Sophos MDR para Microsoft Defender

Respuesta a amenazas a cargo de expertos para entornos de Microsoft

Sophos Managed Detection and Response (MDR) para Microsoft Defender amplía su equipo con expertos altamente cualificados que supervisan, investigan y responden a las alertas de Microsoft Security 24/7.

Maximice su inversión en Microsoft Security

Muchas organizaciones han invertido en la suite de Microsoft Security, pero es posible que no dispongan de suficientes expertos en plantilla para utilizar eficazmente la pila tecnológica multiproducto de Microsoft para detectar, investigar y responder a cientos de alertas de seguridad todos los días:

- El déficit de profesionales de ciberseguridad a escala global asciende a 3,4 millones[1].
- El 71 % de los equipos de seguridad tienen dificultades para determinar qué alertas de seguridad deben investigar en medio del ruido generado por sus herramientas[2].
- El tiempo medio de respuesta a las amenazas para las organizaciones con un equipo de operaciones de seguridad dedicado es de 16 horas, lo que deja a los atacantes tiempo suficiente para operar dentro de la red[3].

Sophos MDR para Microsoft Defender ofrece las funciones de detección, búsqueda y respuesta a amenazas más robustas disponibles para entornos de Microsoft. Nuestros analistas supervisan, investigan y responden a las alertas de Microsoft Security 24/7, ejecutando acciones de respuesta inmediatas realizadas por humanos para detener amenazas confirmadas con un tiempo medio de respuesta líder de 38 minutos, un 96 % más rápido que el estándar del sector.

Detecte y detenga amenazas que escapan a Microsoft Defender

Con Sophos MDR para Microsoft Defender, nuestros expertos en Microsoft Security detectan, investigan y responden a amenazas usando datos de seguridad de los siguientes productos de Microsoft:

- Microsoft Defender for Endpoint
- Microsoft Defender for Identity
- Microsoft Defender for Cloud
- Microsoft Defender for Cloud Apps
- Identity Protection (Azure AD)
- Centro de seguridad y cumplimiento de O365
- Microsoft Sentinel
- Office 365 Management Activity

Asimismo, nuestras detecciones propias, información sobre amenazas de primera clase y búsqueda de amenazas a cargo de humanos añaden capas de defensa adicionales, con lo que se identifican y detienen más amenazas de las que pueden identificar y detener las herramientas de Microsoft Security por sí solas.

Las organizaciones también pueden integrar herramientas de seguridad distintas de Microsoft y fuentes de telemetría de soluciones de Sophos o de decenas de proveedores externos como Palo Alto Networks, Fortinet, Check Point, AWS, Google, Okta, Darktrace y otros para obtener una visibilidad y una protección integrales.

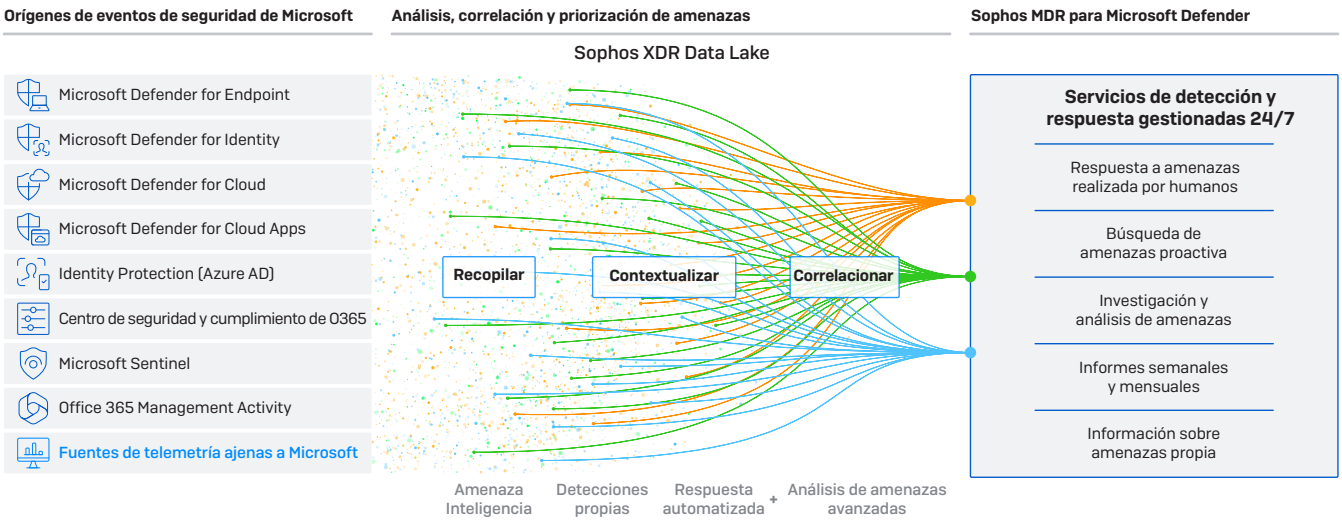
1 Estudio sobre profesionales de ciberseguridad 2022, (ISC)2
2 El estado de la ciberseguridad 2023: el impacto de los adversarios en el negocio, Sophos
3 Base de datos de Gartner Cybersecurity Business Value Benchmark, 2022

Aspectos destacados

- Los analistas de Sophos MDR supervisan, investigan y responden a las alertas de Microsoft Security 24/7 y toman medidas inmediatas para frenar las amenazas confirmadas
- La funcionalidad del servicio va más allá de Microsoft Defender para punto de conexión y Microsoft Sentinel para dar cobertura en toda la plataforma de Microsoft Security
- Cuando se identifica una amenaza activa, el equipo de operaciones de Sophos MDR puede ejecutar un amplio conjunto de acciones de respuesta a amenazas en su nombre
- Las detecciones propias de Sophos, información sobre amenazas y búsquedas de amenazas realizadas por humanos añaden capas adicionales de defensa
- Integre herramientas y fuentes de telemetría ajenas a Microsoft para detener ataques contra su red, sus usuarios y sus clientes

SOPHOS

Sophos MDR para Microsoft Defender: funciones de servicio clave



Supervisión de amenazas 24/7

Nuestros expertos en Microsoft Security detectan y detienen amenazas antes de que puedan comprometer sus datos o interrumpir sus operaciones. Con el respaldo de seis centros de operaciones de seguridad (SOC) globales, Sophos ofrece cobertura las 24 horas.

Respuesta a amenazas realizada por humanos

El equipo de Sophos MDR puede ejecutar un gran número de acciones de respuesta a amenazas en su nombre para interrumpir, contener y neutralizar por completo a los atacantes.
Entre estas acciones de respuesta a amenazas se incluyen:

- Aislar a los hosts mediante Sophos Central
- Aplicar bloqueos de IP de firewall basados en los hosts
- Finalizar procesos
- Forzar el cierre de sesiones de usuarios
- Desactivar cuentas de usuarios
- Eliminar artefactos maliciosos
- Añadir hashes maliciosos a elementos bloqueados en Sophos Central

Para obtener más información, consulte:

sophos.com/microsoft-defender

Búsqueda de amenazas proactiva realizada por humanos

Analistas altamente cualificados buscan amenazas de forma proactiva para detectarlas y eliminarlas rápidamente e identificar comportamientos de atacantes que hayan eludido la detección de los conjuntos de herramientas desplegados.

Compatible con herramientas de seguridad distintas de Microsoft

Sophos MDR se puede integrar con herramientas de seguridad y fuentes de telemetría ajenas a Microsoft para detectar y detener ataques en todo el entorno.

Informes semanales y mensuales

Sophos Central ofrece un acceso sencillo a alertas en tiempo real, informes y opciones de gestión, además de informes semanales y mensuales con datos clave sobre investigaciones de seguridad, ciberamenazas y la postura de seguridad de su organización.

Sesiones informativas mensuales sobre amenazas

El equipo de Sophos MDR presenta todos los meses una sesión llamada "Sophos MDR ThreatCast", que ofrece información sobre las amenazas más recientes y las prácticas de seguridad recomendadas.

Detecciones propias

La plataforma de Sophos incorpora detecciones propias, análisis de amenazas avanzadas y la mejor información sobre amenazas, lo que añade capas de defensa adicionales y permite identificar más amenazas de las que pueden identificar las herramientas de Microsoft Security por sí solas.

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

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

23-07-10 DS-ES (DD)

SOPHOS