

Con Wazuh, el SOC lo armas y lo operas tú. TecnetSOC ya es el SOC: IA que investiga, personas que deciden, en tu idioma.

Con Wazuh, instalas servidor, indexador y panel y pagas el disco (o Wazuh Cloud, por niveles de agentes); tu equipo revisa las alertas porque no hay SOC ni MDR. Con TecnetSOC instalas un agente, la plataforma se despliega sola y el turno es nuestro.



44

capacidades donde TecnetSOC va más allá

6

capacidades en las que coincidimos

0

capacidades donde Wazuh supera a TecnetSOC

De las 50: 44 donde vamos más allá y 6 en las que coincidimos

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

Wazuh es una plataforma abierta de SIEM y XDR que tu equipo instala y opera; no es un servicio de SOC administrado. Lo demás que necesitarías (EDR, SIEM, RMM, respaldo) se compra y se opera por separado, y no todo se integra de forma nativa. Este comparativo muestra, capacidad por capacidad, qué parte de lo que incluye TecnetSOC cubre Wazuh por sí sola y qué tendrías que sumar en productos, contratos y personal.

Diferencias que se notan en el día a día

01

Todo lo opera tu equipo

CON WAZUH

Tu equipo revisa cada alerta, ajusta reglas y decodificadores y decide la respuesta, también a las 3 a.m.; Wazuh no ofrece SOC ni MDR. [1]

CON TECNETSOC

Analistas de TecnetOne operan 24/7 en tu zona horaria y en español; ante un crítico, notifican e inician investigación en 30 minutos, como objetivo.

02

Instalas y actualizas los servidores

CON WAZUH AUTOALOJADO

Instalas servidor, indexador y dashboard con permisos root, y cada actualización exige los tres en la misma versión exacta, parche incluido. [2]

CON TECNETSOC

Instalas un agente y el resto se despliega solo: actividad visible por lo general en 2 a 4 horas, sin servidores que mantener ni proyecto de implementación.

03

El disco de registros lo pagas

CON WAZUH AUTOALOJADO

Compras y administras el disco: la guía estima 200 GB cada 90 días de alertas con hasta 100 equipos, y crece con cada equipo. [3]

CON TECNETSOC

La plataforma es un servicio en la nube operado por TecnetOne: no compras, instalas ni mantienes almacenamiento para tus registros.

04

Detecta vulnerabilidades, no las parchea

CON WAZUH

Detectas vulnerabilidades por CVE, pero no aplica parches: instalarlos, probarlos y programar ventanas queda en tu equipo o en otra herramienta. [4]

CON TECNETSOC

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

05

Respuesta automática sin aprobación humana

CON WAZUH

Active Response ejecuta scripts en automático cuando salta una regla, sin paso de aprobación humana; aislar un equipo exige escribir tu propio script. [5]

CON TECNETSOC

Cada alerta llega investigada por agentes de IA y una persona aprueba toda acción crítica antes de ejecutarla (Compuerta Humana).

06

La red y el correo, aparte

CON WAZUH

Ver tráfico de red exige instalar y configurar Suricata, otro producto; seguridad de correo, filtrado web y simulaciones de phishing no forman parte de la plataforma. [6]

CON TECNETSOC

NDR, IDS/IPS, seguridad de correo, filtrado web y simulaciones de phishing vienen incluidos en su oferta más completa.

Las tres áreas con más diferencia

Detección y respuesta

TecnetSOC 15

Wazuh 2

de 15 capacidades completas en esta área

Operación y servicio

TecnetSOC 14

Wazuh 2

de 14 capacidades completas en esta área

Exposición y gestión de TI

TecnetSOC 12

Wazuh 2

de 12 capacidades completas en esta área

TecnetSOC y Wazuh, lado a lado

Capacidad	TecnetSOC	Wazuh SIEM y XDR abierto	Evidencia sobre Wazuh
✓ 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	2 completas	
		+4 parciales	
Centro de operaciones (SOC) 24/7 con analistas humanos	✓	Lo pone tu equipo	Wazuh no ofrece SOC ni MDR; el soporte profesional es técnico [7]
Agentes de IA que investigan y filtran las alertas antes de pasarlas a un analista	✓	ⓧ	No hay agentes de IA que filtren cada alerta; solo guía para enriquecer con LLM [8]
Compuerta Humana: una persona aprueba cada acción crítica antes de ejecutarse	✓	ⓧ	Active Response se dispara automático por regla; no hay compuerta humana de aprobación [9]
Asistente de investigación con IA en el portal, que cita sus fuentes	✓ Neo	🕒	AI Analyst (solo Wazuh Cloud) genera reportes periódicos; no investiga bajo demanda ni narra casos [10]

Capacidad	TecnetSOC	Wazuh SIEM y XDR abierto	Evidencia sobre Wazuh
☒ Lo ofrece ☒ Lo ofrece como complemento ☐ Parcial, limitado o requiere otro contrato ☐ Sin evidencia pública ☐ No forma parte de su oferta publicada ☐ Lo pone tu equipo			
Operación en LATAM, EE.UU. y Europa, con analistas en tu zona horaria	☒	Lo pone tu equipo	Sin operación de seguridad; soporte "follow the sun" global, no desde LATAM [7]
Analistas, soporte y portal en español nativo	☒	☐	No publica soporte ni analistas en español [7]
Reportes para dirección en español y en lenguaje de negocio	☒	☐	Reportes PDF técnicos y AI Analyst en inglés; no hay reporte ejecutivo en español [10]
Tiempos de notificación e inicio de investigación publicados por severidad	☒ Crítico: 30 min (objetivo)	Lo pone tu equipo	Solo SLA de soporte técnico (Premium 4 h crítico), no de incidentes de seguridad [7]
Resumen ejecutivo cada mañana: lo que pasó en las últimas 24 horas	☒ 07:30	Lo pone tu equipo	AI Analyst envía correos periódicos con resumen de postura; no es resumen diario [10]
Reportes automáticos semanales, mensuales, trimestrales y anuales	☒	☐	Reportes PDF desde el dashboard y reportes AI programados; sin calendario fijo semanal a anual [10]
Gerente técnico de cuenta (TAM) asignado y revisiones trimestrales	☒	☒	Soporte profesional incluye customer success manager dedicado y 4 health checks al año (Premium) [7]
Contacto 24/7 con personas de soporte o seguridad	☒	☐	Premium es 24/7 solo para incidencias críticas; Standard es 8x5 [7]
Certificación independiente de la operación (ISO 27001 o SOC 2 Tipo II)	☒ ISO/IEC 27001:2022	☒	Wazuh Cloud declara SOC 2 y PCI DSS; sin ISO 27001 publicada [11]
Arranque rápido con un agente de software: la actividad de tus dispositivos, visible en horas	☒ Típico: 2 a 4 horas	☐	Wazuh Cloud arranca rápido; la versión autoalojada exige instalar y dimensionar servidores [11]
Detección y respuesta	15 de 15	2 completas +7 parciales	
Monitoreo continuo y correlación de eventos (SIEM), alineado con MITRE ATT&CK (marco de referencia de técnicas de ataque)	☒	☒	Núcleo del producto: SIEM con reglas, correlación y mapeo MITRE ATT&CK [12]
Protección avanzada en cada equipo (EDR/XDR): malware, ransomware y explotación de vulnerabilidades	☒	☐	Detecta malware y rootkits con reglas YARA y VirusTotal; sin prevención nativa de explotación de vulnerabilidades ni antiransomware [13]
Filtrado web en el equipo	☒	☐	No ofrece filtrado web en el equipo [14]
Detección de intrusos (IDS/IPS)	☒	☐	IDS de host nativo; IDS de red solo integrando Suricata (tercero) [15]
Detección de amenazas en la red interna (NDR)	☒	☐	Sin NDR propio; depende de Suricata; monitoreo sin agente limitado a SSH [15]
Investigaciones documentadas y enriquecidas con inteligencia de amenazas	☒	☒	Enriquecimiento con listas CDB, VirusTotal y CTI propio de Wazuh [13]
Gestión de incidentes con bitácora y tiempo de atención medido por caso	☒	☐	No incluye gestión de casos ni MTTR por incidente; se integra con terceros [13]
Respuesta con aislamiento de equipos y bloqueo de direcciones IP	☒	☐	Bloqueo de IP incluido (firewall-drop, netsh); aislamiento del equipo solo con script propio [9]
Respuesta a incidentes con análisis de causa raíz	☒	Lo pone tu equipo	No ofrece servicio de respuesta a incidentes ni forense [7]
Postura de identidad: MFA, cuentas privilegiadas y acceso condicional	☒	☐	Ingiera registros de Entra ID vía MS Graph; no evalúa postura; sin Google Workspace [16]
Zero Trust: DNS seguro, acceso a aplicaciones y control de aplicaciones no autorizadas (shadow IT)	☒	☐	No ofrece DNS seguro, acceso Zero Trust ni control de shadow IT [14]
Seguridad en la nube: alertas y postura	☒	☐	Monitorea registros de Azure y Microsoft 365; postura documentada solo para GCP [17]
Seguridad de correo: spam, phishing, malware y fraude por suplantación (BEC)	☒	☐	No ofrece seguridad de correo [14]
Concientización: simulaciones de phishing y entrenamiento con métricas	☒	☐	No ofrece concientización ni simulaciones de phishing [14]
Recomendaciones de seguridad priorizadas con flujo de aprobación	☒	☐	SCA da recomendaciones de endurecimiento; sin priorización de negocio ni flujo de aprobación [13]

Capacidad	TecnetSOC	Wazuh SIEM y XDR abierto	Evidencia sobre Wazuh
☒ Lo ofrece ☒ Lo ofrece como complemento ☐ Parcial, limitado o requiere otro contrato ☐ Sin evidencia pública ☐ No forma parte de su oferta publicada ☐ Lo pone tu equipo			
Exposición y gestión de TI	12 de 12	2 completas +2 parciales	
Inventario unificado de activos y de software	☒	☒	Syscollector inventaría hardware, sistema, paquetes, puertos y procesos [13]
Vulnerabilidades priorizadas por gravedad y probabilidad de explotación (CVSS, EPSS)	☒	☐	Detección por CVE con CVSS y severidad; sin EPSS publicado [18]
Prioridad a las fallas que ya se están explotando (catálogo KEV de CISA)	☒	☐	CISA figura como fuente de datos; sin priorización explícita por KEV documentada [18]
Parcheo de sistema operativo y aplicaciones de terceros	☒	☐	Detecta vulnerabilidades pero no aplica parches [14]
Parcheo operado por el proveedor, con plazos publicados por severidad	☒ Críticos: 48 h (objetivo)	Lo pone tu equipo	Sin parcheo ni servicio operado con tiempos publicados [14]
Verificación de cierre: el escáner confirma que la vulnerabilidad desapareció	☒	☒	Detecta hotfixes de Windows y marca resueltas las CVE que el parche corrige [18]
Validación de parches en grupo piloto antes del despliegue	☒	☐	Sin parcheo, no hay grupo piloto [14]
Superficie de ataque externa: lo que tu empresa expone en Internet, con puntaje de riesgo	☒ Puntaje 0 a 100	☐	No ofrece superficie de ataque externa (EASM) [14]
Alertas de dominios que imitan tu marca y de credenciales o claves expuestas	☒	☐	No detecta dominios imitadores; GitHub se monitorea solo por auditoría de actividad [19]
Prueba de penetración (pentest) anual	☒ Anual	Lo pone tu equipo	No ofrece pentesting [7]
Gestión remota de equipos (RMM)	☒	☐	No es una herramienta RMM [14]
Monitoreo de disponibilidad (NOC)	☒	☐	Sin monitoreo de disponibilidad tipo NOC [14]
Respaldo y continuidad	3 de 3	0 completas +0 parciales	
Respaldo de servidores, archivos, bases de datos, máquinas virtuales y Microsoft 365	☒ Complemento	☐	No ofrece respaldo [14]
Bóveda de respaldo inmutable (no se puede alterar ni borrar), aislada por cliente	☒ Complemento	☐	No ofrece bóveda de respaldo inmutable [14]
Recuperación ante desastres con simulacros y tiempo de recuperación (RTO) medido	☒ Complemento RTO medido	☐	No ofrece recuperación ante desastres [14]
Cumplimiento	6 de 6	0 completas +2 parciales	
Evidencia mensual lista para auditores y aseguradoras	☒ Mensual	☐	Tableros de cumplimiento (PCI DSS, HIPAA, NIST, GDPR, TSC); no entrega evidencia mensual [20]
Preparación para ISO 27001, SOC 2 y PCI DSS con controles compartidos	☒ Complemento	☐	Mapea alertas a PCI DSS y TSC (SOC 2); sin ISO 27001 ni plataforma GRC [20]
Preparación normativa mexicana: CNBV Fintech, protección de datos (LFPDPPP) y NOM-024	☒ Complemento	☐	Sin marcos mexicanos (CNBV, LFPDPPP, NOM-024) [20]
Gestión de riesgos, controles, declaración de aplicabilidad y auditorías internas	☒ Complemento	☐	No gestiona riesgos, SoA ni auditorías internas [20]

Capacidad	TecnetSOC	Wazuh SIEM y XDR abierto	Evidencia sobre Wazuh
☒ Lo ofrece ☒ Lo ofrece como complemento ☒ Parcial, limitado o requiere otro contrato ☒ Sin evidencia pública	☒ No forma parte de su oferta publicada ☒ Lo pone tu equipo		
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 [20]
Continuidad de negocio, riesgo de proveedores y gestión de brechas de datos	☒ Complemento	☒	Sin módulos de continuidad, proveedores ni gestión de brechas [20]
Cómo se contrata	No suma al conteo		
Precio por dispositivo, con planes que se suman	☒ Por dispositivo	☒	Open source gratis; Cloud por niveles de agentes (100, 250, 500), no por dispositivo acumulativo [11]
Plan gratuito para empezar	☒ Hasta 10 dispositivos	☒ Sin costo de licencia	La plataforma open source es gratuita sin límite de equipos, autoalojada [14]
Prueba gratuita en tu entorno real	☒ 30 días	☒	Prueba de Wazuh Cloud de 14 días (21 vía partner), no 30 [11]
Disponible con la marca de tu proveedor de TI	☒	☒	Programa de partners con consola multiempresa y marca blanca autorizada [21]
Cobertura completa	50	6 +15 parciales	

Lo que tu equipo tendría que poner para operarla 24/7: personas, turnos, tiempos de respuesta, resumen diario, respuesta a incidentes y parcheo operado. TecnetSOC los incluye en el servicio.

SIGUIENTE PASO

De la herramienta al servicio, sin proyecto de implementación

Instalas un solo agente, ves la actividad de tus dispositivos en horas y nuestros analistas operan 24/7 en tu idioma.

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 Wazuh: Wazuh, plataforma open source (gratuita, autoalojada, la instala y opera la propia empresa) y Wazuh Cloud (SaaS de Wazuh Inc. por niveles de agentes, con precio publicado por el fabricante; Wazuh mantiene la plataforma, la empresa opera la seguridad), con soporte profesional Premium y AI Analyst de Wazuh Cloud. Oferta evaluada tal como la adopta una empresa por su cuenta, sin socio proveedor de seguridad administrada. 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.

- documentation.wazuh.com/current/user-manual/ruleset/index.html (Diferencias que se notan en el día a día)
- documentation.wazuh.com/current/upgrade-guide/index.html (Diferencias que se notan en el día a día)
- documentation.wazuh.com/current/quickstart.html (Diferencias que se notan en el día a día)
- documentation.wazuh.com/current/user-manual/capabilities/vulnerabil... (Diferencias que se notan en el día a día)
- documentation.wazuh.com/current/user-manual/capabilities/active-res... (Diferencias que se notan en el día a día)
- documentation.wazuh.com/current/proof-of-concept-guide/integrate-ne... (Diferencias que se notan en el día a día)
- wazuh.com/services/professional-support/ (Centro de operaciones (SOC) 24/7 con analistas humanos)
- documentation.wazuh.com/4.14/proof-of-concept-guide/leveraging-llms... (Agentes de IA que investigan y filtran las alertas...)
- documentation.wazuh.com/4.14/user-manual/capabilities/active-respon... (Compuerta Humana: una persona aprueba cada acción...)
- documentation.wazuh.com/4.14/cloud-service/ai-analyst.html (Asistente de investigación con IA en el portal, que...)
- wazuh.com/cloud/ (Certificación independiente de la operación (ISO 27001...))
- wazuh.com/platform/siem/ (Monitoreo continuo y correlación de eventos (SIEM),...)
- documentation.wazuh.com/4.14/user-manual/capabilities/index.html (Protección avanzada en cada equipo (EDR/XDR): malware,...)
- wazuh.com/platform/overview/ (Filtrado web en el equipo)
- documentation.wazuh.com/4.14/proof-of-concept-guide/integrate-netwo... (Detección de intrusos (IDS/IPS))
- documentation.wazuh.com/4.14/cloud-security/azure/monitoring-ms-gra... (Postura de identidad: MFA, cuentas privilegiadas y...)
- documentation.wazuh.com/4.14/cloud-security/azure/index.html (Seguridad en la nube: alertas y postura)
- documentation.wazuh.com/4.14/user-manual/capabilities/vulnerability... (Vulnerabilidades priorizadas por gravedad y...)
- documentation.wazuh.com/4.14/cloud-security/github/index.html (Alertas de dominios que imitan tu marca y de...)
- documentation.wazuh.com/4.14/compliance/index.html (Evidencia mensual lista para auditores y aseguradoras)
- wazuh.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.



Un SOC que habla tu idioma.

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