SOPHOS
Cybersecurity evolved.

Protegemos la empresa omnipresente

Cualquier ubicación. Cualquier dispositivo. Cualquier recurso.

Monográfico de Sophos Febrero de 2021

El teletrabajo ha llegado para quedarse: según Gartner, el 74 % de las empresas esperan que algunos de sus empleados sigan trabajando a distancia una vez finalizada la pandemia[1]. Al mismo tiempo, los recursos que necesitan las personas para desempeñar sus trabajos se encuentran en múltiples ubicaciones: en servidores en la oficina, en aplicaciones basadas en la nube como Office 365 o Salesforce, y en entornos en la nube pública o privada en Amazon Web Services (AWS) y Microsoft Azure.

Los equipos de TI deben encargarse de proteger a cada usuario y cada recurso, independientemente de dónde estén. Mientras tanto, los ciberdelincuentes siguen buscando formas mejores y más subversivas de penetrar en empresas cada vez más virtuales en cada punto de intersección.

Proteger las empresas en que las personas y los recursos pueden encontrarse en cualquier parte requiere:

- Una conectividad segura para que los usuarios puedan acceder a los recursos desde cualquier lugar: en casa, in situ o en la oficina.
- Protección para los dispositivos utilizados para establecer esas conexiones: ordenadores de escritorio, portátiles, teléfonos móviles y tablets.
- Protección para los datos y las cargas de trabajo a los que los usuarios necesitan acceder, tanto si están en la nube como si se encuentran en su red local.
- Una administración sencilla para que los equipos de TI puedan gestionar sus empresas distribuidas desde cualquier parte sin incrementar su carga de trabajo.

Afortunadamente, Sophos cubre todas estas áreas. Ofrecemos un completo catálogo de productos de seguridad next-gen con una amplísima gama de funciones de protección avanzada. Todo se controla a través de una única plataforma de seguridad web que reduce drásticamente la carga administrativa diaria, al tiempo que permite a los equipos de TI gestionar la seguridad de su empresa desde cualquier ubicación.

En este informe de la solución se explica cómo Sophos satisface cada uno de estos requisitos. También se detallan las ventajas en términos de productividad y protección que experimentan los clientes al emplear un sistema de ciberseguridad de Sophos para proteger su empresa.

Conectarse de forma segura

Es indiscutible que la pandemia de COVID ha provocado un gigantesco aumento del teletrabajo. Durante mayo de 2020, el 62 % de los norteamericanos en activo estaban trabajando desde casa (TDC). Sin embargo, ya se observaba una tendencia hacia el teletrabajo incluso antes de la aparición de la COVID, y muchos empleados de oficinas ya estaban pasándose al trabajo desde casa algunos días a la semana. En el Reino Unido, el teletrabajo se incrementó hasta el 74 % en la última década, mientras que en Australia sobre un tercio de los empleados trabajaba desde casa regularmente.

Con el teletrabajo, tanto las empresas como el personal salen ganando: los empleados se ahorran el tiempo y los costes de los desplazamientos diarios, al tiempo que se benefician de una mayor flexibilidad y productividad. Mientras tanto, las empresas reducen sus costes y tasas de rotación. Pero para los equipos de TI, el teletrabajo a largo plazo genera desafíos adicionales en términos de seguridad. Los empleados pueden iniciar sesión desde el salón de su casa, visitar las instalaciones de un cliente o tomarse un café en una cafetería con Wi-Fi a miles de kilómetros de distancia, pero su red y sus datos deben permanecer protegidos en todo momento.

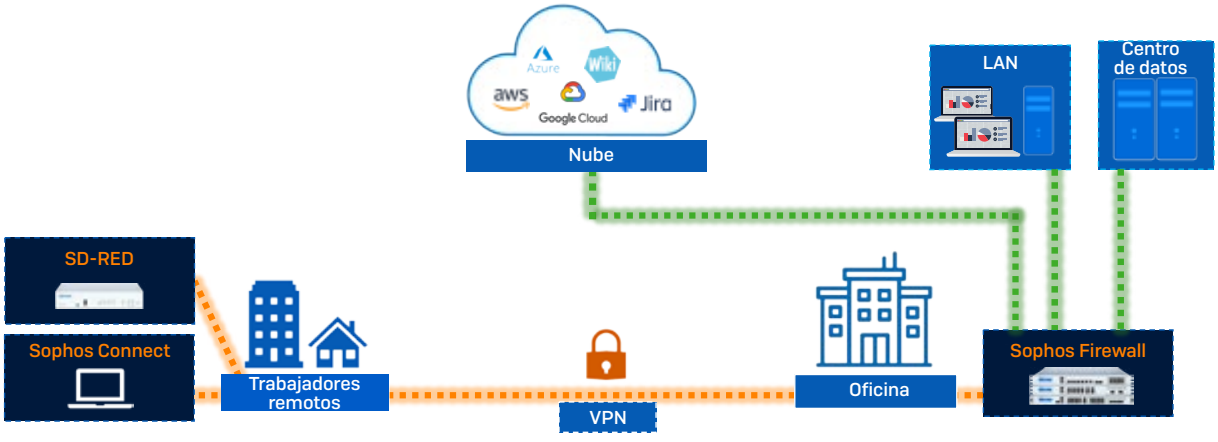
Con Sophos, sus empleados pueden conectarse y trabajar desde cualquier lugar de forma rápida, eficiente y segura, y ofrecemos tanto la opción tradicional basada en VPN como Zero Trust Network Access (ZTNA).

VPN

Utilice nuestro **cliente VPN Sophos Connect**, gratuito y de fácil despliegue, junto con **Sophos Firewall** para conectar trabajadores remotos a los recursos de su oficina principal y en la nube. Con más de 1,4 millones de usuarios en todo el mundo, Sophos Connect da acceso a sus usuarios remotos a los recursos de la red corporativa o la nube pública desde dispositivos Windows y macOS.

Para disfrutar de lo último en conectividad remota, **Sophos SD-RED** (dispositivo Ethernet remoto) es un sencillo dispositivo Plug and Play que funciona con **Sophos Firewall** para conectar sucursales, emplazamientos remotos y personas a su red principal (ya sea física o en la nube).

Proporciona una VPN de túnel dividido o dedicada siempre activa que es fácil de desplegar y administrar con opciones flexibles. También es muy pequeño y portátil, por lo que resulta ideal para directivos y otras personas que necesitan acceder a una conexión segura en cualquier momento y desde cualquier lugar.



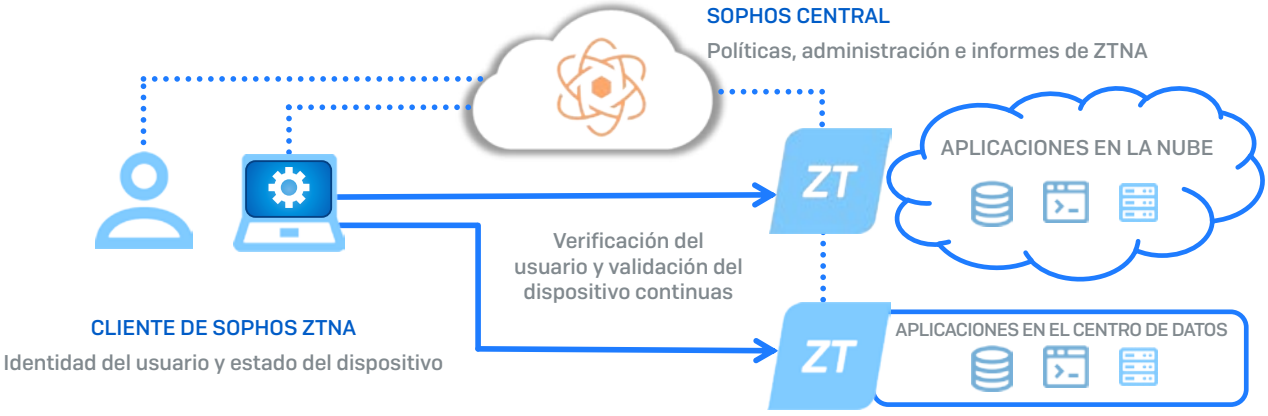
Conectividad remota segura con Sophos Firewall y el cliente VPN Sophos Connect y SD-RED

ZTNA

Durante años, la tecnología VPN ha permitido a los trabajadores conectarse de forma remota. Y fue la salvación al principio de la pandemia, ya que, gracias a ella, las empresas pudieron pasarse rápidamente al teletrabajo seguro en cuestión de días. Sin embargo, muchas empresas empiezan a querer más de lo que una VPN está diseñada para ofrecer.

Sophos Zero Trust Network Access (ZTNA) es una excelente alternativa a la VPN de acceso remoto, puesto que permite a los usuarios conectarse a los recursos corporativos desde cualquier ubicación de una forma sencilla y transparente. Al mismo tiempo, también mejora su seguridad al verificar al usuario (normalmente con autenticación multifactor y un proveedor de identidad) y validar el estado de seguridad y el cumplimiento del dispositivo en todo momento.

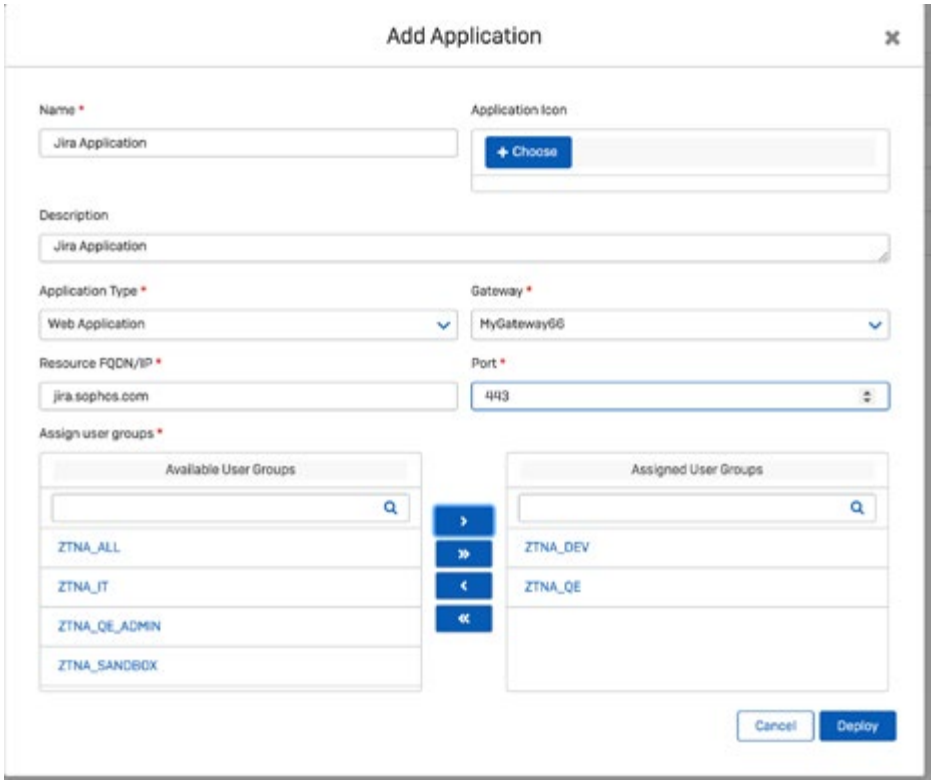
Sophos ZTNA se asegura de que el dispositivo está inscrito, actualizado y adecuadamente protegido y de que tiene activado el cifrado. Después utiliza esta información para tomar decisiones en función de políticas personalizables a fin de determinar el acceso y los privilegios de los usuarios sobre sus aplicaciones en red críticas.



El enfoque de Sophos ZTNA

Con Sophos ZTNA, puede:

- Mejorar sus ciberdefensas. Sophos ZTNA le ofrece controles muy granulares: cada uno de los usuarios, dispositivos o aplicaciones puede controlarse por separado en función de una política corporativa individual y el nivel de riesgo que prefiera. También elimina el concepto de confianza implícita en una persona por el solo hecho de que esté presente en la red. En lugar de ello, eleva la protección y minimiza el riesgo de propagación lateral dentro de la red evaluando de forma continuada la identidad y el estado de seguridad del dispositivo antes de permitir el acceso.
- Aumentar la eficiencia. Puesto que Sophos ZTNA se administra a través de la plataforma Sophos Central, es fácil inscribir nuevos usuarios o adaptarse a un entorno de trabajo cambiante. Además, es más transparente para los usuarios finales, y les proporciona un tipo de experiencia de conexión sin fricciones que simplemente funciona en comparación con la VPN.



Añada aplicaciones fácilmente con Sophos ZTNA

Independientemente del método que elija, los productos de seguridad galardonados de Sophos le ayudarán a proteger a sus empleados en cualquier lugar y dispositivo.

Proteger dispositivos

El 51 % de las empresas sufrió un ataque de ransomware en el último año, y los ciberdelincuentes lograron cifrar los datos en el 73 % de los ataques[2].

Si combinamos estas alarmantes estadísticas con la necesidad de proteger todo tipo de equipos (ordenadores de escritorio, portátiles y dispositivos corporativos y personales) y numerosos sistemas operativos (desde Windows y macOS hasta Linux, Android, Chromebook y iOS), se nos presenta un enorme quebradero de cabeza en términos de ciberseguridad.

Sophos Intercept X le ofrece la mejor protección del mundo en todos estos dispositivos y plataformas. Se beneficia de múltiples capas de tecnología que detienen a los atacantes en numerosos puntos de la cadena de ataque, entre ellas:

- Protección antiransomware, que bloquea el cifrado no autorizado de archivos, discos duros y registros de arranque y los revierte a su estado seguro.
- IA con Deep Learning, que utiliza millones de atributos de archivos para analizar amenazas y evitar malware tanto conocido como desconocido, y lo detiene antes de que pueda ejecutarse.
- Tecnología antiexploits, que bloquea exploits, técnicas de adversarios activos y ataques sin archivos y basados en scripts.
- Protección base con firmas, que detiene las amenazas conocidas.

Además, Sophos Intercept X protege cualquier dispositivo en cualquier plataforma para que sus empleados puedan trabajar de manera segura en cualquier dispositivo que elijan:

- Ordenadores de escritorio y portátiles que ejecuten Windows y macOS
- Servidores Windows y Linux
- Entornos de escritorio virtual alojados con proveedores de la nube
- Dispositivos móviles que ejecuten Android, iOS o Chromebook

Detección y respuesta para endpoints (EDR)

Las ciberamenazas más devastadoras implican ataques perpetrados por humanos, que a menudo explotan herramientas y procesos legítimos como PowerShell. El hacking manual en vivo permite a los atacantes eludir los productos y protocolos de seguridad modificando sus tácticas, técnicas y procedimientos (TTP). Cuando están dentro de su red, los atacantes se mueven lateralmente para exfiltrar datos, desplegar ransomware e instalar malware y puertas traseras para futuros ataques.

Detener estos ataques perpetrados por humanos requiere una búsqueda de amenazas realizada por humanos. **Intercept X with EDR** (Detección y respuesta para endpoints) le proporciona las herramientas que necesita para realizar búsquedas de amenazas desde la misma consola que utiliza para gestionar su protección para endpoints Intercept X.

Es la primera EDR diseñada para analistas de seguridad y administradores de TI. Mientras que otras herramientas de EDR suelen requerir un equipo dedicado o un centro de operaciones de seguridad (SOC) interno propio, Sophos EDR es fácil de utilizar sin sacrificar la capacidad de realizar un análisis robusto.

Con Intercept X with EDR, puede investigar señales sospechosas y amenazas (y mejorar su higiene de TI) con potentes consultas SQL predefinidas y personalizables. Algunos casos de uso comunes son:

- Rendimiento lento de Chrome. Identifique qué extensiones de Chrome no autorizadas se han instalado.
- Comprobación de actividad de red. Busque intentos de inicio de sesión fallidos y comunicación activa de PowerShell.
- Consultas de software. Compruebe que se hayan eliminado los archivos confidenciales de los dispositivos o que no haya excedido el uso de licencias de software.
- Investigación de phishing. Identifique a los usuarios que hayan hecho clic en un enlace sospechoso y si han descargado archivos.

Además, puede acceder a dispositivos de forma remota usando una herramienta de línea de comandos para solucionar problemas, como reiniciar dispositivos, finalizar procesos activos, ejecutar scripts o programas, editar archivos de configuración, ejecutar herramientas forenses o instalar y desinstalar software.

Detección y respuesta gestionadas (MDR)

Si no tiene el tiempo, la capacidad o los conocimientos para llevar a cabo sus propias investigaciones y búsquedas de amenazas, el servicio **Sophos Managed Threat Response** (MTR) está a su disposición para ayudarle.

Sophos MTR es un servicio totalmente administrado prestado por un equipo de cazadores de amenazas y expertos en respuesta que ofrece funciones de supervisión, detección y respuesta 24/7. Este equipo busca y valida de forma proactiva posibles amenazas e incidentes y los detiene antes de que puedan provocar daños.

También correlaciona feeds de datos de sus soluciones de protección de Sophos para identificar indicadores de peligro. A diferencia de otros servicios de detección y respuesta gestionadas, Sophos no se limita a notificarle los problemas, sino que también determina y aplica las acciones más adecuadas para neutralizar la amenaza.

Dispositivos móviles

Cuando los empleados utilizan dispositivos personales para el trabajo, los equipos de TI se enfrentan al reto de proteger los datos de la empresa sin comprometer la privacidad de los usuarios. Nuestra solución de gestión unificada de endpoints, **Sophos Mobile**, protege dispositivos iOS, Android, Chrome OS, Windows 10 y macOS. Le permite proteger cualquier combinación de dispositivos personales y propiedad de la empresa con un esfuerzo mínimo, y es ideal en escenarios de BYOD (uso de dispositivos personales en el trabajo).

Sophos Mobile le permite:

- Detener amenazas para dispositivos móviles. Consiga la solución de defensa líder del sector contra el malware, el phishing y los ataques de intermediario (Man-in-the-Middle) contra móviles, entre otras amenazas, todo ello con el respaldo de Intercept X.
- Proteger datos corporativos. Elija la administración exclusiva de contenedores o de dispositivos completos, en función de sus necesidades.
- Reducir la carga administrativa. El portal de autoservicio flexible permite a los usuarios inscribir sus dispositivos personales macOS, Windows 10 o móviles, restablecer contraseñas y obtener asistencia sin la intervención del departamento informático.

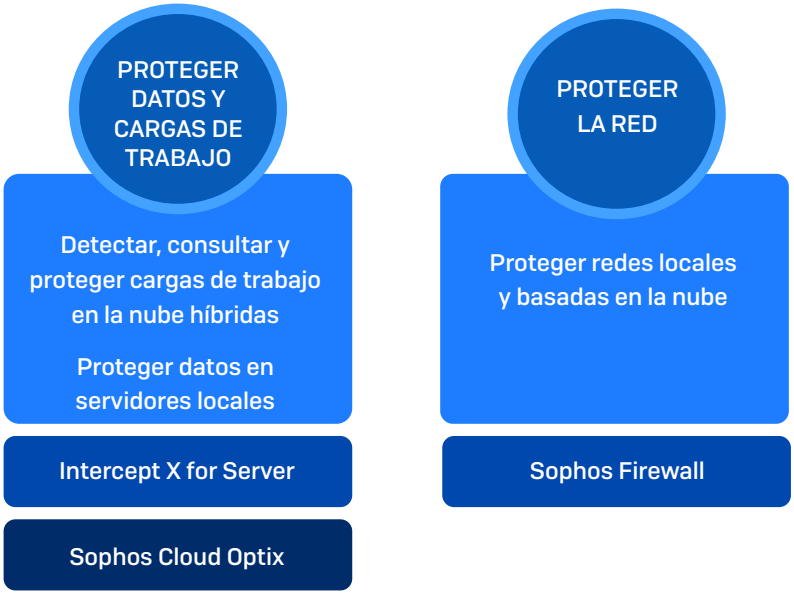
Proteger recursos

En función de las necesidades de su empresa, es posible que ejecute servidores de forma local, que consuma aplicaciones basadas en la nube o que aloje recursos en entornos en la nube pública y privada en AWS, Azure o GCP. Lo más probable es que esté haciendo todas estas cosas.

La nube se está volviendo cada vez más fundamental para las operaciones diarias de la mayoría de empresas. Debido a esto, los ciberdelincuentes están atentos a las oportunidades que les brinda la nube, hasta el punto de que el 70 % de las empresas que utilizan la nube pública han sufrido algún incidente de seguridad en la nube en los últimos 12 meses[3].

A la hora de proteger sus recursos, se encuentren donde se encuentren, necesita hacer dos cosas:

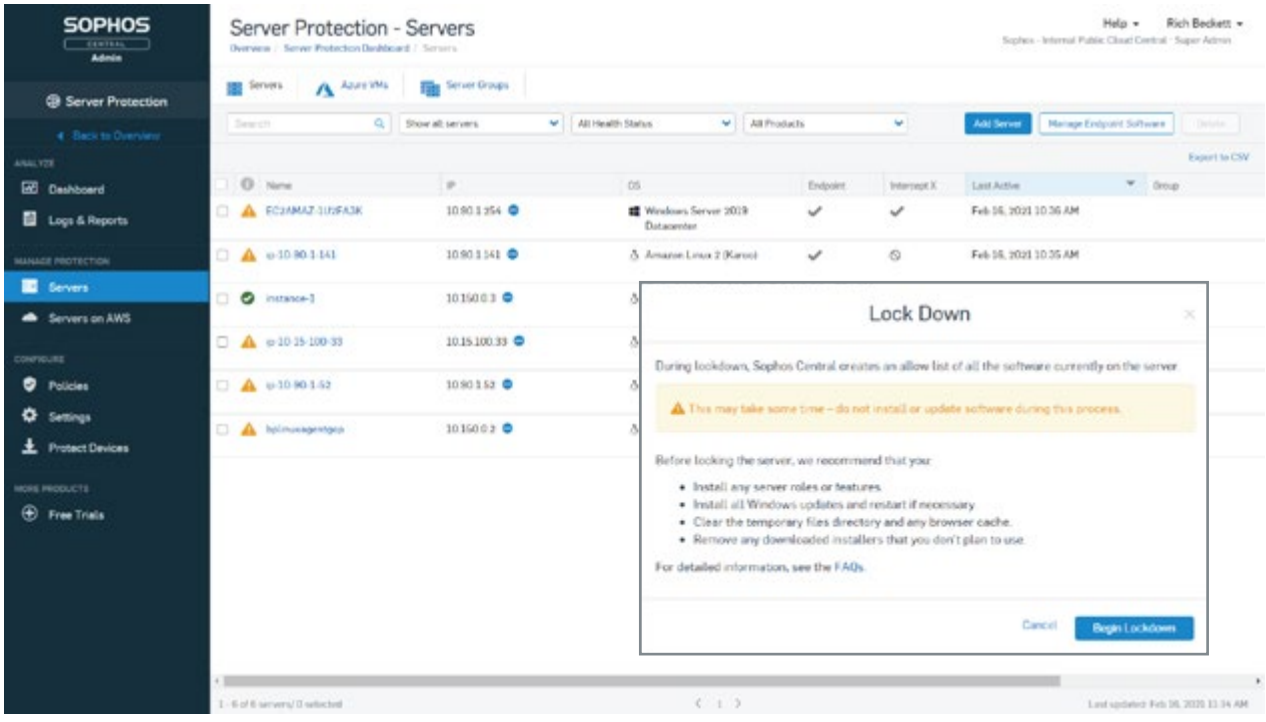
1. Proteger los datos y las propias cargas de trabajo
2. Proteger la red en que se encuentran para impedir el acceso a intrusos



Proteger sus datos y cargas de trabajo

Sus datos y sus cargas de trabajo son sus activos más importantes. **Sophos Intercept X for Server** protege entornos de cargas de trabajo en la nube, locales e híbridos. Protege equipos y escritorios virtuales Windows y Linux frente a las amenazas más recientes.

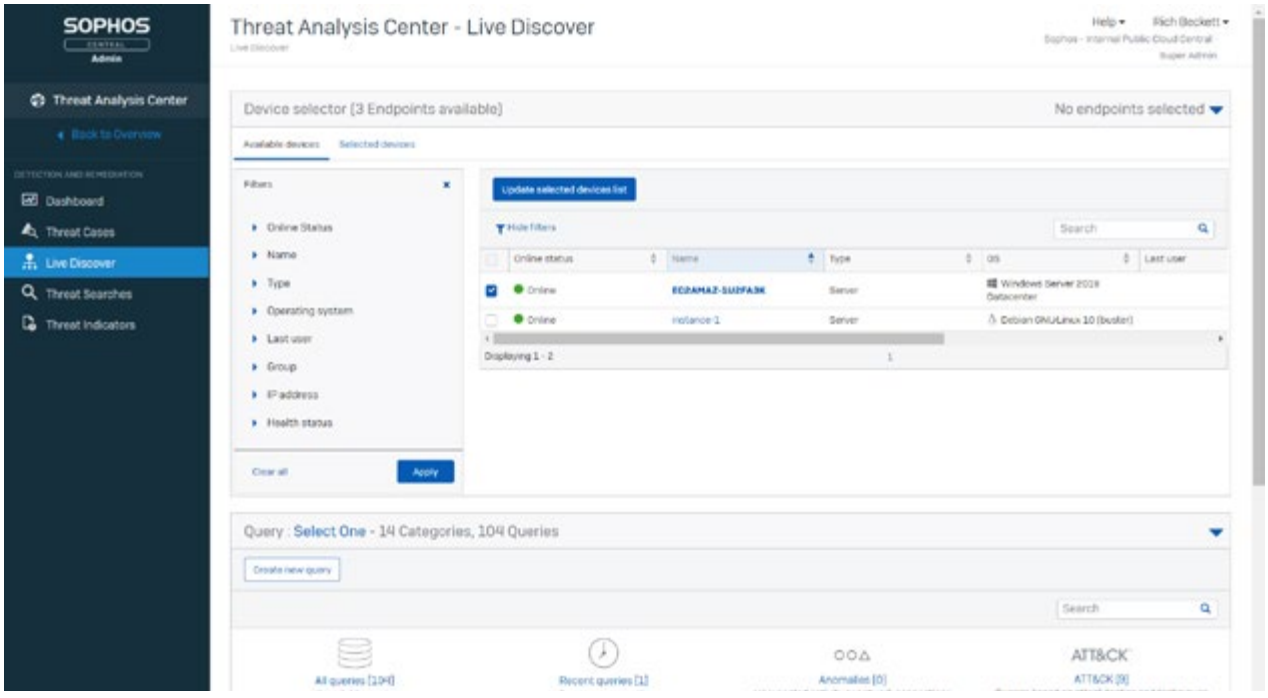
- Detenga ataques avanzados. Incluidos el ransomware, los ataques basados en exploits y el malware desconocido.
- Bloquee las cargas de trabajo de sus servidores. Controle qué puede ejecutarse y qué no, y reciba notificaciones de cualquier intento de cambio no autorizado.
- Administre todo de forma centralizada. Despliegue y mantenga todo desde una única consola, también los entornos mixtos que incluyan cargas de trabajo en la nube y servidores locales.



Intercept X for Server

También puede ampliar sus investigaciones de EDR a sus servidores, ya sea localmente o en la nube, con **Intercept X for Server with EDR**. Esto le permite:

- Realizar tareas críticas de operaciones de TI y búsqueda de amenazas. Identifique problemas de rendimiento, vea qué está instalado dónde y detecte actividad sospechosa.
- Detectar automáticamente cargas de trabajo en la nube. Controle los servicios en la nube críticos, incluidos los buckets de S3, las bases de datos y las funciones sin servidor.
- Detectar despliegues no seguros. Cuente con la supervisión constante con IA de sus entornos en la nube y la notificación de irregularidades.

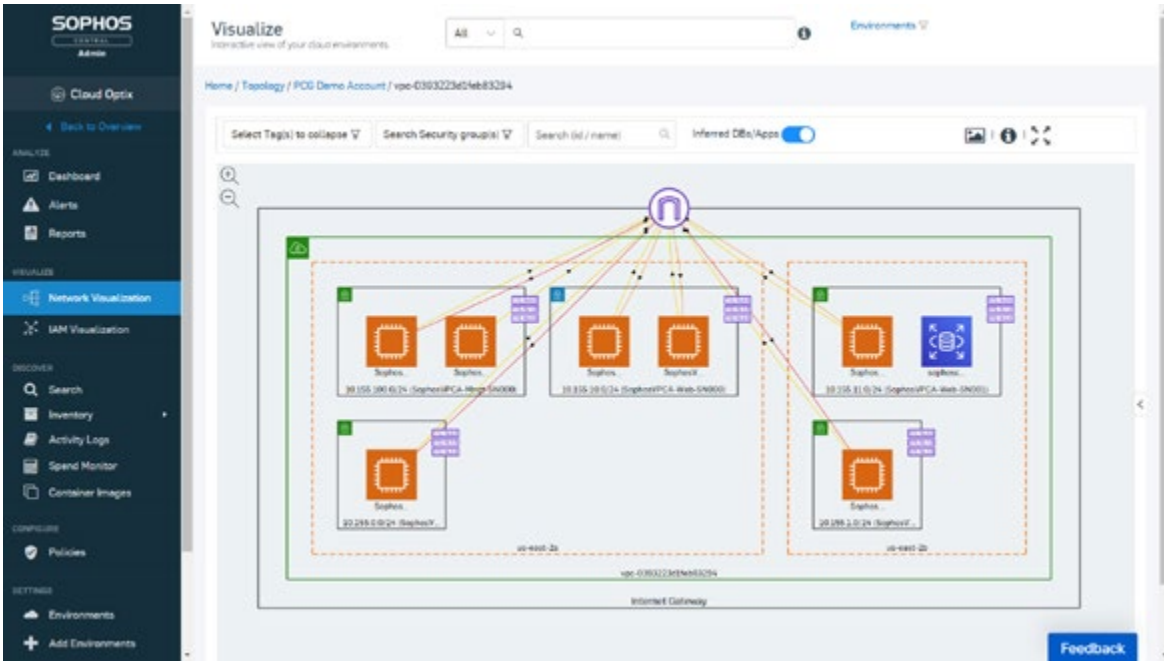


Amplíe sus investigaciones de EDR a su servidor

La protección es una de las caras de la moneda de la protección de datos y cargas de trabajo. La visibilidad es la otra. Necesita una línea de visión clara y continua de lo que tiene ejecutándose y la capacidad de configurar servicios de proveedores de la nube para evitar filtraciones de seguridad.

Sophos Cloud Optix, nuestra solución de gestión de la posición de seguridad en la nube, le proporciona la visibilidad que necesita para proteger su empresa, incluyendo:

- Visibilidad multinube. Inventario detallado de los recursos en la nube, como servidores, contenedores, almacenamiento, red e IAM para AWS, Azure y GCP.
- Priorización basada en riesgos. Analice configuraciones continuamente para detectar riesgos de seguridad y accesos de IAM con demasiados privilegios.
- Gestión del cumplimiento. Supervise el cumplimiento constantemente con plantillas predefinidas, políticas personalizadas y herramientas de colaboración.
- Seguridad integrada. Identifique la protección de cargas de trabajo y firewalls de Sophos en AWS.
- Optimización de costes de la nube. Gestione los gastos de AWS y Azure desde una única pantalla.



Sophos Cloud Optix

Si bien las alertas de seguridad para sus entornos en la nube resultan útiles, con servicios como Amazon GuardDuty que ofrecen un gran valor, es demasiado fácil verse abrumado por la ingente cantidad de notificaciones. Así es prácticamente imposible reconocer sobre qué notificaciones necesita actuar realmente.

En Sophos, utilizamos Sophos Cloud Optix para proteger los entornos de Amazon Web Services utilizados para alojar Sophos Central, nuestra plataforma de ciberseguridad. Uno de los principales beneficios que Cloud Optix ha aportado a nuestro propio equipo de seguridad es la capacidad de centrarse en lo importante.

"Con Sophos Cloud Optix, minimizamos notablemente la fatiga por alertas. La potente inteligencia artificial integrada en Sophos Cloud Optix correlaciona los datos y nos muestra aquello que es verdaderamente importante y procesable".

Ross McKerchar, vicepresidente y director de seguridad de la información, Sophos

Proteger la red

Para proteger sus recursos, también necesita proteger las redes en las que se encuentran. **Sophos Firewall** ofrece una protección y una visibilidad inigualables para entornos de AWS, de Azure y locales.

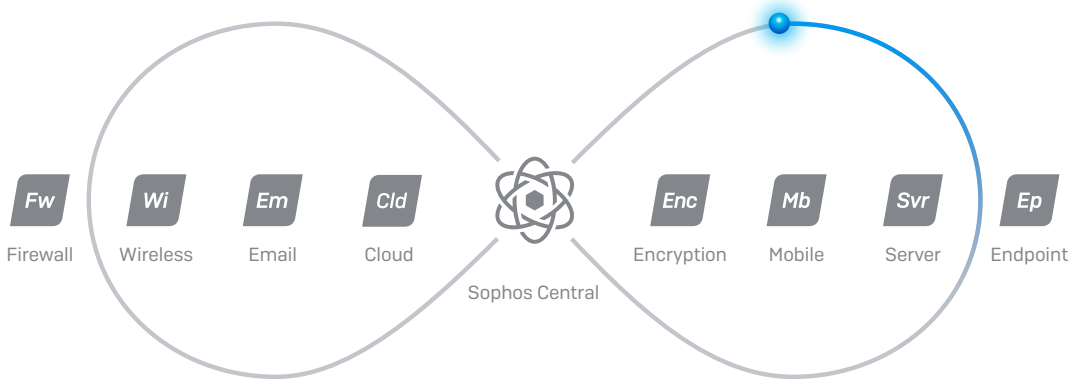
- Protección multicapa integrada para detener incluso las amenazas más avanzadas.
- Potente solución todo en uno para WAF, IPS, ATP, filtrado de URL, enrutamiento basado en rutas y bloqueo por países, con generación de informes detallados, incluida una visión integral de la actividad de los usuarios y la red.
- Visibilidad de las aplicaciones en la nube, detección de TI en la sombra y respuesta automatizada a las amenazas.
- Capacidad para endurecer sus cargas de trabajo en la nube contra los intentos de hacking, como la inyección de código SQL y los ataques de secuencias de comandos entre sitios, a la vez que proporciona un acceso seguro a los usuarios con la autenticación de proxy inverso.
- Flexibilidad para ejecutarse como una solución independiente y de alta disponibilidad.

Y para facilitar el despliegue en la nube, todo está disponible en una única imagen de equipo virtual preconfigurada.

Simplificar la gestión

Con Sophos, puede gestionar toda su seguridad desde una única plataforma web: Sophos Central. Se acabó tener que ir de consola en consola para proteger su empresa: todo se encuentra en un mismo sitio. También le permite llevar a cabo investigaciones entre productos cómodamente, correlacionando datos de múltiples servicios con facilidad.

Y como Sophos Central está alojado en la nube, es ideal para los equipos de TI dispersos. Con más de 400 000 usuarios en todo el planeta, puede tener la tranquilidad de que está utilizando la plataforma de ciberseguridad en la que más confía el mundo.



Sophos Central también permite que los productos de Sophos compartan información sobre seguridad, estados y amenazas en tiempo real y funcionen de forma conjunta para responder automáticamente a las amenazas: es lo que llamamos Seguridad Sincronizada. Algunos beneficios incluyen:

- Respuesta automatizada a incidentes. Si un producto de Sophos detecta algo sospechoso, como una infección de malware o un dispositivo que incumple las políticas, comparte esta información con el resto del sistema de ciberseguridad. Entonces los demás productos responden automáticamente al incidente en cuestión de segundos. Por ejemplo:
  - Sophos Firewall aísla al instante los dispositivos infectados, lo que evita que se propague la amenaza y bloquea el movimiento lateral.
  - Intercept X analiza automáticamente un endpoint cuando se detectan buzones de correo comprometidos, lo que limita el impacto de las amenazas que se propagan por correo electrónico.
  - Sophos Wi-Fi restringe el acceso a los dispositivos que incumplen las políticas, y mantiene así los dispositivos no autorizados y no seguros fuera de su red inalámbrica.
- Visibilidad única. Los equipos de TI disfrutan de una mayor visibilidad y control de su red, incluida la capacidad de:
  - Identificar los dispositivos infectados por el nombre en lugar de la dirección IP, lo que acelera las investigaciones de seguridad.
  - Identificar todas las aplicaciones de la red. De media, el 43 % del tráfico de red se transmite como "no clasificado", por lo que el equipo de TI no tiene idea de si es benigno, erróneo o malicioso. Con la Seguridad Sincronizada, Sophos Firewall e Intercept X funcionan de manera conjunta para identificar y clasificar automáticamente TODAS las aplicaciones de la red.

Protección incomparable. Eficiencia inigualable.

Ejecutar un sistema de ciberseguridad de Sophos le ofrece protección next-gen, una única plataforma de administración, la capacidad de compartir información sobre amenazas entre productos y una respuesta automatizada a incidentes. Todas estas funcionalidades permiten a los equipos de TI obtener enormes beneficios en términos de eficiencia y productividad.

De hecho, los clientes que utilizan Sophos Intercept X y Sophos Firewall, administrados a través de Sophos Central, afirman sistemáticamente que consiguen **duplicar la eficiencia del equipo de TI** al tiempo que se benefician de **una reducción del 85 % en incidentes de seguridad**.

"Tener herramientas que detectan y corrigen automáticamente la mayoría de los eventos de seguridad permite a nuestro pequeño equipo de TI gestionar la seguridad de la empresa y evitar que se vea comprometida".

Director tecnológico, proveedor de servicios de software

Protegemos cualquier ubicación. Cualquier dispositivo. Cualquier recurso.

Ya no hay vuelta atrás de la transición al teletrabajo flexible y del uso creciente de la nube. Nos hacen la vida más fácil, pero también suponen nuevos retos para los equipos de TI y nuevas oportunidades para los ciberdelincuentes. Proteger este nuevo entorno requiere conexiones seguras, recursos seguros y dispositivos seguros, estén donde estén, sin incrementar la carga de trabajo de TI.

Sophos puede ayudarle a hacer frente a estos retos actuales con potentes soluciones de confianza. Póngase en contacto con su representante de Sophos para hablar de sus requisitos o active una evaluación gratuita sin compromiso para poner a prueba cualquiera de nuestros productos.

1 https://www.gartner.com/en/newsroom/press-releases/2020-04-03-gartner-cfo-surey-reveals-74-percent-of-organizations-to-shift-some-employees-to-remote-work-permanently2

2. Nota al pie El estado del ransomware 2020, Sophos

3. Nota al pie El estado de la seguridad en la nube 2020, Sophos

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

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

15-02-21 WPES (MP)

SOPHOS