SOPHOS

Portafolio Sophos

Edgar Melgarejo
Sr Systems Engineer, México



SOPHOS / Secureworks

¿Qué es Sophos?

Sophos es una plataforma unificada de ciberseguridad en la nube, que combina protección de endpoints, servidores, correo electrónico, firewalls y servicios de nube, todo bajo un solo panel de control (Sophos Central).

Además, con Sophos MDR (Managed Detection and Response), tienes un equipo 24/7 de analistas de seguridad monitoreando y respondiendo incidentes a nombre del cliente.

El resultado para el negocio:
- Menos riesgos
- Menor complejidad operativa
- costo total de propiedad más bajo, sin comprometer la seguridad ni la productividad de tus equipos.



¿Quién es Sophos en la industria?

600,000+
Total customers

25,000+
Active Channel Partners

100+
Strategic Partners
(Technology, services, etc.)

350+
Third-party Integrations

30,000+
Sophos MDR Customers

300,000+
Sophos Endpoint Customers

45,000+
Sophos XDR Customers

300,000+
Sophos Firewall Customers

El mayor proveedor de servicios gestionados de detección y respuesta (MDR)

Líder en el Cuadrante Mágico de Gartner para Protección de Endpoints durante 15 informes consecutivos

El único proveedor nombrado como Elección de los Clientes por Gartner y Líder G2 para EPP, Firewall y MDR

Top performer en MITRE ATT&CK Evals para Enterprise Products y Managed Services

La plataforma nativa de IA más grande de la industria, **compatible** con prácticamente cualquier entorno.

El portafolio más amplio de productos de Ciberseguridad

Sophos Portfolio



Firewall Fw

Wireless Wi

Email Em

Switch Sw

Security Heartbeat™

MDR

Managed **D**etection and **R**esponse
Sophos Managed Risk
Rapid **R**esponse

RR

XDR Endpoint/EDR/XDR

Mob Mobile

XDR Server/EDR/XDR

Enc Cifrado

Ph Phish Threat

ZT ZTNA

NDR Network Detection and Response

Ep Endpoint

- Es la solución de protección de endpoints de Sophos con Deep learning AI, Crypto guard y anti-exploits, diseñada para ir mucho más allá del “antivirus tradicional”. Combina varias capas de seguridad para prevenir, detectar y responder a amenazas avanzadas, todo desde la nube con Sophos Central.

- Ejemplo de valor:

  Una empresa es atacada con un ransomware moderno que aprovecha una vulnerabilidad en un navegador.

  1. Anti-Exploit, bloquea el intento de explotación antes de que el malware se ejecute.
  2. El atacante intenta otra vía: descarga un ejecutable disfrazado de PDF.
     - Deep Learning AI lo detecta como malicioso aun cuando no existe firma en ninguna base de datos.
  3. El ransomware consigue activarse en un endpoint e inicia el cifrado de archivos compartidos.
     CryptoGuard detiene el proceso de cifrado y revierte automáticamente los archivos a su estado original.
  4. Todo el incidente se notifica y gestiona desde Sophos Central, sin que el equipo de TI tenga que correr de escritorio en escritorio.

- Versiones

Advanced	Advanced con XDR	Advanced con MDR Complete
• Deep Learning AI • Anti-Exploit • CryptoGuard (rollback anti-ransomware) • Controles web, apps y periféricos	• Todo lo de **Advanced** • Threat Hunting • Live Response • Análisis forense centralizado • Visibilidad en red, correo y nube	• Todo lo de **Advanced con XDR** • Monitoreo 24/7 por analistas certificados • Respuesta gestionada a incidentes • Investigación de causa raíz y contención total

SOPHOS / Secureworks



Endpoint
Server

- Sophos XDR es la plataforma de detección y respuesta extendida que centraliza la visibilidad de seguridad en endpoints, servidores, red, correo electrónico y nube, todo gestionado desde Sophos Central. Su objetivo es detectar, investigar y responder a amenazas avanzadas de forma más rápida y con mayor contexto que un EDR tradicional.

- Ejemplo de valor:
  Un malware se instala en un endpoint, empieza a comunicarse con un servidor externo y envía correos internos con phishing.
  - EDR lo ve en un solo dispositivo.
  - XDR conecta los puntos: endpoint comprometido + comunicación en firewall + phishing en correo. Resultado: el analista detiene el ataque completo, no solo la infección inicial.



Network
Detection &
Response

- Sophos NDR es una solución de detección y respuesta enfocada en la red. Su propósito es descubrir amenazas invisibles que no dejan huella en los endpoints, detectando patrones anómalos y comportamientos maliciosos en el tráfico.

- Ejemplo de valor:
  Un atacante comprometió un servidor sin agente EDR y comenzó a hacer “lateral movement”
  hacia otros sistemas. Sophos NDR detecta la anomalía en el tráfico, alerta al SOC y permite aislar el incidente antes de que llegue al ransomware.



ZTNA

- Es la solución de acceso remoto seguro bajo el modelo Zero Trust de Sophos. Sustituye o complementa las VPN tradicionales, asegurando que solo usuarios, dispositivos y apps de confianza puedan conectarse a los recursos corporativos.

- Ejemplo de valor:
  Un empleado remoto comprometido con malware se conecta a una VPN tradicional → el atacante gana acceso completo a la red.
  Con Sophos ZTNA, el acceso se deniega porque el endpoint no cumple con la política de seguridad, evitando el desastre.

Mobile

- Es la solución de Gestión Unificada de Endpoints (UEM) de Sophos que permite administrar, proteger y asegurar dispositivos móviles y tradicionales (Android, iOS, Windows, macOS y Chromebooks) desde la nube a través de Sophos Central.
- Ejemplo de valor
  - Un empleado pierde su smartphone corporativo con acceso al correo y documentos de la empresa.
  - Sophos Mobile bloquea y borra remotamente la información sensible.
  - Si el dispositivo era personal, solo elimina los datos corporativos sin tocar los personales.
  - Resultado: se evita fuga de información y se respeta la privacidad del usuario.

Cifrado

- Es la tecnología de cifrado de endpoints y archivos de Sophos que protege la información sensible en laptops, PCs, dispositivos externos y archivos individuales. Aprovecha BitLocker (Windows) y FileVault (macOS), gestionados centralmente desde Sophos Central.
- Ejemplo de valor
  - Un colaborador pierde su laptop con datos sensibles de clientes.
  - Gracias al cifrado de disco con BitLocker gestionado por Sophos ENC, la información permanece inaccesible.
  - El equipo de TI puede probar el estado de cifrado en un reporte para la auditoría.
  - El negocio evita sanciones regulatorias y daños reputacionales.

Phish Threat

- Es la plataforma de simulación de phishing y capacitación en concienciación de seguridad de Sophos. Sirve para medir, entrenar y mejorar el comportamiento de los usuarios frente a correos maliciosos, reduciendo el riesgo humano en los ataques de ingeniería social.
- Ejemplo de valor
  - Un colaborador recibe un correo falso de “actualización de cuenta bancaria”.
  - Con Phish Threat, primero se mide si el usuario cae.
  - Si hace clic, inmediatamente se lo redirige a un curso de 5 minutos sobre cómo detectar fraudes.
  - Resultado: el riesgo de la organización baja y el empleado aprende justo en el momento del error.

Firewall

- Next Generation FW
- WAF, IPS, ATP, Filtrado de Correo, Filtrado Web
- Sandboxing con Inteligencia Artificial
- Seguridad Sincronizada
- XDR Ready
- SD-WAN
- Orquestación
- Consola central, reportes y VPN sin costo extra

Wireless

- Administración desde el FW o la nube
- Portal Cautivo
- Autenticación con redes sociales
- Seguridad Sincronizada

Email

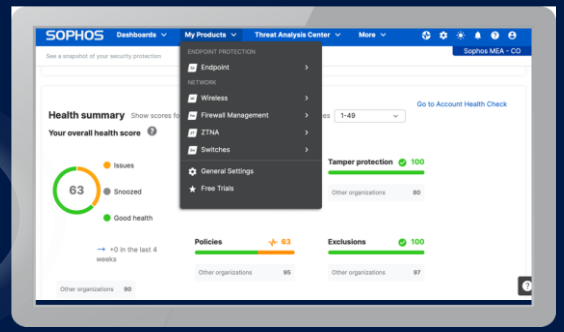
- Antispam, Antiphishing y Antispoofing
- Sandbox con Inteligencia Artificial
- Time to click URL
- DLP
- Cifrado de correo saliente
- Portal Encryption
- XDR Ready

Sophos Network Security

Todo lo que necesitas: gestionado desde una única consola

Sophos Central

- Single cloud management console
- Complex management made easy
- Unmatched dashboarding and reporting



Sophos XGS Series Appliances

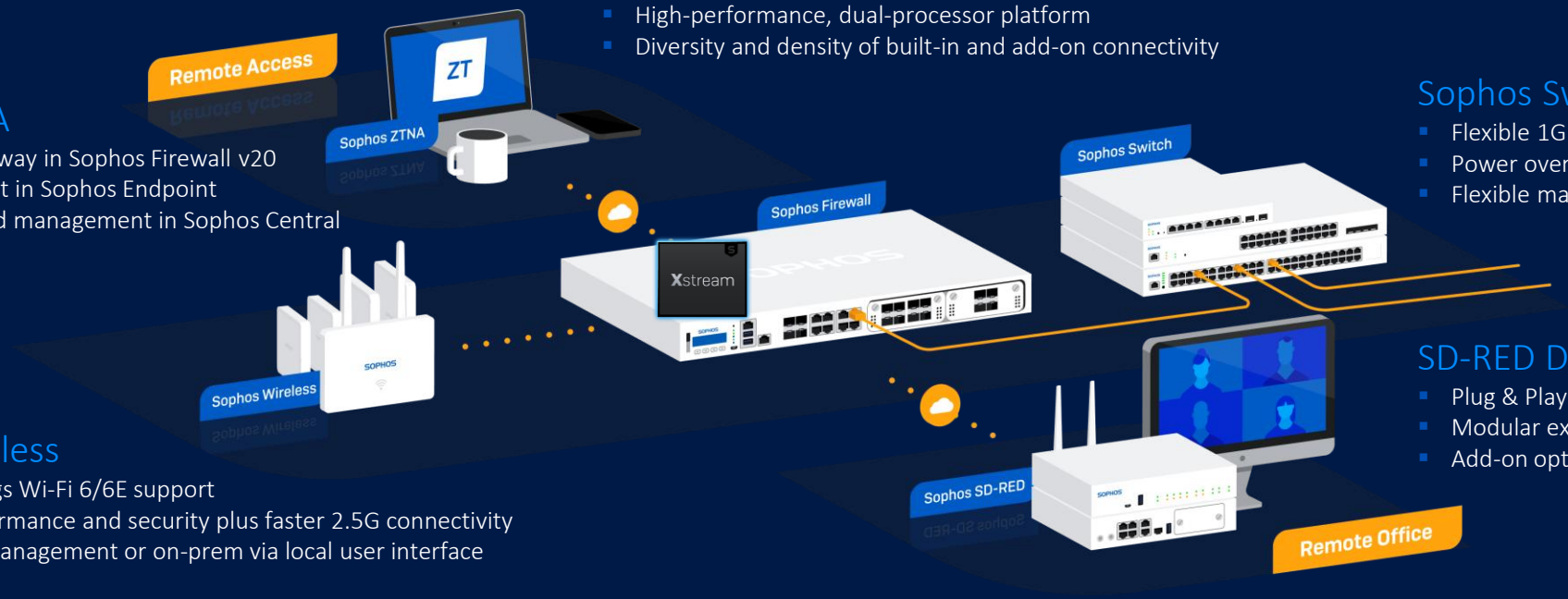
- Future-proof, programmable Xstream architecture
- High-performance, dual-processor platform
- Diversity and density of built-in and add-on connectivity

Sophos ZTNA

- Integrated gateway in Sophos Firewall v20
- Integrated agent in Sophos Endpoint
- Integrated cloud management in Sophos Central

Sophos Switch

- Flexible 1G or 2.5G connectivity to suit any environment
- Power over Ethernet for simple device deployment
- Flexible management – Central, local UI, CLI



SD-RED Devices

- Plug & Play SD-Branch solution
- Modular expansion with flexible connectivity
- Add-on option for Wireless

Sophos Wireless

- AP6 Series brings Wi-Fi 6/6E support
- Improved performance and security plus faster 2.5G connectivity
- Central cloud management or on-prem via local user interface

Sophos DNS Protection

- Included with the Xstream Protection license
- Added layer of AI-powered Web protection
- High performance – enforcement at DNS lookup

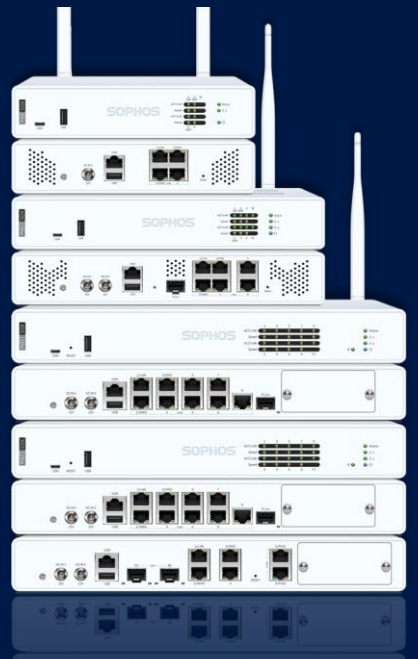
Sophos Messaging Protection

- Industry leading cloud-based email protection
- Block phishing attacks
- Integrated data security

SOPHOS

Sophos Firewall: XGS Series Appliance Portfolio

SMB AND BRANCH OFFICE



DESKTOP (Gen.2)

XGS 88, 88w, 108, 108w

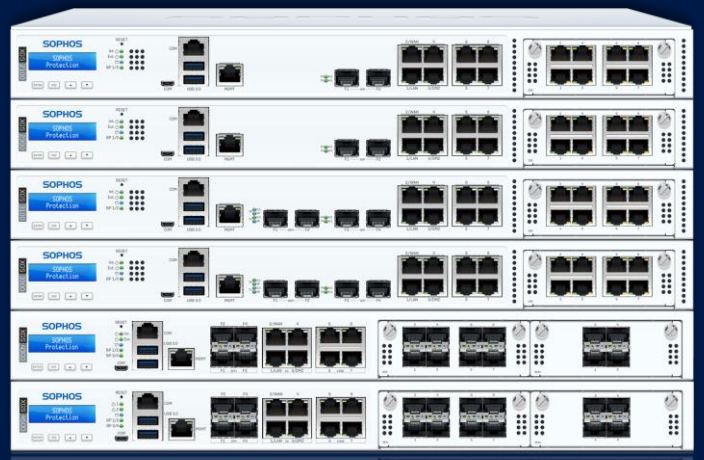
XGS 118, 118w, 128, 128w, 138

DESKTOP (Gen.1)

XGS 87, 87w, 107, 107w

XGS 116, 116w, 126, 126w, 138, 136w

DISTRIBUTED EDGE

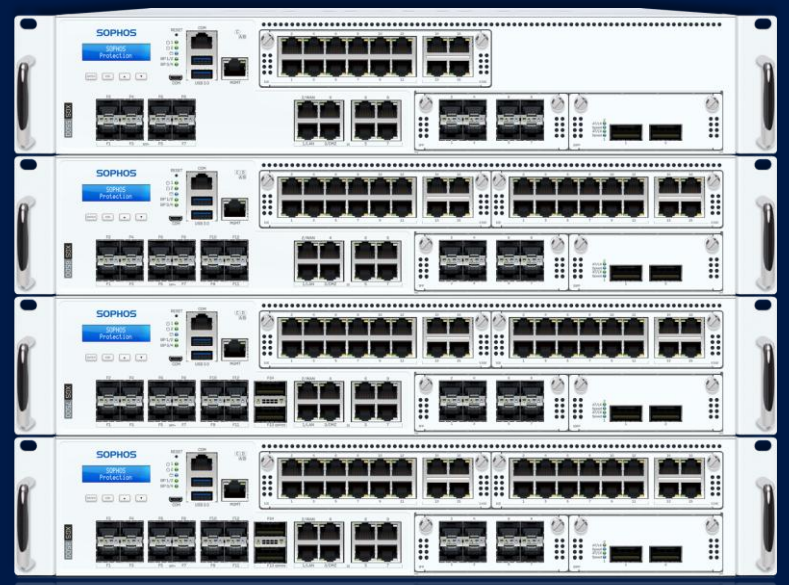


1U RACKMOUNT

XGS 2100, XGS 2300, XGS 3100, XGS 3300

XGS 4300, XGS 4500

ENTERPRISE and CAMPUS EDGE



2U RACKMOUNT

XGS 5500

XGS 6500

XGS 7500

XGS 8500

SOPHOS

DIFERENCIADOR COMPETITIVO



Protección contra amenazas líder para todos los modelos XGS

- Todos los modelos tienen un rendimiento de Protección contra amenazas significativamente mayor
- Hemos cambiado nuestra metodología de prueba para estar a la par con los competidores

Model	Form Factor	Threat Protection (Mbps) OLD	Threat Protection (Mbps) NEW	Increase vs. previously published data
XGS 88(w)	Gen.2 Desktop[2]	n/a	2,000	n/a
XGS 108(w)		n/a	2,500	n/a
XGS 118(w)		n/a	3,250	n/a
XGS 128(w)		n/a	4,000	n/a
XGS 138[1]		n/a	4,750	n/a
XGS 87(w)	Gen.1 Desktop	280	850	3x
XGS 107(w)		370	1,110	3x
XGS 116(w)		720	2,160	3x
XGS 126(w)		900	2,700	3x
XGS 136(w)		1,000	3,000	3x

Model	Form Factor	Threat Protection (Mbps) OLD	Threat Protection (Mbps) NEW	Increase vs. previously published data
XGS 2100	1U	1,250	5,000	4x
XGS 2300		1,500	5,550	3.7x
XGS 3100		2,000	7,400	3.7x
XGS 3300		3,000	10,000	3.3x
XGS 4300		6,500	25,200	3.9x
XGS 4500		8,650	31,850	3.7x
XGS 5500	2U	14,000	46,000	3.3x
XGS 6500		17,850	53,500	3x
XGS 7500		26,000	70,000	2.7x
XGS 8500		34,000	92,500	2.7x

Nueva metodología de Protección contra amenazas:
Medido con firewall, IPS, control de aplicaciones y prevención de malware habilitados mediante el tráfico de Enterprise Mix.

Competitors can no longer attack us on Threat Protection as we now easily beat them using the same test methodology that they use

Watch out for people using the old datasheet numbers to attack us

[1] Currently not available in Japan
[2] All Gen.2 Desktop models include two or more 2.5 GE ports

SOPHOS

SOPHOS

Defeat Cyberattacks