

eSentire te da un SOC. TecnetSOC te da el caso resuelto: la IA investiga, una persona decide y tu equipo no tiene que operarlo.

Con eSentire, EDR y escáner vienen de fabricantes aliados licenciados aparte, el parche lo aplica tu equipo y sus SOC operan desde Canadá e Irlanda. En TecnetSOC, el mismo SOC opera EDR/XDR, SIEM y parcheo, en tu horario.



35

capacidades donde TecnetSOC va más allá

15

capacidades en las que coincidimos

0

capacidades donde eSentire supera a TecnetSOC

De las 50: 35 donde vamos más allá y 15 en las que coincidimos

Misma lista de 50 capacidades y mismo criterio para TecnetSOC y eSentire: 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)

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

eSentire es un servicio de SOC administrado, como TecnetSOC. Aquí comparamos la oferta más completa publicada de cada uno, capacidad por capacidad.

— LO QUE NOS HACE DISTINTOS

Diferencias que se notan en el día a día

01
Sin SOC en LATAM ni atención en español

CON ESENTIRE
Sus SOC están en Canadá e Irlanda, sus líneas de soporte cubren Norteamérica, Europa, Medio Oriente, África y Asia-Pacífico, y no publica atención en español. [\[1\]](#)

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

02
El parche lo aplica tu equipo

CON ESENTIRE
Atlas indica qué parchear, pero el parche lo despliega tu equipo de seguridad desde Atlas o desde tu herramienta actual, sin plazos de parcheo publicados. [\[2\]](#)

CON TECNETSOC
El SOC parchea por ti: valida en grupo piloto, instala críticos en 48 h como objetivo y cierra cuando el escáner lo confirma.

03
Herramientas de otros fabricantes, a tu costo

CON ESENTIRE
Endpoint, nube y vulnerabilidades se apoyan en fabricantes aliados como CrowdStrike, SentinelOne o Tenable, y el precio varía según tu inversión en esa tecnología. [\[3\]](#)

CON TECNETSOC
La oferta más completa ya incluye EDR/XDR, filtrado web, IDS/IPS, NDR y seguridad de correo, operados por el mismo SOC.

04
Identidad, nube y forense, aparte

CON ESENTIRE
Identidad, nube, contrato previo de respuesta a incidentes, monitoreo de dark web y seguridad ofensiva se contratan como complementos aparte del paquete de MDR. [\[3\]](#)

CON TECNETSOC
La oferta más completa incluye postura de identidad, seguridad en la nube, respuesta a incidentes con forense, superficie externa y pentesting anual.

05
Reportes según el paquete que pagues

CON ESENTIRE
Essentials recibe un reporte anual, Advanced uno trimestral y solo Complete suma la revisión mensual a fondo y el asesor de riesgo nombrado. [\[3\]](#)

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

06
Solo seguridad, la TI va aparte

CON ESENTIRE
El servicio se centra en detección y respuesta; gestión remota de equipos, monitoreo de disponibilidad y mesa de soporte de TI los contratas con otro proveedor. [\[4\]](#)

CON TECNETSOC
La oferta más completa suma gestión remota de equipos (RMM), monitoreo de disponibilidad (NOC) y mesa de soporte 24/7.

— DÓNDE ESTÁ LA DIFERENCIA

Las tres áreas con más diferencia

Exposición y gestión de TI

TecnetSOC **12**

eSentire **2**

de 12 capacidades completas en esta área

Operación y servicio

TecnetSOC **14**

eSentire **5**

de 14 capacidades completas en esta área

Detección y respuesta

TecnetSOC **15**

eSentire **8**

de 15 capacidades completas en esta área

— CAPACIDAD POR CAPACIDAD

TecnetSOC y eSentire, lado a lado

Capacidad		TecnetSOC	eSentire SOC	Evidencia sobre eSentire
✓ 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	
			+6 parciales	
Centro de operaciones (SOC) 24/7 con analistas humanos	✓	✓	SOC 24/7 con analistas de seis años de antigüedad promedio [5]	
Agentes de IA que investigan y filtran las alertas antes de pasarlas a un analista	✓	✓	AI Operatives agénticos investigan con 30+ pasos antes del analista [5]	
Compuerta Humana: una persona aprueba cada acción crítica antes de ejecutarse	✓	✓	Ninguna acción ni aislamiento sin revisión y aprobación de un analista [5]	

Capacidad	TecnetSOC	eSentire SOC	Evidencia sobre eSentire
Lo ofrece Lo ofrece como complemento Parcial, limitado o requiere otro contrato Sin evidencia pública			
No forma parte de su oferta publicada			
Asistente de investigación con IA en el portal, que cita sus fuentes	Neo		IA investiga y recomienda; sin evidencia de asistente bajo demanda que cite fuentes [5]
Operación en LATAM, EE.UU. y Europa, con analistas en tu zona horaria			SOC en Waterloo y Cork; sin operación en LATAM [6]
Analistas, soporte y portal en español nativo			Sin evidencia de analistas ni soporte en español [4]
Reportes para dirección en español y en lenguaje de negocio			Reportes en inglés; sin versión en español [3]
Tiempos de notificación e inicio de investigación publicados por severidad	Crítico: 30 min (objetivo)		Tiempo medio de contención de 15 minutos como métrica propia, no como compromiso contractual por severidad [3]
Resumen ejecutivo cada mañana: lo que pasó en las últimas 24 horas	07:30		Sin evidencia de resumen ejecutivo diario [3]
Reportes automáticos semanales, mensuales, trimestrales y anuales			Revisiones mensuales, reportes trimestrales y anual en Complete; sin semanal [3]
Gerente técnico de cuenta (TAM) asignado y revisiones trimestrales			Cyber Risk Advisor o TAM nombrado y revisiones periódicas en Complete [3]
Contacto 24/7 con personas de soporte o seguridad			Línea directa 24/7 al SOC, pero no mesa de soporte de TI [1]
Certificación independiente de la operación (ISO 27001 o SOC 2 Tipo II)	ISO/IEC 27001:2022		Certificada ISO 27001, SOC 2 Tipo II y PCI DSS [1]
Arranque rápido con un agente de software: la actividad de tus dispositivos, visible en horas	Típico: 2 a 4 horas		Valor en horas sin reemplazar herramientas, pero depende del EDR del cliente [5]
Detección y respuesta	15 de 15	8 completas +5 parciales	
Monitoreo continuo y correlación de eventos (SIEM), alineado con MITRE ATT&CK (marco de referencia de técnicas de ataque)			Registro de eventos ilimitado y correlación de múltiples señales en Atlas en todos los paquetes [3]
Protección avanzada en cada equipo (EDR/XDR): malware, ransomware y explotación de vulnerabilidades			Sin EDR propio; usa CrowdStrike, SentinelOne o Defender del cliente [5]
Filtrado web en el equipo			Sin filtrado web propio en el equipo [7]
Detección de intrusos (IDS/IPS)			Señal de red incluida, apoyada en firewalls de terceros; IDS propio no confirmado [5]
Detección de amenazas en la red interna (NDR)			Monitoreo de red incluido en todos los paquetes de MDR [3]
Investigaciones documentadas y enriquecidas con inteligencia de amenazas			Threat Response Unit propia enriquece investigaciones; acciones auditables [7]
Gestión de incidentes con bitácora y tiempo de atención medido por caso			Manejo ilimitado de incidentes con reportes por incidente [3]
Respuesta con aislamiento de equipos y bloqueo de direcciones IP			Aísla hosts, suspende usuarios y corta conexiones TCP [5]
Respuesta a incidentes con análisis de causa raíz			Forense y respuesta a incidentes (DFIR) propios, mediante contrato previo [8]
Postura de identidad: MFA, cuentas privilegiadas y acceso condicional			Monitoreo y respuesta de identidad como complemento; sin gestión de postura publicada [3]
Zero Trust: DNS seguro, acceso a aplicaciones y control de aplicaciones no autorizadas (shadow IT)			Sin DNS seguro, acceso Zero Trust ni control de shadow IT [5]
Seguridad en la nube: alertas y postura			Complemento de nube con postura y protección de cargas de trabajo (CSPM, CWPP y CNAPP) [3]
Seguridad de correo: spam, phishing, malware y fraude por suplantación (BEC)			Correo mediante alianza con Sublime Security (otro fabricante) [2]
Concientización: simulaciones de phishing y entrenamiento con métricas			Managed Phishing and Security Awareness Training propio [8]

Capacidad	TecnetSOC	eSentire SOC	Evidencia sobre eSentire
☒ Lo ofrece ☒ Lo ofrece como complemento ☒ No forma parte de su oferta publicada	☒ Parcial, limitado o requiere otro contrato	☒ Sin evidencia pública	
Recomendaciones de seguridad priorizadas con flujo de aprobación	☒	☒	vCISO y reportes de asesoría; sin flujo de aprobación de recomendaciones evidenciado [8]
Exposición y gestión de TI	12 de 12	2 completas +5 parciales	
Inventario unificado de activos y de software	☒	☒	Correlación multiescáner de activos; inventario de software propio no evidenciado [8]
Vulnerabilidades priorizadas por gravedad y probabilidad de explotación (CVSS, EPSS)	☒	☒	Managed Vulnerability Service incluido en Complete, sobre escáneres de terceros [3]
Prioridad a las fallas que ya se están explotando (catálogo KEV de CISA)	☒	☒	Prioriza por exposición y comportamiento de atacantes; uso de KEV no confirmado [2]
Parcheo de sistema operativo y aplicaciones de terceros	☒	☒	Parcheo desde Atlas (jul 2026) o vía infraestructura del cliente; recién lanzado [2]
Parcheo operado por el proveedor, con plazos publicados por severidad	☒ Críticos: 48 h (objetivo)	☒	Sin SLA de parcheo publicado ni claridad de quién opera el parche [2]
Verificación de cierre: el escáner confirma que la vulnerabilidad desapareció	☒	☒	Sin verificación de cierre publicada [2]
Validación de parches en grupo piloto antes del despliegue	☒	☒	Sin validación de parches en grupo piloto [2]
Superficie de ataque externa: lo que tu empresa expone en Internet, con puntaje de riesgo	☒ Puntaje 0 a 100	☒	CTEM y Preempt cubren reconocimiento externo; sin puntaje de exposición publicado [9]
Alertas de dominios que imitan tu marca y de credenciales o claves expuestas	☒	☒	Monitoreo de dark web para credenciales; typosquatting y secretos no evidenciados [8]
Prueba de penetración (pentest) anual	☒ Anual	☒	Pentesting autónomo continuo (Preempt) y servicios de seguridad ofensiva [9]
Gestión remota de equipos (RMM)	☒	☒	Sin RMM [4]
Monitoreo de disponibilidad (NOC)	☒	☒	Sin NOC ni monitoreo de disponibilidad [4]
Respaldo y continuidad	3 de 3	0 completas +0 parciales	
Respaldo de servidores, archivos, bases de datos, máquinas virtuales y Microsoft 365	☒ Complemento	☒	Sin respaldo [4]
Bóveda de respaldo inmutable (no se puede alterar ni borrar), aislada por cliente	☒ Complemento	☒	Sin bóveda inmutable [4]
Recuperación ante desastres con simulacros y tiempo de recuperación (RTO) medido	☒ Complemento RTO medido	☒	Sin recuperación ante desastres [4]
Cumplimiento	6 de 6	0 completas +1 parcial	
Evidencia mensual lista para auditores y aseguradoras	☒ Mensual	☒	Sin evidencia mensual para auditores o aseguradoras [3]
Preparación para ISO 27001, SOC 2 y PCI DSS con controles compartidos	☒ Complemento	☒	Sin plataforma GRC para el cliente [4]
Preparación normativa mexicana: CNBV Fintech, protección de datos (LFPDPPP) y NOM-024	☒ Complemento	☒	Sin normativa mexicana [4]
Gestión de riesgos, controles, declaración de aplicabilidad y auditorías internas	☒ Complemento	☒	Su CISO virtual evalúa la madurez del programa; sin plataforma de riesgos, declaración de aplicabilidad ni auditorías [8]

Capacidad	TecnetSOC	eSentire SOC	Evidencia sobre eSentire
✓ Lo ofrece + Lo ofrece como complemento ✗ No forma parte de su oferta publicada	○ Parcial, limitado o requiere otro contrato	? Sin evidencia pública	
Portal para tu auditor con sala de evidencias y página pública de confianza (trust center)	+ Complemento	✗	Sin portal del auditor ni Trust Center para el cliente [4]
Continuidad de negocio, riesgo de proveedores y gestión de brechas de datos	+ Complemento	✗	Sin continuidad de negocio ni gestión de proveedores [4]
Cómo se contrata	No suma al conteo		
Precio por dispositivo, con planes que se suman	✓ Por dispositivo	○	Por equipo con paquetes escalonados; sin precios públicos, se cotiza a la medida [3]
Plan gratuito para empezar	✓ Hasta 10 dispositivos	✗	Sin plan gratuito permanente [3]
Prueba gratuita en tu entorno real	✓ 30 días	✓	Despliegue gratis de Atlas por 30 días en el entorno real [7]
Disponible con la marca de tu proveedor de TI	✓	○	Reventa con marca eSentire; marca propia solo si el partner opera su SOC [10]
Cobertura completa	50	15 +17 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

ANEXO

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 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.esentire.com/what-we-do/security-operations-center (Diferencias que se notan en el día a día)

2. www.esentire.com/news-releases/esentire-unifies-detection-response-... (Diferencias que se notan en el día a día)

3. www.esentire.com/how-we-do-it/mdr-pricing-packaging (Diferencias que se notan en el día a día)

4. www.esentire.com/ (Diferencias que se notan en el día a día)
5. www.esentire.com/what-we-do/security-operations-platform (Centro de operaciones (SOC) 24/7 con analistas humanos)

6. mdrproviders.io/providers/esentire (Operación en LATAM, EE.UU. y Europa, con analistas en...)

7. www.esentire.com/what-we-do/xdr-extended-detection-and-response (Filtrado web en el equipo)
8. www.esentire.com/what-we-do/exposure-vulnerability-and-risk-management (Respuesta a incidentes con análisis de causa raíz)

9. www.businesswire.com/news/home/20260618356205/en/eSentire-Launches-... (Superficie de ataque externa: lo que tu empresa expone...)

10. www.esentire.com/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.

TecnetOne

Un SOC que habla tu idioma. [¿Ves un dato desactualizado o inexacto? Escríbenos y lo corregimos.](#)