SOPHOS

Cybersecurity made simple.

Sophos Sandstorm

Defensa de última generación contra amenazas avanzadas sin complicaciones

Sophos Sandstorm utiliza una tecnología next-gen de espacio seguro en la nube para ofrecer a su empresa un nivel de seguridad adicional contra el ransomware y los ataques dirigidos.

Se trata del único espacio seguro de red que utiliza análisis con Deep Learning para ofrecer una detección más efectiva, y se integra con Sophos XG Firewall, Sophos UTM, Sophos Web Appliance, Sophos Email Appliance y Sophos Email en Sophos Central sin necesidad de hardware adicional.

Y ofrece una excelente relación calidad-precio. Obtendrá todas las ventajas de una protección de estándar empresarial sin el coste del estándar empresarial.

Aspectos destacados

- Perfecta integración con su solución de seguridad de Sophos
- En marcha en cuestión de minutos
- Protección contra ransomware, APT, malware desconocido, PUA y ataques dirigidos
- Información sobre amenazas sobre la que puede tomar medidas
- Análisis con Deep Learning
- Informes granulares centrados en incidentes

Protección avanzada frente a ataques dirigidos

Mantenga el ransomware y el malware desconocido que roba datos fuera de su red. Nuestra potente tecnología next-gen de espacio seguro basada en la nube y el análisis con Deep Learning le permiten detectar, bloquear y responder de forma rápida y precisa ante amenazas avanzadas recurrentes y amenazas de día cero.

Ofrecemos seguridad sin complicaciones

Sophos Sandstorm se integra por completo en su solución de seguridad de Sophos. Solo tiene que actualizar su suscripción y aplicar la política de Sandstorm, y estará protegido al instante frente a amenazas dirigidas. Tendrá todo en funcionamiento en cuestión de minutos.

Bloquee amenazas esquivas que otros no ven

Detecte ransomware y amenazas desconocidas diseñadas específicamente para eludir los dispositivos de espacio seguro de primera generación. Nuestro enfoque de simulación de sistema completo ofrece el nivel de visibilidad más profundo sobre el comportamiento de programas maliciosos desconocidos y la detección de los ataques maliciosos que simplemente escapan a otros.

Informes en profundidad

Acelere la respuesta a las amenazas avanzadas con un análisis simple de las infracciones centrado en los incidentes. Le proporcionamos información sobre amenazas avanzadas recurrentes priorizada gracias a la correlación de pruebas. Este enfoque reduce los datos irrelevantes y a la vez le ahorra tiempo.

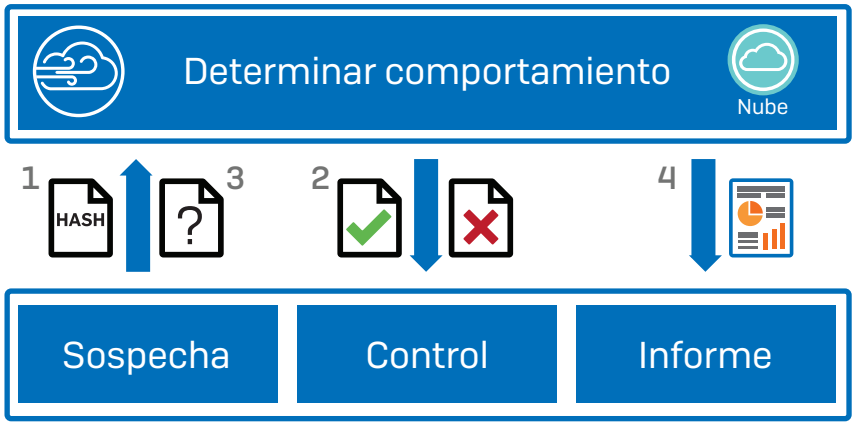
Alto rendimiento

Su solución de seguridad de Sophos realiza un filtrado previo preciso del tráfico, de modo que solo los archivos sospechosos se envían a Sandstorm, con lo que se minimiza la latencia y el impacto sobre el usuario final.

Funciones de Sophos Sandstorm

- Total integración en el panel de control de su solución de seguridad de Sophos
- Inspecciona los ejecutables y los documentos que incluyen contenido ejecutable
  - Ejecutables de Windows (incluidos .exe, .com y .dll)
  - Documentos de Word (incluidos .doc, .docx, docm y .rtf)
  - Documentos PDF
  - Archivos comprimidos que contengan cualquiera de los tipos de archivo mencionados anteriormente (ZIP, BZIP, GZIP, RAR, TAR, LHA/LZH, 7Z, Microsoft Cabinet)
  - Admite más de 20 tipos de archivo
- El análisis dinámico de comportamientos de malware y el Deep Learning ejecutan archivos en entornos reales
- Informes detallados de archivos maliciosos y capacidad de liberar archivos desde el panel de control
  - Tiempo de análisis medio inferior a 120 segundos
  - Opciones de políticas de grupos y usuarios flexibles para el tipo de archivo, exclusiones y acciones sobre el análisis
  - Admite enlaces de descarga de un solo uso

Cómo funciona



1. La solución de seguridad de Sophos escanea los archivos mediante todas las comprobaciones de seguridad convencionales (p. ej., firmas contra programas maliciosos, URL incorrectas, etc.). Si el archivo es ejecutable o incluye contenido ejecutable y no se descarga de un sitio web seguro, el archivo se trata como sospechoso. La solución de seguridad de Sophos envía el hash de archivo sospechoso a Sophos Sandstorm para determinar si se ha analizado anteriormente.
2. Si el hash de archivo se ha analizado anteriormente, Sophos Sandstorm pasa la información de la amenaza a la solución de seguridad de Sophos. En este punto, el archivo se entrega al dispositivo del usuario o se bloquea, en función de la información proporcionada por Sophos Sandstorm.
3. Si el hash no se ha visto previamente, se envía una copia del archivo sospechoso a Sophos Sandstorm. En este punto, se hace detonar el archivo y se supervisa su comportamiento. Una vez que se ha analizado de forma exhaustiva, Sophos Sandstorm pasa la información de la amenaza a la solución de seguridad de Sophos. De nuevo, el archivo se entrega al dispositivo del usuario o se bloquea, en función de la información proporcionada por Sophos Sandstorm.
4. La solución de seguridad de Sophos utiliza la información detallada proporcionada por Sophos Sandstorm para crear informes en profundidad de cada uno de los incidentes de la amenaza.

Pruébelo gratis hoy mismo

Regístrese para una evaluación gratuita de 30 días en es.sophos.com/sandstorm

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

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

03-01-2019 DS (PC)

SOPHOS