

Huntress vigila tus equipos. TecnetSOC es un SOC agéntico que opera toda tu seguridad por ti, 24/7.

Huntress licencia por separado EDR, identidades, SIEM y capacitación, y su módulo de postura señala parches faltantes sin aplicarlos. En TecnetSOC pagas por dispositivo y el SOC parchea, valida en piloto y cierra con escáner.



42

capacidades donde TecnetSOC va más allá

8

capacidades en las que coincidimos

0

capacidades donde Huntress supera a TecnetSOC

De las 50: 42 donde vamos más allá y 8 en las que coincidimos

Misma lista de 50 capacidades y mismo criterio para TecnetSOC y Huntress: 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

Huntress es un servicio de SOC administrado que se vende a través de proveedores de TI, con módulos que se contratan por separado. 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
Señala parches, no los opera

CON HUNTRESS
Su módulo de postura (ESPM) está en acceso anticipado (Early Access), con disponibilidad general anunciada para 2027, y señala parches faltantes con datos de Microsoft Defender; no publica tiempos de parcheo. [\[1\]](#)

CON TECNETSOC
El SOC prioriza el parcheo según lo que ya se explota en el mundo real (KEV, EPSS), lo valida en un grupo piloto, tiene como objetivo 48 h en críticos y cierra solo cuando el escáner confirma la corrección.

02
Una licencia por cada módulo

CON HUNTRESS
EDR, identidades, SIEM, capacitación y postura se licencian por separado, cada uno con su propia unidad de cobro, y en compra directa piden un mínimo de 50 licencias por producto. [\[2\]](#)

CON TECNETSOC
Pagas por dispositivo con planes acumulativos; Visibility es gratis hasta 10 dispositivos y puedes probar Response 30 días en tu entorno.

03
El antivirus lo pones tú

CON HUNTRESS
La prevención antivirus la aporta Microsoft Defender u otro antivirus que ya tengas, y la plataforma no incluye filtrado web ni IDS/IPS. [\[3\]](#)

CON TECNETSOC
La protección avanzada en cada equipo (EDR/XDR), el filtrado web y el IDS/IPS vienen en la oferta más completa.

04
Sin sensor de red ni antispam

CON HUNTRESS
La red interna se ve solo por los registros de firewall que envías a su SIEM, y el correo se vigila en el buzón, sin antispam. [\[4\]](#)

CON TECNETSOC
La oferta más completa incluye detección en la red interna (NDR) y seguridad de correo contra spam, phishing, malware y BEC.

05
RMM, NOC y pentest: otro proveedor

CON HUNTRESS
No hay RMM, monitoreo de disponibilidad, pentesting ni respaldo; se conecta al RMM que ya tengas y lo demás lo contratas con otros proveedores. [\[5\]](#)

CON TECNETSOC
RMM, NOC, pentesting anual, TAM y mesa de soporte 24/7 vienen en la oferta más completa; el respaldo inmutable es complemento.

06
Sin operación en LATAM ni atención en español

CON HUNTRESS
Sus anuncios de canal apuntan a EE.UU., Reino Unido y la región de Europa, Medio Oriente y África (EMEA); no publica operación en LATAM ni analistas que te atiendan en español. [\[6\]](#)

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

— DÓNDE ESTÁ LA DIFERENCIA

Las tres áreas con más diferencia

Detección y respuesta

TecnetSOC **15**

Huntress **3**

de 15 capacidades completas en esta área

Exposición y gestión de TI

TecnetSOC **12**

Huntress **0**

de 12 capacidades completas en esta área

Operación y servicio

TecnetSOC **14**

Huntress **5**

de 14 capacidades completas en esta área

— CAPACIDAD POR CAPACIDAD

TecnetSOC y Huntress, lado a lado

Capacidad	TecnetSOC	Huntress SOC para proveedores de TI	Evidencia sobre Huntress
✓ Lo ofrece + Lo ofrece como complemento ⓧ No forma parte de su oferta publicada	⓪ Parcial, limitado o requiere otro contrato	? Sin evidencia pública	
Operación y servicio	14 de 14	5 completas +5 parciales	
Centro de operaciones (SOC) 24/7 con analistas humanos	✓	✓	SOC 24/7 propio, dirigido por personas y asistido por IA, incluido en todos los módulos [2]
Agentes de IA que investigan y filtran las alertas antes de pasarlas a un analista	✓	✓	Athena: más de 40 agentes de IA investigan y dictaminan cada señal [7]

Capacidad	TecnetSOC	Huntress SOC para proveedores de TI	Evidencia sobre Huntress
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			Una persona revisa los casos dudosos; los de alta confianza se reportan sin revisión humana; el aislamiento se ejecuta sin aprobación previa [7]
Asistente de investigación con IA en el portal, que cita sus fuentes	 Neo		Athena trabaja dentro del SOC; no hay asistente bajo demanda en el portal [7]
Operación en LATAM, EE.UU. y Europa, con analistas en tu zona horaria			Operación en EE.UU.; sin oficina ni operación en LATAM [6]
Analistas, soporte y portal en español nativo			Sin evidencia de analistas ni soporte en español [5]
Reportes para dirección en español y en lenguaje de negocio			Los reportes de amenazas mensual y trimestral se pueden generar en español desde la configuración de marca, con página de resumen [8]
Tiempos de notificación e inicio de investigación publicados por severidad	 Crítico: 30 min (objetivo)		Publica promedios de tiempo de respuesta, no tiempos de notificación por severidad [9]
Resumen ejecutivo cada mañana: lo que pasó en las últimas 24 horas	 07:30		Sin evidencia de resumen diario [10]
Reportes automáticos semanales, mensuales, trimestrales y anuales			Reportes semanales, mensuales y trimestrales; sin evidencia pública de reporte anual [11]
Gerente técnico de cuenta (TAM) asignado y revisiones trimestrales			Su centro de ayuda menciona un gerente de cuenta de canal asignado; no publica un gerente técnico (TAM) ni revisiones trimestrales [12]
Contacto 24/7 con personas de soporte o seguridad			SOC 24/7 incluido; horario 24/7 de la mesa de soporte no confirmado [2]
Certificación independiente de la operación (ISO 27001 o SOC 2 Tipo II)	 ISO/IEC 27001:2022		Su trust center muestra SOC 2 Tipo II, GDPR y CCPA; sin ISO 27001 [13]
Arranque rápido con un agente de software: la actividad de tus dispositivos, visible en horas	 Típico: 2 a 4 horas		Agente ligero desplegable por RMM, sin proyecto de implementación [5]
Detección y respuesta	15 de 15	3 completas +8 parciales	
Monitoreo continuo y correlación de eventos (SIEM), alineado con MITRE ATT&CK (marco de referencia de técnicas de ataque)			Managed SIEM con reglas de correlación; MITRE ATT&CK no mencionado explícitamente [4]
Protección avanzada en cada equipo (EDR/XDR): malware, ransomware y explotación de vulnerabilidades			EDR propio de detección; la prevención antivirus se apoya en Microsoft Defender [9]
Filtrado web en el equipo			Sin filtrado web en el equipo [9]
Detección de intrusos (IDS/IPS)			Sin IDS/IPS propio [9]
Detección de amenazas en la red interna (NDR)			Sin NDR; solo ingesta logs de firewall y DNS en el SIEM [4]
Investigaciones documentadas y enriquecidas con inteligencia de amenazas			Athena arma contexto, línea de tiempo e infraestructura maliciosa conocida [7]
Gestión de incidentes con bitácora y tiempo de atención medido por caso			Reportes de incidente con línea de tiempo; MTTR por incidente no publicado [7]
Respuesta con aislamiento de equipos y bloqueo de direcciones IP			Aislamiento de equipos sí; bloqueo de IP no documentado [14]
Respuesta a incidentes con análisis de causa raíz			Investigación y remediación incluidas; sin evidencia pública de un servicio de análisis forense [9]
Postura de identidad: MFA, cuentas privilegiadas y acceso condicional			ISPM cubre MFA, privilegios y acceso condicional solo en M365, Early Access [15]
Zero Trust: DNS seguro, acceso a aplicaciones y control de aplicaciones no autorizadas (shadow IT)			Sin DNS seguro, ZTNA ni control de shadow IT [2]

Capacidad	TecnetSOC	Huntress SOC para proveedores de TI	Evidencia sobre Huntress
☒ Lo ofrece ☒ Lo ofrece como complemento ☒ No forma parte de su oferta publicada	☒ Parcial, limitado o requiere otro contrato	☒ Sin evidencia pública	
Seguridad en la nube: alertas y postura	☒	☒	SIEM ingesta AWS CloudTrail; sin postura ni alertas de Azure [4]
Seguridad de correo: spam, phishing, malware y fraude por suplantación (BEC)	☒	☒	ITDR detecta BEC y reglas maliciosas; sin gateway antispam ni cuarentena [16]
Concientización: simulaciones de phishing y entrenamiento con métricas	☒	☒	Managed SAT propio con simulaciones de phishing y métricas [2]
Recomendaciones de seguridad priorizadas con flujo de aprobación	☒	☒	ESPM e ISPM priorizan y corrigen postura, en Early Access [1]
Exposición y gestión de TI	12 de 12	0 completas +4 parciales	
Inventario unificado de activos y de software	☒	☒	ESPM muestra las aplicaciones y el RMM detectados; en acceso anticipado, con disponibilidad general anunciada para 2027 [1]
Vulnerabilidades priorizadas por gravedad y probabilidad de explotación (CVSS, EPSS)	☒	☒	Vulnerabilidades vía datos de Defender for Endpoint; CVSS/EPSS no mencionados [1]
Prioridad a las fallas que ya se están explotando (catálogo KEV de CISA)	☒	☒	Prioriza lo explotado en el mundo real; KEV no citado; Early Access [17]
Parcheo de sistema operativo y aplicaciones de terceros	☒	☒	ESPM resalta parches faltantes pero no los despliega [1]
Parcheo operado por el proveedor, con plazos publicados por severidad	☒ Críticos: 48 h (objetivo)	☒	No opera parcheo ni ofrece tiempos de parcheo [1]
Verificación de cierre: el escáner confirma que la vulnerabilidad desapareció	☒	☒	Sin verificación de cierre de vulnerabilidades por escáner [1]
Validación de parches en grupo piloto antes del despliegue	☒	☒	Sin despliegue de parches, por tanto sin grupo piloto [1]
Superficie de ataque externa: lo que tu empresa expone en Internet, con puntaje de riesgo	☒ Puntaje 0 a 100	☒	External Recon detecta puertos abiertos en los equipos; sin gestión de superficie de ataque externa ni puntaje de riesgo [9]
Alertas de dominios que imitan tu marca y de credenciales o claves expuestas	☒	☒	Sin detección de typosquatting ni secretos expuestos [2]
Prueba de penetración (pentest) anual	☒ Anual	☒	Sin pentesting en su oferta [2]
Gestión remota de equipos (RMM)	☒	☒	No ofrece RMM; se integra con RMM de terceros [5]
Monitoreo de disponibilidad (NOC)	☒	☒	Sin monitoreo de disponibilidad ni NOC [2]
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 [2]
Bóveda de respaldo inmutable (no se puede alterar ni borrar), aislada por cliente	☒ Complemento	☒	Sin bóveda inmutable [2]
Recuperación ante desastres con simulacros y tiempo de recuperación (RTO) medido	☒ Complemento RTO medido	☒	Sin recuperación ante desastres [2]

Capacidad	TecnetSOC	Huntress	Evidencia sobre Huntress
✓ 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	
Evidencia mensual lista para auditores y aseguradoras	✓ Mensual	⦿	SIEM "audit-ready" con retención hasta 7 años; sin paquete mensual de evidencia [4]
Preparación para ISO 27001, SOC 2 y PCI DSS con controles compartidos	+ Complemento	✗	Sin plataforma GRC; solo cursos de concientización orientados a SOC 2 e ISO 27001 [18]
Preparación normativa mexicana: CNBV Fintech, protección de datos (LFPDPPP) y NOM-024	+ Complemento	✗	Sin cobertura de normativa mexicana [2]
Gestión de riesgos, controles, declaración de aplicabilidad y auditorías internas	+ Complemento	✗	Sin gestión de riesgos, controles ni SoA [2]
Portal para tu auditor con sala de evidencias y página pública de confianza (trust center)	+ Complemento	✗	Trust Center solo para su propia empresa, no para el cliente [13]
Continuidad de negocio, riesgo de proveedores y gestión de brechas de datos	+ Complemento	✗	Sin módulos de continuidad, proveedores ni brechas [2]
Cómo se contrata	No suma al conteo		
Precio por dispositivo, con planes que se suman	✓ Por dispositivo	⦿	Precio por unidad y por módulo (endpoint, identidad, fuente); sin planes acumulativos [2]
Plan gratuito para empezar	✓ Hasta 10 dispositivos	✗	Sin plan gratuito permanente [2]
Prueba gratuita en tu entorno real	✓ 30 días	✓	Prueba completa gratis con SOC 24/7; duración no publicada oficialmente [2]
Disponible con la marca de tu proveedor de TI	✓	⦿	Marca compartida: reportes con el logo del proveedor de TI; la plataforma y la capacitación muestran la marca Huntress [19]
Cobertura completa	50	8	+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 Huntress: Huntress, plataforma completa (Managed EDR, ITDR, SIEM, SAT, ISPM y ESPM en Early Access, con SOC 24/7), 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.huntress.com/platform/managed-espm (Diferencias que se notan en el día a día)
- www.huntress.com/pricing (Diferencias que se notan en el día a día)
- www.huntress.com/platform/managed-edr/managed-microsoft-defender (Diferencias que se notan en el día a día)
- www.huntress.com/platform/siem (Diferencias que se notan en el día a día)
- www.huntress.com/partners/msps (Diferencias que se notan en el día a día)
- www.huntress.com/press-release/huntress-expands-channel-ecosystem-w... (Diferencias que se notan en el día a día)
- www.huntress.com/use-cases/athena (Agentes de IA que investigan y filtran las alertas...)
- support.huntress.io/hc/en-us/articles/19223729361939-Huntress-Relea... (Reportes para dirección en español y en lenguaje de...)
- www.huntress.com/platform/managed-edr (Tiempos de notificación e inicio de investigación...)
- support.huntress.io/hc/en-us/sections/22539292694547-Reports (Resumen ejecutivo cada mañana: lo que pasó en las...)
- support.huntress.io/hc/en-us/articles/4404012804115-Monthly-and-Qua... (Reportes automáticos semanales, mensuales, trimestrales...)
- support.huntress.io/hc/en-us/articles/10962580083731-How-can-I-chan... (Gerente técnico de cuenta (TAM) asignado y revisiones...)
- trust.huntress.com/ (Certificación independiente de la operación (ISO 27001...))
- support.huntress.io/hc/en-us/articles/4404960349459-Managed-Host-Is... (Respuesta con aislamiento de equipos y bloqueo de...)
- www.huntress.com/platform/managed-ispm (Postura de identidad: MFA, cuentas privilegiadas y...)
- www.huntress.com/platform/managed-itdr (Seguridad de correo: spam, phishing, malware y fraude...)
- www.huntress.com/press-release/huntress-platform-expands-new-postur... (Prioridad a las fallas que ya se están explotando...)
- www.huntress.com/platform/security-awareness-training/compliance/is... (Preparación para ISO 27001, SOC 2 y PCI DSS con...)
- support.huntress.io/hc/en-us/articles/4414363214995-Add-Your-Compan... (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.