SOPHOS

LIBRO ELECTRÓNICO

EDR, XDR Y MDR

¿Cuál es la diferencia? ¿Y qué solución es la adecuada para su negocio?

CONTENIDO

EDR, XDR Y MDR

¿Cuál es la diferencia? ¿Y qué solución es la adecuada para su negocio?

Los responsables de TI y seguridad se enfrentan a una presión cada vez mayor para reforzar la ciberresiliencia sin sobrecargar a unos equipos y unos presupuestos ya de por sí limitados. Debido al creciente volumen de amenazas y a la sofisticación de los ataques, resulta imprescindible realizar inversiones inteligentes en funcionalidades de detección y respuesta.

Tanto si opera a escala global como si gestiona un equipo más reducido, la clave reside en adaptar su enfoque de seguridad al perfil de riesgo y la situación operativa de su organización. Para muchos líderes, elegir el enfoque adecuado hacia la detección y respuesta también significa decidir si gestionarlo por cuenta propia o trabajar con un Partner de confianza. La detección y respuesta para endpoints (EDR), la detección y respuesta ampliadas (XDR) y la detección y respuesta gestionadas (MDR) ofrecen ventajas únicas, pero el verdadero reto es identificar cuál de estas soluciones aporta más valor a su organización. EDR y XDR son herramientas que ayudan a su equipo a detectar, investigar y responder. La MDR ofrece servicios de supervisión y respuesta 24/7 por parte de analistas expertos, que suelen utilizar XDR y otras tecnologías.

El primer paso para desarrollar una estrategia de seguridad, que le proteja hoy y le prepare para ser resiliente en el futuro, consiste en comprender qué diferencia a estos enfoques y cómo pueden complementarse entre sí.

Por qué son importantes la detección y la respuesta

Disponer de una protección robusta para endpoints sigue siendo una primera línea de defensa crítica. Sin embargo, los ciberdelincuentes sofisticados explotan credenciales legítimas, suplantan la identidad de usuarios de confianza y hacen un uso indebido de las herramientas de TI nativas para eludir las defensas. Posiblemente estos ataques parezcan inofensivos para una sola herramienta preventiva, y precisamente por eso tienen éxito.

Las capacidades de detección y respuesta, como EDR, XDR y MDR, cubren esta carencia crítica. Le ayudan a identificar y neutralizar las amenazas que logran eludir las medidas de prevención antes de que puedan convertirse en incidentes en toda regla.

¿QUÉ ES LA EDR?

La detección y respuesta para endpoints (EDR) forma parte de una estrategia de seguridad continua para endpoints. Ayuda a los equipos a supervisar, detectar y responder a amenazas e incidentes de seguridad en endpoints como, por ejemplo, ordenadores portátiles, ordenadores de sobremesa y servidores.

Ventajas principales de la EDR:

Proporciona visibilidad en tiempo real de la actividad de los endpoints (por ej. ejecución de archivos, comportamiento de procesos y movimientos laterales) para que los equipos puedan detectar y detener rápidamente las amenazas antes de que se propaguen.

Detecta amenazas esquivas mediante la identificación de indicadores de comportamiento, contribuyendo a detectar ataques que las herramientas de prevención tradicionales suelen pasar por alto con frecuencia.

Automatiza acciones de respuesta como el aislamiento de endpoints afectadas o la terminación de procesos maliciosos, lo que reduce el tiempo de permanencia y evita que los atacantes obtengan más acceso.

Descubra cómo Sophos EDR puede proteger sus endpoints y servidores frente a ataques avanzados perpetrados por humanos, ya sea en la oficina, la red o la nube.

¿QUÉ ES LA XDR?

La detección y respuesta ampliadas (XDR) mejoran la visibilidad de las amenazas mediante la integración de datos de todo su ecosistema de seguridad, más allá de los endpoints y los servidores. Incluye firewalls, correo electrónico, infraestructura en la nube, sistemas de identidad, soluciones de copia de seguridad y recuperación, herramientas de productividad, endpoints y servidores, y más. La XDR permite una correlación más eficaz de las actividades sospechosas, contribuyendo a identificar ataques multivectoriales sofisticados que las herramientas aisladas podrían pasar por alto.

Mientras que la EDR examina con detalle lo que ocurre en cada endpoint, la XDR amplía esa visibilidad a todo el ecosistema de seguridad y permite correlacionar eventos entre todos los sistemas. Proporciona una visión integral de un ataque, lo que facilita la detección de amenazas multivectoriales de varias fases que, de otro modo, pasarían desapercibidas.

Ventajas principales de la XDR:

Correlaciona señales procedentes de múltiples vectores de ataque para descubrir patrones y priorizar alertas de alta fiabilidad. Esto reduce el ruido y permite enfocar amenazas complejas que afectan a múltiples sistemas.

Optimiza los flujos de trabajo de investigación para que su equipo pueda responder más rápido y con mayor confianza. Los analistas obtienen una visibilidad clara de cómo se desarrolló un ataque y cómo evitar que vuelva a ocurrir.

Admite flujos de trabajo de investigación y respuesta utilizando herramientas basadas en IA que aceleran el análisis y la remediación, facilitando una solución de incidentes más rápida y segura.

Descubra cómo Sophos XDR le permite detectar, investigar y responder a actividades sospechosas en todo tu ecosistema.

¿QUÉ ES LA MDR?

La detección y respuesta gestionadas (MDR) es un modelo basado en servicios que combina IA con analistas humanos expertos para proporcionar supervisión continua 24/7, búsqueda de amenazas y respuesta a incidentes. Es especialmente valiosa para organizaciones que no operan 24/7 o que sufren brechas en la cobertura de su SOC, dificultades para contratar personal o un incremento en la complejidad de su entorno.

La MDR puede funcionar como una solución totalmente externalizada o como una extensión cogestionada de su propio equipo interno, contribuyendo a reducir el tiempo de permanencia y deteniendo incidentes, por ejemplo, ataques de ransomware, antes de que se agraven.

Ventajas principales de la MDR:

Cobertura 24/7. Las amenazas no siguen un horario de 9 a 5: El 88 % de los ataques de ransomware se producen fuera del horario laboral habitual. La MDR garantiza una cobertura 24/7.

Acceso a analistas de seguridad expertos que comprenden el comportamiento de los atacantes y actúan con decisión. Estos especialistas gestionan incidentes a diario, priorizando y conteniendo las amenazas para que su empresa siga funcionando sin problemas.

Eliminación de la fatiga provocada por la sobrecarga de alertas y la clasificación manual. La MDR se abre paso a través del ruido, para que su equipo pueda centrarse en iniciativas estratégicas en lugar de perseguir falsos positivos.

Solución rápida cuando más importa. En incidentes críticos como los ataques de ransomware, los equipos de MDR pueden detectar y contener amenazas antes incluso de que los equipos internos sean conscientes de ellas, evitando interrupciones y reduciendo el riesgo.

Descubra cómo Sophos MDR, con su plataforma abierta basada en IA y su equipo de analistas expertos, puede complementar a su organización y acompañarle en su andadura en seguridad.

CUÁNDO PLANTEARSE QUE SOLUCIÓN, EDR, XDR O MDR, ES LA ADECUADA

Solución	Podría planteársela si...	Puede que no sea la mejor opción si...
EDR	• Necesita una detección y respuesta robusta para endpoints. • Desea mejorar sus defensas más allá de las herramientas preventivas para la protección de endpoints. • Está desarrollando una estrategia de defensa por capas que pueda integrarse en el futuro con XDR o MDR.	• Necesita una mayor visibilidad en todo su entorno (nube, identidad, red, copias de seguridad, etc.). • Busca funcionalidades de detección y respuesta 24/7 sin tener que externalizar el servicio ni contratar a más personas.
XDR	• Necesita una visión unificada de todos los vectores de ataque clave, incluidos endpoints, firewalls, red, nube, identidad, copias de seguridad y herramientas de productividad. • Desea una correlación de amenazas más rápida y una reducción de la fatiga provocada por alertas. • Quiere mejorar el ROI de sus inversiones actuales y futuras en tecnología de seguridad y TI.	• Solo supervisa endpoints y servidores. • Necesita más apoyo en la práctica del que su equipo puede ofrecer. • No cuenta con los recursos internos necesarios para gestionar una plataforma XDR.
MDR	• Necesita detección y respuesta a amenazas 24/7 a cargo de expertos. • Su plantilla está sufriendo fatiga provocada por alertas, escasez de personal experto o agotamiento. • Desea un Partner proactivo que investigue y neutralice amenazas en su nombre. • Desea mejorar su posición frente a la ciberaseguradoras, reducir potencialmente las primas y ampliar la cobertura.	• Ya cuenta con operaciones de seguridad maduras, una plantilla completa y capacidades a nivel interno que proporcionan cobertura 24/7/365. • No está preparado para externalizar parte de sus operaciones de detección y respuesta.

OTROS ASPECTOS A TENER EN CUENTA ANTES DE TOMAR UNA DECISIÓN

A la hora de evaluar sus opciones, existen varios factores críticos que pueden determinar si EDR, XDR o MDR es la opción más adecuada, y qué Partner puede cumplir esa promesa.

La información sobre amenazas es importante

La eficacia de cualquier solución de detección y respuesta depende de la calidad de la información sobre amenazas que la sustenta. Cuanto más amplia, profunda y actualizada sea, antes será posible identificar y detener las amenazas. Asegúrese de que cualquier proveedor que se esté planteando pueda explicar el origen y el alcance de sus datos sobre amenazas.

Un servicio debe ser algo más que una promesa

Incluso la mejor tecnología puede resultar insuficiente si se carece de un soporte con capacidad de respuesta. Ya gestione usted mismo la solución o cuente con el apoyo de un Partner de servicios gestionados, necesita saber que obtendrá ayuda cuando la necesite. Pregunte a los proveedores cómo funciona el soporte en la práctica: Quién responde, con qué rapidez, qué se incluye y cómo obtener ayuda durante un incidente activo.

El coste no siempre es lo que parece

No asuma que alguna opción es intrínsecamente más cara. Los precios varían en gran medida en cómo se implemente y se preste soporte para cada solución. Céntrese en el análisis de sus necesidades específicas, su personal e inversiones actuales, incluidos los posibles compromisos entre tecnologías y coste de recursos internos frente a recursos externalizados.

Las soluciones de detección y respuesta, especialmente la MDR, pueden influir en los costes de los ciberseguros. Muchas aseguradoras valoran ahora positivamente disponer de supervisión y respuesta a amenazas 24/7, lo que puede traducirse en primas más bajas o mejores condiciones de cobertura.

Un análisis detallado del ROI, que tenga en cuenta el ahorro operativo, la reducción del riesgo e incluso las prestaciones del seguro, puede ayudarle a comprender el coste y el valor reales de cada enfoque.

CONCLUSIÓN

1,53 millones USD

El coste medio de recuperarse de un ataque de ransomware, antes de incluir el pago de cualquier rescate, *

40 %

de las organizaciones afectadas por ransomware afirman que la falta de expertos en ciberseguridad facilitó el ataque*

Hay demasiado en juego como para apoyarse en conjeturas.

Elegir la estrategia adecuada de detección y respuesta no trata solo de la tecnología, sino de capacitar a su equipo, proteger sus operaciones y construir una ciberdefensa resiliente y duradera.

*Informe del estado del ransomware 2025 de Sophos

SOPHOS

SOPHOS
DEFEAT CYBERATTACKS

OBTENGA MÁS INFORMACIÓN SOBRE LAS SOLUCIONES Y LOS SERVICIOS DE SOPHOS

Sophos le ayuda a detectar y responder mejor a las amenazas tanto ahora como en el futuro, conforme vayan evolucionando sus necesidades de seguridad.

Hable con un experto de Sophos y trabajemos juntos para encontrar la solución adecuada para su empresa.