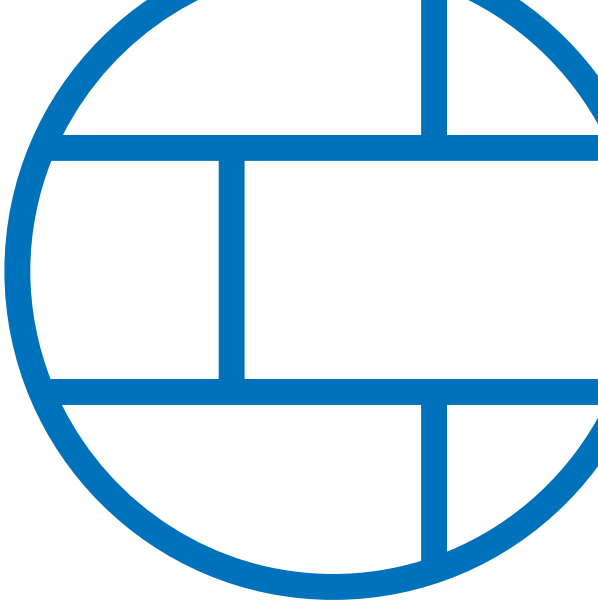
SOPHOS



Guía para la adquisición de firewalls next-gen

Realizamos una encuesta a los administradores de redes sobre los principales problemas que veían en sus firewalls actuales. Algunas de las respuestas fueron las siguientes:

- Visibilidad sobre el tráfico de aplicaciones, los riesgos y las amenazas
- Protección contra las amenazas más recientes
- Sin respuesta ni asistencia cuando hay una amenaza en la red

Si alguno de estos problemas le resulta familiar, no es usted el único. La realidad es que la mayoría de firewalls next-gen no están cumpliendo con su trabajo. No pueden proporcionar la visibilidad adecuada, la protección apropiada ni respuesta alguna.

Puede resultar desafiante incluso saber por dónde comenzar. En primer lugar, conviene que identifique sus requisitos clave. Una vez hecho esto, no tendrá más remedio que enfrentarse a la ardua tarea de leer todos los sitios web y las hojas de datos de los proveedores para determinar qué firewall puede no solo cubrir sus necesidades, sino también hacer el trabajo que se dice que hace.

Cómo utilizar esta guía

Esta guía de compra está diseñada para ayudarle a tomar la decisión más acertada para su empresa y evitar acabar lamentándose como otros compradores de firewalls. Detalla todas las características y funciones que debe tener en cuenta a la hora de evaluar un firewall y decidir su adquisición. También hemos incluido preguntas importantes para su partner o proveedor de soluciones informáticas para determinar si el producto que ofrecen satisface sus necesidades. Y en la última página encontrará un cuadro sinóptico para ayudarle a crear una lista con los proveedores de firewalls más adecuados y así ahorrar tiempo.

Concienciación y control en los firewalls next-gen

Hace tiempo que los firewalls next-gen prometen visibilidad sobre el tráfico de aplicaciones y la actividad de los usuarios en la red pero, a día de hoy, la mayoría no cumplen con esta tarea básica. El problema reside en la antigua tecnología de identificación de aplicaciones basada en firmas que utilizan los firewalls modernos. Ya no es efectiva a la hora de identificar aplicaciones personalizadas, esquivas y cifradas, o incluso esas aplicaciones que se camuflan de navegadores web que utilizan conexiones HTTP y HTTPS genéricas. Como consecuencia, en la mayoría de redes, aplicaciones como los clientes de túnel VPN de intercambio de archivos y los juegos pasan totalmente desapercibidas. Las nuevas técnicas y tecnologías deben resolver este problema.

Las tecnologías clave que un firewall debe incluir para proporcionar mecanismos de concienciación de usuarios y control next-gen son cuatro:

Control de aplicaciones: el Control de aplicaciones le permite priorizar el tráfico de aplicaciones de vital importancia al tiempo que bloquea o limita las aplicaciones no deseadas. La mayoría de firewalls next-gen no consiguen proporcionar una visibilidad ni un control adecuados sobre las aplicaciones debido a las limitaciones de la identificación de aplicaciones basada en firmas. Asegúrese de que su firewall next-gen utiliza las técnicas más recientes para solventar este problema, es decir, que detecta los cientos de aplicaciones que seguramente están pasando desapercibidas en su red.

Control web: las políticas de filtrado de direcciones URL son importantes para el cumplimiento de las políticas a fin de poder ofrecer un entorno seguro a todos sus usuarios, especialmente en el sector educativo. Si bien esta característica se ha convertido en fundamental en casi todos los firewalls, la facilidad con que se pueden implementar y gestionar a diario políticas sofisticadas basadas en grupos y usuarios sí presenta diferencias importantes. Asegúrese de que su próximo firewall ofrece un conjunto de herramientas de políticas sencillas a la vez que flexibles para que el mantenimiento en el día a día de este importante aspecto no presente complicaciones y sea rápido.

Visibilidad de los riesgos: tener información detallada sobre sus usuarios y las aplicaciones con un mayor índice de riesgo es fundamental para garantizar la imposición de políticas adecuadas antes de que se produzcan incidentes graves. Asegúrese de que su firewall ofrezca informes de evaluación del riesgo de sus usuarios correlacionados con su actividad en la red para identificar aquellos que representen un mayor riesgo. Busque también indicadores claros en cuanto al uso de aplicaciones sospechosas en la nube, TI en la sombra, descargas peligrosas, sitios web dudosos y la presencia de amenazas.

Escaneado HTTPS: con más de un 80 % del tráfico de Internet cifrado hoy en día, la imposición de las políticas es un verdadero reto salvo que se disponga de un escaneado HTTPS adecuado. Como el escaneado HTTPS puede ser invasivo y consumir muchos recursos, asegúrese de que su próximo firewall ofrece opciones de escaneado selectivo y soluciones sencillas para administrar excepciones sin afectar negativamente al rendimiento.

Debe proporcionar	Descripción	Preguntas para los proveedores
Visibilidad y control de aplicaciones	Cuando tiene visibilidad sobre las aplicaciones que se están usando, es capaz de tomar decisiones fundamentadas sobre qué permitir, qué priorizar y qué bloquear para asegurar que su ancho de banda se aproveche al máximo sin perder tiempo en bloquear aplicaciones que no son un problema. Si echa un vistazo a los informes de la mayoría de firewalls, la mayor parte del tráfico de red aparecerá como "sin clasificar" o "Internet general"; hay muchas aplicaciones personalizadas, crípticas, esquivas o que simplemente utilizan HTTP o HTTPS genérico y que, por tanto, siguen sin identificarse.	‣ ¿Se integra su firewall con los hosts de la red para identificar todas las aplicaciones esquivas y desconocidas que generan tráfico de tipo HTTP o cifrado? ‣ ¿Puede facilitar un informe de firewall de muestra en el que se vea qué tráfico se identifica realmente? ‣ ¿Le ofrece su control de aplicaciones visibilidad a nivel de usuarios y grupos y la opción de imponer políticas? ‣ ¿Proporciona control de aplicaciones por categoría, nivel de riesgo, tecnología o características (como mal uso o baja productividad)?
Conformado de tráfico web y de aplicaciones (Web and App Traffic Shaping)	Opciones de conformado de tráfico avanzado (QoS) por categoría web o aplicaciones para limitar o garantizar la prioridad de las cargas/descargas o del tráfico total y la velocidad de forma individual o compartida.	‣ ¿Ofrece su solución opciones de conformado de tráfico o QoS por aplicaciones, categorías, usuarios, grupos o reglas?
Filtrado de direcciones web	Controla el uso de la web para evitar infracciones y mantener los contenidos inapropiados y el malware fuera de la red.	‣ ¿Incluye su firewall un motor de políticas de puerta de enlace a Internet basado en la herencia? Por ejemplo, si necesita modificar algo solo un poco para un usuario, ¿tiene que crear una política web completamente nueva o puede definir solo lo que ha cambiado y heredar el resto? ¿Tiene políticas preconfiguradas para centros de trabajo, cumplimiento de la ley de protección de menores en Internet, etc.? ‣ Además de bloquear, ¿también puede avisar sobre sitios web potencialmente inadecuados permitiendo al usuario seguir? ‣ ¿Incluye su firewall la monitorización de palabras clave web? ¿Puede cargar sus propias listas según lo relevantes que sean para su industria o región?
Características de cumplimiento web	Garantiza el cumplimiento de las políticas e identifica comportamientos peligrosos al navegar por Internet, realizar búsquedas o utilizar Google Apps.	‣ ¿Puede su solución de control web imponer nuestro dominio de Google Apps? ‣ ¿Aplica las restricciones de SafeSearch y YouTube en función de políticas de grupo o usuario? ‣ ¿Puede imponer un filtrado de imágenes adicional para, p. ej., permitir solo imágenes con licencia Creative Commons? ‣ ¿Puede identificar comportamientos potencialmente problemáticos relacionados con el acoso escolar, la autolesión o la radicalización en función del filtrado de contenido dinámico y la monitorización de palabras clave? ‣ ¿Permite a miembros del personal como profesores establecer excepciones temporales en las políticas para usuarios o grupos?
Evaluación del riesgo de usuarios	Proporciona una visión general de los usuarios que representan un mayor riesgo según su actividad en la red y su historial reciente.	‣ ¿Proporciona su firewall información detallada sobre los usuarios que representan un mayor riesgo según su comportamiento y actividad recientes en la red? ‣ ¿Hay un widget en el panel de control para acceder fácilmente a la información? ‣ ¿Hay informes detallados y completos?
Evaluación del riesgo de aplicaciones	Proporciona una métrica del riesgo en general en la red de su organización.	‣ ¿Proporciona su firewall una evaluación en general del riesgo de las aplicaciones? ‣ ¿Ofrece informes históricos detallados sobre el uso de las aplicaciones?
Escaneado HTTPS	Permite ver el tráfico web cifrado para garantizar el cumplimiento e identificar las amenazas ocultas.	‣ ¿Ofrece su firewall descifrado intermediario para HTTPS? ‣ ¿Ofrece opciones para la gestión de excepciones? ‣ ¿Bloquea protocolos SSL/TLS no reconocidos y certificados no válidos? ‣ ¿Admite el escaneado del tráfico que se cifra usando los protocolos de cifrado más recientes?

La importancia de varias capas de defensa contra las amenazas

Para evitar ser detectados, los ciberdelincuentes transforman constantemente sus métodos de ataque. Actualmente, casi todas las instancias de malware son una variante de día cero no vistas antes y más sofisticadas, ocultas y dirigidas que las anteriores. Este hecho ha convertido en obsoleta la forma de detección tradicional basada en firmas. Lo que se necesita es una defensa multicapa en varios vectores, en que cada uno utilice análisis de comportamientos, Deep Learning y otras técnicas next-gen para proporcionar una protección adecuada.

Las tecnologías clave que el perímetro de su red necesita para proporcionar una defensa adecuada contra las amenazas modernas son siete.

Protección contra amenazas avanzadas: la protección contra amenazas avanzadas es importante para identificar bots, APT y otras amenazas que se encuentran actuando en su red. Asegúrese de que su próximo firewall ofrezca detección de tráfico malicioso, detección de redes de bots y detección del tráfico de llamada a casa a los servidores de comando y control. El firewall debe usar un enfoque colaborativo que combine IPS, DNS y telemetría web para identificar el tráfico de llamada a casa. También debe integrarse e interactuar con los hosts de la red para entender su estado de seguridad y posibles peligros.

Identificar y aislar sistemas comprometidos: para evitar la pérdida de datos y la propagación de infecciones a otros sistemas de la red, además de acelerar la remediación, su firewall no solo debe identificar inmediatamente el host infectado, sino también el usuario y el proceso en el caso de un incidente. Idealmente, también debe bloquear o aislar automáticamente los sistemas comprometidos hasta que se puedan investigar y limpiar.

Prevención de intrusiones: los sistemas de prevención de intrusiones (IPS) pueden detectar los intentos por parte de hackers de entrar en su red. Asegúrese de que su firewall dispone de un IPS next-gen capaz de identificar patrones de ataque avanzados en el tráfico de su red a fin de detectar intentos de ataque y malware propagándose lateralmente por los segmentos de la red. Para reducir aún más su área de superficie de ataque, considere las soluciones que ofrezcan la posibilidad de bloquear rangos IP geográficos completos para las regiones del mundo con las que no trabaja.

Espacios seguros: el uso de espacios seguros permite detectar las instancias más recientes y evasivas de malware y amenazas avanzadas como ransomware y redes de bots antes de que lleguen a sus ordenadores. Asegúrese de que su firewall ofrece espacios seguros avanzados con las últimas tecnologías como Deep Learning, detección de exploits, detección de ransomware, análisis de comportamientos, actividad de red y uso de memoria.

Protección web: una protección web efectiva puede evitar la entrada en su red de las amenazas web más recientes como el criptojacking y el malware que se sirve de redes de bots. Asegúrese de que su firewall cuente con motores antivirus dobles y una protección web basada en el comportamiento que pueda emular o simular el código JavaScript del contenido web a fin de determinar su intención o comportamiento antes de que pase al navegador del usuario.

Protección del correo electrónico: el correo electrónico sigue siendo uno de los principales puntos de entrada de amenazas y exploits de ingeniería social. Asegúrese de que su próximo firewall o solución de filtrado de correo electrónico tenga tecnologías antispam y antiphishing de primera categoría para detectar el malware más reciente oculto en el correo electrónico y sus archivos adjuntos.

Firewall de aplicaciones web (WAF): un WAF protege sus servidores, dispositivos y aplicaciones empresariales de los ataques de hackers. Si administra internamente algún servidor o aplicación de empresa a los que es necesario acceder desde Internet, asegúrese de que su firewall ofrece una protección WAF completa. Un firewall de aplicaciones web debe incluir un proxy inverso y la autenticación de descargas y reforzar los sistemas contra ataques de hackers.

Debe proporcionar	Descripción	Preguntas para los proveedores
Protección contra amenazas avanzadas	Identifica bots y otras amenazas avanzadas y malware que intentan realizar llamadas a casa o comunicarse con servidores de comando y control.	‣ ¿Qué nivel de protección contra amenazas avanzadas ofrece su firewall? ‣ ¿Coordina información de distintas fuentes para detectar tráfico malicioso o es sencillamente una base de datos de redes de bots? ‣ ¿Se integra su firewall con los hosts de la red para entender si muestran cualquier señal de peligro aunque no haya pruebas en la red?
Detección de sistemas comprometidos	Identifica sistemas infectados en su red.	‣ ¿Es capaz su firewall de señalar exactamente el host, el usuario y el proceso infectados? ‣ ¿Está su firewall al tanto del estado de seguridad de los endpoints conectados? ‣ ¿Proporciona una visibilidad instantánea del estado de seguridad de sus endpoints?
Aislamiento de sistemas comprometidos	Usa reglas de firewall para aislar sistemas comprometidos hasta que se puedan limpiar.	‣ ¿Es capaz su firewall de aislar automáticamente sistemas infectados o potencialmente comprometidos en la red sin que intervengan los usuarios o el administrador? ‣ ¿Restaura el acceso normal automáticamente una vez se han limpiado los endpoints?
Espacios seguros	Protege contra amenazas de día cero enviando archivos potencialmente peligrosos a un espacio seguro en la nube para detonarlos y observarlos en un entorno seguro.	‣ ¿Es necesario comprar hardware adicional para obtener capas adicionales de seguridad? ‣ ¿Cuánto tiempo tarda su solución en analizar los archivos sospechosos? ‣ ¿Qué tecnologías next-gen utiliza su solución de espacio seguro para detectar amenazas de día cero como el ransomware más reciente? Por ejemplo, Deep Learning, detección de exploits y detección de cifrado.
Protección web	Proporciona protección contra malware basado en la web, sitios web comprometidos y descargas web.	‣ ¿Ofrece su motor de protección web análisis de comportamiento no basado en firmas de códigos web como JavaScript? ‣ ¿Ofrece su protección web múltiples motores antivirus? ‣ ¿Están disponibles actualizaciones en línea?
Escaneado HTTPS	Permite ver el tráfico web cifrado para proteger la red contra amenazas que pueden transmitirse a través de HTTPS.	‣ ¿Ofrece su firewall descifrado intermediario para HTTPS? ‣ ¿Admite su firewall el estándar TLS más reciente para inspeccionar tráfico cifrado? ‣ ¿Ofrece opciones para la gestión de excepciones? ‣ ¿Bloquea protocolos SSL no reconocidos y certificados no válidos?
Antispam y antiphishing	Impide la entrega de spam, phishing y otros tipos de correo electrónico no deseado a los buzones de los empleados.	‣ ¿Qué tasas de detección de spam y falsos positivos ofrece? ‣ ¿Qué técnicas utiliza para la identificación de spam y phishing? ‣ ¿Ofrece su solución para el correo electrónico enrutamiento basado en dominios y un modo MTA completo para almacenar y reenviar mensajes? ‣ ¿Ofrece un portal de usuarios para la administración de cuarentenas?
Firewall de aplicaciones web	Proporciona protección a los servidores y las aplicaciones de empresa expuestos a Internet.	‣ ¿Incluye su firewall un WAF? ‣ ¿Proporciona plantillas? ‣ ¿Proporciona protección contra todo tipo de ataques con refuerzo de formularios, refuerzo de URL, protección contra manipulaciones de cookies y protección contra secuencias de comandos entre sitios? ‣ ¿Proporciona un proxy inverso con descarga de autenticación?

Comparando soluciones de firewall

Al comparar soluciones de firewall, se deben considerar varios factores adicionales además de las funciones de seguridad y control.

Conectividad SD-WAN, VPN e inalámbrica

Las funciones SD-WAN tienen un peso cada vez mayor en la decisión de compra de un nuevo firewall. Asegúrese de que su firewall admita múltiples enlaces WAN y que incluya opciones para la priorización, el enrutamiento y la conmutación por error. Usar una solución de firewall con SD-WAN integrado le permitirá conectar emplazamientos remotos, distribuir aplicaciones y compartir datos por un coste mucho menor que el de MPLS.

La conexión sitio a sitio y el acceso remoto VPN son componentes críticos de cualquier solución de firewall. Asegúrese de que su próximo firewall incluya todas las conexiones estándar basadas en VPN que necesita y vea qué otras opciones ofrece en materia de conexión de los usuarios a recursos internos y protección de sus ubicaciones remotas. Asegúrese de que estas opciones consuman pocos recursos y sean fáciles de utilizar.

Ahora que la comunicación inalámbrica es básica en todas las redes, considere un firewall que integre un controlador inalámbrico con todo tipo de funciones y que sea compatible con una amplia gama de puntos de acceso inalámbricos de alto rendimiento para satisfacer todas sus necesidades.

Opciones de despliegue

Al investigar su próxima solución de firewall, asegúrese de que sea el firewall el que encaja en su empresa, y no a la inversa. No piense solo en su topología e infraestructura actuales, sino también en dónde puede estar el año que viene o dentro de unos cuantos años. Elija un firewall que ofrezca opciones flexibles de despliegue, tanto a nivel local como en la nube, y que cuente con las correspondientes herramientas de administración. Si tiene varias ubicaciones remotas pequeñas, valore tecnologías como SD-WAN para conectar esas ubicaciones a su red de forma sencilla y asequible.

Rendimiento

Otra cuestión importante son las exigencias en cuanto al rendimiento de la red y no solo a fecha de hoy, sino también en el futuro, ya que estas no dejan de crecer. Considerando que todos los usuarios usan múltiples dispositivos, además de que cada vez más servicios están alojados en la nube, las exigencias en cuando al ancho de banda de la red y el rendimiento del firewall no tienen precedente.

Escoja una solución que sea sencilla de ampliar y que se adapte a sus necesidades según vayan cambiando con funciones como la alta disponibilidad y el equilibrio de enlaces WAN para redundancia o rendimiento. También debe considerar si el firewall incluye tecnologías de mejora del rendimiento, como la optimización de paquetes FastPath, que coloca el tráfico conocido en la ruta rápida a través de la pila del firewall para acelerar el rendimiento.

Integración con otras soluciones de seguridad informática

La integración de sus soluciones de seguridad TI, como su firewall y sus endpoints, puede aportar beneficios importantes como protección coordinada, identificación inmediata de sistemas infectados en su red, funciones mejoradas de control de aplicaciones y respuesta automatizada mediante el aislamiento de sistemas infectados hasta que puedan limpiarse. Aunque se trata de una forma relativamente nueva de sincronizar la seguridad, es sumamente efectiva y se ha convertido rápidamente en un requisito clave para muchas empresas. Por lo que se debe escoger un proveedor cuya tecnología sea líder tanto en firewalls como otras áreas de seguridad TI, como endpoints, servidores, cifrado y protección móvil, y que permita que todas ellas funcionen conjuntamente de forma coordinada y sincronizada.

Informes y alertas

Como ya se ha mencionado al principio de este documento, entre las carencias principales que se observan en los firewalls actuales se encuentran la falta de visibilidad y no disponer de información detallada sobre la actividad de la red. Asegúrese de que estas carencias no sean un problema seleccionando un firewall que incluya completos y detallados informes históricos con la flexibilidad de poder añadir informes centralizados en todos sus firewalls si lo necesita. Asegúrese también de comprobar cómo de detallada es la información que el firewall proporciona en el panel de control y en otras áreas importantes. No permita que su firewall le tenga rebuscando la información que necesita.

Facilidad de uso

Las tareas de configuración y mantenimiento de un firewall pueden ser desde muy sencillas a eternas. No es necesario pertenecer al grupo de los que luchan por averiguar cómo se configura su firewall correctamente, solo porque el proveedor lo ha creado demasiado complejo. Encuentre una solución que piense como usted de un proveedor cuyo objetivo es hacer que su día a día sea lo más efectivo y fácil posible.

Otra característica que ahorra tiempo y que frecuentemente suele ignorarse es asegurarse de que sus usuarios se puedan autoayudar. Busque un firewall que ofrezca un portal de autoservicio seguro para que los usuarios puedan descargarse clientes VPN y administrar su correo en cuarentena.

Comparación punto por punto

Utilice nuestra lista comparativa de productos en la página siguiente para ver qué soluciones debe incluir en su lista definitiva. Una vez que haya encontrado algunos que cumplan sus criterios, pruébelos y compare los precios.

Lista comparativa de productos

Después de revisar las secciones anteriores para identificar sus requisitos mínimos, utilice esta tabla para evaluar las distintas soluciones y decidir las que quiere incluir en su lista definitiva para probarlas. Por supuesto, también puede añadir otros requisitos adicionales que puedan ser necesarios para satisfacer las exigencias específicas de su empresa.

	Sophos XG	Cisco Meraki	Fortinet FortiGate	SonicWall NSa	WatchGuard Firebox
FUNCIONES DE FIREWALL NEXT-GEN					
Simulador de pruebas de políticas web y reglas de firewall	✓		✓		✓
Motores antivirus dobles	✓				✓
Optimización de paquetes FastPath	✓		✓		
Sistema de prevención de intrusiones	✓	✓	✓	✓	✓
Control de aplicaciones	✓	Parcial	✓	✓	✓
Control de aplicaciones sincronizado (usando la telemetría de Endpoint)	✓				
Visibilidad de aplicaciones en la nube de TI en la sombra	✓		✓	✓	
Bloqueo de aplicaciones no deseadas (PUA)	✓		✓	✓	
Control y protección web	✓	✓	✓	✓	✓
Monitorización e imposición de palabras clave web	✓		✓	✓	✓
Visibilidad del riesgo de usuarios y apps (cociente de amenazas por usuario)	✓		Parcial		
Filtrado de datos HTTPS	✓	✓	✓	✓	✓
Modo de inspección SSL – Soporte de la versión TLS 1.3	✓		Solo motor IPS		✓
PROTECCIÓN CONTRA AMENAZAS AVANZADAS					
Protección contra amenazas avanzadas	✓	✓	✓	✓	✓
Detección de sistemas comprometidos	✓		+1 producto *		✓
Aislamiento de sistemas comprometidos	✓		+1 producto *		✓
Protección contra la propagación lateral	✓				✓
Espacios seguros	✓	✓	✓	✓	✓

	Sophos XG	Cisco Meraki	Fortinet FortiGate	SonicWall NSa	WatchGuard Firebox
PROTECCIÓN DE SERVIDORES Y CORREO ELECTRÓNICO					
WAF con funciones completas	✓		+1 producto *	+1 producto *	
Correo completo: antivirus, antispam, cifrado, DLP	✓		+1 producto *	+1 producto *	
CONEXIÓN DE USUARIOS/OFICINAS REMOTAS					
VPN IPSec y SSL	✓	Menos VPN SSL	✓	✓	✓
Redes de malla inalámbricas	✓	✓	✓	✓	✓
Protección de oficinas remotas lista para usar (RED)	✓				
SD-WAN	✓	✓	✓	✓	✓
FACILIDAD DE USO Y DESPLIEGUE					
Despliegue flexible (HW, SW, VM, IaaS)	✓	Solo hardware	Menos SW	Menos SW	Menos SW
Integración con otros productos de seguridad informática (p. ej., endpoints)	✓		✓	✓	
Seguridad sincronizada en despliegues en modo de descubrimiento (TAP)	✓				
Informes históricos gratuitos	✓		+1 producto *	+1 producto *	+1 producto *
Administración central gratuita	✓	✓	Parcial		
Administración central para partners	✓	✓	✓	✓	
Portal de autoservicio para usuarios	✓		✓	✓	

* Estas funciones requieren un producto/dispositivo adicional que eleva los costes y la complejidad.

Las afirmaciones que contiene este documento se basan en datos a disposición del público en enero de 2020. Este documento ha sido elaborado por Sophos y no por los otros fabricantes que se mencionan. Las funciones o características de los productos que se comparan, que pueden repercutir directamente en la precisión o validez de esta comparativa, pueden sufrir cambios. La información que incluye esta comparativa tiene como finalidad ofrecer un conocimiento y una comprensión generales de la información objetiva de varios productos y podría no ser exhaustiva. Cualquiera que utilice este documento debe tomar su propia decisión de compra en función de sus requisitos individuales, además de consultar las fuentes de información originales y no basarse solo en esta comparativa a la hora de seleccionar un producto. Sophos no ofrece ninguna garantía acerca de la fiabilidad, precisión, utilidad o exhaustividad de este documento. La información de este documento se proporciona "tal cual está" y sin garantía de ninguna clase, ya sea explícita o implícita. Sophos se reserva el derecho de modificar o retirar el documento en cualquier momento.

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

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

19-12-2019 BG-ES (RP)