

Trend Micro te da la plataforma y el MDR. TecnetSOC te da el servicio completo, operado en tu idioma y en tu zona horaria.

Con Trend Micro, el SIEM consume créditos por cada GB ingerido y retenido, y su parcheo es virtual: el parche oficial lo instalas tú. TecnetSOC cobra por dispositivo, no por gigabyte, y su SOC instala los parches.



29

capacidades donde TecnetSOC va más allá

21

capacidades en las que coincidimos

0

capacidades donde Trend Micro (TrendAI) supera a TecnetSOC

De las 50: 29 donde vamos más allá y 21 en las que coincidimos

Misma lista de 50 capacidades y mismo criterio para TecnetSOC y Trend Micro (TrendAI): 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

Trend Micro (TrendAI) ofrece una plataforma de seguridad con servicio MDR; sus módulos 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

Sus centros de operaciones, lejos de LATAM

CON TREND MICRO (TRENDIAI)
El MDR se opera desde centros de operaciones (SOC) en Dallas, Cork, Manila y Singapur; ninguno está en Latinoamérica. [1]

CON TECNETSOC
Te atienden analistas propios en tu zona horaria y en español nativo, con operación 24/7 en LATAM, EE.UU. y Europa.

02

El SIEM cobra por gigabyte, no por equipo

CON TREND MICRO (TRENDIAI)
El SIEM consume créditos por cada GB de datos de terceros que ingiere y, además, cada mes por cada GB retenido. [2]

CON TECNETSOC
Pagas un precio por dispositivo, no por gigabyte, con planes acumulativos y Visibility gratis hasta 10 dispositivos.

03

Parche virtual; el real, tuyo

CON TREND MICRO (TRENDIAI)
El parcheo es virtual (bloquea el ataque en la red sin corregir el software); el fabricante dice que el parche oficial sigue siendo la corrección definitiva y no documenta instalarlo por ti. [3]

CON TECNETSOC
El SOC instala parches priorizados por KEV y EPSS, valida en piloto y cierra solo cuando el escáner lo confirma.

04

Recomienda auto-aprobar todas las acciones

CON TREND MICRO (TRENDIAI)
El MDR puede actuar sin tu visto bueno previo, y el fabricante recomienda activar la auto-aprobación para todas las acciones. [4]

CON TECNETSOC
Los agentes de IA investigan cada alerta, y una persona aprueba toda acción crítica antes de ejecutarla (Compuerta Humana).

05

Condiciones del servicio, bajo contraseña

CON TREND MICRO (TRENDIAI)
Las descripciones del servicio MDR están protegidas con contraseña; antes de comprar debes pedirla a tu ejecutivo de cuenta. [5]

CON TECNETSOC
Los tiempos están publicados: ante un crítico, notificación e inicio de investigación en 30 minutos, como objetivo.

06

Sin RMM ni monitoreo NOC

CON TREND MICRO (TRENDIAI)
La plataforma no incluye gestión remota de equipos (RMM) ni monitoreo de disponibilidad; eso lo contratas y operas aparte. [6]

CON TECNETSOC
La gestión remota de equipos (RMM) y el monitoreo de disponibilidad (NOC) vienen en la oferta más completa.

— DÓNDE ESTÁ LA DIFERENCIA

Las tres áreas con más diferencia

Operación y servicio

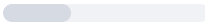
TecnetSOC  **14**

Trend Micro (TrendAI)  **4**

de 14 capacidades completas en esta área

Exposición y gestión de TI

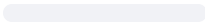
TecnetSOC  **12**

Trend Micro (TrendAI)  **4**

de 12 capacidades completas en esta área

Cumplimiento

TecnetSOC  **6**

Trend Micro (TrendAI)  **0**

de 6 capacidades completas en esta área (incluye complementos)

— CAPACIDAD POR CAPACIDAD

TecnetSOC y Trend Micro (TrendAI), lado a lado

Capacidad		TecnetSOC	Trend Micro (TrendAI) XDR y MDR	Evidencia sobre Trend Micro (TrendAI)
 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 	4 completas +7 parciales	
Centro de operaciones (SOC) 24/7 con analistas humanos			MDR 24/7/365 con analistas humanos; SOC's en Dallas, Cork, Manila y Singapur [1]	
Agentes de IA que investigan y filtran las alertas antes de pasarlas a un analista			Equipos MDR ya usan agentes de triaje con IA, como apoyo al analista; alcance no detallado [7]	

Capacidad		TecnetSOC	Trend Micro (TrendAI) XDR y MDR	Evidencia sobre Trend Micro (TrendAI)
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			Aprobación manual por acción configurable por el cliente; el proveedor recomienda auto-aprobación [4]	
Asistente de investigación con IA en el portal, que cita sus fuentes	 Neo		Companion explica alertas y sugiere pasos; sin evidencia de que cite sus fuentes [8]	
Operación en LATAM, EE.UU. y Europa, con analistas en tu zona horaria			SOCs en EE.UU., Irlanda, Filipinas y Singapur (follow the sun); ninguno en LATAM [1]	
Analistas, soporte y portal en español nativo			Sitio y oficina en México en español; sin evidencia de analistas MDR ni consola en español [9]	
Reportes para dirección en español y en lenguaje de negocio			Resúmenes ejecutivos mensuales; sin evidencia de que se entreguen en español [10]	
Tiempos de notificación e inicio de investigación publicados por severidad	 Crítico: 30 min (objetivo)		Publica objetivos (SLO), no acuerdos de nivel de servicio (SLA); los tiempos están en descripciones protegidas con contraseña [5]	
Resumen ejecutivo cada mañana: lo que pasó en las últimas 24 horas	 07:30		Sin evidencia de resumen ejecutivo diario [11]	
Reportes automáticos semanales, mensuales, trimestrales y anuales			Resumen ejecutivo mensual y revisión de servicio trimestral; sin semanal ni anual publicados [10]	
Gerente técnico de cuenta (TAM) asignado y revisiones trimestrales			TAM nombrado, service manager designado y revisiones trimestrales de negocio en Complete [12]	
Contacto 24/7 con personas de soporte o seguridad			Soporte 24/7/365 por teléfono, correo y portal de casos [12]	
Certificación independiente de la operación (ISO 27001 o SOC 2 Tipo II)	 ISO/IEC 27001:2022		Vision One certificada ISO 27001, ISO 27017 y SOC 2 Tipo II [13]	
Arranque rápido con un agente de software: la actividad de tus dispositivos, visible en horas	 Típico: 2 a 4 horas		Sin evidencia pública de tiempo de arranque con datos de actividad visible [11]	
Detección y respuesta	15 de 15	13 completas +2 parciales		
Monitoreo continuo y correlación de eventos (SIEM), alineado con MITRE ATT&CK (marco de referencia de técnicas de ataque)			Agentic SIEM y XDR correlacionan capas; técnicas observadas mapeadas a MITRE ATT&CK [14]	
Protección avanzada en cada equipo (EDR/XDR): malware, ransomware y explotación de vulnerabilidades			EDR/XDR propio con antiransomware y protección contra explotación de vulnerabilidades [15]	
Filtrado web en el equipo			Filtrado web incluido en la protección de endpoint [15]	
Detección de intrusos (IDS/IPS)			IPS de red (TippingPoint, filtros ZDI) e IPS de host propios [16]	
Detección de amenazas en la red interna (NDR)			NDR propio con IA y análisis de cientos de protocolos [16]	
Investigaciones documentadas y enriquecidas con inteligencia de amenazas			Investigación con inteligencia de amenazas propia (ZDI) y reportes de incidente detallados [11]	
Gestión de incidentes con bitácora y tiempo de atención medido por caso			Case Management con prioridad y responsable; sin evidencia de tiempo medido por caso [17]	
Respuesta con aislamiento de equipos y bloqueo de direcciones IP			Aislamiento de endpoint y bloqueo de IP como acciones de respuesta [18]	
Respuesta a incidentes con análisis de causa raíz			Análisis de causa raíz en MDR y 40 horas de respuesta a incidentes en Complete [12]	
Postura de identidad: MFA, cuentas privilegiadas y acceso condicional			ITDR y postura de identidad: MFA, cuentas privilegiadas; Entra ID, AD, Okta [19]	
Zero Trust: DNS seguro, acceso a aplicaciones y control de aplicaciones no autorizadas (shadow IT)			Zero Trust Secure Access: acceso a aplicaciones (ZTNA), puerta web segura y control de apps no autorizadas; DNS seguro no explícito [20]	
Seguridad en la nube: alertas y postura			Cloud Security propio (CNAPP, CSPM) con alertas y postura multinube [21]	

Capacidad	TecnetSOC	Trend Micro (TrendAI) XDR y MDR	Evidencia sobre Trend Micro (TrendAI)
✓ Lo ofrece + Lo ofrece como complemento ✗ No forma parte de su oferta publicada	◐ Parcial, limitado o requiere otro contrato	? Sin evidencia pública	
Seguridad de correo: spam, phishing, malware y fraude por suplantación (BEC)	✓	✓	Email and Collaboration Security: phishing, malware, ransomware y BEC por estilo de escritura [22]
Concientización: simulaciones de phishing y entrenamiento con métricas	✓	✓	Capacitación de concientización con simulaciones de phishing realistas dentro de CREM [23]
Recomendaciones de seguridad priorizadas con flujo de aprobación	✓	◐	CREM da recomendaciones priorizadas y playbooks; sin evidencia de flujo de aprobación [23]
Exposición y gestión de TI	12 de 12	4 completas +4 parciales	
Inventario unificado de activos y de software	✓	✓	CREM descubre dispositivos, identidades, aplicaciones, nube y activos no administrados [23]
Vulnerabilidades priorizadas por gravedad y probabilidad de explotación (CVSS, EPSS)	✓	◐	CVSS v3.1 más potencial de explotación propio; sin EPSS explícito [24]
Prioridad a las fallas que ya se están explotando (catálogo KEV de CISA)	✓	✓	Verifica estado KEV y filtra vulnerabilidades explotadas activamente [24]
Parcheo de sistema operativo y aplicaciones de terceros	✓	◐	Solo parcheo virtual (IPS de host y red); sin despliegue de parches propio documentado [3]
Parcheo operado por el proveedor, con plazos publicados por severidad	✓ Críticos: 48 h (objetivo)	?	Sin evidencia de parcheo operado por el proveedor con plazos [11]
Verificación de cierre: el escáner confirma que la vulnerabilidad desapareció	✓	◐	Evaluación continua de vulnerabilidades; sin flujo explícito de verificación de cierre [23]
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	✓	EASM propio con puntaje de riesgo organizacional y benchmarking [23]
Alertas de dominios que imitan tu marca y de credenciales o claves expuestas	✓	◐	Monitoreo de fugas en dark web por dominio; sin evidencia de alertas de dominios imitadores [25]
Prueba de penetración (pentest) anual	✓ Anual	✓	Red y purple teaming con pruebas de penetración como servicio propio [10]
Gestión remota de equipos (RMM)	✓	?	Sin evidencia de RMM propio [6]
Monitoreo de disponibilidad (NOC)	✓	?	Sin evidencia de monitoreo de disponibilidad (NOC) [26]
Respaldo y continuidad	3 de 3	0 completas +0 parciales	
Respaldo de servidores, archivos, bases de datos, máquinas virtuales y Microsoft 365	+ Complemento	?	Sin evidencia de respaldo propio de servidores ni Microsoft 365 [6]
Bóveda de respaldo inmutable (no se puede alterar ni borrar), aislada por cliente	+ Complemento	?	Sin evidencia de bóveda inmutable [6]
Recuperación ante desastres con simulacros y tiempo de recuperación (RTO) medido	+ Complemento RTO medido	?	Sin evidencia de recuperación ante desastres con RTO medido [26]
Cumplimiento	6 de 6	0 completas +3 parciales	
Evidencia mensual lista para auditores y aseguradoras	✓ Mensual	◐	Reportes de cumplimiento listos para auditor bajo demanda; sin entrega mensual publicada [23]
Preparación para ISO 27001, SOC 2 y PCI DSS con controles compartidos	+ Complemento	◐	Mapeo a NIST, FedRAMP, GDPR y marcos CSPM; no es preparación ISO/SOC 2 completa [23]

Capacidad	TecnetSOC	Trend Micro (TrendAI) XDR y MDR	Evidencia sobre Trend Micro (TrendAI)
✓ Lo ofrece + Lo ofrece como complemento ✗ No forma parte de su oferta publicada	● Parcial, limitado o requiere otro contrato	? Sin evidencia pública	
Preparación normativa mexicana: CNBV Fintech, protección de datos (LFPDPPP) y NOM-024	+ Complemento	?	Sin evidencia de preparación normativa mexicana [19]
Gestión de riesgos, controles, declaración de aplicabilidad y auditorías internas	+ Complemento	●	Cuantificación de riesgo y controles automatizados; sin declaración de aplicabilidad ni auditoría interna [23]
Portal para tu auditor con sala de evidencias y página pública de confianza (trust center)	+ Complemento	?	Sin evidencia de portal para auditor ni página pública de confianza del cliente [19]
Continuidad de negocio, riesgo de proveedores y gestión de brechas de datos	+ Complemento	?	Sin evidencia de módulos de continuidad, riesgo de proveedores ni gestión de brechas [19]
Cómo se contrata	No suma al conteo		
Precio por dispositivo, con planes que se suman	✓ Por dispositivo	●	Modelo de créditos; MDR por rangos de usuarios, mínimo 251 [27]
Plan gratuito para empezar	✓ Hasta 10 dispositivos	?	Sin evidencia de plan gratuito permanente [28]
Prueba gratuita en tu entorno real	✓ 30 días	✓	Prueba gratuita de 30 días de la plataforma [28]
Disponible con la marca de tu proveedor de TI	✓	●	Vision One for Service Providers multiempresa; sin evidencia de marca blanca [28]
Cobertura completa	50	21 +16 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 Trend Micro (TrendAI): Trend Micro (TrendAI desde mar 2026): TrendAI Vision One con TrendAI Vision One Services Complete (MDR, respuesta a incidentes, soporte premium con TAM) más módulos propios CREM, Endpoint, Email, Network, Cloud, Identity y Zero Trust Secure Access, 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.

1. success.trendmicro.com/en-US/solution/ka-0019617 (Diferencias que se notan en el día a día)
2. docs.trendmicro.com/en-us/documentation/article/trend-vision-one-cr... (Diferencias que se notan en el día a día)
3. www.trendaisecurity.com/en-us/resources-insights/deep-research/secu... (Diferencias que se notan en el día a día)
4. success.trendmicro.com/en-US/solution/KA-0019492 (Diferencias que se notan en el día a día)
5. success.trendmicro.com/en-US/solution/KA-0008963 (Diferencias que se notan en el día a día)
6. www.trendaisecurity.com/en/platform (Diferencias que se notan en el día a día)
7. newsroom.trendmicro.com (Agentes de IA que investigan y filtran las alertas...)
8. www.trendmicro.com/en_us/business/ai/companion.html (Asistente de investigación con IA en el portal, que...)
9. www.trendmicro.com/es_mx/business/services/support-services.html (Analistas, soporte y portal en español nativo)
10. www.trendmicro.com/content/dam/trendmicro/global/en/core/docs/solut... (Reportes para dirección en español y en lenguaje de...)
11. www.trendmicro.com/en/business/services/managed-xdr.html (Resumen ejecutivo cada mañana: lo que pasó en las...)
12. www.trendmicro.com/en/business/services/service-one.html (Gerente técnico de cuenta (TAM) asignado y revisiones...)
13. www.trendmicro.com/en_us/about/trust-center/compliance.html (Certificación independiente de la operación (ISO 27001...))
14. www.docs.trendmicro.com/en-us/enterprise/trend-vision-one/xdr-part/... (Monitoreo continuo y correlación de eventos (SIEM),...)
15. www.trendaisecurity.com/en/platform/endpoint-security (Protección avanzada en cada equipo (EDR/XDR): malware,...)
16. www.trendaisecurity.com/en/platform/network-security (Detección de intrusos (IDS/IPS))
17. docs.trendmicro.com/en-us/documentation/article/trend-vision-one-ca... (Gestión de incidentes con bitácora y tiempo de atención...)
18. www.trendaisecurity.com/en/platform/security-operations (Respuesta con aislamiento de equipos y bloqueo de...)
19. www.trendaisecurity.com/en/platform/cyber-risk-exposure-management (Postura de identidad: MFA, cuentas privilegiadas y...)
20. www.trendmicro.com/en_us/business/products/network-zero-trust-secur... (Zero Trust: DNS seguro, acceso a aplicaciones y control...)
21. www.trendaisecurity.com/en/platform/cloud-security (Seguridad en la nube: alertas y postura)
22. www.trendaisecurity.com/en/platform/email-security (Seguridad de correo: spam, phishing, malware y fraude...)
23. www.trendmicro.com/content/dam/trendmicro/global/en/core/docs/solut... (Concientización: simulaciones de phishing y...)
24. docs.trendmicro.com/en-us/documentation/article/trend-vision-one-TI... (Vulnerabilidades priorizadas por gravedad y...)
25. docs.trendmicro.com/en-us/documentation/article/trend-vision-one-da... (Alertas de dominios que imitan tu marca y de...)
26. www.trendaisecurity.com/en/services (Monitoreo de disponibilidad (NOC))
27. mdrproviders.io/providers/trend-micro (Precio por dispositivo, con planes que se suman)
28. www.trendmicro.com/en_us/partners/service-providers.html (Plan gratuito para empezar)

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.