Informe de la solución

Sophos XDR

Defiéndase de los adversarios activos con EDR y XDR

Los adversarios mejoran continuamente sus técnicas para explotar vulnerabilidades y acelerar los tiempos de ataque. Reducir el tiempo necesario para detectar y responder a las amenazas nunca ha sido tan importante. La plataforma de detección y respuesta ampliadas (XDR) de Sophos le permite detectar, investigar y responder rápidamente a amenazas de varias fases y a los adversarios activos en todo su ecosistema de seguridad.

Casos de uso

1 | EMPIECE POR UNA DEFENSA SÓLIDA

Resultado deseado: detenga más amenazas desde un principio para reducir su carga de trabajo.

Solución: detenga más filtraciones antes de que comiencen y céntrese en las investigaciones. Sophos XDR ofrece una protección inigualable para detener amenazas avanzadas rápidamente antes de que se agraven. Proteja sus endpoints y servidores usando tecnologías sofisticadas, como la IA, el análisis de comportamientos y funciones antiransomware y antiexploits.

2 | ACELERE LA RESPUESTA A LAS AMENAZAS

Resultado deseado: detecte, investigue y responda a las amenazas rápidamente.

Solución: las detecciones priorizadas por IA que se sirven de la información sobre amenazas procedente de Sophos X-Ops permiten identificar de forma rápida y sencilla los eventos sospechosos que requieren atención inmediata. Realice búsquedas de amenazas y responda rápidamente con flujos de trabajo de investigación optimizados, potentes funciones de búsqueda, herramientas de gestión de casos colaborativas y respuestas automatizadas.

3 | VISIBILIDAD EN TODAS LAS SUPERFICIES DE ATAQUE

Resultado deseado: obtenga una visibilidad total e información clave sobre las amenazas esquivas en todas sus superficies de ataque más importantes.

Solución: utilice las soluciones preparadas para XDR y totalmente integradas de Sophos para obtener visibilidad más allá de los endpoints o sacar partido de sus actuales inversiones tecnológicas. Integre un amplio ecosistema de soluciones de seguridad de terceros para endpoints, firewalls, redes, correo electrónico, identidades y la nube para detectar y responder a las amenazas con una plataforma XDR unificada.

4 | POTENCIA PARA TODOS LOS USUARIOS

Resultado deseado: los técnicos informáticos y analistas de seguridad pueden investigar y responder a las amenazas con facilidad.

Solución: Sophos XDR, diseñado tanto para equipos SOC internos dedicados como para administradores encargados de la seguridad y otras cuestiones de TI, ayuda a maximizar la eficiencia del usuario y ofrece una visibilidad total y orientación para ayudarle a responder a las amenazas.

Gartner

Reconocido en la Guía de mercado de Gartner para la XDR 2023

MITRE ATT&CK

Resultados excepcionales en las evaluaciones MITRE Engenuity ATT&CK 2023

G2 Leader

Valorada como solución XDR n.º 1 por los usuarios de G2 (primavera 2023)

Obtenga más información y pruebe Sophos XDR:
es.sophos.com/xdr

© Copyright 2023. Sophos Ltd. Todos los derechos reservados. Constituida en Inglaterra y Gales N.º 2096520, The Pentagon, Abingdon Science Park, Abingdon, OX14 3YP, Reino Unido Sophos es la marca registrada de Sophos Ltd. Los demás nombres de productos y empresas mencionados son marcas comerciales o marcas registradas de sus respectivos propietarios. El logotipo Gartner Peer Insights es una marca de servicio y marca comercial de Gartner, Inc. y/o sus afiliados, y se utiliza aquí con su permiso. Todos los derechos reservados. El contenido de Gartner Peer Insights consiste en las opiniones de usuarios finales individuales basadas en sus propias experiencias con los proveedores que aparecen en la plataforma; no deben considerarse declaraciones de hecho, ni representan las opiniones de Gartner ni de sus afiliados. Gartner no apoya a ningún proveedor, producto o servicio mencionado en este contenido ni ofrece ninguna garantía, expresa o implícita, con respecto a este contenido, sobre su exactitud o integridad, incluida cualquier garantía de comercialización o conveniencia para fines particulares.

2023-11-08 DS-ES (MP)

SOPHOS