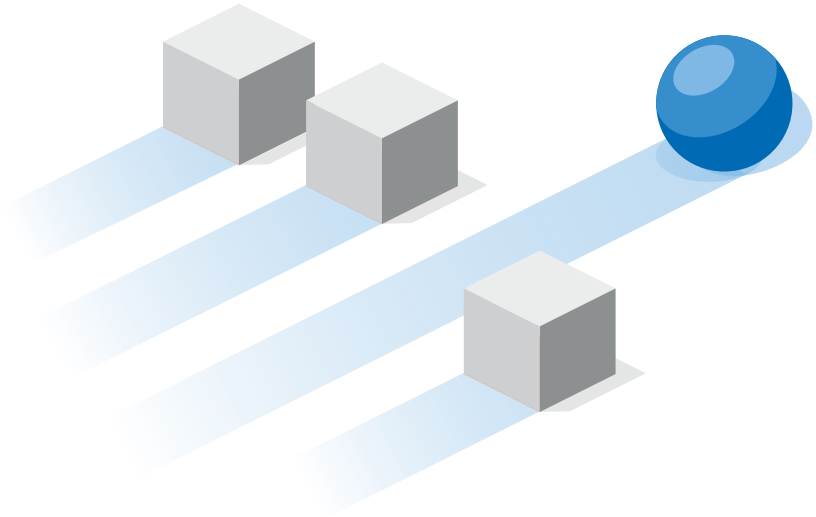
SOPHOS



El talón de Aquiles de los firewalls next-gen

Resultados de una encuesta global a 3100 directores de TI de 12 países

La seguridad de red es la base de las ciberdefensas de todas las empresas, los cimientos sobre los que se construyen otros servicios de protección como aquellos para endpoints, servidores, dispositivos móviles y cifrado. Es la fiable bestia de carga que desempeña un papel fundamental a la hora de mantener la actividad de las empresas.

Para comprender mejor las realidades de la seguridad de red a día de hoy, Sophos encargó al especialista líder en investigación Vanson Bourne que realizara una encuesta independiente a 3100 directores de TI que abarcó 12 países y 6 continentes.

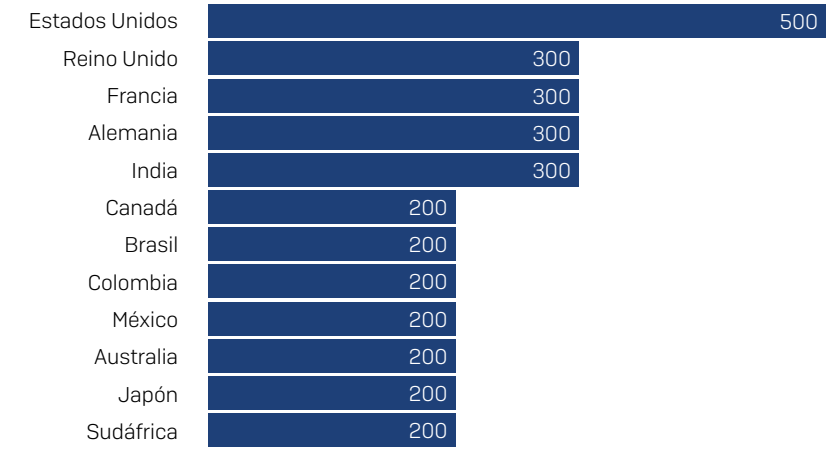
Los resultados revelan las experiencias cotidianas de equipos de TI de todo el mundo en relación con las amenazas de red y los firewalls next-gen. La encuesta arroja nueva luz sobre la realidad específica de la actual seguridad de red y los retos a los que se enfrentan los equipos de TI. También revela el talón de Aquiles de los firewalls next-gen: la lucha por equilibrar rendimiento, privacidad y protección.

Monográficos de Sophos Enero de 2020

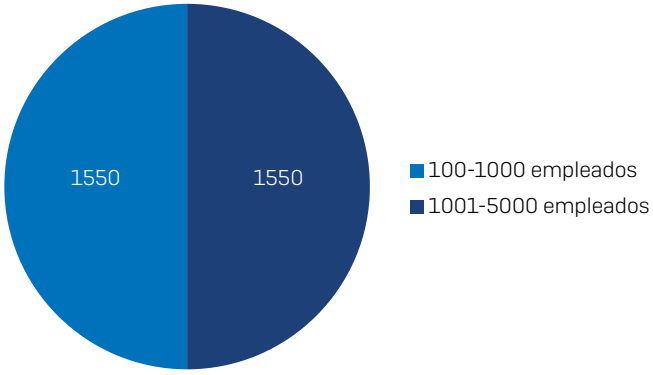
La encuesta

La consultora británica Vanson Bourne entrevistó a 3100 responsables de TI entre diciembre de 2018 y enero de 2019. Para proporcionar una distribución representativa dentro de cada país, los encuestados se dividieron a partes iguales entre empresas de 100-1000 usuarios y empresas de 1001-5000 usuarios.

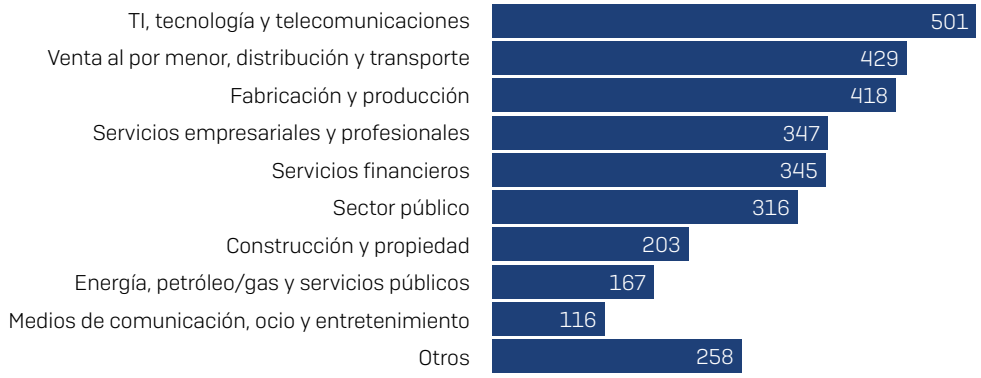
Número de encuestados por país



Distribución de los encuestados por tamaño de la empresa



Distribución de los encuestados por sector



Cuente con encontrar una amenaza en su red

La primera conclusión de la encuesta es que las empresas han de contar con que sufrirán un ciberataque. Más de dos tercios (68 %) de los encuestados fueron víctimas de un ciberataque el año pasado.

Esta tendencia a sufrir una amenaza no es resultado de una falta de protección: el 91 % de las empresas afectadas contaban con una solución de protección de ciberseguridad actualizada en el momento del ataque. Sin embargo, está claro que no basta con buenas prácticas e intenciones: siguen existiendo brechas en las defensas de las empresas que permiten a las amenazas infiltrarse.

La encuesta también puso de relieve la amplia gama de tácticas y técnicas que utilizan los ciberdelincuentes para diseminar sus ataques. Los datos de los equipos de TI que saben cómo entró la amenaza en su empresa revelan que:

- El 33 % entró a través del correo electrónico
- El 30 % entró a través de un sitio web malicioso o comprometido
- El 23 % entró a través del software que utilizaban
- El 14 % entró a través de un dispositivo externo o una memoria USB

Sin embargo, en el 20 % de los casos, el equipo de TI no sabía cómo entró la amenaza. Esta falta de visibilidad destaca un importante reto para los equipos de TI a la hora de proteger su empresa: si no se sabe cómo ha entrado una amenaza, es difícil evitar futuros ataques.

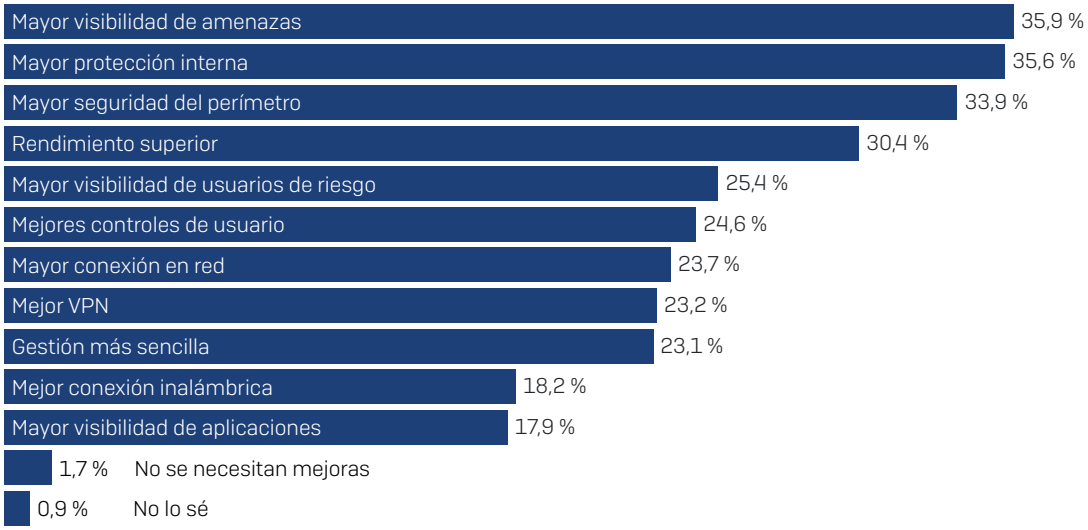
Cuanto más tiempo permanece la amenaza en la red, mayor es el riesgo para la empresa. La encuesta reveló que, de media, las empresas tardaron 13 horas en detectar las amenazas en su red. Evidentemente, durante este período, los hackers pueden liberar incontables cargas.

Al mismo tiempo, el 17 % de los directores de TI no saben cuánto tiempo permaneció la amenaza en su entorno antes de detectarla, lo que demuestra una vez más los problemas de visibilidad a los que se enfrentan los equipos de TI en relación con la protección de sus redes.

Lista de deseos para la mejora del firewall

Una mejor visibilidad de las amenazas encabeza la lista global de mejoras que los encuestados desean para su firewall, ya que un 36 % la incluyó como una de sus tres mejoras más codiciadas. El hecho de que la visibilidad superara (por los pelos) a una mejor protección en la lucha por el primer puesto demuestra hasta qué punto es un problema importante la falta de visibilidad para los equipos de TI.

Las principales mejoras que desean ver los encuestados en su firewall de red (combinación de respuestas en primera, segunda y tercera posición)



La necesidad de una mejor visibilidad de las amenazas fue mayor en Australia y Canadá, donde el 41 % de los encuestados la incluyeron entre sus tres primeras mejoras, seguida de cerca por los encuestados de EE. UU, donde el 40 % le dio un puesto en el podio. Los encuestados de Japón fueron los únicos en romper la tendencia, puesto que solo un 21 % incluyó una mejor visibilidad de las amenazas en su lista de deseos para la mejora del firewall.

Dada la prevalencia de las amenazas para las redes, no es de sorprender que una mejor seguridad del perímetro estuviera también en los primeros puestos de las listas de deseos de los encuestados: un 34 % la citó como una de sus tres mejoras preferidas.

Sin embargo, la seguridad no fue la única área en que los encuestados querían ver mejoras con respecto a su firewall. Tres de cada diez citaron un mejor rendimiento como una de las mejoras más importantes necesarias en sus firewalls.

En términos generales, se hizo evidente que ya no se trata de una cuestión de mejor rendimiento o mejor protección, sino de que los equipos de TI de hoy requieren tanto rendimiento como protección.

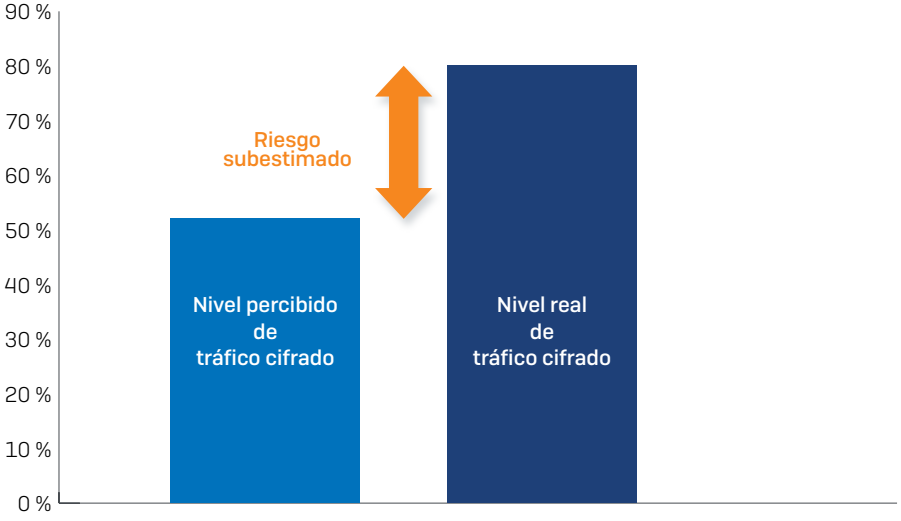
Un riesgo subestimado: el tráfico cifrado

El cifrado mantiene la privacidad del tráfico de red, pero no lo protege. De hecho, el tráfico cifrado es un enorme riesgo de seguridad, porque oculta a los firewalls lo que se mueve por la red y les impide identificar y bloquear el contenido malicioso. Es como si los pasajeros de una aerolínea se cubrieran con una sábana y permanecieran en el anonimato al pasar por el control de seguridad.

Los hackers están explotando de forma activa el cifrado para permitir que sus ataques penetren sin ser detectados. La investigación de SophosLabs reveló que, en los ocho primeros meses de 2019, el 25 % de las direcciones URL a las que llamaba el malware utilizaban cifrado, lo que ilustra la magnitud del problema.

El nivel de tráfico de red cifrado está aumentando rápidamente. Los datos del Informe de transparencia de Google indican que actualmente se cifra más del 80 % de las sesiones web en todas las plataformas, cuando hace solo dos años era un 60 %. Sin embargo, parece que los encuestados tienen una impresión diferente: como promedio, piensan que solo el 52 % de su tráfico de red está cifrado. Las respuestas fueron parecidas en todos los países; todos estaban entre Japón (46 % cifrado) y Alemania (57 % cifrado).

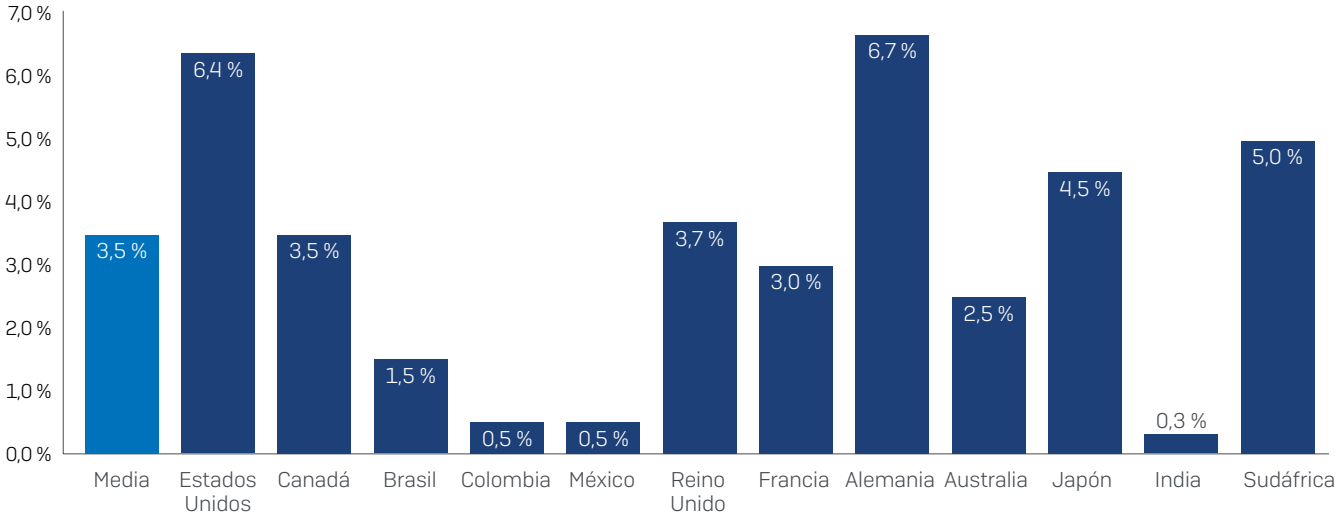
La discrepancia entre los niveles de cifrado percibido y real junto con el uso extendido del cifrado en ciberataques sugiere que el tráfico cifrado es un riesgo de seguridad infravalorado. El rápido incremento de los niveles de cifrado de tráfico ha cogido desprevenidos a los equipos de TI. Asimismo, según las tendencias actuales, el porcentaje de tráfico que se cifra aumentará más en un futuro próximo.



El talón de Aquiles de la seguridad de red

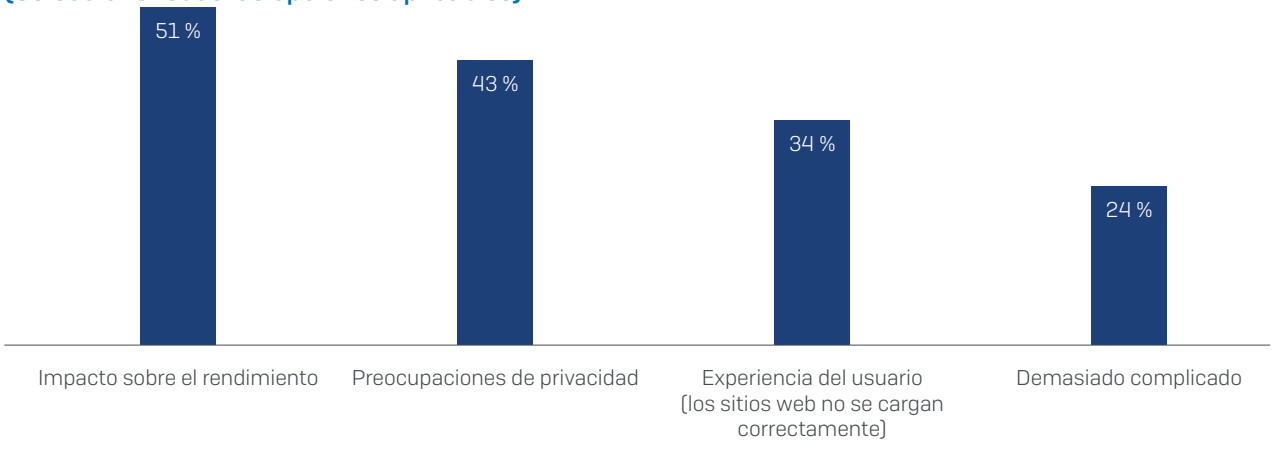
Si bien el 82 % de los encuestados estuvieron de acuerdo en que la inspección TLS es necesaria, solo el 3,5 % de las empresas descifran su tráfico para inspeccionarlo debidamente. Alemania y los EE. UU. están a la cabeza, ya que más de un 6 % de los encuestados descifran todo su tráfico; en cambio, la India, Colombia y México tienen los porcentajes de descifrado más bajos.

Porcentaje de empresas que descifran todo su tráfico de red para inspeccionarlo debidamente



La encuesta reveló que las empresas no descifran su tráfico de red por varias razones: preocupaciones sobre el rendimiento del firewall, falta de controles de políticas adecuados, experiencia del usuario deficiente y complejidad.

¿Qué impide a su empresa descifrar todo su tráfico de red para inspeccionarlo debidamente? (Seleccione todas las opciones aplicables)

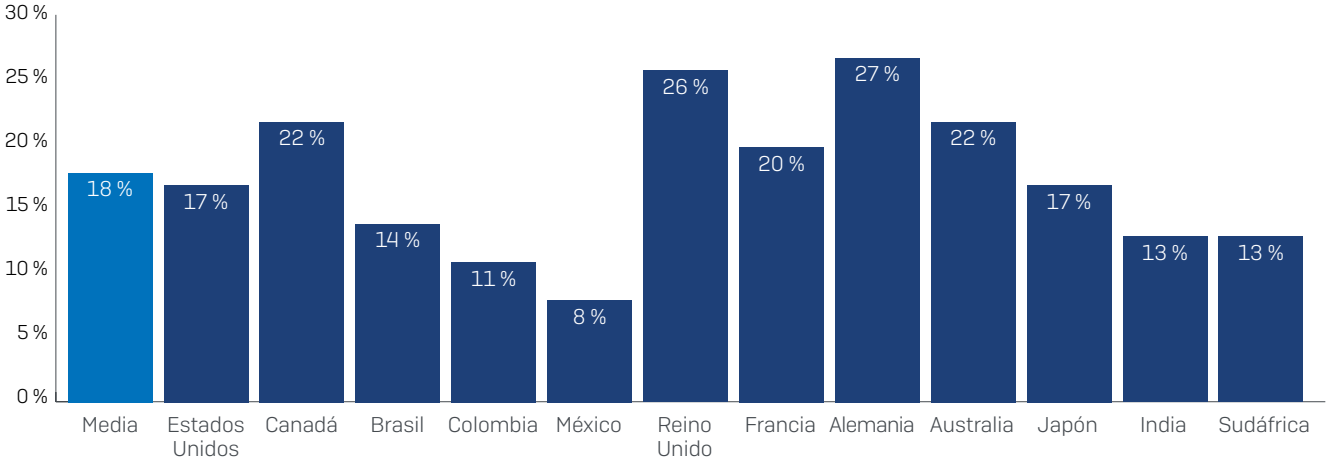


La realidad es que la mayoría de empresas necesitan equilibrar cuidadosamente el rendimiento, la privacidad y la seguridad. Sin embargo, carecen de las herramientas necesarias para hacerlo de forma efectiva y eficiente. En consecuencia, optan por permitir que el tráfico cifrado pase sin revisarse, exponiéndose a los riesgos de las amenazas de red ocultas.

Esta incapacidad de equilibrar el rendimiento, la privacidad y la protección es el talón de Aquiles, la flaqueza oculta, de muchas soluciones de firewall y UTM next-gen.

Al mismo tiempo, una minoría significativa de encuestados desconocía la necesidad de descifrar el tráfico de red. Tanto en Alemania como en el Reino Unido, más de una cuarta parte de los encuestados dijeron que no era necesario descifrar todo el tráfico de red; en cambio, en México, solo el 8 % compartía esta opinión.

Porcentaje de encuestados que piensan que no es necesario descifrar todo el tráfico de red



Esto indica que la industria de la seguridad todavía tiene trabajo que hacer a la hora de educar sobre los riesgos asociados con el tráfico de red cifrado.

Funciones del firewall para minimizar el riesgo del tráfico cifrado

A medida que nos acercamos a un nivel de cifrado del tráfico de red del 100 %, Sophos recomienda que busque las siguientes funcionalidades en su próximo firewall:

1. **El soporte más reciente para conjuntos de cifrado y TLS 1.3.** Aunque la adopción de TLS 1.3 aún está en fases iniciales, sería poco inteligente comprar un firewall sin soporte para TLS 1.3.
2. **Una solución de motor de transmisión** que permita la inspección de todo el tráfico TLS en todos los puertos/protocolos y que sea más rápida usando menos conexiones que una solución web tradicional basada en proxy.
3. **Una validación de certificados robusta** capaz de gestionar certificados de no confianza, revocados, autofirmados y no válidos para evitar posibles ataques de intermediarios (Man-in-the-Middle o MitM) maliciosos.
4. **Herramientas de políticas potentes y flexibles** que ofrezcan un control granular sobre qué descifrar e inspeccionar a fin de que pueda generar el equilibrio correcto entre privacidad, protección y rendimiento en su empresa.
5. **Un alto rendimiento** con suficiente gestión de conexiones, cifrado eficiente, aceleración de hardware y potencia general para procesar sus volúmenes de tráfico cifrado de forma eficiente.

Presentamos Sophos XG Firewall: diseñado para el Internet cifrado moderno

La arquitectura de Xstream de XG Firewall ofrece una solución desde cero para eliminar el punto ciego del tráfico de red sin perjudicar el rendimiento. Ofrece:

- Alto rendimiento: un motor de transmisión ligero con una alta capacidad de conexión
- Visibilidad inigualable: sobre los flujos de su tráfico cifrado y los errores que se produzcan
- La mejor seguridad: con soporte para TLS 1.3 y todos los conjuntos de cifrado modernos con una validación de certificados robusta
- Inspección de todo el tráfico: independiente de aplicaciones y puertos
- Gran experiencia del usuario: con una amplia interoperabilidad para evitar degradar Internet
- Potentes herramientas de políticas: ofrece el equilibrio perfecto entre rendimiento, privacidad y protección

Conclusión

Las tendencias actuales indican que, para finales de 2020, se cifrará más del 90 % del tráfico de red. Al mismo tiempo, los hackers seguirán explotando el cifrado en sus ciberataques. Para minimizar el riesgo de seguridad del tráfico de red cifrado, las empresas deben descifrar todo su tráfico de red de forma sistemática. Esto ayudará a conseguir la visibilidad de las amenazas y la protección de red mejoradas que los equipos de TI necesitan. Simultáneamente, el rendimiento del firewall sigue siendo un requisito clave. Al elegir su próximo firewall, busque una solución que pueda equilibrar sus necesidades de rendimiento, protección y privacidad.

Obtenga más información e inicie una demostración online instantánea en www.sophos.com/es-es/xgfirewall

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

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

12-12-2019 WPES (NP)

SOPHOS