

Automox automatiza una tarea. TecnetSOC opera toda tu seguridad por ti: IA que investiga y personas que deciden.

Con Automox, incluso con Turnkey Results tú apruebas y operas, dependes del escáner de otro fabricante y la detección de ataques va en otra herramienta. En TecnetSOC, el SOC prioriza por explotación real, parchea y vigila 24/7.



44

capacidades donde TecnetSOC va más allá

6

capacidades en las que coincidimos

0

capacidades donde Automox 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 Automox: 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

Automox es una herramienta de automatización de parches que tu equipo configura; no es un servicio de SOC administrado. La detección, la respuesta y la vigilancia 24/7 son productos y servicios que se compran y se operan por separado. Este comparativo muestra, capacidad por capacidad, qué parte de lo que incluye TecnetSOC cubre Automox por sí sola y qué tendrías que sumar en productos, contratos y personal.

— LO QUE NOS HACE DISTINTOS

Diferencias que se notan en el día a día

01

Automox configura, tú operas

CON AUTOMOX

Incluso en su programa Turnkey Results, Automox configura y tú apruebas: las decisiones de parcheo y la operación diaria quedan en tu equipo. [1]

CON TECNETSOC

Nuestro SOC opera el parcheo: valida en grupo piloto e instala críticos en 48 h e importantes en 7 días, como objetivo.

02

Parchea, pero no detecta ataques

CON AUTOMOX

La detección y respuesta queda en otra herramienta: se presenta como complemento de CrowdStrike, así que EDR, SIEM y quien los vigile se contratan aparte. [2]

CON TECNETSOC

EDR/XDR, SIEM con correlación MITRE ATT&CK y analistas propios vigilando 24/7 vienen en la oferta más completa.

03

Necesitas otro escáner de vulnerabilidades

CON AUTOMOX

Para saber qué vulnerabilidades tienes dependes de un escáner de otro fabricante (CrowdStrike, Tenable o Qualys) cuyos hallazgos importas a la consola. [3]

CON TECNETSOC

Priorizamos por explotación real (KEV de CISA y EPSS) y damos una vulnerabilidad por cerrada solo cuando el escáner lo confirma.

04

Atención en horario de EE.UU

CON AUTOMOX

Abres tickets a cualquier hora, pero el horario de atención publicado es de 6 a 18 h (hora de la Montaña, EE.UU.), lunes a viernes. [4]

CON TECNETSOC

Mesa de soporte 24/7 y analistas en tu zona horaria, en español nativo y con atención multidioma.

05

Cinco tickets al mes

CON AUTOMOX

El soporte estándar permite hasta 5 tickets al mes; tickets ilimitados, puesta en marcha personalizada y revisiones trimestrales del servicio están en niveles de soporte superiores. [5]

CON TECNETSOC

La oferta más completa incluye mesa de soporte 24/7, TAM y revisiones trimestrales.

06

Lo demás, con otros proveedores

CON AUTOMOX

El propio fabricante indica que su producto es para quien ya tiene RMM y respaldo por separado; correo, identidad y nube también quedan con otros proveedores. [6]

CON TECNETSOC

Correo, identidad, nube, RMM y NOC vienen en la oferta más completa; el respaldo inmutable es un complemento aparte.

— DÓNDE ESTÁ LA DIFERENCIA

Las tres áreas con más diferencia



— CAPACIDAD POR CAPACIDAD

TecnetSOC y Automox, lado a lado

Capacidad	TecnetSOC	Automox Parcheo	Evidencia sobre Automox
✓ Lo ofrece ⊕ Lo ofrece como complemento ⓪ No forma parte de su oferta publicada Ⓜ Lo pone tu equipo Ⓜ Parcial, limitado o requiere otro contrato ? Sin evidencia pública			
Operación y servicio	14 de 14	3 completas	
Centro de operaciones (SOC) 24/7 con analistas humanos	✓	Lo pone tu equipo	Herramienta que opera el cliente o proveedor de TI; sin SOC ni NOC [4]
Agentes de IA que investigan y filtran las alertas antes de pasarlas a un analista	✓	✗	IA genera scripts y mitigaciones; no investiga alertas [7]
Compuerta Humana: una persona aprueba cada acción crítica antes de ejecutarse	✓	Ⓜ	Personas de Automox revisan mitigaciones de IA antes de publicarlas; no por acción [7]
Asistente de investigación con IA en el portal, que cita sus fuentes	✓ Neo	✗	Otto AI solo genera Worklets (scripts de automatización) desde lenguaje natural; no investiga casos [8]

Capacidad	TecnetSOC	Automox Parcheo	Evidencia sobre Automox
☒ Lo ofrece ☒ Lo ofrece como complemento ☐ No forma parte de su oferta publicada	☐ Parcial, limitado o requiere otro contrato ☐ Lo pone tu equipo	☐ Sin evidencia pública	
Operación en LATAM, EE.UU. y Europa, con analistas en tu zona horaria	☒	Lo pone tu equipo	Sin operación en LATAM; soporte en horario de la Montaña (EE.UU.) [4]
Analistas, soporte y portal en español nativo	☒	☐	Soporte en inglés; LATAM solo vía revendedores [4]
Reportes para dirección en español y en lenguaje de negocio	☒	☐	Reportes técnicos; reseñas de usuarios los señalan como insuficientes para auditoría [9]
Tiempos de notificación e inicio de investigación publicados por severidad	☒ Crítico: 30 min (objetivo)	Lo pone tu equipo	Sin SLA de notificación ni respuesta publicados [4]
Resumen ejecutivo cada mañana: lo que pasó en las últimas 24 horas	☒ 07:30	Lo pone tu equipo	Sin resumen ejecutivo diario [4]
Reportes automáticos semanales, mensuales, trimestrales y anuales	☒	☒	Tableros de Analytics programables por minutos, hora, día, semana o mes, enviados en PDF, XLSX o CSV a varios destinatarios [10]
Gerente técnico de cuenta (TAM) asignado y revisiones trimestrales	☒	Lo pone tu equipo	Niveles de soporte Preferred y Turnkey con costo extra; TAM no publicado [5]
Contacto 24/7 con personas de soporte o seguridad	☒	☐	Soporte estándar con acceso 24/7 para abrir hasta 5 tickets al mes; atención de lunes a viernes, de 6 a 18 h, hora de la Montaña (EE.UU.) [5]
Certificación independiente de la operación (ISO 27001 o SOC 2 Tipo II)	☒ ISO/IEC 27001:2022	☒	Sitio oficial lista SOC 2, CSA STAR; ISO 27001 solo según un directorio independiente [11]
Arranque rápido con un agente de software: la actividad de tus dispositivos, visible en horas	☒ Típico: 2 a 4 horas	☒	Solo nube, agente ligero, sin servidores ni VPN [4]
Detección y respuesta	15 de 15	0 completas +1 parcial	
Monitoreo continuo y correlación de eventos (SIEM), alineado con MITRE ATT&CK (marco de referencia de técnicas de ataque)	☒	☐	Sin SIEM; se integra con Splunk [4]
Protección avanzada en cada equipo (EDR/XDR): malware, ransomware y explotación de vulnerabilidades	☒	☐	Sin EDR/XDR; se integra con CrowdStrike y SentinelOne [4]
Filtrado web en el equipo	☒	☐	Sin filtrado web [4]
Detección de intrusos (IDS/IPS)	☒	☐	Sin IDS/IPS [4]
Detección de amenazas en la red interna (NDR)	☒	☐	Sin NDR [4]
Investigaciones documentadas y enriquecidas con inteligencia de amenazas	☒	☐	Sin investigaciones de amenazas [4]
Gestión de incidentes con bitácora y tiempo de atención medido por caso	☒	☐	Sin gestión de incidentes [4]
Respuesta con aislamiento de equipos y bloqueo de direcciones IP	☒	☐	Sin aislamiento nativo; solo scripts que el cliente escriba [4]
Respuesta a incidentes con análisis de causa raíz	☒	Lo pone tu equipo	Sin respuesta a incidentes ni forense [4]
Postura de identidad: MFA, cuentas privilegiadas y acceso condicional	☒	☐	Sin postura de identidad [4]
Zero Trust: DNS seguro, acceso a aplicaciones y control de aplicaciones no autorizadas (shadow IT)	☒	☐	Sin capacidades Zero Trust [4]
Seguridad en la nube: alertas y postura	☒	☐	Sin seguridad de nube [4]
Seguridad de correo: spam, phishing, malware y fraude por suplantación (BEC)	☒	☐	Sin seguridad de correo [4]
Concientización: simulaciones de phishing y entrenamiento con métricas	☒	☐	Sin concientización [4]
Recomendaciones de seguridad priorizadas con flujo de aprobación	☒	☐	Vulnerability Sync convierte hallazgos externos en tareas de remediación aprobables [12]

Capacidad	TecnetSOC	Automox Parcheo	Evidencia sobre Automox
☒ 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	3 completas +3 parciales	
Inventario unificado de activos y de software	☒	☒	Inventario de equipos y software instalado [5]
Vulnerabilidades priorizadas por gravedad y probabilidad de explotación (CVSS, EPSS)	☒	☐	No escanea; importa hallazgos de CrowdStrike, Tenable, Qualys o Rapid7 [12]
Prioridad a las fallas que ya se están explotando (catálogo KEV de CISA)	☒	☐	Sin evidencia pública de priorización KEV propia; depende del escáner externo [12]
Parcheo de sistema operativo y aplicaciones de terceros	☒	☒	Windows, macOS, Linux y más de 630 aplicaciones de terceros [5]
Parcheo operado por el proveedor, con plazos publicados por severidad	☒ Críticos: 48 h (objetivo)	Lo pone tu equipo	Sin SLA de parcheo; la responsabilidad es del cliente [4]
Verificación de cierre: el escáner confirma que la vulnerabilidad desapareció	☒	☐	Sin escáner propio; reporta estado del parche, no confirma cierre de vulnerabilidad [12]
Validación de parches en grupo piloto antes del despliegue	☒	☒	Grupos piloto con políticas escalonadas por anillos [13]
Superficie de ataque externa: lo que tu empresa expone en Internet, con puntaje de riesgo	☒ Puntaje 0 a 100	☐	Sin superficie de ataque externa [4]
Alertas de dominios que imitan tu marca y de credenciales o claves expuestas	☒	☐	Sin detección de dominios imitadores ni secretos expuestos [4]
Prueba de penetración (pentest) anual	☒ Anual	Lo pone tu equipo	Sin pentesting [4]
Gestión remota de equipos (RMM)	☒	☐	Control remoto básico (Splashtop) y Worklets; no es RMM completo [5]
Monitoreo de disponibilidad (NOC)	☒	☐	Sin monitoreo de disponibilidad ni NOC [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	☐	Reportes de cumplimiento de parches; reseñas de usuarios los señalan como insuficientes para auditoría [14]
Preparación para ISO 27001, SOC 2 y PCI DSS con controles compartidos	☒ Complemento	☐	Sin plataforma GRC [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	☐	Sin gestión de riesgos, declaración de aplicabilidad ni auditorías internas [4]

Capacidad	TecnetSOC	Automox Parcheo	Evidencia sobre Automox
☒ 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 de auditor 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 tres planes acumulativos (Patch OS, Essentials, Enterprise) [5]
Plan gratuito para empezar	☒ Hasta 10 dispositivos	☒	Sin plan gratuito; tras cancelar solo queda monitoreo gratuito, sin gestión [4]
Prueba gratuita en tu entorno real	☒ 30 días	☒	Prueba de plataforma completa; duración no publicada [5]
Disponible con la marca de tu proveedor de TI	☒	☒	multiempresa para proveedor de TI, pero sin marca del proveedor de TI [15]
Cobertura completa	50	6 +7 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 Automox: Automox, plan Automate Enterprise (el más alto) con programa proveedor de TI multi-organización, 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. www.automox.com/solutions/turnkey-results (Diferencias que se notan en el día a día)
2. www.automox.com/automox-and/crowdstrike (Diferencias que se notan en el día a día)
3. www.automox.com/platform/vulnerability-remediation (Diferencias que se notan en el día a día)
4. www.automox.com/faq (Diferencias que se notan en el día a día)
5. www.automox.com/pricing (Diferencias que se notan en el día a día)
6. www.automox.com/blog/automated-patching-solutions-compared-2026 (Diferencias que se notan en el día a día)
7. www.globenewswire.com/news-release/2026/09/10/3359585/0/en/automox-... (Agentes de IA que investigan y filtran las alertas...)
8. www.automox.com/resources/news/automox-launches-otto-ai (Asistente de investigación con IA en el portal, que...)
9. www.peerspot.com/products/automox-pros-and-cons (Reportes para dirección en español y en lenguaje de...)
10. docs.automox.com/product/Product_Documentation/Automox_Reports/Anal... (Reportes automáticos semanales, mensuales, trimestrales...)
11. www.automox.com/platform/security (Certificación independiente de la operación (ISO 27001...))
12. community.automox.com/automox-q-a-92/about-vulnerability-sync-1627 (Recomendaciones de seguridad priorizadas con flujo de...)
13. www.automox.com/blog/patch-management-best-practices (Validación de parches en grupo piloto antes del...)
14. capterra.com/p/148872/Automox/reviews/ (Evidencia mensual lista para auditores y aseguradoras)
15. www.automox.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.