

Sophos protege tus equipos y te avisa. TecnetSOC te entrega el caso resuelto, en tu idioma y con todo incluido.

Con Sophos, el MDR excluye restaurar sistemas, el parcheo queda fuera del alcance y NDR se licencia aparte. En TecnetSOC, el SOC parchea, la detección en tu red va incluida y puedes sumar respaldo inmutable y recuperación ante desastres con TecnetProtect.



31

capacidades donde TecnetSOC va más allá

19

capacidades en las que coincidimos

0

capacidades donde Sophos supera a TecnetSOC

De las 50: 31 donde vamos más allá y 19 en las que coincidimos

Misma lista de 50 capacidades y mismo criterio para TecnetSOC y Sophos: la oferta más completa publicada de cada uno, con la fuente de cada dato. [Cómo lo hicimos](#)

Pedir la prueba de Response por 30 días

o empieza gratis con Visibility, hasta 10 dispositivos

tecnetone.com/servicios/soc-as-a-service

✓ SOC agéntico 24/7 en LATAM, EE.UU. y Europa

✓ Español nativo y atención multidioma

✓ Compuerta Humana en lo crítico

✓ Operación certificada ISO/IEC 27001:2022

✓ Crítico: aviso e inicio de investigación en 30 min (objetivo)

Información pública consultada al 29 de septiembre de 2026. Versión 2026.09. Comparativo informativo elaborado por TecnetOne, no afiliado a las marcas mencionadas.

— ANTES DE COMPARAR

Sophos combina sus productos de protección con su servicio MDR; correo, firewall, red e identidad se licencian por separado. Aquí comparamos su servicio más completo con sus complementos propios, capacidad por capacidad.

— LO QUE NOS HACE DISTINTOS

Diferencias que se notan en el día a día

01

El parcheo queda de tu lado

CON SOPHOS

Managed Risk escanea y prioriza vulnerabilidades, pero el parcheo queda fuera del servicio: tu equipo instala cada parche y responde por el resultado. [1]

CON TECNETSOC

El SOC parchea por explotación real (KEV y EPSS), valida en grupo piloto y da por cerrado solo cuando el escáner confirma.

02

Recuperar tu operación va aparte

CON SOPHOS

La respuesta a incidentes del MDR excluye la restauración o recuperación de sistemas: volver a operar después del ataque queda en tus manos. [2]

CON TECNETSOC

Puedes sumar TecnetProtect (costo aparte): respaldo en bóveda inmutable por cliente y recuperación ante desastres con simulacros.

03

NDR, retención e integraciones, con licencia aparte

CON SOPHOS

El MDR guarda 90 días de datos; un año de retención, NDR e integrar firewall, correo o nube de terceros requieren licencias adicionales. [3]

CON TECNETSOC

La oferta más completa ya incluye SIEM, detección en la red interna (NDR), identidad, nube y correo en un solo servicio.

04

Sesenta días para quedar cubierto

CON SOPHOS

El arranque del MDR es un plan de 60 días en fases: tu equipo instala el agente hasta cubrir el 90% de los equipos. [4]

CON TECNETSOC

Instalas un agente, el resto se despliega solo y, por lo general, ves actividad en 2 a 4 horas; operación completa típicamente en menos de 7 días.

05

Sin línea directa para LATAM

CON SOPHOS

Las líneas telefónicas del MDR cubren EMEA, APAC y Norteamérica; desde LATAM te piden contactar al centro de operaciones más cercano. [5]

CON TECNETSOC

Operamos en LATAM, EE.UU. y Europa, con analistas en tu zona horaria y atención en español nativo.

06

Sin resumen ejecutivo cada mañana

CON SOPHOS

El MDR genera reportes automáticos semanales y mensuales para los administradores de la consola; no documenta un resumen ejecutivo diario ni reportes trimestrales. [6]

CON TECNETSOC

Recibes un resumen ejecutivo cada mañana a las 07:30 y reportes semanales a anuales en PDF, en lenguaje de negocio.

— DÓNDE ESTÁ LA DIFERENCIA

Las tres áreas con más diferencia

Exposición y gestión de TI

TecnetSOC 12

Sophos 2

de 12 capacidades completas en esta área

Operación y servicio

TecnetSOC 14

Sophos 5

de 14 capacidades completas en esta área

Cumplimiento

TecnetSOC 6

Sophos 0

de 6 capacidades completas en esta área (incluye complementos)

— CAPACIDAD POR CAPACIDAD

TecnetSOC y Sophos, lado a lado

Capacidad	TecnetSOC	Sophos EDR y MDR	Evidencia sobre Sophos
✓ Lo ofrece ⊕ Lo ofrece como complemento ✗ No forma parte de su oferta publicada	🕒 Parcial, limitado o requiere otro contrato	❓ Sin evidencia pública	
Operación y servicio	14 de 14	5 completas +7 parciales	
Centro de operaciones (SOC) 24/7 con analistas humanos	✓	✓	Monitoreo, investigación y respuesta 24/7/365 por el equipo MDR Ops [2]
Agentes de IA que investigan y filtran las alertas antes de pasarlas a un analista	✓	✓	Triage Agent y Case Investigation Agent filtran y analizan antes del analista [7]
Compuerta Humana: una persona aprueba cada acción crítica antes de ejecutarse	✓	🕒	Modo Collaborate exige tu consentimiento; en modo Authorize actúa sin consultarte [8]

Capacidad	TecnetSOC	Sophos EDR y MDR	Evidencia sobre Sophos
✓ Lo ofrece + Lo ofrece como complemento ✗ No forma parte de su oferta publicada ◐ Parcial, limitado o requiere otro contrato ? Sin evidencia pública			
Asistente de investigación con IA en el portal, que cita sus fuentes	✓ Neo	◐	AI Assistant investiga en lenguaje natural; no documenta cita de fuentes; solo inglés [9]
Operación en LATAM, EE.UU. y Europa, con analistas en tu zona horaria	✓	◐	Nueve equipos regionales; teléfonos solo EMEA, APAC y Norteamérica, sin LATAM [5]
Analistas, soporte y portal en español nativo	✓	◐	Consola en español; IA solo en inglés; atención de analistas en español sujeta a disponibilidad o mediante traducción de terceros [10]
Reportes para dirección en español y en lenguaje de negocio	✓	?	Informes mensuales técnicos; sin evidencia de reporte ejecutivo en español [11]
Tiempos de notificación e inicio de investigación publicados por severidad	✓ Crítico: 30 min (objetivo)	◐	Publica caso en 2 min, acción en 30 min y SLA 60 min; no por severidad [2]
Resumen ejecutivo cada mañana: lo que pasó en las últimas 24 horas	✓ 07:30	?	Sin evidencia de resumen ejecutivo diario [6]
Reportes automáticos semanales, mensuales, trimestrales y anuales	✓	◐	Reportes automáticos semanales y mensuales; sin trimestrales ni anuales [12]
Gerente técnico de cuenta (TAM) asignado y revisiones trimestrales	✓	✓	TAM nombrado con revisiones trimestrales, complemento pagado sobre Enhanced Plus [13]
Contacto 24/7 con personas de soporte o seguridad	✓	✓	Línea directa 24/7/365 con Sophos para revisar incidentes [2]
Certificación independiente de la operación (ISO 27001 o SOC 2 Tipo II)	✓ ISO/IEC 27001:2022	✓	ISO 27001:2022 y SOC 2 publicados en su Trust Center [14]
Arranque rápido con un agente de software: la actividad de tus dispositivos, visible en horas	✓ Típico: 2 a 4 horas	◐	Onboarding por fases de 60 días; sin compromiso de datos de actividad en horas [4]
Detección y respuesta	15 de 15	12 completas +3 parciales	
Monitoreo continuo y correlación de eventos (SIEM), alineado con MITRE ATT&CK (marco de referencia de técnicas de ataque)	✓	✓	XDR con data lake, correlación, MITRE ATT&CK y Next-Gen SIEM propio [15]
Protección avanzada en cada equipo (EDR/XDR): malware, ransomware y explotación de vulnerabilidades	✓	✓	Sophos Endpoint (Intercept X) con EDR/XDR contra malware, explotación de vulnerabilidades y ransomware [16]
Filtrado web en el equipo	✓	✓	DNS Protection y control web en el equipo contra contenido malicioso [17]
Detección de intrusos (IDS/IPS)	✓	✓	Sophos Firewall propio con inspección profunda y prevención de intrusos [18]
Detección de amenazas en la red interna (NDR)	✓	✓	Sophos NDR propio monitorea tráfico interno, IoT/OT y dispositivos no autorizados [19]
Investigaciones documentadas y enriquecidas con inteligencia de amenazas	✓	✓	Enriquecimiento con Sophos X-Ops; veredicto documentado con IoC y línea de tiempo [7]
Gestión de incidentes con bitácora y tiempo de atención medido por caso	✓	◐	Casos con seguimiento en Fusion; SLA medido mensual, no por caso [2]
Respuesta con aislamiento de equipos y bloqueo de direcciones IP	✓	✓	Aislamiento de equipos, bloqueo de indicadores y Active Threat Response en firewall [2]
Respuesta a incidentes con análisis de causa raíz	✓	✓	MDR Plus: respuesta completa sin tope de horas y análisis de causa raíz [20]
Postura de identidad: MFA, cuentas privilegiadas y acceso condicional	✓	✓	ITDR: más de 160 revisiones de postura en Entra ID y Active Directory [21]
Zero Trust: DNS seguro, acceso a aplicaciones y control de aplicaciones no autorizadas (shadow IT)	✓	✓	Workspace Protection: ZTNA, DNS Protection y control de shadow IT [17]
Seguridad en la nube: alertas y postura	✓	◐	Protección de cargas y alertas cloud; CSPM Cloud Optix en fin de vida 30 sep 2026 [22]
Seguridad de correo: spam, phishing, malware y fraude por suplantación (BEC)	✓	✓	Sophos Email: spam, phishing, malware, BEC y suplantación, integrado con MDR [23]

Capacidad	TecnetSOC	Sophos EDR y MDR	Evidencia sobre Sophos
Lo ofrece Lo ofrece como complemento Parcial, limitado o requiere otro contrato Sin evidencia pública No forma parte de su oferta publicada			
Concientización: simulaciones de phishing y entrenamiento con métricas			Phish Threat: simulaciones, más de 30 módulos de entrenamiento, nueve idiomas [24]
Recomendaciones de seguridad priorizadas con flujo de aprobación			Account Health Check prioriza y corrige tras confirmar; solo configuración de Sophos [25]
Exposición y gestión de TI	12 de 12	2 completas +5 parciales	
Inventario unificado de activos y de software			Managed Risk descubre activos; inventario de software solo por consultas XDR [26]
Vulnerabilidades priorizadas por gravedad y probabilidad de explotación (CVSS, EPSS)			Prioriza con VPR de Tenable; CVSS y EPSS no explícitos [26]
Prioridad a las fallas que ya se están explotando (catálogo KEV de CISA)			Escanea cuando aparecen nuevas vulnerabilidades explotadas; uso del catálogo KEV no documentado [27]
Parcheo de sistema operativo y aplicaciones de terceros			Sin parcheo propio; Managed Risk deja la remediación al cliente [1]
Parcheo operado por el proveedor, con plazos publicados por severidad	 Críticos: 48 h (objetivo)		Parcheo y remediación fuera del alcance del servicio [1]
Verificación de cierre: el escáner confirma que la vulnerabilidad desapareció			Escaneos semanales reflejan cierre; sin verificación formal de remediación [1]
Validación de parches en grupo piloto antes del despliegue			Sin evidencia de grupo piloto para parches [1]
Superficie de ataque externa: lo que tu empresa expone en Internet, con puntaje de riesgo	 Puntaje 0 a 100		Managed Risk: inventario semanal de activos externos y priorización de riesgo [1]
Alertas de dominios que imitan tu marca y de credenciales o claves expuestas			ITDR busca credenciales filtradas en dark web; sin alertas de dominios similares [21]
Prueba de penetración (pentest) anual	 Anual		Advisory Services: pentest externo, interno, inalámbrico y de aplicaciones web [28]
Gestión remota de equipos (RMM)			Sin RMM en el portafolio de Sophos Fusion [15]
Monitoreo de disponibilidad (NOC)			Sin evidencia de monitoreo de disponibilidad (NOC) [15]
Respaldo y continuidad	3 de 3	0 completas +0 parciales	
Respaldo de servidores, archivos, bases de datos, máquinas virtuales y Microsoft 365	 Complemento		Sin producto de respaldo en el portafolio de Sophos Fusion [15]
Bóveda de respaldo inmutable (no se puede alterar ni borrar), aislada por cliente	 Complemento		Sin evidencia de bóveda de respaldo [15]
Recuperación ante desastres con simulacros y tiempo de recuperación (RTO) medido	 Complemento RTO medido		La respuesta a incidentes excluye restauración o recuperación de sistemas [2]
Cumplimiento	6 de 6	0 completas +3 parciales	
Evidencia mensual lista para auditores y aseguradoras	 Mensual		CISO Advantage guarda evidencia para auditoría y seguros; despliegue por regiones [29]
Preparación para ISO 27001, SOC 2 y PCI DSS con controles compartidos	 Complemento		CISO Advantage mapea a NIST y CIS; ISO 27001, SOC 2 y PCI no documentados [29]
Preparación normativa mexicana: CNBV Fintech, protección de datos (LFPDPPP) y NOM-024	 Complemento		Sin evidencia de normativa mexicana [29]

Capacidad	TecnetSOC	Sophos EDR y MDR	Evidencia sobre Sophos
✓ Lo ofrece + Lo ofrece como complemento ✗ No forma parte de su oferta publicada	🕒 Parcial, limitado o requiere otro contrato	? Sin evidencia pública	
Gestión de riesgos, controles, declaración de aplicabilidad y auditorías internas	+ Complemento	🕒	CISO Advantage: evaluación de riesgo y hoja de ruta; sin SoA ni auditoría interna [29]
Portal para tu auditor con sala de evidencias y página pública de confianza (trust center)	+ Complemento	?	Sin evidencia de portal para auditor ni página de confianza para el cliente [29]
Continuidad de negocio, riesgo de proveedores y gestión de brechas de datos	+ Complemento	?	Sin evidencia de continuidad, riesgo de proveedores ni gestión de brechas [29]
Cómo se contrata	No suma al conteo		
Precio por dispositivo, con planes que se suman	✓ Por dispositivo	🕒	Precio por usuario y por servidor; dos niveles de MDR más complementos [16]
Plan gratuito para empezar	✓ Hasta 10 dispositivos	?	Sin plan gratuito empresarial; solo herramientas gratis y pruebas [30]
Prueba gratuita en tu entorno real	✓ 30 días	🕒	Pruebas gratis de XDR, Email, Firewall y más; sin prueba del servicio MDR [31]
Disponible con la marca de tu proveedor de TI	✓	🕒	Co-branding con logo del partner en portal y reportes; servicio con marca Sophos [32]
Cobertura completa	50	19 +18 parciales	

— SIGUIENTE PASO

Compruébalo en tu operación

Pruébalo en un entorno real, sin cambiar lo que ya te funciona.
El primer SOC agéntico en español: plataforma, analistas y soporte.

Pedir la prueba de Response por 30 días

Empezar gratis con Visibility (hasta 10 dispositivos)

[O habla con un especialista](#)

tecnetone.com/servicios/soc-as-a-service

ASÍ FUNCIONA LA PRUEBA DE RESPONSE

- 1

Instalas un solo agente
- 2

Recibes el resumen ejecutivo cada mañana
- 3

Decides con datos de tu entorno

Metodología y fuentes

Quién y con qué

Lo preparamos en TecnetOne y te mostramos la fuente de cada dato. La lista de capacidades parte del catálogo de TecnetSOC. Evaluamos la oferta más completa publicada de cada proveedor, con sus complementos propios, y la nuestra con el mismo rigor. Usamos solo información pública (sitios oficiales, documentación y comunicados) consultada al 29 de septiembre de 2026.

Qué significa cada estado

Lo ofrece: el proveedor lo entrega, lo opera y responde por ello dentro de su servicio, venga de donde venga la tecnología. Complemento: disponible con costo aparte. Parcial: alcance limitado o que requiere otro contrato u otro operador. Sin evidencia pública: no hay información pública que lo confirme al momento de la consulta; no significa que el proveedor no lo ofrezca. No forma parte de su oferta publicada: su documentación indica que no lo incluye. Lo pone tu equipo: en una herramienta, esa capacidad depende de tu personal, tus turnos y tus tiempos de respuesta, no del proveedor. Si dudamos entre dos valores, elegimos el más conservador.

Cómo corregimos

Un proveedor puede ofrecer algo que no publica: confírmalo directamente con él. Si ves un dato desactualizado o incorrecto, escríbenos por nuestro formulario de contacto y lo corregimos en la siguiente versión. Revisamos este comparativo cada trimestre y cada vez que cambia la oferta publicada de un proveedor o nuestro catálogo.

Evaluado en Sophos: Sophos MDR, oferta más completa (Sophos MDR Plus, antes MDR Complete, con Sophos XDR y SOC 24/7, más complementos propios: NDR, ITDR, Email, Phish Threat, Firewall, Workspace Protection con ZTNA y DNS Protection, Managed Risk con Tenable, Advisory Services, TAM y CISO Advantage, todo en la consola Sophos Fusion, antes Sophos Central), consulta 29 sep 2026

Evaluado en TecnetSOC: TecnetSOC en su oferta más completa (plan Compliance, con complementos TecnetProtect y TecnetGRC), catálogo de plataforma soc.catalogo.tecnetone.com y tecnetone.com/servicios/soc-as-a-service, consulta 29 sep 2026. Mismo estándar que los demás. Los complementos con costo aparte cuentan como parte de la oferta, igual que los complementos propios de los demás proveedores.

- www.sophos.com/en-us/legal/managed-risk-description (Diferencias que se notan en el día a día)
- www.sophos.com/en-us/legal/mdr-description (Diferencias que se notan en el día a día)
- docs.sophos.com/central/customer/help/en-us/ManageYourProducts/MDR/... (Diferencias que se notan en el día a día)
- docs.sophos.com/central/customer/help/en-us/GettingStarted/onboardi... (Diferencias que se notan en el día a día)
- docs.sophos.com/central/customer/help/en-us/ManageYourProducts/MDR/... (Diferencias que se notan en el día a día)
- docs.sophos.com/central/customer/help/en-us/ManageYourProducts/MDR/... (Diferencias que se notan en el día a día)
- www.sophos.com/en-us/blog/sophos-ai-agents-accelerating-mdr-and-pow... (Agentes de IA que investigan y filtran las alertas...)
- docs.sophos.com/central/customer/help/en-us/ManageYourProducts/MDR/... (Computura Humana: una persona aprueba cada acción...)
- docs.sophos.com/central/customer/help/en-us/AI/AIfeatures/index.html (Asistente de investigación con IA en el portal, que...)
- docs.sophos.com/central/customer/help/en-us/ManageYourAccount/Langu... (Analistas, soporte y portal en español nativo)
- docs.sophos.com/central/customer/help/en-us/ManageYourProducts/MDR/... (Reportes para dirección en español y en lenguaje de...)
- docs.sophos.com/central/enterprise/help/en-us/MDR/MDRreporthisory/... (Reportes automáticos semanales, mensuales, trimestrales...)
- docs.sophos.com/support/help/en-us/services-guide/tam/ (Gerente técnico de cuenta (TAM) asignado y revisiones...)
- www.sophos.com/en-us/trust/business-certifications (Certificación independiente de la operación (ISO 27001...))
- www.sophos.com/en-us/press/press-releases/2026/07/sophos-fusion-ai-... (Monitoreo continuo y correlación de eventos (SIEM),...)
- www.sophos.com/en-us/products/endpoint-security/how-to-buy (Protección avanzada en cada equipo (EDR/XDR): malware,...)
- www.sophos.com/en-us/products/workspace-protection (Filtrado web en el equipo)
- www.sophos.com/en-us/products/next-gen-firewall (Detección de intrusos (IDS/IPS))
- www.sophos.com/en-us/products/network-detection-and-response (Detección de amenazas en la red interna (NDR))
- www.sophos.com/en-us/services/managed-detection-and-response (Respuesta a incidentes con análisis de causa raíz)
- www.sophos.com/en-us/products/identity-threat-detection-and-response (Postura de identidad: MFA, cuentas privilegiadas y...)
- community.sophos.com/sophos-cloud-optix/b/blog/posts/sophos-cloud-o-... (Seguridad en la nube: alertas y postura)
- www.sophos.com/en-us/products/sophos-email (Seguridad de correo: spam, phishing, malware y fraude...)
- www.sophos.com/en-us/products/phish-threat (Concientización: simulaciones de phishing y...)
- docs.sophos.com/central/customer/help/en-us/ManageYourProducts/Acco... (Recomendaciones de seguridad priorizadas con flujo de...)
- www.sophos.com/en-us/products/managed-risk (Inventario unificado de activos y de software)
- www.sophos.com/en-us/services/managed-risk (Prioridad a las fallas que ya se están explotando...)
- www.sophos.com/en-us/products/advisory-services/security-testing (Prueba de penetración (pentest) anual)
- www.sophos.com/en-us/products/ciso-advantage (Evidencia mensual lista para auditores y aseguradoras)
- www.sophos.com/en-us/free-tools (Plan gratuito para empezar)
- www.sophos.com/en-us/free-trials (Prueba gratuita en tu entorno real)
- docs.sophos.com/central/partner/help/en-us/Help/GlobalSettings/Plat... (Disponible con la marca de tu proveedor de TI)

Fuentes y fecha. Este comparativo es informativo y lo elabora TecnetOne para que compares, capacidad por capacidad, qué incluye TecnetSOC frente a la oferta más completa publicada de cada proveedor mencionado. La lista de capacidades es un catálogo propio de TecnetOne y puede no incluir todas las funciones de cada proveedor. Usamos solo información pública (sitios oficiales, documentación técnica y comunicados) consultada al 29 de septiembre de 2026; versión 2026.09, con revisión trimestral. "Sin evidencia pública" significa que no hay información pública que lo confirme al momento de la

consulta, no que el proveedor no pueda ofrecerlo de otra forma: confirma cada detalle directamente con él. Las fuentes de cada dato están en el comparativo individual de cada proveedor, enlazado al pie de la tabla.

Marcas. Los nombres y las marcas de terceros pertenecen a sus respectivos dueños y se usan solo para identificarlos y comparar de forma informativa. Ninguno de esos proveedores está afiliado a TecnetOne ni patrocina o avala este documento.

Alcance de TecnetSOC. El respaldo y la plataforma de cumplimiento (TecnetGRC) son complementos con costo aparte. Nuestros tiempos son objetivos de servicio de notificación e inicio de investigación, no de resolución (crítico: 30 minutos, como objetivo). El parcheo está sujeto a las ventanas de mantenimiento acordadas contigo y a las aplicaciones incluidas en tu perfil. El cumplimiento se entrega como preparación y evidencia, no como certificación. TecnetSOC es un servicio de TecnetOne, con operación certificada ISO/IEC 27001:2022, disponible de forma directa o a través de tu proveedor de TI.



Un SOC que habla tu idioma.

¿Ves un dato desactualizado o inexacto? Escríbenos y lo corregimos.