

Action1 es una herramienta que tu equipo configura. TecnetSOC es un SOC agéntico que opera tu seguridad completa.

Con Action1, no hay EDR ni SIEM y su propia guía sugiere sumar un servicio de detección y respuesta administrado (MDR); tu equipo define aprobaciones, etapas y plazos, y responde por cumplirlos. En TecnetSOC, el mismo SOC que parchea vigila, investiga y responde 24/7.



42

capacidades donde TecnetSOC va más allá

8

capacidades en las que coincidimos

0

capacidades donde Action1 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 Action1: 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 multidioma
- ✓ 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

Action1 es una herramienta de parcheo y vulnerabilidades 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 Action1 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
Parchea, pero no detecta ataques

CON ACTION1
La plataforma no incluye EDR, SIEM ni respuesta a incidentes; su propia guía sugiere desplegar EDR o XDR, o contratar un proveedor MDR. [\[1\]](#)

CON TECNETSOC
La oferta más completa incluye EDR/XDR, SIEM con MITRE ATT&CK y respuesta a incidentes con análisis forense, operados por analistas propios 24/7.

02
El parcheo lo operas tú

CON ACTION1
Tu equipo configura aprobaciones, etapas de despliegue, horarios, reinicios y plazos de remediación, y responde por cumplirlos; la plataforma ejecuta lo que tú defines. [\[2\]](#)

CON TECNETSOC
El SOC opera el parcheo: prioriza por KEV y EPSS, valida en piloto e instala críticos en 48 h como objetivo.

03
Alertas a un solo correo

CON ACTION1
Cada regla de alerta avisa por correo a un solo usuario de la consola y se silencia si supera 10 por hora en un equipo. [\[3\]](#)

CON TECNETSOC
Agentes de IA investigan, correlacionan y enriquecen cada alerta, y una persona aprueba toda acción crítica antes de ejecutarla.

04
Soporte en inglés y horario hábil

CON ACTION1
Su política lista inglés como idioma de soporte para Latinoamérica, y el soporte estándar atiende de lunes a viernes, de 8 a 20 h. [\[4\]](#)

CON TECNETSOC
Analistas en tu zona horaria, en español nativo y con atención multiidioma, operan tu seguridad 24/7.

05
Reportes técnicos, no ejecutivos

CON ACTION1
Los reportes de vulnerabilidades listan CVE, CVSS, KEV y equipos afectados, exportables en CSV o HTML; traducirlos a riesgo de negocio queda en tu equipo. [\[5\]](#)

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

06
Gratis hasta 200 equipos, sin soporte del fabricante

CON ACTION1
La edición gratuita hasta 200 equipos anuncia soporte comunitario en Discord (foro de la comunidad); abrir casos con su soporte técnico es para clientes con suscripción. [\[6\]](#)

CON TECNETSOC
Desde la prueba de Response de 30 días en tu entorno real, analistas propios de TecnetOne operan tu servicio 24/7.

— DÓNDE ESTÁ LA DIFERENCIA

Las tres áreas con más diferencia

Detección y respuesta

TecnetSOC **15**

Action1 **0**

de 15 capacidades completas en esta área

Operación y servicio

TecnetSOC **14**

Action1 **2**

de 14 capacidades completas en esta área

Exposición y gestión de TI

TecnetSOC **12**

Action1 **6**

de 12 capacidades completas en esta área

— CAPACIDAD POR CAPACIDAD

TecnetSOC y Action1, lado a lado

Capacidad		TecnetSOC	Action1 Parcheo	Evidencia sobre Action1
✓ 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 y servicio		14 de 14	2 completas +2 parciales	
Centro de operaciones (SOC) 24/7 con analistas humanos	✓	Lo pone tu equipo	Herramienta autoservicio; no hay SOC ni analistas del proveedor [7]	
Agentes de IA que investigan y filtran las alertas antes de pasarlas a un analista	✓	✗	Sin agentes de IA que investiguen alertas; no maneja alertas de seguridad [7]	
Compuerta Humana: una persona aprueba cada acción crítica antes de ejecutarse	✓	✗	No aplica: el administrador define y ejecuta las políticas [7]	
Asistente de investigación con IA en el portal, que cita sus fuentes	✓ Neo	?	Sin evidencia pública de un asistente de investigación con IA en la consola [7]	

Capacidad	TecnetSOC	Action1 Parcheo	Evidencia sobre Action1
☒ Lo ofrece ☒ Lo ofrece como complemento ☐ Parcial, limitado o requiere otro contrato ☐ Sin evidencia pública	☒ Lo pone tu equipo		
☒ No forma parte de su oferta publicada			
Operación en LATAM, EE.UU. y Europa, con analistas en tu zona horaria	☒	Lo pone tu equipo	Sin operación ni oficina en LATAM; sede en Houston [7]
Analistas, soporte y portal en español nativo	☒	☒	Su política de soporte lista inglés como idioma para Latinoamérica [7]
Reportes para dirección en español y en lenguaje de negocio	☒	☒	Reportes técnicos de parches; reseñas de usuarios señalan que faltan reportes para dirección [8]
Tiempos de notificación e inicio de investigación publicados por severidad	☒ Crítico: 30 min (objetivo)	Lo pone tu equipo	Sin SLA de notificación ni de respuesta publicados [7]
Resumen ejecutivo cada mañana: lo que pasó en las últimas 24 horas	☒ 07:30	Lo pone tu equipo	Sin resumen ejecutivo diario [7]
Reportes automáticos semanales, mensuales, trimestrales y anuales	☒	☐	Reportes de parches y remediación; no hay reportes ejecutivos periódicos entregados [5]
Gerente técnico de cuenta (TAM) asignado y revisiones trimestrales	☒	Lo pone tu equipo	Programa proveedor de TI con soporte dedicado asignado; sin TAM ni revisiones trimestrales publicadas [9]
Contacto 24/7 con personas de soporte o seguridad	☒	☐	Con suscripción vigente se abren casos por correo, teléfono o web 24x7x365; la atención estándar es de lunes a viernes de 8 a 20 h, con prioridad para Severidad 1 [4]
Certificación independiente de la operación (ISO 27001 o SOC 2 Tipo II)	☒ ISO/IEC 27001:2022	☒	ISO 27001, SOC 2 Type II y TX-RAMP declarados [10]
Arranque rápido con un agente de software: la actividad de tus dispositivos, visible en horas	☒ Típico: 2 a 4 horas	☒	Nube nativa, agente ligero, puesta en marcha en minutos [7]
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 [7]
Protección avanzada en cada equipo (EDR/XDR): malware, ransomware y explotación de vulnerabilidades	☒	☒	Sin EDR/XDR [7]
Filtrado web en el equipo	☒	☒	Sin filtrado web [7]
Detección de intrusos (IDS/IPS)	☒	☒	Sin IDS/IPS [7]
Detección de amenazas en la red interna (NDR)	☒	☒	Sin NDR [7]
Investigaciones documentadas y enriquecidas con inteligencia de amenazas	☒	☒	Enriquece vulnerabilidades (VulnCheck), no investigaciones de incidentes [11]
Gestión de incidentes con bitácora y tiempo de atención medido por caso	☒	☒	Sin gestión de incidentes [7]
Respuesta con aislamiento de equipos y bloqueo de direcciones IP	☒	☒	Sin aislamiento de equipos ni bloqueo de IP como respuesta [7]
Respuesta a incidentes con análisis de causa raíz	☒	Lo pone tu equipo	Sin respuesta a incidentes ni forense [7]
Postura de identidad: MFA, cuentas privilegiadas y acceso condicional	☒	☒	Sin postura de identidad [7]
Zero Trust: DNS seguro, acceso a aplicaciones y control de aplicaciones no autorizadas (shadow IT)	☒	☒	Sin capacidades Zero Trust [7]
Seguridad en la nube: alertas y postura	☒	☒	Sin seguridad de nube [7]
Seguridad de correo: spam, phishing, malware y fraude por suplantación (BEC)	☒	☒	Sin seguridad de correo [7]
Concientización: simulaciones de phishing y entrenamiento con métricas	☒	☒	Sin concientización ni simulaciones de phishing [7]

Capacidad	TecnetSOC	Action1 Parcheo	Evidencia sobre Action1
☒ 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			
Recomendaciones de seguridad priorizadas con flujo de aprobación	☒	☐	Priorización y controles compensatorios de vulnerabilidades; limitado a parches y configuración [5]
Exposición y gestión de TI	12 de 12	6 completas +1 parcial	
Inventario unificado de activos y de software	☒	☒	Inventario de hardware y software incluido [7]
Vulnerabilidades priorizadas por gravedad y probabilidad de explotación (CVSS, EPSS)	☒	☒	Evaluación de vulnerabilidades en tiempo real con CVSS e inteligencia de explotación [5]
Prioridad a las fallas que ya se están explotando (catálogo KEV de CISA)	☒	☒	Atributo CISA KEV y uso en ransomware en cada vulnerabilidad [12]
Parcheo de sistema operativo y aplicaciones de terceros	☒	☒	Windows, macOS, Linux y más de 630 aplicaciones de terceros [13]
Parcheo operado por el proveedor, con plazos publicados por severidad	☒ Críticos: 48 h (objetivo)	Lo pone tu equipo	El cliente o proveedor de TI ejecuta; los plazos de remediación los define el cliente [5]
Verificación de cierre: el escáner confirma que la vulnerabilidad desapareció	☒	☒	El reporte vincula cada CVE con el parche que la cerró, con fecha [5]
Validación de parches en grupo piloto antes del despliegue	☒	☒	Update Rings para despliegue por fases [10]
Superficie de ataque externa: lo que tu empresa expone en Internet, con puntaje de riesgo	☒ Puntaje 0 a 100	☐	Sin superficie de ataque externa [7]
Alertas de dominios que imitan tu marca y de credenciales o claves expuestas	☒	☐	Sin detección de dominios imitadores ni secretos expuestos [7]
Prueba de penetración (pentest) anual	☒ Anual	Lo pone tu equipo	Sin pentesting [7]
Gestión remota de equipos (RMM)	☒	☐	Acceso remoto, scripts y despliegue de software; no es RMM completo [7]
Monitoreo de disponibilidad (NOC)	☒	☐	Sin monitoreo de disponibilidad ni NOC [7]
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 [7]
Bóveda de respaldo inmutable (no se puede alterar ni borrar), aislada por cliente	☒ Complemento	☐	Sin bóveda inmutable [7]
Recuperación ante desastres con simulacros y tiempo de recuperación (RTO) medido	☒ Complemento RTO medido	☐	Sin recuperación ante desastres [7]
Cumplimiento	6 de 6	0 completas +1 parcial	
Evidencia mensual lista para auditores y aseguradoras	☒ Mensual	☐	Reportes de cumplimiento de parches y remediación; no evidencia mensual gestionada [5]
Preparación para ISO 27001, SOC 2 y PCI DSS con controles compartidos	☒ Complemento	☐	Sin plataforma GRC; solo líneas base CIS, NIST, STIG (módulo aparte) [14]
Preparación normativa mexicana: CNBV Fintech, protección de datos (LFPDPPP) y NOM-024	☒ Complemento	☐	Sin normativa mexicana [7]

Capacidad	TecnetSOC	Action1 Parcheo	Evidencia sobre Action1
☒ 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		
Gestión de riesgos, controles, declaración de aplicabilidad y auditorías internas	☒ Complemento	☒	Sin gestión de riesgos, declaración de aplicabilidad ni auditorías internas [7]
Portal para tu auditor con sala de evidencias y página pública de confianza (trust center)	☒ Complemento	☒	Sin portal de auditor ni Trust Center para el cliente [7]
Continuidad de negocio, riesgo de proveedores y gestión de brechas de datos	☒ Complemento	☒	Sin continuidad de negocio ni gestión de proveedores [7]
Cómo se contrata	No suma al conteo		
Precio por dispositivo, con planes que se suman	☒ Por dispositivo	☒	Por equipo, pero un solo plan; módulos extra licenciados aparte [15]
Plan gratuito para empezar	☒ Hasta 10 dispositivos	☒ Hasta 200 dispositivos	Edición gratuita permanente hasta 200 equipos, con todas las funciones [10]
Prueba gratuita en tu entorno real	☒ 30 días	☒	Nivel gratis funciona como prueba permanente en entorno real [10]
Disponible con la marca de tu proveedor de TI	☒	☒	Reventa por proveedor de TI permitida, pero sin marca del proveedor de TI [9]
Cobertura completa	50	8 +5 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 Action1: Action1, plataforma Autonomous Endpoint Management en su nivel más alto (Enterprise para proveedor de TI, con módulos Configuration Management y Enrollment and Provisioning), 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.action1.com/blog/endpoint-management/endpoint-security-management/ (Diferencias que se notan en el día a día)
2. www.action1.com/documentation/review-and-approve-updates/ (Diferencias que se notan en el día a día)
3. www.action1.com/documentation/alerts/ (Diferencias que se notan en el día a día)
4. www.action1.com/legal/support-policy/ (Diferencias que se notan en el día a día)
5. www.action1.com/documentation/vulnerability-management/ (Diferencias que se notan en el día a día)
6. www.action1.com/pricing/ (Diferencias que se notan en el día a día)
7. ifeeltech.com/blog/action1-review-free-patch-management (Centro de operaciones (SOC) 24/7 con analistas humanos)
8. www.capterra.com/p/180609/Action1-RMM/reviews/ (Reportes para dirección en español y en lenguaje de...)
9. www.prnewswire.com/news-releases/action1-unveils-msp-partner-progra... (Gerente técnico de cuenta (TAM) asignado y revisiones...)
10. www.prnewswire.com/news-releases/action1-expands-its-free-offering-... (Certificación independiente de la operación (ISO 27001...))
11. www.prnewswire.com/news-releases/action1-expands-vulnerability-inte... (Investigaciones documentadas y enriquecidas con...)
12. www.action1.com/blog/kev-catalog-integration-enhancing-vulnerabilit... (Prioridad a las fallas que ya se están explotando...)
13. www.prnewswire.com/news-releases/action1-expands-to-linux-deliverin... (Parcheo de sistema operativo y aplicaciones de terceros)
14. www.prnewswire.com/news-releases/action1-expands-endpoint-managemen... (Preparación para ISO 27001, SOC 2 y PCI DSS con...)
15. mspcompared.com/action1/pricing/ (Precio por dispositivo, con planes que se suman)

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.