EXXODA
CIBERSECURITY

Nuestro mundo depende de la seguridad para seguir conectado. Como industria de ciberseguridad nos encargamos de continuar introduciendo tecnologías inteligentes y conectadas que vinculen más elementos de la vida cotidiana juntos.

# Tu **SEGURIDAD** es nuestra **RESPONSABILIDAD**

CONOCE NUESTROS SERVICIOS

# SOBRE LA MARCA

**“EXXODA”** somos una empresa especializada en ciberseguridad, ofrecemos servicios que previenen las amenazas informáticas y ciberataques avanzados. Brindamos el control seguro para sus redes de información, protección de datos confidenciales.

## MISIÓN

Garantizar la ciberseguridad de nuestros clientes, a través de soluciones ágiles, adaptables y proactivas.

## VISIÓN

Ser un proveedor de servicios de ciberseguridad en Latinoamérica, ofreciendo soluciones tecnológicas innovadoras y efectivas.

## VALORES

- Honestidad
- Proactividad
- Innovación
- Confianza

## PARTNERS

SOPHOS

paloalto NETWORKS

FORTINET

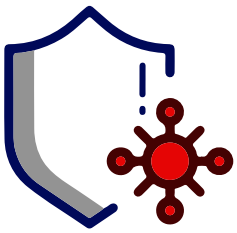
# ENDPOINT SECURITY

## 1 REDUCIR LA EXPOSICIÓN A LAS AMENAZAS

- **Bloqueo de amenazas basadas en la web y controlar el acceso a la web:** Para todos esos dispositivos finales con los que se trabajan fuera de la seguridad perimetral de la empresa, Sophos Endpoint bloquea el acceso a sitios web maliciosos y de phishing mediante el análisis de archivos, páginas web y direcciones IP. Además, SophosLabs y el equipo de Sophos MDR proporcionan inteligencia sobre amenazas en tiempo real sobre menazas emergentes.


- **Control de aplicaciones, periféricos y web:** Sophos ofrece una gama de políticas de control para garantizar la integridad de sus equipos e información:

  - El control web restringe el acceso a URL's tanto de manera específica como por categorías preestablecidas por Sophos (Redes sociales, contenido Sexual, Juegos, Stream, etc). Garantiza el uso correcto de su ancho de banda.

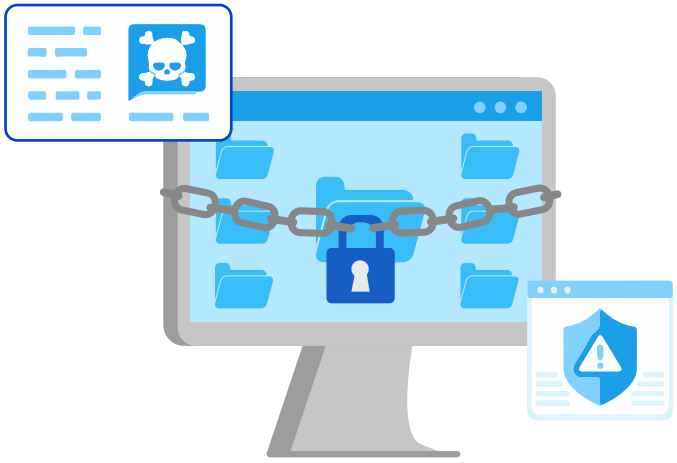



  - El control de periféricos administra todo dispositivo independiente al equipo que quiera acceder para compartir información. Bloqueando el uso de USB's se puede evitar que la máquina quede infectada de malwares independientes de la red, instalación de sofwares no permitidos, robo de información, etc.

  - El control de aplicaciones, al igual que el web, puede restringir aplicaciones de manera específica (PowerShell, AutoC, Super Mario Smash Bros, etc) como por categorias (System Tool, Internet Browser, Telnet client).

## 2 BLOQUEAR ACTIVIDAD MALICIOSA

- **Anti-ransomware:** Sophos ofrece una avanzada tecnología antiransomware con el enfoque de señales de encriptación independientemente de la fuente. Este enfoque previene nuevas variantes nunca antes vistas de ransomware. Si se detecta una acción de esta naturaleza se creará una copia de seguridad del archivo afectado en un caché local del dispositivo, se finalizará el proceso de la amenaza y se restaura los archivos del caché.



- **Anti-exploit:** Detecta el comportamiento y técnicas que los atacantes usan para comprometer dispositivos, robar credenciales y distribución de malwares. Sophos se basa en la protección básica ofrecida por Windows y añade al menos 60 mitigaciones de exploits patentadas, preconfiguradas y ajustadas, dando como resultado un antivirus inteligente a lo largo de la cadena de ataque.

## 3 DEFENSAS SENSIBLES AL CONTEXTO

- **Protección del comportamiento:** El motor de comportamiento detiene las primeras fases de los ataques activos de adversarios.

"SHIELDS ON!"

- **Protección adaptable contra ataques:** Habilita dinámicamente las defensas reforzadas en un endpoint cuando se detecta un ataque con las manos en el teclado. Esto elimina la capacidad del atacante para realizar más acciones, minimiza la superficie de ataque, interrumpe y contiene el ataque y gana un tiempo valioso para responder.

"SHIELDS UP!"

- **Advertencia de ataque crítico:** La alerta sobre un ataque grave si se detecta actividad adversaria en múltiples puntos finales o servidores en su entorno con indicadores adicionales de alto impacto. La tecnología automatizada le informa la situación y le proporciona el contexto y los detalles del ataque.

"RED ALERT!"

**PRODUCTO**

# XDR

## ¡Eleve sus defensas contra ataques avanzados dirigidos por humanos con el nuevo Sophos XDR!

Los adversarios tardan sólo 16 horas en promedio en comprometer un Directorio Activo (AD).

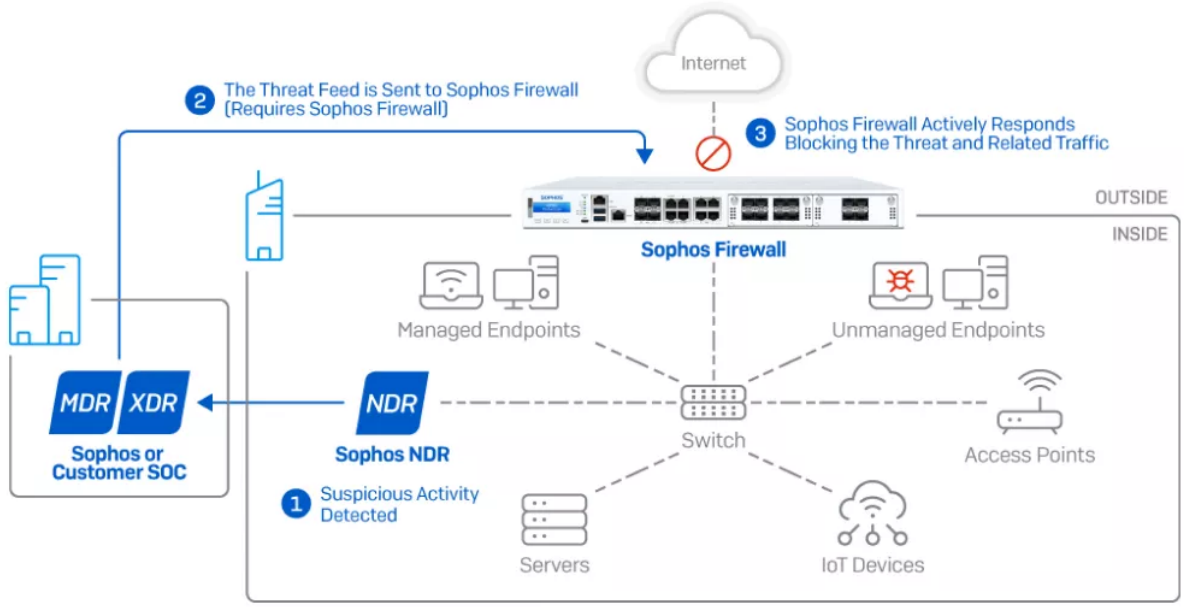
Sophos XDR le brinda las herramientas que necesita para detectar y responder a actividades sospechosas en su entorno antes de que los adversarios puedan afectar sus sistemas, aprovechando los datos de sus soluciones de seguridad existentes (los de Sophos y terceros).

- **DETECCIÓN:** Las detecciones impulsadas por IA brindan visibilidad instantánea de actividades sospechosas en su entorno y la búsqueda simplificada sin SQL le permite detectar amenazas a gran velocidad.

- **INVESTIGAR:** Las puntuaciones de riesgo para cada detección facilitan centrarse en lo que es importante, mientras que nuestra nueva UX de Detecciones le brinda toda la información y las herramientas que necesita para llevar a cabo investigaciones.

- **RESPONDER:** Las potentes acciones de respuesta y gestión de casos le permiten neutralizar rápidamente los ataques.

Además, con Sophos XDR ahora puede agregar Sophos Network Detection and Response (NDR) a sus defensas, lo que le permite detectar dispositivos no autorizados y no administrados en su red y ataques a dispositivos IoT y OT.




Fuente: sophos.com

## SERVICIO

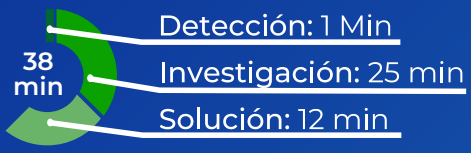
# MDR

La seguridad endpoint es una capa de protección esencial, pero no puede detener todas las amenazas. Con Sophos MDR, los analistas de Sophos monitorean y responden a las alertas de seguridad de los endpoints las 24 horas del día, los 7 días de la semana, tomando medidas inmediatas para detener las amenazas confirmadas.


- **Integraciones:** Sophos MDR se integra con las soluciones de punto final, red, firewall, correo electrónico, nube y de identidad que una organización ya está utilizando, tanto de Sophos como de terceros.

- **Protección sólida:** Sophos protege el 98% de las amenazas y para este 2% restante, el equipo de MDR Sophos, conformado por más de “500” especialistas en ciberseguridad alrededor del mundo, ofrecen detección y respuesta acelerada en un tiempo promedio de 38 min.

**Tiempo de resolución de problema:**




- **Respuesta totalmente gestionada:** Puede participar plenamente y tomar el control de una amenaza, desde la detección hasta la neutralización, pasando por la investigación.

**Sólida búsqueda de amenazas con y sin pistas. Los cazadores de amenazas de Sophos utilizan la inteligencia más reciente y su experiencia para buscar y validar de forma proactiva amenazas potenciales.**

**Sophos MDR Complete:** Cubre hasta 1 millón USD en gastos de respuesta para los clientes QUE CUMPLAN CON LOS REQUISITOS. No hay niveles de garantía, ni condiciones mínimas de contrato ni requisitos de compra adicionales.

PRODUCTO

# SOPHOS FIREWALL

**EMPODERADO POR XSTREAM**

**CONECTIVIDAD DE ALTA VELOCIDAD**

**RENDIMIENTO EN BASE AL DISEÑO**

**DEEP PACKET INSPECTION**

**ACELERACION DE APLICACIONES**


Solución de seguridad Next-Generation basado en zonas, que protege contra las últimas amenazas de hoy, además de su fácil y escalable gestión desde Sophos Central. La serie XGS ofrece una gran protección gracias a la poderosa performance del procesador Xstream.

Ofrece la mejor protección y performance optimizada para el tráfico de internet encriptado. Capacidades de SD-WAN para orquestar e interconectar de manera fácil y segura tus oficinas y sucursales. Integración con Sophos MDR y Sophos XDR para detener amenazas de manera automatizada. Soporte para SSE y SASE incluyendo ZTNA, protección SWG DNS y más. Funcionalidad ZTNA para asegurar acceso remoto de usuarios.

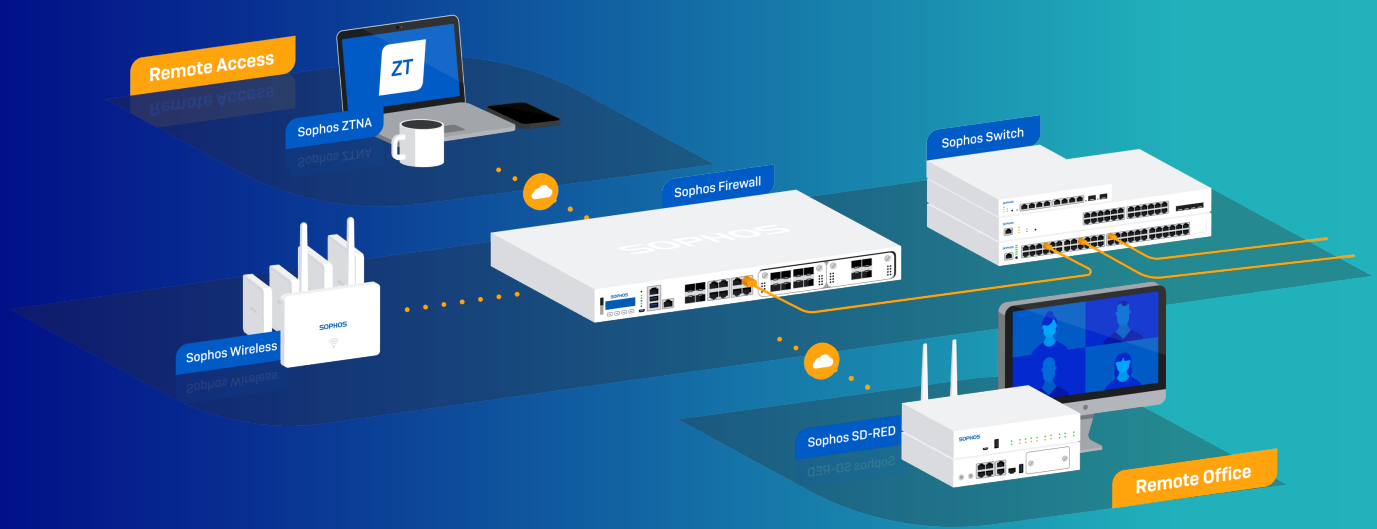
## DETECCIÓN Y RESPUESTA CONTRA AMENAZAS AUTOMATIZADAS

**Provee respuestas automatizadas a amenazas activas**

**Automáticamente identifica y bloquea amenazas activas**

**Previene el movimiento lateral**

**Vista inmediata a dispositivos comprometidos, usuarios y aplicaciones**




Fuente: sophos.com

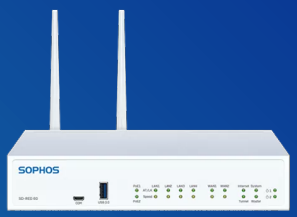
# PRODUCTO

## Sophos Wireless

-Conectividad sincronizada: El acceso para los clientes gestionados es automáticamente controlado basado en el “health status”.
-Descubrimiento de amenazas: Amenazas a tu red WiFi son clasificadas automáticamente, por ejemplo, Rogue APs, intentos de suplantación o dispositivos desconocidos.
- Gestión modular: Con Sophos Central, gestiona Sophos Wireless conjuntamente con tus soluciones de Sophos.

## Sophos SD-RED

- Extender la red a lugares remotos o sucursales con dispositivos perimetrales remotos SD-RED no podría ser más sencillo; de hecho, no requieren intervención, y orquestar su red de superposición SD-WAN desde Sophos Central no es más que una tarea de apuntar y hacer clic.
- Los túneles SD-RED de capa 2 ligeros ofrecen una solución VPN segura y robusta. Funciona de manera fiable en las situaciones de red más hostiles y de alta latencia.




## Sophos Switch

- Sophos Switch provee acceso escalable y seguro para tus dispositivos alámbricos e inalámbricos poniendo tu conectividad LAN bajo tu control.
- Sophos Switch Series ofrece un rango de switches de acceso a la red que conecta y energiza los dispositivos que se conectan a la LAN, mientras se añaden controles de seguridad y segmentación al borde de la red.

## Sophos ZTNA

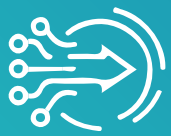
- Micro-segmenta tus aplicaciones: Elimina la confianza implícita y asegura tus aplicaciones estén libres del movimiento lateral.
- Mejora tu postura de seguridad: Reduce notablemente la superficie de ataque, añadiendo el “Check Health” a las políticas de acceso haciendo que tus apps sean invisibles a los ataques.
- Trabajadores remotos: Reemplaza al tradicional SSL VPN con los privilegios necesarios para acceder a tus apliaciones, haciéndolo más fácil y transparente.


## NDR

Detecta los comportamientos sospechosos que se extienden más allá de sus endpoints.

Dispositivos desprotegidos: Identifica dispositivos legítimos que no están protegidos y que podrían utilizarse como puntos de entrada, como recursos de IoT y TO.

NDR forma parte de Sophos MDR, monitoriza el tráfico de la red para identificar flujos de red sospechosos, lo que permite a los analistas de Sophos MDR identificar qué dispositivos pueden estar en peligro durante un incidente de seguridad.



Ataques de día cero: Detecta intentos de comando y control por parte de servidores en función a patrones observados de paquetes de sesiones.

EXXODA
CIBERSECURITY

## ESCRÍBENOS

(+51) 934 298 422 -Asesora de ventas
(+51) 967 762 316 -Soporte Técnico

ventas@exxoda.com

## LLÁMANOS

(01) 7019216

## SÍGUENOS

**EXXODA CIBERSECURITY**

## UBÍCANOS

Av. El Carmen 689 Departamento 202 Urb. San Roque Surco

Fuente de información: sophos.com