SOPHOS
Cybersecurity evolved.

Guía de ciberseguridad para el sector sanitario

Ciberseguridad para el sector sanitario que detiene a los atacantes al instante sin interferir en la atención al paciente

Informes de soluciones de Sophos. Abril de 2021

Ciberseguridad y atención al paciente

Cuando pensamos en la atención al paciente, lo primero que se nos viene a la cabeza son los médicos, el personal de enfermería y otros profesionales sanitarios que prestan servicios médicos. Pero, a medida que la atención sanitaria depende cada vez más de la tecnología (desde la IA hasta la informática en la nube, pasando por los dispositivos conectados) y los atacantes siguen perfeccionando sus técnicas, la ciberseguridad desempeña un papel directo y significativo para poder prestar asistencia a los pacientes.

"Una ciberseguridad deficiente es un peligro claro e inminente para la seguridad de los pacientes... los ciberincidentes pueden alterar significativamente los sistemas sanitarios y asistenciales y contribuir directamente a perjudicar a los pacientes".

Institute of Global Health Innovation, Imperial College London

La pandemia de COVID-19 ha acelerado la adopción de tecnologías sanitarias digitales, como las soluciones de monitorización remota de pacientes, las consultas online y los dispositivos para uso domiciliario, y ha supuesto un aumento del personal móvil/remoto. Aunque estos cambios han aportado importantes mejoras de eficiencia en el sector sanitario que se mantendrán a largo plazo, también han aumentado el reto de la ciberseguridad al que se enfrentan los equipos de TI de este sector.

"(Los ciberatacantes) pretenden explotar el hecho de que la digitalización en el futuro de la sanidad va a ser cada vez más importante".

John Noble, presidente del Comité de Garantía de la Información y Ciberseguridad, NHS Digital

Retos de ciberseguridad para el sector sanitario

Una encuesta realizada por Sophos en 2021 a 328 profesionales de TI del sector sanitario de 30 países reveló que la ciberseguridad es cada vez más difícil. El 63 % de los encuestados afirmó que el número de ciberataques sufridos aumentó en el transcurso de 2020, probablemente debido, al menos en parte, a que los adversarios se aprovecharon de la pandemia en sus ataques. Por ello, no es de extrañar que el 70 % dijera que su carga de trabajo en ciberseguridad aumentó durante 2020.

No solo aumenta el volumen de los ataques, sino también su complejidad. El 60 % afirmó que los ciberataques ahora son demasiado avanzados para que su equipo de TI se ocupe de ellos por su cuenta.

63 %
El número de ciberataques aumentó a lo largo de 2020

60 %
Los ciberataques son demasiado avanzados para que el equipo de TI los resuelva sin ayuda

70 %
La carga de trabajo en ciberseguridad aumentó en el transcurso de 2020

La complejidad es el enemigo de la seguridad

Las organizaciones sanitarias suelen tener una proporción de usuarios por personal informático superior a la media. Cuanto más compleja es la infraestructura de seguridad, más difícil es para los desbordados equipos de TI mantenerla al día, y también aprovechar al máximo las funciones de protección que se ofrecen.

Informes de soluciones de Sophos. Abril de 2021

Sophos: protección en el sector sanitario

Sophos trabaja con organizaciones sanitarias de todo el mundo para hacer frente a sus retos de ciberseguridad y posibilitar una atención al paciente ininterrumpida. Ante la creciente frecuencia y sofisticación de los ataques, podemos ayudarle a proteger sus datos y su organización, al tiempo que permitimos a los ocupados equipos de TI reducir su carga de trabajo en ciberseguridad. Siga leyendo para saber cómo podemos ayudar a resolver los desafíos de ciberseguridad más comunes a los que se enfrentan las organizaciones sanitarias.

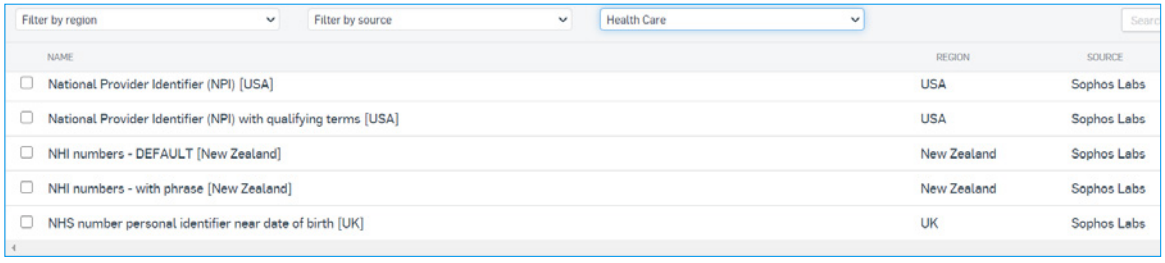
Proteja los datos confidenciales estén donde estén

Las organizaciones sanitarias almacenan muchas formas de datos sensibles, desde historiales médicos hasta números de la Seguridad Social e información de identificación personal (PII). Con tantos tipos diferentes de datos confidenciales dentro de una organización sanitaria (y tantos lugares donde se almacenan y utilizan), protegerlos todos puede ser complicado.

Las herramientas de protección preventiva y activa de Sophos aportan seguridad a toda la red sanitaria, hasta el nivel de los dispositivos individuales.

Proteja el dispositivo o la carga de trabajo que contiene los datos

La protección para endpoints y servidores **Sophos Intercept X** despliega varias capas de protección para custodiar los datos de sus equipos Windows, Mac, Linux y virtuales. Las reglas de protección contra la pérdida de datos específicas del sector sanitario, que utilizan términos o tipos de datos sanitarios, incrementan su protección.



Sophos Device Encryption ofrece una forma rápida y sencilla de garantizar que los dispositivos Windows y macOS estén cifrados de forma segura, lo que protege sus datos (y demuestra su cumplimiento) en caso de pérdida o robo.

Proteja la red por la que se transmiten los datos

Sophos Firewall utiliza una tecnología de detección de amenazas con IA para evitar que los ataques alcancen sus datos sanitarios sensibles, sistemas médicos críticos y otras partes de su ecosistema.

Detenga las filtraciones por correo, deliberadas o accidentales

Sophos Email cifra la información de identificación personal, los historiales de los pacientes, las imágenes médicas y otros datos sensibles, frenando así las filtraciones de datos tanto accidentales como malintencionadas.

Controle el acceso a sus datos

Sophos Zero Trust Network Access (ZTNA) le ofrece un control absoluto sobre quién puede acceder a los datos de su red. Dispone de controles muy granulares que bloquean la propagación lateral y garantizan que solo las personas autorizadas puedan acceder a los datos sensibles.

Haga frente a la amenaza del ransomware del sector sanitario

El ransomware es cada vez más inteligente y destructivo, y el sector sanitario es un objetivo lucrativo. En el ámbito sanitario, el coste del ransomware no se limita a pagar el rescate. El coste de perder datos de los pacientes y retrasar o cancelar procedimientos médicos puede ser enorme y devastador. Las herramientas de prevención y búsqueda de amenazas proactiva de Sophos evolucionan constantemente para adelantarse al ransomware y defender sus datos y su red de estos ataques.

Evite que el ransomware secuestre sus datos

En Sophos, estamos orgullosos de ser líderes mundiales en la protección de empresas contra el ransomware.

Sophos Intercept X constituye la mejor protección contra ransomware del mundo para endpoints y servidores. Introduce múltiples capas de seguridad para reconocer y detener el ransomware en cada fase, entre ellas:

- CryptoGuard, que revierte automáticamente los archivos a un estado seguro si son cifrados por un usuario no autorizado
- Deep Learning con IA que bloquea el ransomware conocido y desconocido
- Protección contra exploits que detiene las técnicas que utilizan los atacantes para descargar e instalar ransomware
- Protección base con firmas de SophosLabs

Sophos Managed Threat Response (MTR) ofrece nuestro más alto nivel de protección contra el ransomware, proporcionando funciones proactivas de búsqueda, detección y respuesta a amenazas, un servicio 24/7 prestado por un equipo de expertos. Seguimos vigilando, incluso cuando duerme.

Sophos Rapid Response ofrece soporte de emergencia durante ataques de ransomware activos, aunque no sea cliente de Sophos. Nuestro equipo le ayudará a controlar rápidamente un ataque para proteger sus redes, aplicaciones y datos, así como para mitigar los daños y las interrupciones.

La realidad del ransomware en el ámbito sanitario

El 34 % se vio afectado por el ransomware en el último año

El 65 % de los ataques cifraron datos

El 34 % pagó el rescate

1,27 millones USD de coste de recuperación medio

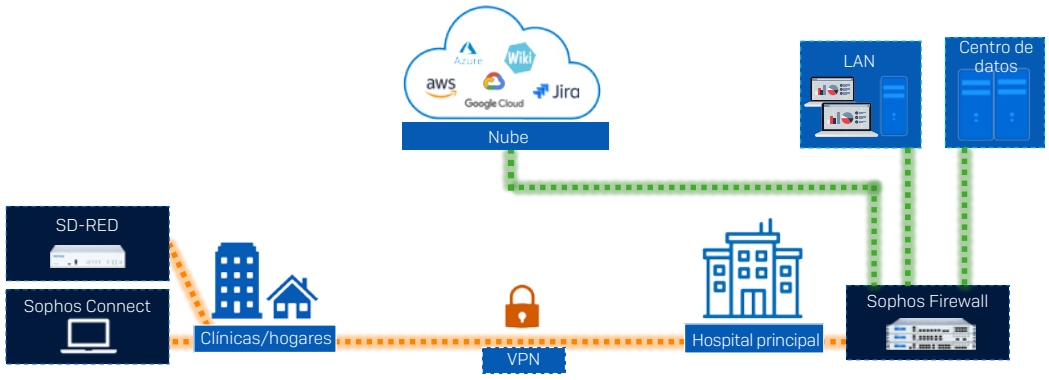
El estado del ransomware 2021, Sophos

Dé a los usuarios acceso seguro desde cualquier lugar

El personal sanitario, ya sea de primera línea en los hospitales, en la comunidad o trabajando desde casa, necesita acceder en cualquier momento a los datos sensibles de los pacientes y a los sistemas sanitarios. Las herramientas de Sophos permiten a sus usuarios conectarse de forma segura desde cualquier lugar, sin que ello afecte a las labores de atención sanitaria vitales.

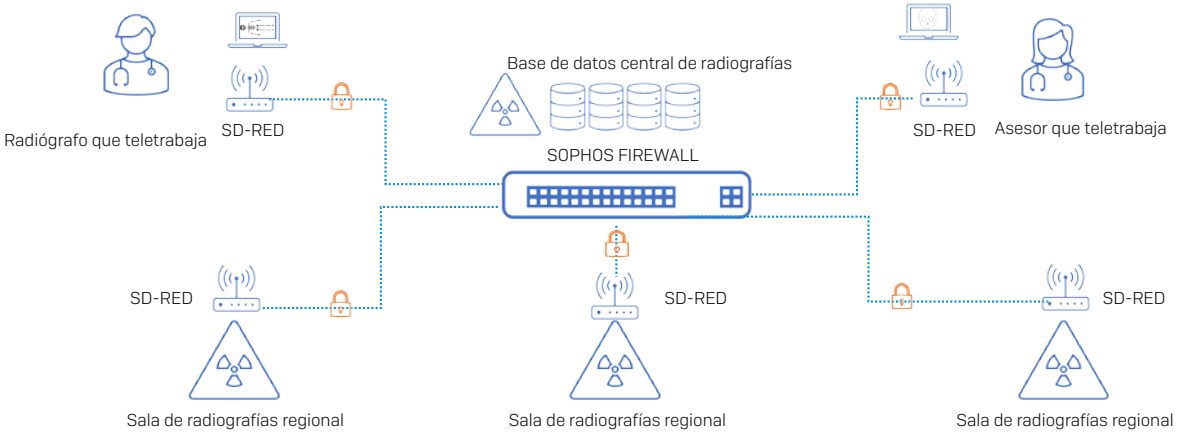
Permita a los usuarios conectarse de forma segura desde cualquier lugar

Sophos Firewall ofrece conexiones seguras para Windows y macOS a través de la VPN gratuita Sophos Connect. Es fácil de desplegar y configurar, y da acceso seguro a sus usuarios remotos a los recursos de la red o la nube pública desde dispositivos Windows y macOS. Con más de 1,4 millones de usuarios en todo el mundo, sabe que está en buenas manos.



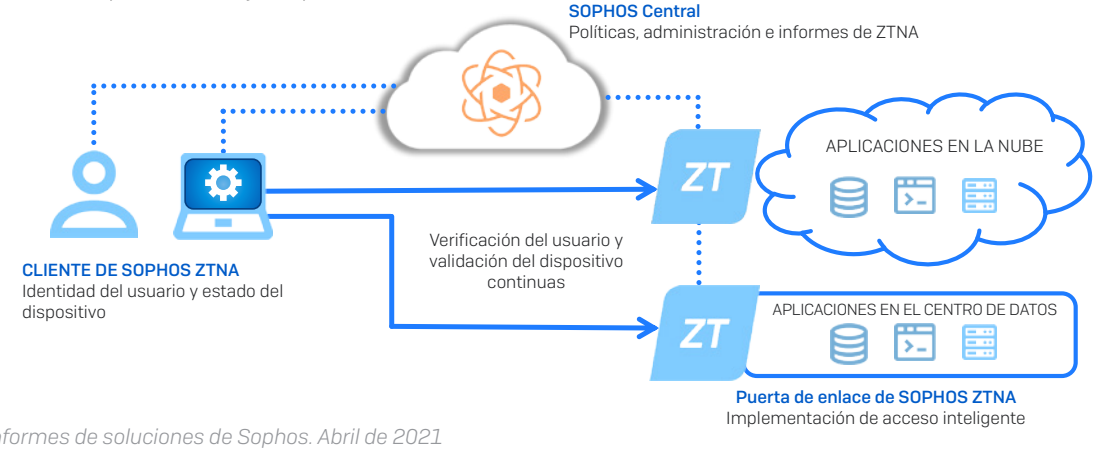
Sophos Firewall ofrece acceso remoto seguro a través del cliente Sophos Connect y los dispositivos SD-RED

Para disfrutar de lo último en conectividad remota segura, **SD-RED** (dispositivo Ethernet remoto) es un pequeño dispositivo Plug and Play que funciona con **Sophos Firewall** para conectar a personas y emplazamientos remotos a su red principal. Es ideal para clínicas locales y salas médicas, así como para personas con datos muy sensibles.



Ejemplo de uso de Sophos Firewall y SD-RED para radiografías

Para un acceso seguro next-gen, **Sophos Zero Trust Network Access** sitúa la identidad en el centro de la defensa, validando constantemente al usuario, el dispositivo y el cumplimiento de las políticas. Ofrece a los usuarios una experiencia transparente que simplemente funciona, al tiempo que permite a los equipos de TI ayudar a que los nuevos usuarios puedan empezar a trabajar rápidamente.



Refuerce su equipo de TI

Según nuestra encuesta realizada en 2020 a 5000 directores de TI de diversos sectores, incluido el sanitario, el 81 % de los encuestados reconoció que su capacidad para encontrar y retener a profesionales de seguridad TI cualificados es un gran reto a la capacidad de su empresa de ofrecer seguridad TI.

Tanto si necesita añadir experiencia como ampliar capacidad para complementar sus recursos, los profesionales de seguridad de Sophos pueden convertirse en una extensión de su equipo para proteger sus sistemas sanitarios y los datos de sus pacientes 24/7.

Expertos en ciberseguridad dedicados para reforzar su equipo de TI

Sophos Managed Threat Response (MTR) es un equipo de expertos en búsqueda y respuesta a amenazas que trabaja como una extensión de su propio equipo. Proporciona a los equipos de TI desbordados del sector sanitario la capacidad y la experiencia adicionales que necesitan para hacer frente a cualquier amenaza.

El equipo de Sophos MTR supervisa su entorno 24/7, buscando y validando posibles amenazas e incidentes de forma proactiva. Si ve algo sospechoso, puede recurrir a los expertos en malware de SophosLabs para que investiguen y desentrañen los indicadores sospechosos.

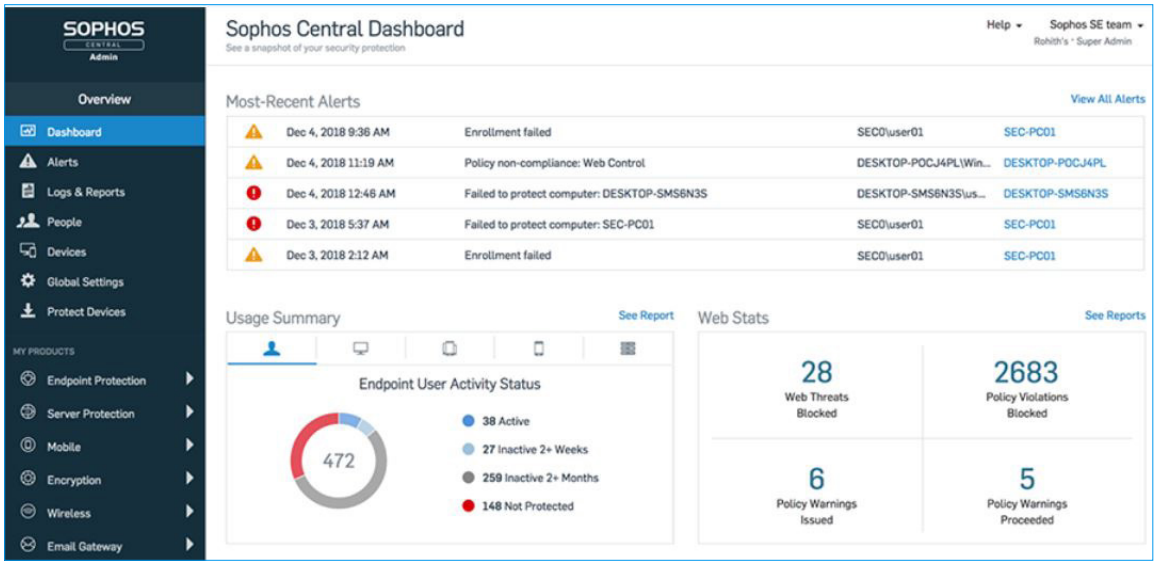
Además, si lo desea, los equipos de Sophos MTR también pueden actuar en su nombre. A diferencia de otros servicios de detección y respuesta gestionadas, nuestro equipo no se limita a notificarle los problemas, sino que también puede neutralizar la amenaza por usted. En última instancia, usted decide qué nivel de intervención quiere que adoptemos y cómo trabajamos con su equipo.

Dedique menos tiempo a administrar la ciberseguridad

Cuando los recursos de TI son limitados, se hace difícil hacer una criba del aluvión de alertas de seguridad para decidir cuáles atender primero. Sophos le ayuda a reducir las interferencias ofreciéndole una visión de su seguridad desde una única consola, así como una automatización que resuelve los problemas antes de que tenga que preocuparse por ellos, para que pueda dedicar su tiempo a lograr una diferencia estratégica.

Simplifique la gestión de la ciberseguridad

Sophos Central es nuestra plataforma web unificada donde puede administrar todos sus productos de seguridad de Sophos. Ya no tendrá que ir de consola en consola para proteger su empresa; con Sophos Central, puede desplegar y gestionar fácilmente su protección y realizar investigaciones entre productos que correlacionan datos de varios servicios, todo desde un único lugar.



Gestione toda su ciberseguridad a través de la plataforma Sophos Central

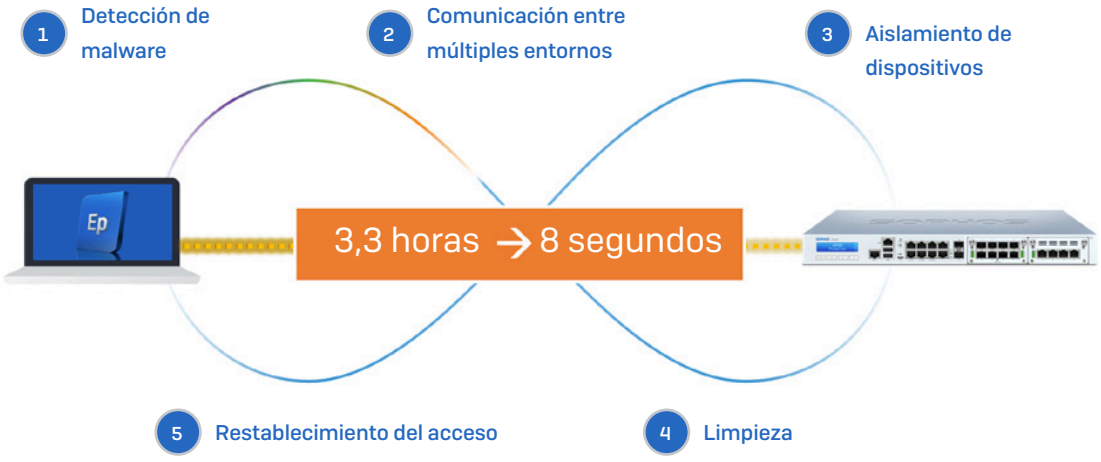
Automatice su protección

Sophos Central permite que los productos de Sophos compartan información de forma activa y funcionen conjuntamente en tiempo real para responder automáticamente a los incidentes. Esta integración y automatización aumentan su protección al tiempo que reducen la carga de trabajo de los equipos de TI.

Ejemplo 1: Respuesta automatizada a incidentes

- Si Sophos Intercept X identifica una amenaza en el endpoint, notifica a Sophos Firewall al instante.
- Sophos Firewall aísla automáticamente el endpoint infectado de la red, incluso de otros dispositivos de la misma LAN.
- Intercept X limpia la amenaza y notifica a Sophos Firewall cuando ha terminado.
- Sophos Firewall restablece inmediatamente el acceso a la red.

Todo este proceso, que de forma manual tarda unas tres horas y media, se realiza en menos de ocho segundos.

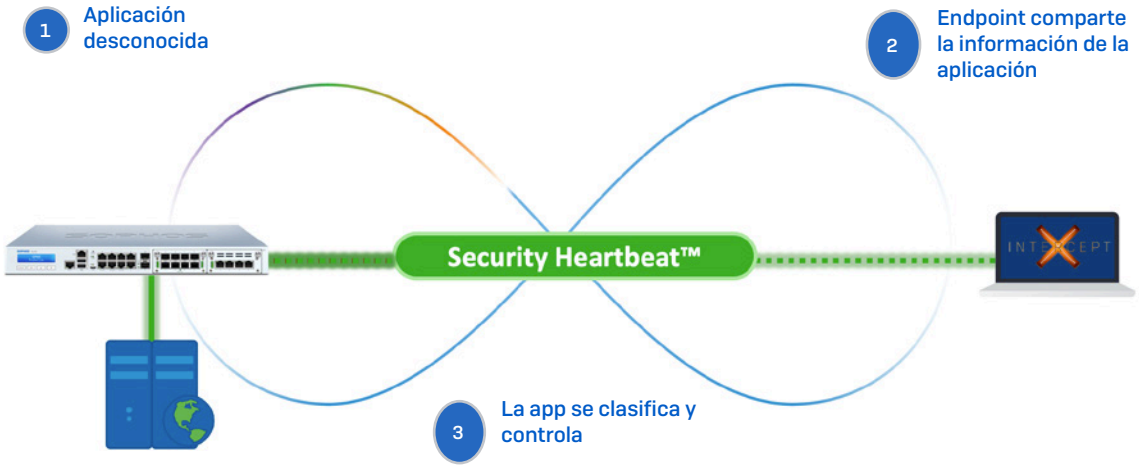


Automatice la respuesta a incidentes

Ejemplo 2: Identificar todas las aplicaciones no deseadas de la red

Un promedio del 43 % del tráfico de red no se identifica. Algunas son aplicaciones personalizadas que no tienen una firma estándar. Otras veces se debe a que la aplicación quiere ocultar su identidad al firewall porque no tiene buenas intenciones.

- Si Sophos Firewall ve una aplicación que no coincide con una firma conocida, en lugar de asignarla a un compartimento de tráfico genérico como "HTTPS", Sophos Firewall contacta con Sophos Intercept X.
- Intercept X devuelve el nombre de la aplicación, el parche y la categoría a Sophos Firewall para que la clasifique. Entonces la aplicación se asigna automáticamente al grupo correspondiente.
- Si ese grupo tiene aplicadas medidas de control (por ejemplo, bloquear), se aplican las mismas reglas. Si es necesario, por ejemplo con aplicaciones personalizadas, el administrador puede establecer manualmente una categoría y una política que aplicar.



Identifique todas las aplicaciones y procesos de la red

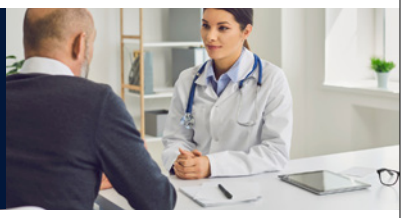
Reduzca el TCO en entornos reales

Las ventajas de un sistema de ciberseguridad de Sophos son muchas. La combinación de tecnologías next-gen, la respuesta automatizada a incidentes, el intercambio de información en tiempo real y una plataforma de administración unificada tiene un enorme impacto, tanto en la protección como en el coste total de propiedad (TCO).

Los clientes que utilizan Sophos Intercept X Endpoint y Sophos Firewall afirman que tendrían que ***duplicar su plantilla de seguridad para mantener el mismo nivel de protección*** *si no tuvieran un sistema de Sophos, y constatan una reducción de los incidentes de seguridad de hasta el 85 %.*

CUSTOMER CASE STUDY **HEALTHCARE PROVIDER, U.S.**

A regional healthcare provider whose services include inpatient and outpatient care, medical practices, nursing homes, and a range of specialist services.



Business impact of a Sophos cybersecurity ecosystem

50% reduction in IT security resource requirements
The customer has three employees dedicated to cybersecurity. They calculate they would, if they didn't use Sophos, need to employ three additional full-time security analysts solely to cover incident response.

90%-plus reduction in day-to-day cybersecurity workload
Prior to Sophos, reviewing logs and investigating areas of concern would take an entire day. Now they achieve the same level of confidence in just 30 minutes.

85% reduction in security incidents
Previously, they experienced three incidents each day on average. This has now dropped to an average of one every three days.

90%-plus reduction in time to investigate an incident
Before using Sophos, it took the team roughly three hours to thoroughly investigate an incident. This has now dropped to less than 15 minutes, with everything done remotely via the Sophos Central platform and without disrupting other users and impacting system availability.

CUSTOMER-AT-A-GLANCE

Number of users
4,500 employees

Sophos solutions
- Sophos XG Firewall
- Sophos Intercept X Advanced with EDR
- Sophos Intercept X for Server Protection (Windows, Linux, and virtual machines)

CUSTOMER CASE STUDY **CLINICAL TRIALS PROVIDER, U.S.**

A private sector organization that provides the clinical trial data needed to secure regulatory approval for new medications.

Business impact of a Sophos cybersecurity ecosystem

50% reduction in IT resource requirements
Currently, the customer spends one hour a day reviewing logs and investigating issues. They advise that they would need to hire one or two more security engineers just to manage the logs if they moved away from Sophos.

33% reduction in time to deal with a potential issue
Previously, to address a security issue with a device, they would reimage the machine, which took between 90 minutes and two hours. With Sophos, they can conduct a full investigation and remediate in approximately one hour – with no reimaging.

88% reduction in threat risk due to faster issue identification
Prior to using Sophos, it took a full day just to investigate the logs to find the issues. With Sophos, the IT team can identify new issues for investigation within minutes of a suspicious event arriving.

Improved user behavior
As users are aware that the IT team can now address issues quickly and without impacting work, they are far more willing to report issues or concerns.

CUSTOMER-AT-A-GLANCE

Number of users
150 employees across four locations

IT team
Two IT staff, covering all areas including cybersecurity

Sophos solutions
- Sophos XG Firewall
- Sophos Intercept X Advanced with EDR
- Sophos Device Encryption

Dote al personal sanitario ocupado de una red de seguridad

En un entorno sanitario sometido a una gran presión, los riesgos derivados de los errores humanos siempre serán difíciles de eliminar y controlar. Sophos ofrece una red de seguridad vital para que los usuarios puedan trabajar ágilmente y sin preocupaciones.

Evite que las amenazas lleguen a sus usuarios

Podemos ayudar a aliviar la presión de sus usuarios (y, por extensión, de su equipo de TI) impidiendo que las amenazas lleguen a sus usuarios desde un principio:

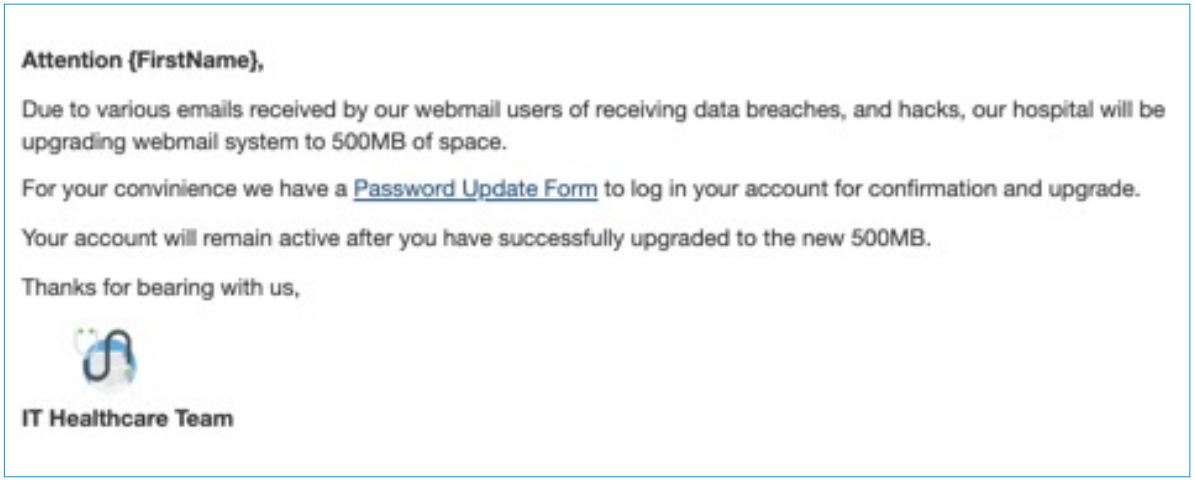
Intercept X with EDR combina prevención de exploits, antiransomware y detección con IA para detener las amenazas en varios puntos de la cadena de ataque. Los usuarios pueden tener la tranquilidad de saber que cuentan con la mejor protección para endpoints del mundo.

Sophos Email ofrece una protección predictiva con IA directamente en la bandeja de entrada de sus usuarios. Identifica los correos electrónicos maliciosos y los elimina automáticamente, antes de que los usuarios puedan siquiera hacer clic en un enlace sospechoso.

El **ecosistema de ciberseguridad de Sophos** permite que los productos de Sophos funcionen de forma conjunta para responder automáticamente a las amenazas, deteniéndolas y limpiándolas en cuestión de segundos.

Forme a sus usuarios para detectar amenazas

Sophos Phish Threat ayuda a los usuarios a identificar los correos electrónicos maliciosos mediante mensajes de phishing simulados y formación online. Puede destinar la formación a quienes más la necesitan, ya sea por la naturaleza de su puesto o por su rendimiento en las pruebas de simulación.



Attention {FirstName},

Due to various emails received by our webmail users of receiving data breaches, and hacks, our hospital will be upgrading webmail system to 500MB of space.

For your convinience we have a Password Update Form to log in your account for confirmation and upgrade.

Your account will remain active after you have successfully upgraded to the new 500MB.

Thanks for bearing with us,

IT Healthcare Team

Ejemplo de correo electrónico de simulación de phishing en Sophos Phish Threat

Implemente una protección que no ralentice la asistencia sanitaria

Hacer que todo funcione ininterrumpidamente es más importante en el sector sanitario que en la mayoría de las demás industrias. Y para ello, muchos usuarios del ámbito sanitario despliegan aplicaciones no aprobadas para facilitar su trabajo. Esto deja su red y sus datos expuestos a un alto riesgo. Sophos le ayuda a combatir la TI en la sombra sin interferir en sus operaciones diarias.

Protección avanzada que hace que todo siga funcionando

Intercept X with EDR protege sus endpoints y servidores, evitando que las amenazas afecten a los usuarios. Las funciones de EDR le permiten consultar de forma remota los dispositivos de sus usuarios y, si es necesario, remediarlos.

Sophos Firewall mantiene su red a salvo de las amenazas y facilita que se dé prioridad al tráfico de red de confianza, lo que garantiza que los procesos críticos puedan continuar sin interrupciones. Además, le ofrece visibilidad y control de la TI en la sombra, lo que le permite identificar y detener la actividad que pueda poner en riesgo a su organización.

Los productos de Sophos son excelentes por sí solos, y aún mejores en conjunto. Como hemos visto, Sophos Intercept X y Sophos Firewall funcionan juntos para responder automáticamente a las amenazas y mejorar su visibilidad.

Proteja la tecnología heredada

Un reto que escuchamos de muchas organizaciones sanitarias es la necesidad de proteger los equipos heredados. Estos dispositivos suelen ejecutar sistemas operativos desfasados que no pueden actualizarse por cuestiones normativas, pero que necesitan estar conectados a la red. Si un dispositivo no se puede parchear o actualizar y no tiene una solución antivirus o antimalware compatible, hay que buscar una solución física.

Sophos Firewall y **SD-RED** (dispositivo Ethernet remoto) pueden ayudar en este sentido. Al poner un SD-RED delante del dispositivo expuesto, puede canalizar todo el tráfico a un Sophos Firewall de protección para escanearlo. Si su red es muy plana, es probable que tenga que hacer algunos pequeños cambios en los esquemas de direcciones IP y en la posible topología de los switches; nuestros especialistas técnicos pueden analizar su situación particular y aconsejarle cómo hacerlo.

Protección de equipos heredados

Conclusión

La protección de los entornos de TI del sector sanitario y de los datos confidenciales que albergan requiere una seguridad por capas. Al implantar una seguridad inteligente en todos los puntos vulnerables, desde las redes hasta los datos, puede proteger sus sistemas, su personal y sus pacientes de los riesgos internos y externos.

Todas las soluciones de Sophos forman parte de nuestro ecosistema de ciberseguridad adaptativa. Son excelentes por separado (muchas organizaciones empiezan con un solo producto), pero funcionan aún mejor juntas. A medida que crece su protección de Sophos, también lo hacen las ventajas añadidas de un ecosistema integrado: el intercambio de información, la gestión centralizada en una única consola, la respuesta automatizada, los análisis más detallados, etc. Todo ello funciona de forma conjunta y aumenta aún más su protección, a la vez que mejora la eficiencia de su equipo de TI.

Protección en el sector sanitario: ecosistema de ciberseguridad de Sophos

Para obtener más información sobre cómo Sophos protege a las organizaciones sanitarias y analizar sus necesidades, póngase en contacto con su representante de Sophos o solicite una llamada de nuestros especialistas en seguridad.

Solicite una llamada de nuestros especialistas en seguridad hoy mismo.

Sophos ofrece soluciones de ciberseguridad líderes en la industria a empresas de todos los tamaños a fin de protegerlas en tiempo real de amenazas avanzadas como el malware, el ransomware y el phishing. Gracias a nuestras funcionalidades next-gen probadas, los datos de su empresa estarán protegidos de forma eficiente por productos con tecnologías de inteligencia artificial y Machine Learning.

05-05-2021 (SB-NP)

SOPHOS