Sophos Rapid Response

Preguntas más frecuentes

¿Tengo que ser cliente de Sophos actualmente para convertirme en cliente de Rapid Response?
No. El servicio Sophos Rapid Response está disponible tanto para los actuales clientes de Sophos como para los que no lo son.

Tengo una infracción de seguridad activa en estos momentos. ¿Qué debo hacer?
Llame a nuestros números regionales de abajo en cualquier momento para hablar con uno de nuestros asesores de incidentes:

Alemania +49 61171186766
Australia +61 272084454
Austria +43 73265575520
Canadá +1 7785897255
EE. UU. +1 4087461064
Francia +33 186539880
Italia +39 02 94752 897
Reino Unido +44 1235635329
Suecia +46 858400610
Suiza +41 445152286

¿Cómo es de rápido el servicio Rapid Response?
Muy rápido. La mayoría de los clientes se incorporan en cuestión en horas y se les clasifica en 48 horas. Puesto que el servicio es totalmente remoto, la respuesta puede iniciarse en cuestión de horas después de contactar con Sophos.

¿Qué es el proceso de incorporación?
El equipo de Rapid Response puede empezar con el proceso de incorporación y comenzar su investigación tan pronto como reciba aprobación. Para las organizaciones que no tengan Sophos XDR instalado en su entorno, Sophos ofrece una opción de despliegue rápido. El equipo de despliegue rápido se especializa en instalaciones rápidas en entornos que estén experimentando un incidente activo en ese momento.

¿Hay algún coste adicional asociado al despliegue rápido?
No. El despliegue rápido está incluido como parte del servicio.

¿Cuál es la metodología de Rapid Response?
Una vez que se ha aprobado Rapid Response y que el cliente ha aceptado nuestro acuerdo de servicio, nos ponemos manos a la obra de inmediato. Rapid Response consta de cuatro fases principales: incorporación, clasificación, neutralización y supervisión.

Incorporación

- Organizar una llamada inicial para establecer las preferencias de comunicación y confirmar (si procede) qué pasos de remediación se han tomado ya
- Identificar la magnitud y el impacto del ataque
- Definir entre las dos partes un plan de respuesta
- Empezar a desplegar el software del servicio

Clasificación

- Evaluar el entorno operativo
- Identificar indicadores de peligro conocidos o la actividad de adversarios
- Recopilar datos e iniciar actividades de investigación
- Colaborar en un plan para iniciar actividades de respuesta

Neutralización

- Retirar el acceso a los atacantes
- Impedir más daños en datos y recursos
- Evitar que continúe la exfiltración de datos
- Recomendar acciones preventivas en tiempo real para abordar el problema

SOPHOS

Preguntas frecuentes sobre Sophos Rapid Response

Monitorización

- Transición al servicio MDR Advanced
- Realizar una supervisión continuada para detectar reincidencias
- Proporcionar un resumen de amenazas tras el incidente

¿En qué idiomas se ofrece Rapid Response?
Actualmente el servicio se ofrece solo en inglés.

¿Sustituye Sophos los servicios de respuesta a incidentes con datos forenses (DFIR) o colabora con ellos?
Sophos puede trabajar en colaboración con servicios DFIR y lo ha hecho en múltiples contratos. Sophos Rapid Response se centra en el aspecto de la respuesta a los incidentes de los servicios DFIR y no proporciona todos los servicios que suele ofrecer un contrato DFIR tradicional.

¿Envía Sophos equipamiento físico? ¿Se envía a los gestores de incidentes a las instalaciones del cliente?
No. Todos los servicios de respuesta a incidentes se realizan de forma remota.

¿Los clientes tienen que instalar Sophos en sus endpoints?
Sí. El servicio Rapid Response se presta a través de Managed Detection and Response (MDR) / Sophos XDR para poder garantizar una supervisión y una respuesta efectivas 24/7. Esto significa que también deberán desinstalar o deshabilitar temporalmente su actual protección para endpoints de otros proveedores.

El equipo de Rapid Response no necesita esperar a que finalice el despliegue para poder empezar a tomar medidas correctivas a fin de contener y neutralizar la amenaza. El equipo se servirá de cualquier dato que esté disponible y utilizará las herramientas que considere adecuadas para ayudar en la respuesta.

¿Cómo se calculan los precios?
Los precios se basan en el número total de usuarios y servidores y se cobra como un plazo fijo de 45 días.

¿Hay algún coste adicional?
No. El servicio no tiene costes ocultos.

¿Qué ocurre al finalizar el período de Rapid Response?
Al final del plazo, los clientes pueden optar por pasarse al servicio completo Sophos Managed Detection and Response (MDR) o dejar que la licencia caduque.

¿Podemos desplegar Rapid Response en un segmento del entorno, o se tiene que actuar sobre la totalidad del entorno?
En situaciones concretas, se puede aplicar Rapid Response solo a un segmento del entorno del cliente. Un especialista de Rapid Response podrá proporcionarle más detalles sobre la definición del alcance del proyecto.

¿Puede trabajar Sophos con un intermediario que represente al cliente, como un gabinete jurídico, en el contrato?
Sí. Es posible trabajar con un intermediario.

¿Puede determinar Sophos qué archivos se han exfiltrado/robado en el ataque?
Como parte del servicio Rapid Response, haremos lo posible por determinar qué archivos (si los hay) se han exfiltrado durante un ataque. Sin embargo, no podemos ofrecer garantías, ya que esto puede depender de los datos que estén disponibles para la investigación.

¿Descifrará Sophos el ransomware en nombre del cliente?
No. Esto no forma parte del servicio Rapid Response.

¿Ayudará Sophos al cliente a negociar o pagar un rescate?
No. Esto no forma parte del servicio Rapid Response.

2023-03-31 (FAQ-PC)

SOPHOS