ideal es que el servicio de MDR no se limite a alertarle de una amenaza, sino que también proporcione una respuesta a incidentes integral y actúe en su nombre.

Si combinamos la experiencia humana con tecnologías de protección potentes e inteligencia artificial, los analistas de seguridad pueden detectar, investigar y responder incluso a los ataques más avanzados perpetrados por humanos, lo que permite detener el ransomware, prevenir las filtraciones de datos y evitar interrumpir las operaciones.

No hay que confundir la MDR con la EDR (detección y respuesta para endpoints) ni la XDR (detección y respuesta ampliadas). Aunque tanto la MDR como la EDR y la XDR permiten la búsqueda de amenazas, la EDR y la XDR son herramientas que permiten a los analistas de seguridad de una organización buscar e investigar posibles amenazas; con la MDR, el equipo de analistas especializados de un proveedor de seguridad busca, investiga y neutraliza amenazas en nombre de la organización.

Como mínimo, un proveedor de servicios de MDR debe ofrecer:

- **Supervisión de amenazas 24/7**: un equipo de expertos monitoriza el entorno para identificar comportamientos sospechosos que puedan indicar un ataque o una filtración.
- **Respuesta realizada por humanos**: mitigación remota inmediata para responder, investigar y contener más allá del envío de alertas y notificaciones, sin limitaciones de volumen ni de tiempo dedicado al proceso de detección, investigación y respuesta.
- **Visibilidad completa**: se utiliza una pila tecnológica operada por el proveedor (ya sea propia o seleccionada de Partners exclusivos) para proporcionar visibilidad en todos los endpoints, firewalls, identidades, correo electrónico, red, nube, copias de seguridad y otras fuentes de datos de seguridad.
- **Búsqueda de amenazas realizada por humanos**: se centra en buscar «incógnitas desconocidas», es decir, amenazas no detectables en estos momentos por las actuales tecnologías de prevención o detección.
- **Información sobre amenazas**: los contenidos y análisis centrados en las amenazas, también conocidos como ingeniería de detección, se utilizan para detectar amenazas nuevas y emergentes.
- **Detección de amenazas superior**: los proveedores de servicios de MDR especializados detectan más ciberamenazas de las que pueden identificar las herramientas de seguridad por sí solas.

Ventajas de la MDR: resultados de seguridad y empresariales superiores

Hemos señalado las funciones que debe ofrecer un servicio de MDR, pero a la hora de seleccionar un proveedor de MDR, es esencial tener una visión más amplia de cómo puede beneficiar a su organización. Los servicios de MDR deben permitir obtener unos resultados óptimos en materia de seguridad y negocio.

Mejora de las ciberdefensas y reducción del ciberriesgo

Una ventaja significativa de utilizar un proveedor de MDR frente a los programas de operaciones de seguridad internos es una protección superior (y un ciberriesgo menor) contra el ransomware y otras ciberamenazas avanzadas.

Con la MDR, se beneficiará de la amplia y profunda experiencia que aportan los analistas de amenazas del proveedor. Un proveedor de MDR trata con un volumen y una variedad de ataques muy superiores a los de una organización individual, lo que les da una experiencia que es prácticamente imposible de replicar internamente.

Los equipos de MDR también investigan y responden a incidentes todos los días, por lo que utilizan las herramientas de búsqueda de amenazas con más soltura. De esta forma, pueden responder con más rapidez y precisión en todas las fases del proceso, desde la identificación de las señales más relevantes hasta la investigación de posibles incidentes y la neutralización de actividades maliciosas.

Trabajar como parte de un gran equipo también permite a los analistas compartir sus conocimientos e información, lo que acelera aún más la respuesta. Los equipos de MDR con más experiencia recopilan runbooks o playbooks (procesos y protocolos documentados) para cada amenaza o adversario particular que detectan. Una vez que se ha identificado a un adversario durante una investigación, en lugar de tener que realizar una investigación extensa en el momento de un ataque, los analistas se remiten al runbook y pasan directamente a la acción.

Otra ventaja de un servicio de MDR es que puede aplicar información a todos los clientes que compartan el mismo perfil, lo que les permite prevenir de forma proactiva ataques similares en ese conjunto. Si los analistas detectan cualquier señal sospechosa, pueden investigar y remediar la situación rápidamente y así crear inmunidad colectiva para el grupo objetivo.

Aumento de la eficiencia de TI

El 64 % de las empresas quiere que sus equipos de TI dediquen menos tiempo a combatir ciberataques y más a cuestiones estratégicas[8]. Los servicios de MDR deberían hacer posible este objetivo.

La búsqueda de amenazas lleva tiempo y es imprevisible. Para los profesionales de TI que compaginan múltiples tareas y prioridades, puede resultar difícil hacer frente al reto: El 79 % de las organizaciones pequeñas y medianas admiten que no están totalmente al día de la revisión de registros para identificar señales o actividades sospechosas.

Dado el posible impacto de un ataque en la organización, cuando se detecta una actividad sospechosa, es necesario dejarlo todo para que la amenaza pueda investigarse y gestionarse de inmediato. La urgencia inherente a este trabajo puede impedir a los equipos centrarse en tareas más estratégicas y a menudo más interesantes.

Trabajar con un servicio de MDR le permite liberar la carga de trabajo de TI para respaldar las iniciativas centradas en el negocio.

Añada experiencia, no personal

Otra ventaja de utilizar un servicio de MDR es que elimina el problema de contratar cazadores de amenazas y analistas de seguridad especializados. La búsqueda de amenazas es una operación altamente compleja. Los profesionales de este campo deben reunir un conjunto específico y especializado de habilidades, lo que hace que contratar a expertos sea una tarea ardua, si no imposible, para muchas organizaciones.

Mejora del retorno de la inversión (ROI) en ciberseguridad

Un proveedor de MDR de primera clase le ayuda a sacar más partido de sus inversiones en seguridad existentes al integrarse con su pila tecnológica de ciberseguridad actual. Este enfoque desvinculado de cualquier proveedor permite a los analistas optimizar la telemetría de sus tecnologías actuales para aumentar la visibilidad en múltiples puntos de control de seguridad y acelerar la detección, investigación y respuesta a amenazas. Cuanto más puedan ver los analistas, más rápido podrán actuar.

Sin embargo, si se encuentra en una fase más temprana en su camino hacia la ciberseguridad, busque un proveedor de MDR que también ofrezca una amplia cartera de soluciones de seguridad que estén profundamente integradas con su conjunto de herramientas de detección y respuesta, ya que puede disfrutar de importantes ventajas operativas y financieras al consolidarse con un proveedor de plataforma única. En lugar de pagar a un proveedor por la protección de endpoints y a otro por un servicio de MDR, trabajar con el mismo proveedor puede reducir los costes de licencias y los gastos de gestión diarios, al tiempo que ofrece una experiencia integrada.

Además, al reforzar su protección, los servicios de MDR también reducen significativamente el riesgo de sufrir una costosa filtración de datos o un ataque de ransomware y evitan los perjuicios financieros de gestionar un incidente importante. En 2023, el coste medio para remediar un ataque de ransomware fue la desorbitada cifra de 1,82 millones de USD[9]. Por lo tanto, invertir en un servicio como MDR tiene sentido desde el punto de vista financiero.

Mejora de la posición frente a las ciberaseguradoras

En los últimos años, las primas de los ciberseguros han aumentado considerablemente y las solicitudes de pólizas se han vuelto más complejas y lentas. Las aseguradoras están exigiendo controles cibernéticos más estrictos; de hecho, el 95 % de las organizaciones que contrataron un seguro el año pasado afirmaron que la calidad de sus defensas afectó directamente a su posición en el mercado asegurador[10].

La clave para optimizar su posición frente a las aseguradoras es minimizar su ciberriesgo. Invertir en defensas sólidas, incluidos servicios de seguridad 24/7 y herramientas de detección y respuesta líderes en la industria, aporta múltiples ventajas para el seguro:

1. Facilita la contratación de un ciberseguro (es decir, mejora la asegurabilidad).
2. Ayuda a reducir las primas y a mejorar las condiciones.
3. Reduce la probabilidad de una reclamación y el consiguiente aumento de las primas.
4. Reduce el riesgo de impago en el caso de una reclamación.

Los servicios que ofrecen capacidades de detección y respuesta optimizadas y, por tanto, minimizan el riesgo de que se produzca un ciberincidente, son considerados el criterio de referencia por las ciberaseguradoras. Las organizaciones que utilizan servicios de MDR suelen ser consideradas clientes de «nivel 1» por las aseguradoras, ya que representan el nivel de riesgo más bajo.

Consideraciones clave

Ahora que tiene una idea más clara de los elementos que caracterizan a un servicio de MDR de primera categoría, le presentamos algunos factores que debe tener en cuenta antes de valorar a los posibles proveedores.

1. **Identifique lo que quiere conseguir.**
   Para su organización, ¿cuál es la definición de éxito? Todo ello dependerá de sus retos y motivaciones actuales para utilizar un servicio de MDR.
2. **Identifique cómo desea trabajar con el servicio de MDR.**
   Analice sus operaciones de TI/ciberseguridad actuales, el papel (si lo hay) que quiere que desempeñe su equipo actual y lo que quiere que haga el servicio de MDR. ¿Necesita cobertura adicional para las noches, los fines de semana y los días festivos? ¿Quiere que el servicio de MDR le notifique los problemas para que pueda tomar medidas o que ejecute acciones de respuesta en su nombre?
3. **Identifique sus inversiones actuales en seguridad.**
   Conozca bien las tecnologías de TI y de seguridad que ya utiliza, como la protección de endpoints, los firewalls de red, las puertas de enlace de correo electrónico, las soluciones de identidad, etc. Lo ideal es que el servicio de MDR pueda utilizar la telemetría de esos productos para darle más visibilidad de su entorno con el fin de detectar, investigar y responder más rápidamente.

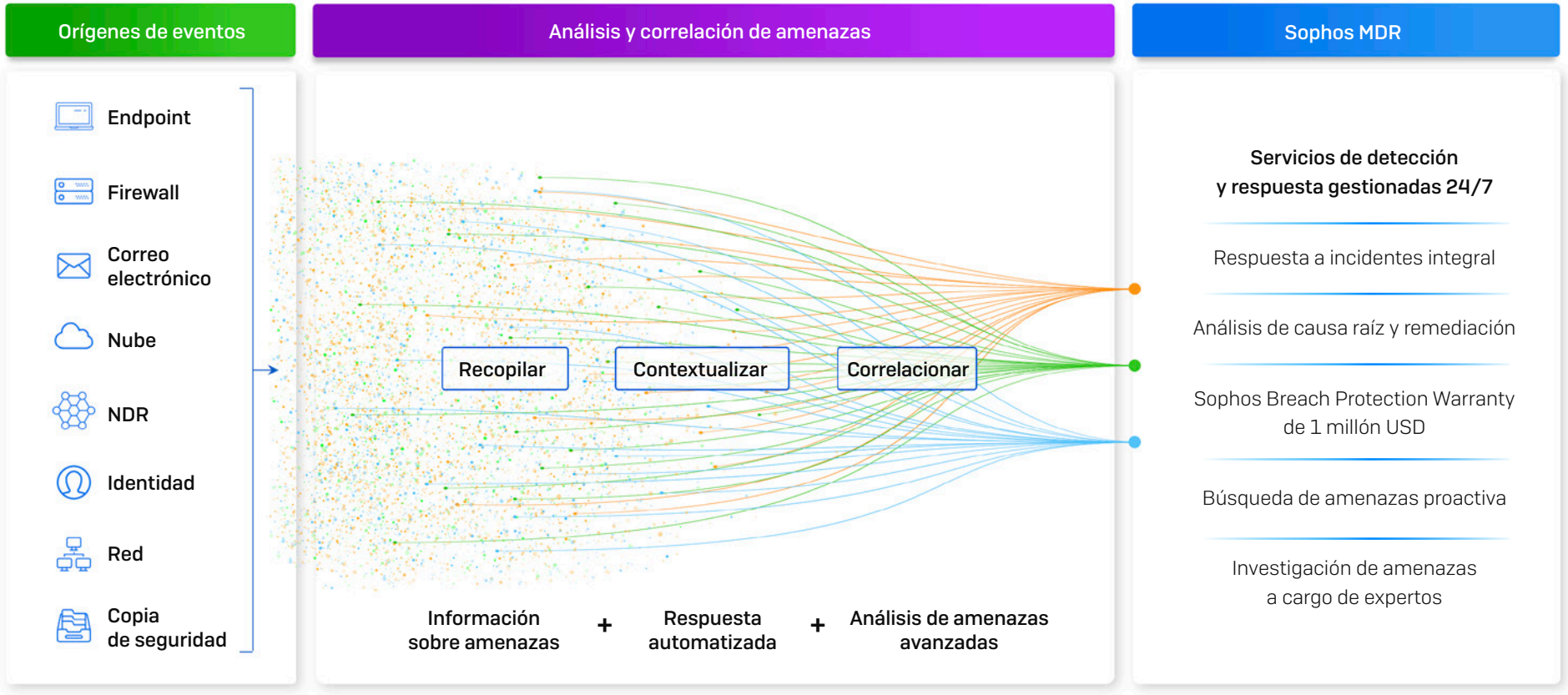
Evaluación de los servicios de MDR: las 10 principales preguntas que hacer

Una vez que haya concretado sus requisitos, a continuación le sugerimos las preguntas que debe plantear a un posible proveedor.

1. ¿Qué soluciones de seguridad nativas ofrece que puedan usar sus analistas de MDR (por ejemplo, protección de endpoints, seguridad del correo electrónico, etc.)?
2. ¿Puede el servicio integrarse con las soluciones de ciberseguridad que ya tengo de otros proveedores?
3. ¿Qué valor aportan estas integraciones a sus analistas de MDR?
4. ¿Cuánto tiempo suele tardar su equipo en responder a las amenazas?
5. ¿Qué acciones de respuesta puede ejecutar su equipo en mi nombre y qué medidas debe tomar mi equipo?
6. Si mi organización crece de forma repentina, ¿puede el servicio de MDR adaptarse a ese crecimiento?
7. ¿Qué niveles de soporte e interacción ofrece? ¿Ofrece niveles de servicio personalizados?
8. ¿Qué opinan sus clientes actuales de su servicio?
9. ¿Incluye su servicio una respuesta a incidentes integral para interrumpir, contener y eliminar por completo las amenazas activas? ¿Se incluye esta capacidad en el servicio principal o se considera un extra?
10. ¿Ofrece una garantía de protección contra filtraciones?

Sophos Managed Detection and Response (MDR)

Sophos MDR es un servicio 24/7 totalmente gestionado prestado por expertos que detectan y responden a ciberataques dirigidos contra sus ordenadores, servidores, redes, cargas de trabajo en la nube, cuentas de correo electrónico y más Con Sophos MDR, nuestro equipo de expertos detiene los ataques avanzados dirigidos por humanos y toma medidas inmediatas para neutralizar las amenazas antes de que puedan interrumpir las operaciones de su negocio o vulnerar sus datos confidenciales.



Una MDR que se adapta a sus necesidades

Sophos MDR es el servicio de detección y respuesta gestionadas más utilizado del mundo. Protege a organizaciones de todos los sectores, desde pequeñas empresas con recursos de TI limitados hasta grandes compañías con equipos internos de operaciones de seguridad. Los tres modelos de respuesta de Sophos MDR más populares son:

- Sophos MDR gestiona la respuesta a amenazas en su nombre.
- Sophos MDR trabaja en colaboración con su equipo de seguridad interno para gestionar la detección de amenazas y las medidas de respuesta.
- Sophos MDR da soporte y complementa a su equipo interno, alertándoles de incidentes que requieren atención y ofreciendo información sobre amenazas y orientación para remediarlas.

Gracias a nuestro enfoque flexible, Sophos puede satisfacer las necesidades específicas de su organización. Tanto si desea un servicio 24/7 totalmente gestionado como si requiere apoyo para su equipo interno, nosotros nos adaptamos.

Cobertura 24/7 desde siete centros de operaciones de seguridad (SOC)

Las amenazas las investiga y remedia un equipo global de expertos en detección y respuesta a amenazas basados en siete centros de operaciones de seguridad (SOC) globales repartidos por Norteamérica (Indiana, Utah, Hawái), Europa (Reino Unido/Irlanda, Alemania) y Asia-Pacífico (India, Australia).

Con más de 500 analistas experimentados que abarcan todo el entorno de amenazas, incluidos expertos en malware, automatización, IA y remediación, Sophos MDR cuenta con una amplia y profunda experiencia que es casi imposible de reproducir internamente.

Tiempos de detección y respuesta líderes en el mundo

Esta combinación única de experiencia humana, tecnológica y en amenazas permite a Sophos MDR ofrecer un tiempo de respuesta a incidentes único en el mundo de tan solo 38 minutos que, a su vez, ofrece resultados superiores en ciberseguridad:

- Tiempo medio de detección (MTTD): 1 minuto
- Tiempo medio de investigación (MTTI): 25 minutos
- Tiempo medio de respuesta (MTTR): 12 minutos

Sophos Breach Protection Warranty

Más organizaciones confían en Sophos para la MDR que en cualquier otro proveedor de seguridad. Con la Sophos Breach Protection Warranty, los clientes de Sophos MDR Complete disfrutan de la confianza y la tranquilidad de saber que cuentan con cobertura financiera si se produce una filtración.

La Sophos Breach Protection Warranty se incluye sin ningún cargo adicional en nuestra suscripción a **Sophos MDR Complete**. Cubre:

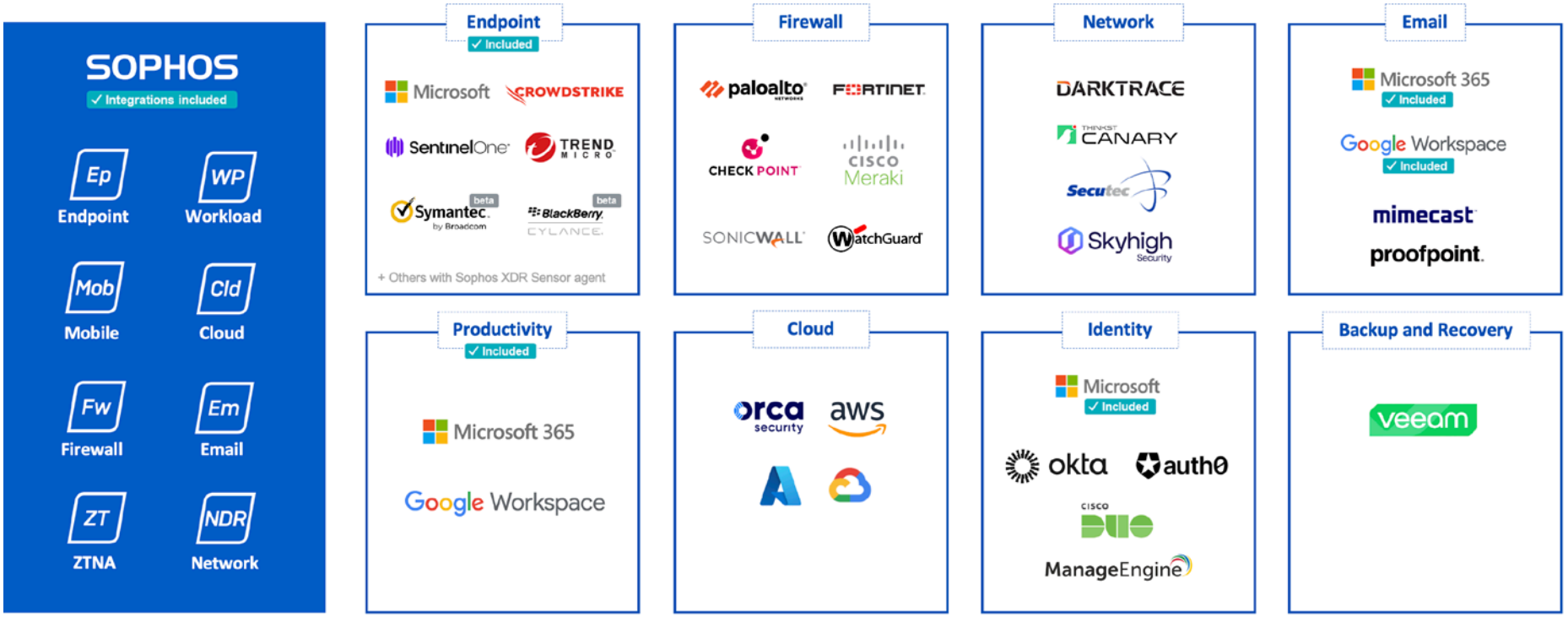
- Hasta 1 millón USD en gastos totales de respuesta para los clientes que cumplan los requisitos.
- Hasta 100 000 USD de pago de rescate (como parte del límite por dispositivo).
- Hasta 1000 USD por equipo vulnerado.
- Cubre varios gastos incurridos, como los de notificación de filtraciones de datos, de RR. PP., legales y de cumplimiento.

Para conocer todos los términos y condiciones de la garantía, consulte es.sophos.com/legal.

Compatibilidad líder en el sector

Tanto si desea utilizar las herramientas de Sophos como si prefiere las tecnologías que ya tiene o una combinación de ambas, Sophos MDR cuenta con extensas integraciones en toda la pila de TI, incluidas soluciones nativas y de terceros para endpoints, redes, la nube, el correo electrónico y Microsoft 365.

Nuestro enfoque desvinculado de cualquier proveedor permite a los analistas tener una visibilidad amplia de todo su entorno de TI, lo que refuerza la detección, investigación y respuesta a amenazas. Además, estas integraciones aumentan el rendimiento de sus inversiones actuales. Las integraciones son, entre otras:



Las soluciones Sophos Endpoint y Sophos Workload Protection están incluidas con Sophos XDR y MDR. Las integraciones de otros productos de Sophos requieren una suscripción a la solución correspondiente.

Las integraciones con soluciones de endpoints, Microsoft y Google Workspace de terceros se incluyen con las suscripciones a Sophos XDR y MDR sin cargo adicional.

Los paquetes de integración para otras soluciones que no sean de Sophos están disponibles como suscripciones complementarias para cada categoría de integración. Las licencias se basan en el número total de usuarios y servidores.

Integraciones a fecha de 8 de febrero de 2024. Para obtener una lista actualizada, póngase en contacto con su representante o Partner de Sophos.

Sophos MDR: ofrezca resultados de seguridad y empresariales superiores

Al principio de esta guía hemos hablado de los resultados que debe ofrecer cualquier servicio de MDR. Analicemos ahora cómo Sophos MDR ofrece unos resultados empresariales y de seguridad superiores.

Mejora de las ciberdefensas y reducción del ciberriesgo

Los analistas de Sophos tienen una amplia y profunda experiencia y una soltura en el uso de las herramientas de telemetría y búsqueda de amenazas que son casi imposibles de reproducir internamente. De esta forma, pueden responder con rapidez y precisión en todas las fases del proceso, desde la identificación de señales relevantes hasta la investigación de posibles incidentes y la neutralización de actividades maliciosas.

Sophos MDR protege a más organizaciones que ningún otro proveedor, lo que nos permite ofrecer una «inmunidad comunitaria» sin igual. La información que se obtiene al defender a un cliente se aplica automáticamente a todos los demás con un perfil similar, lo que permite a Sophos prevenir ataques similares de forma proactiva en ese grupo.

★★★★★

«Los técnicos de pruebas de penetración se sorprendieron enormemente de que no lograron entrar de ninguna manera. En ese punto supimos que podíamos confiar plenamente en el servicio de Sophos».

University of South Queensland, Australia

★★★★★

«Con Sophos MDR, hemos reducido nuestro tiempo de respuesta a amenazas drásticamente».

Tata BlueScope Steel, India

★★★★★

«Recibimos notificaciones de cualquier amenaza en tiempo real».

Bardiani Valvole, Italia

Mayor eficacia e impacto de sus inversiones en seguridad

Sophos MDR le permite incrementar la eficacia y el efecto de su personal y sus herramientas de seguridad. La detección y respuesta a las amenazas consumen grandes cantidades de recursos de TI. Sophos MDR asume esta carga, lo que libera valiosos recursos de TI para la ejecución de programas estratégicos.

Paralelamente, el acceso telefónico 24/7 a los expertos en operaciones de seguridad de Sophos y los informes detallados sobre la actividad de las amenazas a través de la plataforma Sophos Central agilizan la labor de los equipos internos al permitirles responder con mayor rapidez y precisión a las alertas.

Sophos MDR refuerza sus defensas al utilizar la telemetría de sus herramientas de seguridad existentes para aumentar la visibilidad y acelerar la detección y respuesta a amenazas. Esto le permite aumentar el rendimiento de sus inversiones actuales.

★★★★★

«En lugar de dedicar tiempo a investigar y buscar información sobre amenazas manualmente, con Sophos MDR tengo a mi disposición a un gran equipo de expertos en la materia que se encargan de gestionar esas alertas por mí».

United Musculoskeletal Partners, EE. UU.

★★★★★

«Desde que implementamos Sophos, hemos logrado liberar un número importante de horas operativas, lo que ha permitido a nuestros equipos centrarse en iniciativas que han incrementado la satisfacción de nuestros estudiantes».

London South Bank University, Reino Unido

★★★★★

«La capacidad de Sophos MDR para remediar o eliminar amenazas de forma rápida y alertarnos sobre ellas nos libera para que podamos centrarnos en tareas de alto valor».

Tomago Aluminium, Australia

Añada experiencia, no personal

En Sophos, más de 500 analistas expertos prestan servicios de MDR de forma continuada a más de 20 000 clientes de todo el mundo. Sophos MDR permite a las organizaciones ampliar sus capacidades en operaciones de seguridad sin incrementar su plantilla.

★★★★★

«Ahora disponemos de un centro de seguridad ampliado sin necesidad de crear nuestro propio departamento interno».

Hammondcare, Australia

★★★★★

«Con un equipo de MDR experimentado como el de Sophos, contamos con profesionales que dominan su oficio».

United Musculoskeletal Partners, EE. UU.

★★★★★

«Sophos MDR nos ha ayudado a seguir el ritmo a las ciberamenazas, cada vez más numerosas y sofisticadas, sin tener que ampliar nuestro equipo de operaciones de seguridad».

Tourism Finance Corporation of India Limited, India

★★★★★

«Sophos nos ahorra el gasto de contratar a cinco nuevos empleados para hacer este trabajo».

AG Barr, Reino Unido

Mejora de la posición frente a las ciberaseguradoras

Sophos MDR permite a las organizaciones cumplir muchos de los requisitos de control cibernético esenciales para garantizar la asegurabilidad y mejores ofertas de pólizas, como la detección y respuesta 24/7, la planificación de la respuesta a ciberincidentes, el registro y la supervisión, y mucho más.

Los clientes de Sophos MDR afirman haber mejorado el acceso a la cobertura de ciberseguridad, así como a pólizas que reconozcan y recompensen el hecho de haber reducido sus ciberriesgos. Además, varias aseguradoras líderes reconocen la reducción del ciberriesgo que supone nuestro servicio y ofrecen descuentos exclusivos en las primas y elegibilidad automática para los clientes de Sophos MDR. Para obtener más información, póngase en contacto con su Partner de Sophos.

★★★★★

«Nuestra decisión de asociarnos con Sophos para XDR y MDR fue un factor importante para conseguir una reducción de las primas de ciberseguridad frente a lo que nos dijeron al principio, que habría supuesto duplicarlas. Es una gran victoria que demuestra un valor real. De hecho, recibí un mensaje del director financiero dando las gracias al equipo por lo que habíamos conseguido, y MDR fue una parte muy importante de ello».

Bob Pellerin, CISO, The Fresh Market, Estados Unidos

El servicio MDR en el que más confía el mundo

Sophos es el primer proveedor de MDR del mundo, ya que protege a más organizaciones que cualquier otro proveedor contra el ransomware, las filtraciones y otras amenazas que la tecnología por sí sola no puede detener. Sophos MDR protege a organizaciones de todos los sectores en todo el mundo, lo que nos aporta una experiencia con una profundidad y amplitud sin precedentes sobre las amenazas a las que se enfrentan los distintos sectores.

Gartner® Peer Insights™

Sophos es la solución MDR mejor valorada y con más reseñas en Gartner® Peer Insights™, con una puntuación de 4,8/5 en 435 reseñas (más que cualquier otro proveedor) a 23 de enero de 2024 y un 97 % de clientes que afirman que nos recomendarían. Además, Sophos fue el único proveedor en recibir la distinción Customers' Choice en 2023 en todas estas categorías:

- Detección y respuesta gestionadas
- Plataformas de protección de endpoints
- Firewalls de red
- Defensa frente a amenazas móviles

Magic Quadrant™ de Gartner® de plataformas de protección de endpoints

Sophos ha sido nombrado líder en el Magic Quadrant™ de Gartner® 2023 para plataformas de protección de endpoints (EPP), lo que supone nuestro 14.º reconocimiento consecutivo como líder en esta categoría.

El informe ofrece una evaluación exhaustiva de las soluciones de protección para endpoints más predominantes del sector y analiza las ofertas de XDR y MDR. La solidez de nuestra plataforma XDR y de nuestro servicio de MDR contribuyó a que sigamos siendo líderes en esta evaluación.

IDC MarketScape 2024 para la seguridad moderna mundial de endpoints para pequeñas y medianas empresas

Estos informes de IDC MarketScape evalúan a los proveedores en función de cómo sus capacidades de protección de endpoints, EDR y MDR satisfacen las necesidades de las pequeñas y medianas empresas. La solidez de nuestro servicio de MDR contribuyó a posicionarnos como líder en ambas evaluaciones.

Informes G2 Grid®

Sophos ha sido nombrado líder en los informes G2 Grid® de detección y respuesta gestionadas, y líder para MDR en los segmentos de G2 General, Medianas empresas y Grandes empresas. En los informes de G2 de invierno de 2024, Sophos ha sido nombrado líder en varias categorías, como XDR, EDR, firewalls de red y protección de endpoints.

Evaluaciones MITRE Engenuity ATT&CK 2023

Sophos destacó en las evaluaciones MITRE Engenuity ATT&CK® de 2023, centradas explícitamente en la detección y respuesta a amenazas. Nuestra solución XDR, Sophos XDR, detectó el 99 % de los comportamientos de los adversarios en el estudio y registró datos analíticos exhaustivos para el 98 % de los subpasos de las evaluaciones.

El resultado es significativo, ya que Sophos XDR apuntala nuestro servicio de MDR. Los analistas de Sophos MDR utilizan nuestras funciones XDR para ayudar a acelerar la detección y respuesta a amenazas.

Evaluación MITRE Engenuity ATT&CK 2022 para proveedores de servicios de seguridad

Sophos MDR sobresalió en cada uno de los componentes de la evaluación ATT&CK® 2022 para proveedores de servicios de seguridad, la primera evaluación ATT&CK para servicios gestionados. Sophos logró un rendimiento excepcional en las detecciones analíticas, la cobertura de los subpasos, la consolidación de alertas y el análisis humano durante la evaluación.

Resumen

A medida que los adversarios evolucionan y se adaptan, la MDR se está convirtiendo rápidamente en una protección indispensable para las organizaciones de todos los tamaños. Trabajar con un proveedor de MDR de confianza y eficacia probada como Sophos ofrece numerosos beneficios, tanto si desea externalizar por completo la búsqueda de amenazas como si prefiere complementar y mejorar sus propios servicios:

1. Reforzar sus ciberdefensas
2. Aumentar su eficiencia de TI
3. Añadir experiencia y no personal
4. Mejorar su ROI de ciberseguridad
5. Optimizar su posición frente a las ciberaseguradoras

Para obtener más información acerca de Sophos MDR, hable con su Partner de Sophos o visite es.sophos.com/mdr.

1 Informe de protección digital de Microsoft 2023
2 El estado de la ciberseguridad 2023: el impacto de los adversarios en el negocio, Sophos
3 Detenga a los adversarios activos: Lecciones desde la primera línea de combate cibernética, Sophos [hace referencia a los ataques de ransomware por tener los indicadores más fiables y objetivos en el análisis]
4 Detenga a los adversarios activos: Lecciones desde la primera línea de combate cibernética, Sophos
5 El estado de la ciberseguridad 2023: el impacto de los adversarios en el negocio, Sophos
6 El estado de la ciberseguridad 2023: el impacto de los adversarios en el negocio, Sophos
7 Guía de mercado de servicios de detección y respuesta gestionadas de Gartner® 2023
8 El estado de la ciberseguridad 2023: el impacto de los adversarios en el negocio, Sophos
9 El estado del ransomware 2023, Sophos
10 Guía de Sophos sobre ciberseguros, Sophos

Para obtener más información sobre Sophos MDR y cómo permite a las organizaciones reducir los ciberriesgos, aumentar la eficacia y el impacto de las inversiones en seguridad y mejorar la asegurabilidad, visite es.sophos.com/mdr.

2023-02-27 (WP-NP)

SOPHOS