

SentinelOne frena y revierte ataques en el equipo; su vigilancia 24/7 se contrata aparte. TecnetSOC opera tu seguridad, con el caso resuelto en tu idioma.

Con SentinelOne, el correo, el parcheo automático y la detección en tu red vienen de otros fabricantes, y no hay respaldo propio. En TecnetSOC, el SOC parchea, la protección de correo va incluida y puedes sumar respaldo inmutable con TecnetProtect.



33

capacidades donde TecnetSOC va más allá

17

capacidades en las que coincidimos

0

capacidades donde SentinelOne supera a TecnetSOC

De las 50: 33 donde vamos más allá y 17 en las que coincidimos

Misma lista de 50 capacidades y mismo criterio para TecnetSOC y SentinelOne: 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 multiidioma

✓ Compuerta Humana en lo crítico

✓ Operación certificada ISO/IEC 27001:2022

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

— ANTES DE COMPARAR

SentinelOne es una plataforma de protección de equipos (EDR/XDR) que se compra por paquetes y módulos; con Wayfinder MDR, su servicio administrado con costo aparte, sus analistas vigilan y responden 24/7. Correo, parcheo automático y detección en la red vienen de otros fabricantes integrados a Singularity. Aquí comparamos la plataforma, Wayfinder MDR y sus módulos propios con lo que incluye TecnetSOC, capacidad por capacidad.

Diferencias que se notan en el día a día

01
El parche lo instala otra herramienta

CON SENTINELONE
Vulnerability Management escanea y prioriza, pero no publica parcheo propio: su marketplace ofrece parcheo automático de otros fabricantes, como Adaptiva. [\[1\]](#)

CON TECNETSOC
El SOC parchea por explotación real (KEV y EPSS), con plazos objetivo por severidad, válida en grupo piloto y da por cerrado solo cuando el escáner confirma.

02
Tu correo lo protege otro fabricante

CON SENTINELONE
No hay seguridad de correo propia: su XDR recibe las señales de productos de correo de otros fabricantes, como Proofpoint, para responder en el equipo. [\[2\]](#)

CON TECNETSOC
La protección contra spam, phishing, malware y suplantación (BEC) va dentro del mismo servicio, con cuarentena en autoservicio.

03
La reversión no sustituye al respaldo

CON SENTINELONE
La reversión (rollback) deshace en el equipo los cambios de un ataque, pero su portafolio publicado no incluye respaldo de servidores, bóveda inmutable ni recuperación ante desastres. [\[3\]](#)

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

04
Amenazas en tu red, con sensores de otro fabricante

CON SENTINELONE
La detección de amenazas en tu red interna (NDR) y de intrusos llega integrando a su XDR productos de otros fabricantes, como Vectra o ExtraHop. [\[4\]](#)

CON TECNETSOC
La detección en la red interna (NDR) y el IDS/IPS van incluidos en la oferta más completa, con un sensor en puerto espejo.

05
Cumplimiento: sus certificados, no tus auditorías

CON SENTINELONE
Su página de cumplimiento muestra las certificaciones de su propia plataforma y un documento de un tercero sobre cómo apoya PCI DSS; no publica herramientas para preparar tus auditorías. [\[5\]](#)

CON TECNETSOC
Recibes evidencia mensual para auditores y aseguradoras y, con TecnetGRC (costo aparte), preparas ISO 27001, SOC 2, PCI DSS y normativa mexicana.

06
Tu personal, sin simulacros de phishing

CON SENTINELONE
Sus paquetes publicados no incluyen simulaciones de phishing ni entrenamiento de concientización para tu personal. [\[6\]](#)

CON TECNETSOC
La oferta más completa incluye simulaciones de phishing y entrenamiento con métricas por usuario, junto con la protección de correo.

Las tres áreas con más diferencia

Exposición y gestión de TI

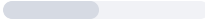
TecnetSOC  **12**

SentinelOne  **3**

de 12 capacidades completas en esta área

Detección y respuesta

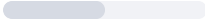
TecnetSOC  **15**

SentinelOne  **7**

de 15 capacidades completas en esta área

Operación y servicio

TecnetSOC  **14**

SentinelOne  **7**

de 14 capacidades completas en esta área

TecnetSOC y SentinelOne, lado a lado

Capacidad	TecnetSOC	SentinelOne EDR/XDR y MDR	Evidencia sobre SentinelOne
 Lo ofrece  Lo ofrece como complemento  Parcial, limitado o requiere otro contrato  Sin evidencia pública  No forma parte de su oferta publicada			
Operación y servicio	14 de 14	7 completas  +5 parciales	
Centro de operaciones (SOC) 24/7 con analistas humanos			Wayfinder MDR: analistas certificados monitorean, investigan y contienen amenazas 24/7/365 [7]
Agentes de IA que investigan y filtran las alertas antes de pasarlas a un analista			Purple AI enriquece el contexto de cada alerta; analistas certificados confirman la severidad y filtran falsos positivos [7]

Capacidad	TecnetSOC	SentinelOne EDR/XDR y MDR	Evidencia sobre SentinelOne
Lo ofrece Lo ofrece como complemento Parcial, limitado o requiere otro contrato Sin evidencia pública No forma parte de su oferta publicada			
Compuerta Humana: una persona aprueba cada acción crítica antes de ejecutarse			Contiene amenazas según la política de respuesta que configuras; aprobación caso por caso no documentada [7]
Asistente de investigación con IA en el portal, que cita sus fuentes	 Neo		Purple AI investiga en lenguaje natural y explica cada veredicto con una justificación [8]
Operación en LATAM, EE.UU. y Europa, con analistas en tu zona horaria			Expertos en 16 países con operación 24/7; no publica ubicaciones ni operación en LATAM [9]
Analistas, soporte y portal en español nativo			Sitio en español y línea de soporte en México; idioma de analistas y de la consola no publicado [10]
Reportes para dirección en español y en lenguaje de negocio			MDR Elite asigna un asesor de amenazas con revisiones operativas; reportes ejecutivos en español no documentados [9]
Tiempos de notificación e inicio de investigación publicados por severidad	 Crítico: 30 min (objetivo)		Sin tiempos por severidad; publica un tiempo medio de detección de 3.3 minutos [7]
Resumen ejecutivo cada mañana: lo que pasó en las últimas 24 horas	 07:30		Sin evidencia de resumen ejecutivo diario [7]
Reportes automáticos semanales, mensuales, trimestrales y anuales			Revisiones de salud trimestrales con el TAM; sin reportes automáticos semanales a anuales documentados [11]
Gerente técnico de cuenta (TAM) asignado y revisiones trimestrales			Gerente técnico de cuenta (TAM, costo aparte) con revisiones de salud trimestrales [11]
Contacto 24/7 con personas de soporte o seguridad			Acceso 24/7/365 a especialistas en respuesta a incidentes y línea telefónica para brechas [12]
Certificación independiente de la operación (ISO 27001 o SOC 2 Tipo II)	 ISO/IEC 27001:2022		ISO/IEC 27001:2022 y examen SOC 2 Tipo 2 de su plataforma [5]
Arranque rápido con un agente de software: la actividad de tus dispositivos, visible en horas	 Típico: 2 a 4 horas		Un solo agente ligero con despliegue automatizado para equipo, identidad y nube [3]
Detección y respuesta	15 de 15	7 completas +6 parciales	
Monitoreo continuo y correlación de eventos (SIEM), alineado con MITRE ATT&CK (marco de referencia de técnicas de ataque)			XDR correlaciona datos de actividad de equipos, nube e identidad; búsqueda de amenazas con técnicas de MITRE ATT&CK [3]
Protección avanzada en cada equipo (EDR/XDR): malware, ransomware y explotación de vulnerabilidades			Contención autónoma de ransomware, ataques de día cero y malware sin archivos en cada equipo [13]
Filtrado web en el equipo			Control de firewall y de dispositivos USB en el equipo; filtrado web por categorías no documentado [14]
Detección de intrusos (IDS/IPS)			Sin IDS/IPS propio; integra en su XDR firewalls y sensores de red de otros fabricantes [4]
Detección de amenazas en la red interna (NDR)			Detección de amenazas en la red con NDR de otros fabricantes (Vectra, ExtraHop) integrados a su XDR [4]
Investigaciones documentadas y enriquecidas con inteligencia de amenazas			Investigaciones enriquecidas con inteligencia de amenazas: indicadores, atribución de actores y campañas [7]
Gestión de incidentes con bitácora y tiempo de atención medido por caso			Purple AI documenta cada investigación en cuadernos; tiempo de atención por caso no publicado [8]
Respuesta con aislamiento de equipos y bloqueo de direcciones IP			Aísla equipos, detiene procesos, revierte cambios y bloquea tráfico de red entrante y saliente [3]
Respuesta a incidentes con análisis de causa raíz			Especialistas en forense (DFIR) contienen, investigan y analizan la causa raíz; las horas vienen con retainer [12]
Postura de identidad: MFA, cuentas privilegiadas y acceso condicional			Singularity Identity: Active Directory, Entra ID y Okta, acceso condicional y nueva autenticación MFA por política [15]

Capacidad	TecnetSOC	SentinelOne EDR/XDR y MDR	Evidencia sobre SentinelOne
Lo ofrece Lo ofrece como complemento No forma parte de su oferta publicada	Parcial, limitado o requiere otro contrato	Sin evidencia pública	
Zero Trust: DNS seguro, acceso a aplicaciones y control de aplicaciones no autorizadas (shadow IT)			Prompt Security controla herramientas de IA no autorizadas (shadow AI); sin DNS seguro documentado [16]
Seguridad en la nube: alertas y postura			Singularity Cloud: postura, protección de cargas en ejecución y datos en tu nube [17]
Seguridad de correo: spam, phishing, malware y fraude por suplantación (BEC)			Sin seguridad de correo propia; su XDR recibe datos de Proofpoint para responder en el equipo [2]
Concientización: simulaciones de phishing y entrenamiento con métricas			Sin simulaciones de phishing ni entrenamiento de usuarios en sus paquetes publicados [6]
Recomendaciones de seguridad priorizadas con flujo de aprobación			Hyperautomation ejecuta respuestas con aprobación humana cuando se requiere; recomendaciones priorizadas con aprobación no documentadas [18]
Exposición y gestión de TI	12 de 12	3 completas	
Inventario unificado de activos y de software			Descubre equipos administrados y no administrados (IoT, personales) y evalúa aplicaciones y sistema operativo [19]
Vulnerabilidades priorizadas por gravedad y probabilidad de explotación (CVSS, EPSS)			Prioriza con EPSS, catálogo KEV de CISA y su puntaje de riesgo, no solo con CVSS [19]
Prioridad a las fallas que ya se están explotando (catálogo KEV de CISA)			Usa las señales del catálogo KEV de CISA para priorizar lo que ya se explota [19]
Parcheo de sistema operativo y aplicaciones de terceros			Sin parcheo propio publicado; su marketplace ofrece parcheo automático de otros fabricantes, como Adaptiva [1]
Parcheo operado por el proveedor, con plazos publicados por severidad	Críticos: 48 h (objetivo)		Sin evidencia de que SentinelOne instale los parches ni de plazos por severidad [19]
Verificación de cierre: el escáner confirma que la vulnerabilidad desapareció			Escaneos programados y bajo demanda reflejan el estado; verificación formal de cierre no documentada [19]
Validación de parches en grupo piloto antes del despliegue			Sin evidencia de validación de parches en grupo piloto [19]
Superficie de ataque externa: lo que tu empresa expone en Internet, con puntaje de riesgo	Puntaje 0 a 100		Valida qué exposiciones de tu nube son explotables; sin monitoreo documentado de lo que expones en Internet [20]
Alertas de dominios que imitan tu marca y de credenciales o claves expuestas			Detecta credenciales robadas expuestas en la web oscura; alertas de dominios que imitan tu marca no documentadas [15]
Prueba de penetración (pentest) anual	Anual		Ejercicios de purple team y evaluaciones de compromiso; pentest no publicado como servicio propio [12]
Gestión remota de equipos (RMM)			RemoteOps ejecuta scripts e instala, actualiza o elimina software en equipos; no se presenta como RMM [21]
Monitoreo de disponibilidad (NOC)			Sin evidencia de monitoreo de disponibilidad (NOC) [13]
Respaldo y continuidad	3 de 3	0 completas	
Respaldo de servidores, archivos, bases de datos, máquinas virtuales y Microsoft 365	Complemento		Sin respaldo propio; la reversión (rollback) deshace en el equipo los cambios de un ataque, no es respaldo [3]
Bóveda de respaldo inmutable (no se puede alterar ni borrar), aislada por cliente	Complemento		Sin bóveda de respaldo propia [13]
Recuperación ante desastres con simulacros y tiempo de recuperación (RTO) medido	Complemento RTO medido		Sin recuperación ante desastres ni simulacros en su portafolio publicado [13]

Capacidad	TecnetSOC	SentinelOne EDR/XDR y MDR	Evidencia sobre SentinelOne
✓ Lo ofrece + Lo ofrece como complemento ✗ No forma parte de su oferta publicada	● Parcial, limitado o requiere otro contrato	? Sin evidencia pública	
Cumplimiento	6 de 6	0 completas	+1 parcial
Evidencia mensual lista para auditores y aseguradoras	✓ Mensual	?	Sin evidencia mensual documentada para tus auditores; comparte el SOC 2 de su propia plataforma [5]
Preparación para ISO 27001, SOC 2 y PCI DSS con controles compartidos	+ Complemento	●	Un documento de un tercero explica cómo apoya PCI DSS; preparación ISO 27001 o SOC 2 no documentada [5]
Preparación normativa mexicana: CNBV Fintech, protección de datos (LFPDPPP) y NOM-024	+ Complemento	?	Sin evidencia de normativa mexicana [5]
Gestión de riesgos, controles, declaración de aplicabilidad y auditorías internas	+ Complemento	?	Sin gestión de riesgos, controles ni auditorías internas para tu empresa [5]
Portal para tu auditor con sala de evidencias y página pública de confianza (trust center)	+ Complemento	?	Su centro de confianza es el de SentinelOne; sin portal para tu auditor ni página de confianza tuya [5]
Continuidad de negocio, riesgo de proveedores y gestión de brechas de datos	+ Complemento	?	Sin evidencia de continuidad de negocio, riesgo de proveedores ni gestión de brechas [5]
Cómo se contrata	No suma al conteo		
Precio por dispositivo, con planes que se suman	✓ Por dispositivo	✓	Paquetes anuales por equipo (Complete, Commercial); Enterprise y MDR por cotización [6]
Plan gratuito para empezar	✓ Hasta 10 dispositivos	?	Sin plan gratuito publicado [6]
Prueba gratuita en tu entorno real	✓ 30 días	●	Prueba gratis de 30 días de Singularity Control anunciada en 2024 para pymes; sin prueba publicada del MDR [22]
Disponible con la marca de tu proveedor de TI	✓	●	Programa para proveedor de seguridad administrada con plataforma multiempresa; marca blanca o compartida no documentada [23]
Cobertura completa	50	17	+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 SentinelOne: SentinelOne, oferta más completa publicada para empresa mediana (plataforma Singularity en su paquete Enterprise más Wayfinder MDR Elite, servicio 24/7 operado por SentinelOne que sucede a Vigilance Respond Pro y WatchTower, con asesor de amenazas dedicado, retainer de respuesta a incidentes y acceso a forense; más sus módulos propios de costo aparte: Purple AI, Singularity AI SIEM, Singularity Identity, Singularity Cloud Security, Singularity Vulnerability Management y Network Discovery, Hyperautomation, RemoteOps, Singularity Mobile, Prompt Security, Wayfinder Threat Hunting y soporte con TAM), consulta 13 oct 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.

1. www.sentinelone.com/partners/singularity-marketplace/ (Diferencias que se notan en el día a día)
2. www.sentinelone.com/press/sentinelone-integrates-with-proofpoint-fo... (Diferencias que se notan en el día a día)
3. www.sentinelone.com/platform/singularity-complete/ (Diferencias que se notan en el día a día)
4. www.sentinelone.com/press/sentinelone-expands-firewall-and-ndr-capability/ (Diferencias que se notan en el día a día)
5. www.sentinelone.com/security-compliance/ (Diferencias que se notan en el día a día)
6. www.sentinelone.com/pricing/ (Diferencias que se notan en el día a día)
7. www.sentinelone.com/global-services/managed-detection-and-response/ (Centro de operaciones (SOC) 24/7 con analistas humanos)
8. www.sentinelone.com/platform/purple/ (Asistente de investigación con IA en el portal, que...)
9. www.sentinelone.com/blog/managed-defense-reimagined-introducing-way... (Operación en LATAM, EE.UU. y Europa, con analistas en...)
10. www.sentinelone.com/global-services/get-support-now/ (Analistas, soporte y portal en español nativo)
11. www.sentinelone.com/global-services/technical-account-management/ (Reportes automáticos semanales, mensuales, trimestrales...)
12. www.sentinelone.com/global-services/incident-readiness-and-response/ (Contacto 24/7 con personas de soporte o seguridad)
13. www.sentinelone.com/platform/ (Protección avanzada en cada equipo (EDR/XDR): malware,...)
14. www.sentinelone.com/platform/singularity-control/ (Filtrado web en el equipo)
15. www.sentinelone.com/platform/identity/ (Postura de identidad: MFA, cuentas privilegiadas y...)
16. www.sentinelone.com/platform/securing-ai-prompt/ (Zero Trust: DNS seguro, acceso a aplicaciones y control...)
17. www.sentinelone.com/platform/cloud-security/ (Seguridad en la nube: alertas y postura)
18. www.sentinelone.com/platform/singularity-hyperautomation/ (Recomendaciones de seguridad priorizadas con flujo de...)
19. www.sentinelone.com/platform/singularity-vulnerability-management/ (Inventario unificado de activos y de software)
20. www.sentinelone.com/platform/singularity-cloud-native-security/ (Superficie de ataque externa: lo que tu empresa expone...)
21. www.sentinelone.com/press/sentinelone-remote-script-orchestration-r... (Gestión remota de equipos (RMM))
22. www.sentinelone.com/press/sentinelone-delivers-leading-cyber-threat... (Prueba gratuita en tu entorno real)
23. www.sentinelone.com/partners/mssp-partners/ (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.