SOPHOS

# *LA EVOLUCIÓN DE LA CIBERSEGURIDAD: EL IMPACTO EMPRESARIAL DE SOPHOS*

Cuantificamos las ventajas de eficiencia y protección en condiciones reales del sistema de ciberseguridad de Sophos a través de cinco casos de clientes

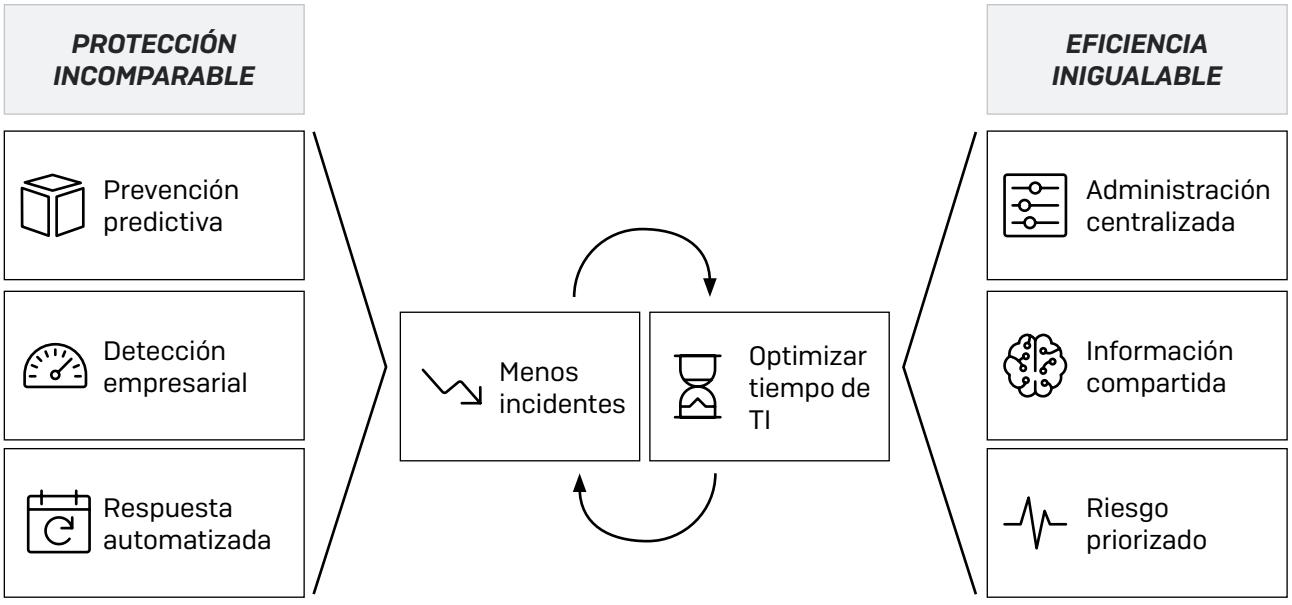
Monográficos de Sophos Junio de 2020

# Introducción

Al elegir Sophos como su sistema de protección contra amenazas, se estará beneficiando del primer (y el mejor) sistema de ciberseguridad del mundo:

- **Completa cartera de productos y servicios next-gen.** Podemos ayudarle con todas sus necesidades en términos de ciberseguridad: protección de endpoints, dispositivos móviles y servidores; EDR; firewall next-gen; correo electrónico; gestión unificada de endpoints, y otros. Tanto si gestiona un despliegue completo en la nube como si es híbrido o local, tenemos la solución para usted.
- **Protección sin precedentes.** Benefíciese tanto de la última tecnología como de la eficiencia de nuestra ciencia de datos mundialmente conocida, la búsqueda de amenazas y los equipos de SophosLabs. Esta detección de nivel empresarial bloquea las amenazas avanzadas de hoy día, mientras que nuestras redes neuronales de Deep Learning con IA detienen de forma predictiva las amenazas desconocidas. Los productos de Sophos también actúan de forma conjunta en tiempo real para ampliar aún más su protección. Comparten información de seguridad, estados y amenazas y responden automáticamente a los incidentes.
- **Plataforma de administración única.** Gestione toda su protección de Sophos a través de Sophos Central, nuestra plataforma de administración basada en la nube. Utiliza información compartida para proporcionar datos priorizados sobre los riesgos, además de ofrecer investigaciones guiadas con acciones recomendadas para cada situación.

El sistema de ciberseguridad de Sophos **incrementa su protección** a la vez que **reduce su coste total de propiedad (TCO)**. Lo hace creando un círculo virtuoso en que una protección incomparable y una eficiencia inigualable se refuerzan mutuamente de forma continuada.




Este círculo virtuoso le permite aumentar significativamente la eficiencia de su equipo de TI y reducir su exposición a las amenazas, todo ello sin aumentar la plantilla.

# Impacto para el cliente

A fin de evaluar el impacto del sistema de ciberseguridad de Sophos en entornos activos de clientes, hemos entrevistado a cinco clientes de Sophos de Norteamérica, Europa y Asia. La situación de cada cliente era distinta, con estructuras organizativas, retos y requisitos empresariales diferentes. Sin embargo, sacamos una importante conclusión común en todos los casos:

*Los clientes afirmaron que necesitarían* ***duplicar*** *su plantilla de seguridad para mantener el mismo nivel de protección si no utilizaran un sistema de ciberseguridad next-gen de Sophos.*

También nos contaron que experimentan menos incidentes de seguridad y que pueden identificar y responder más rápido a los problemas que se producen. Los resultados de utilizar Sophos incluyen:

- Una reducción del 50 % en los gastos de personal de seguridad TI
- Una reducción de más del 90 % en el tiempo dedicado a la gestión diaria de la ciberseguridad
- Una reducción de más del 90 % en el tiempo para identificar problemas
- Una reducción del 85 % en el número de incidentes de seguridad
- Una reducción significativa en el tiempo de inactividad en toda la empresa

# Cliente A: Proveedor sanitario, EE. UU.

- 4500 empleados
- 80 empleados de TI, de los que tres se dedican a la ciberseguridad
- Productos de Sophos: Intercept X Advanced with EDR, XG Firewall, Intercept X for Server Protection (Windows, Linux y equipos virtuales)

El cliente A es un proveedor sanitario regional cuyos servicios incluyen la atención de pacientes hospitalizados y ambulatorios, consultas médicas, residencias geriátricas y varios servicios especializados.

## Impacto empresarial

- **Reducción del 50 % en los requisitos de recursos de seguridad TI**
  Actualmente el cliente emplea a tres trabajadores dedicados a la ciberseguridad. Calculó que necesitaría contratar a tres analistas de seguridad a tiempo completo adicionales únicamente para cubrir la respuesta a incidentes si no utilizara Sophos.

  Antes de Sophos, el equipo tenía que realizar mucho trabajo manual para identificar lo que ocurría en la red, y dedicaba una gran parte de su tiempo a identificar incidentes. Ahora Sophos identifica de forma proactiva los problemas y resuelve la situación automáticamente en el 95 % de los casos. En consecuencia, el equipo puede centrarse en la resolución del 5 % de los problemas que requieren intervención humana.

- **Reducción de más del 90 % en la gestión diaria de la seguridad**
  El responsable de la seguridad TI dedica 30 minutos todos los días a revisar registros e investigar cualquier indicio sospechoso. Antes de Sophos, solía tardar un día entero en obtener el mismo nivel de información y confianza. Con Sophos, todos los datos se consolidan en una única plataforma de administración y se presentan en un formato uniforme, lo que facilita la identificación de problemas y la respuesta a los mismos. Esto elimina la onerosa tarea diaria de asignar datos entre múltiples fuentes para tratar de identificar lo que es sospechoso, malicioso o benigno.

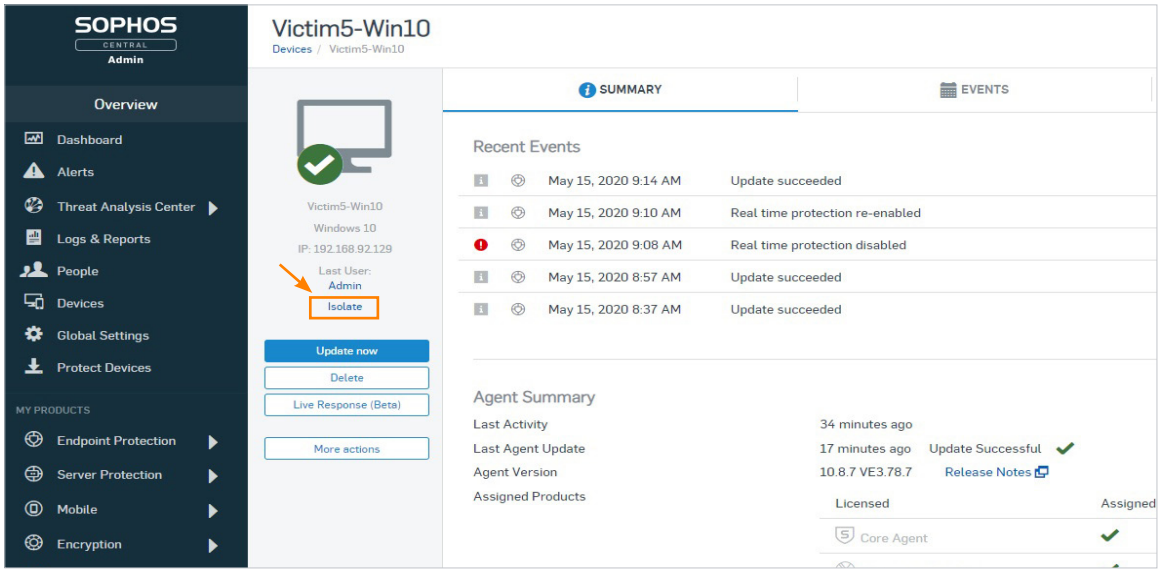
- **Reducción del 85 % en los incidentes de seguridad**
  Como hospital, el cliente gestiona grandes cantidades de información de identificación personal (PII) confidencial, además de información de pago, lo que lo convierte en un objetivo para los ciberdelincuentes. Antes de Sophos, experimentaba, de media, tres incidentes al día que requerían una investigación adicional. Con Sophos, esta cifra se ha reducido un promedio de un incidente cada tres días.

- **Reducción de más del 90 % en el tiempo para investigar un incidente**
  Antes de Sophos, llevar a cabo una investigación exhaustiva de un incidente tomaba unas tres horas, lo que incluía el acceso local al ordenador afectado. Ahora se tarda un máximo de 15 minutos gracias a que la gestión se realiza íntegramente de forma remota a través de la plataforma Sophos Central.

  Anteriormente, el equipo necesitaba desactivar el adaptador de red y, después, acceder físicamente al dispositivo para investigar y solucionar el problema antes de volver a conectarlo manualmente. También tenía que respetar los flujos de trabajo de sus usuarios, por ejemplo, esperar a que un médico no estuviera tratando a un paciente a fin de obtener acceso a ese sistema para la remediación. La posibilidad de aislar el dispositivo a través de la consola de Sophos Central permite al equipo investigar el problema de forma remota sin que afecte al usuario ni a la disponibilidad del sistema.

  La reducción del tiempo de investigación y la capacidad de gestionarlo todo de forma remota también reducen considerablemente las molestias para los demás usuarios del hospital.

- **Protección completa durante las investigaciones**
  Anteriormente, los dispositivos se desconectaban de la red para su investigación manual y no recibían actualizaciones de seguridad mientras estaban sin conexión. Con Sophos, cuando el equipo de TI aísla un dispositivo para investigar un problema, permanece online y continúa recibiendo actualizaciones de seguridad.



# Cliente B: Proveedor de servicios educativos, India

- 700 empleados
- Sede en Bangalore, además de responsables locales in situ en la India y todo el Sudeste Asiático
- Productos de Sophos: Intercept X Advanced with EDR, Intercept X Advanced for Server, XG Firewall

El cliente B presta servicios educativos a centros de estudios superiores y universidades en toda la India y la región del Sudeste Asiático. Protegen decenas de miles de alumnos a través de un equipo de TI centralizado ubicado en la sede central de Bangalore, junto con un equipo local de responsables de TI in situ.

## Impacto empresarial

- **Reducción del 50 % en los recursos requeridos para la gestión diaria de la seguridad**
  Anteriormente, el cliente empleaba a cuatro ingenieros para gestionar la seguridad diaria. Desde que se pasó a Sophos, solo ha necesitado dos ingenieros para cubrir la seguridad de toda la empresa.
- **Reducción del 94 % en el tiempo para identificar áreas de alto riesgo que requieren investigación**
  Antes de Sophos, el cliente tardaba entre tres y cuatro horas en identificar los problemas críticos en que debían centrarse para seguir investigando. Ahora solo tarda entre diez y quince minutos en identificar las prioridades de seguridad de toda la empresa con Sophos Central.
- **Reducción del 98 % en el tiempo para identificar la fuente de tráfico malicioso en la red**
  Con la anterior implementación de seguridad de red, se tardaba dos días (y a veces más) en identificar el dispositivo de la red que causaba problemas de seguridad o rendimiento. Ahora solo se tarda 15 minutos en localizar el problema y empezar a solucionarlo.
- **Reducción del 95 % en el tiempo dedicado a la gestión de actualizaciones de firmware**
  La anterior implementación de seguridad de red también generaba problemas de disponibilidad y riesgo, puesto que cada actualización de software tardaba entre tres y cuatro horas. Ahora, con Sophos, solo se tarda diez minutos por actualización. Con 20 o 25 actualizaciones al año, esto se traduce en un ahorro de 75 horas al año en actualizaciones (el equivalente a dos semanas laborables enteras).

# Cliente C: Proveedor de ensayos clínicos, EE. UU.

- 150 empleados en cuatro ubicaciones
- Dos empleados de TI para cubrir todas las áreas, incluida la ciberseguridad
- Productos de Sophos: Intercept X Advanced with EDR, XG Firewall, Central Device Encryption

El cliente C es una empresa del sector privado que proporciona los datos de ensayos clínicos necesarios para garantizar la aprobación reglamentaria de nuevos medicamentos. Debido al tipo de negocio que operan, gestionan grandes cantidades de información personal confidencial.

## Impacto empresarial

- **Reducción del 50 % en los requisitos de recursos de TI**
  Este cliente tiene un pequeño equipo de solo dos personas para gestionar todos los aspectos de TI. Actualmente pasa una hora al día revisando registros e investigando cualquier indicio sospechoso. Si no utilizara Sophos, afirma que necesitaría contratar a uno o dos ingenieros de seguridad más solo para gestionar los registros.

- **Reducción del 33 % en el tiempo para gestionar un posible problema**
  Anteriormente, cuando tenía un problema de seguridad con un dispositivo, su solución era restablecer la imagen inicial del equipo, lo que llevaba entre 90 minutos y dos horas. Ahora puede realizar una investigación en profundidad desde el aislamiento del sistema y la búsqueda de amenazas exhaustiva hasta un escaneado de seguridad completo y la remediación final en aproximadamente una hora sin restablecer la imagen inicial. Una ventaja adicional de la que se está beneficiando con el enfoque de Sophos es que el usuario puede empezar a ser productivo inmediatamente después de la investigación, mientras que con el restablecimiento de la imagen inicial también perdía tiempo restableciendo la configuración y las personalizaciones del equipo.
- **Reducción del 88 % en el riesgo de amenazas porque puede identificar problemas mucho más rápido**
  Con el sistema de ciberseguridad de Sophos, el equipo de TI puede identificar nuevos problemas que deben investigarse en cuestión de minutos desde la llegada de un evento sospechoso. Antes de Sophos, tardaba un día entero en revisar los registros para encontrar los problemas que necesitaban investigarse. Esta reducción en el tiempo de respuesta mitiga notablemente la exposición a las amenazas.
- **Comportamiento de los usuarios mejorado**
  Con Sophos, ahora los usuarios saben que el equipo de TI puede resolver los problemas e incidentes rápidamente sin que esto les ocasione interrupciones o les suponga más trabajo. En consecuencia, el equipo de TI afirma que ahora los usuarios están mucho más dispuestos a comunicar problemas o preocupaciones (por ejemplo, si han hecho clic en un posible enlace malicioso en un correo electrónico).

# Cliente D: Proveedor de servicios públicos, Serbia

- 300 empleados
- 10 empleados de TI, de los que cuatro se centran en la ciberseguridad
- Productos de Sophos: Intercept X Advanced, Intercept X Advanced for Server, XG Firewall, Sophos Email, Sophos Mobile

El cliente D es una empresa del sector público que presta servicio en la capital de Serbia, Belgrado. Este fiel cliente de Sophos se ha migrado a nuestros productos de última generación gestionados a través de Sophos Central.

## Impacto empresarial

- **Reducción del 50 % en el tiempo dedicado a la gestión diaria de la seguridad**
  Ahora dedica 30 minutos al día a la administración de la seguridad, revisando alertas, registros, usuarios, dispositivos, tráfico y aplicaciones en la consola de administración de Sophos Central para asegurarse de que todo funciona correctamente. Anteriormente, esta gestión diaria de la seguridad requería al menos el doble de tiempo para determinar los problemas que debían solucionarse de forma prioritaria y las medidas que se debían tomar.
- **Reducción de más del 90 % en el tiempo dedicado a la gestión diaria de la seguridad en comparación con otros proveedores**
  El cliente calcula que, basándose en su anterior experiencia, la gestión diaria de la seguridad le llevaría un día entero con otros proveedores, en comparación con solo 30 minutos con Sophos.
- **Cero incidentes de seguridad importantes**
  El cliente ha estado utilizando Sophos durante muchos años y no ha tenido ningún problema de seguridad importante en los últimos 8-10 años. Esto no significa que no reciba amenazas, sino que sus productos de Sophos las resuelven de forma rápida y silenciosa en segundo plano sin que el usuario se percate.

## Cliente E: Organismo de aprobación normativa, Eslovenia

- 150 empleados, de los que un tercio trabajan de forma remota y dos tercios en la sede central
- Dos empleados de TI para cubrir todas las áreas incluida la ciberseguridad, más soporte de proveedores externos en proyectos grandes
- Productos de Sophos: Sophos Endpoint Protection, Intercept X Advanced for Server, XG Firewall, Sophos Mobile, Sophos Device Encryption

El cliente E es una empresa del sector público responsable de garantizar que los productos cumplen los estándares requeridos. Este fiel cliente de Sophos se ha migrado a nuestros productos de última generación gestionados a través de Sophos Central.

### Impacto empresarial

- **Reducción del 50 % en el tiempo dedicado a la gestión diaria de la seguridad**
  Este cliente dedica 15-30 minutos diarios a la gestión de la seguridad: comprobar el firewall, revisar las alertas, limpiar el correo electrónico en cuarentena, etc. Anteriormente, tardaba por lo menos el doble de tiempo en hacerlo. Esta eficiencia mejorada resulta de la capacidad de gestionar todos sus productos de seguridad desde un único lugar y de que no hay necesidad de cambiar entre aplicaciones y servidores.
- **Cero incidentes de seguridad importantes**
  El cliente no recuerda ni un solo incidente de seguridad importante desde que utiliza Sophos.

## Conclusión

Tal como demuestran los testimonios de los clientes, el enfoque de Sophos a la ciberseguridad ofrece una protección real y una mayor eficiencia. Permite aumentar significativamente la eficiencia de su equipo de TI y reducir su exposición a las amenazas, todo ello sin aumentar la plantilla.

Aunque los entornos, recursos y retos empresariales de nuestros clientes varían de una empresa a otra, todos ellos informan de una reducción del 50 % en la carga de trabajo de seguridad TI al utilizar un sistema de ciberseguridad de Sophos. Los clientes disfrutan de una reducción de más del 90 % en el tiempo dedicado a la gestión diaria de la ciberseguridad, así como una reducción del 85 % en el número de incidentes de seguridad.

Para obtener más información sobre las soluciones de ciberseguridad de Sophos e iniciar una evaluación gratuita sin compromiso, visite es.sophos.com o hable con un representante de Sophos.

Ventas en España:
Tel: (+34) 91 375 67 56
Email: comercialES@sophos.com

Ventas en América Latina:
Email: Latamsales@sophos.com



200612 WPES (NP)

SOPHOS