

FortiSOAR automatiza lo que tu equipo diseña. TecnetSOC investiga, decide y responde por ti, con una persona en lo crítico.

Con FortiSOAR, SIEM, EDR y correo se compran aparte, tu equipo opera casos y automatizaciones y el arranque se cotiza como proyecto aparte. TecnetSOC ya trae plataforma y analistas 24/7, y está operativo en menos de 7 días.



44

capacidades donde TecnetSOC va más allá

6

capacidades en las que coincidimos

0

capacidades donde FortiSOAR 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 FortiSOAR: 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

FortiSOAR es una plataforma de orquestación y automatización de respuesta: no detecta amenazas por sí sola ni es un servicio de SOC administrado. El SIEM, el EDR y las demás herramientas que coordina son productos que se compran y se operan por separado. Este comparativo muestra, capacidad por capacidad, qué parte de lo que incluye TecnetSOC cubre FortiSOAR 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
Tu equipo tiene que operarlo

CON FORTISOAR
Compras una plataforma para que tu SOC la opere: tu equipo atiende casos y playbooks, y el turno 24/7 lo cubres tú o un servicio aparte. [\[1\]](#)

CON TECNETSOC
Analistas propios de TecnetOne operan tu seguridad 24/7, en tu zona horaria y en español nativo.

02
Orquesta herramientas que compras aparte

CON FORTISOAR
No trae SIEM, EDR, firewall ni seguridad de correo propios: coordina los que ya compraste y licencias por separado. [\[1\]](#)

CON TECNETSOC
La oferta más completa ya incluye SIEM, EDR/XDR, IDS/IPS, NDR, filtrado web y seguridad de correo.

03
IA con límite mensual de uso

CON FORTISOAR
La IA agéntica incluye 5 millones de tokens al mes por instancia, unas 60 investigaciones según Fortinet; para más, compras paquetes adicionales de tokens. [\[1\]](#)

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

04
Muestra vulnerabilidades, pero no las parchea

CON FORTISOAR
La vista de vulnerabilidades sale de escáneres externos que integras y licencias aparte, y el parcheo depende de tu equipo y otras herramientas. [\[2\]](#)

CON TECNETSOC
El SOC prioriza el parcheo por explotación real (KEV y EPSS), valida en piloto y da por cerrada cada vulnerabilidad solo cuando el escáner lo confirma.

05
Arranque con servicios profesionales aparte

CON FORTISOAR
Eliges despliegue, tamaño, complementos y capacitación, y Fortinet ofrece aparte Quick-Start, proyectos de alcance definido (SOW) cobrados por día o un Resident Engineer de 6 a 12 meses. [\[1\]](#)

CON TECNETSOC
Instalas un agente, ves actividad en 2 a 4 horas y operas en menos de 7 días, sin proyecto de implementación ni oficina de proyectos.

06
Servidores que tú dimensionas

CON FORTISOAR
Instalas y mantienes servidores RHEL o Rocky Linux desde 8 vCPU y 24 GB de RAM, o eliges su nube hospedada, que de todas formas opera tu equipo. [\[2\]](#)

CON TECNETSOC
La plataforma es un servicio en la nube operado por TecnetOne: no instalas ni mantienes servidores.

— DÓNDE ESTÁ LA DIFERENCIA

Las tres áreas con más diferencia

Detección y respuesta

TecnetSOC **15**

FortiSOAR **2**

de 15 capacidades completas en esta área

Exposición y gestión de TI

TecnetSOC **12**

FortiSOAR **0**

de 12 capacidades completas en esta área

Operación y servicio

TecnetSOC **14**

FortiSOAR **4**

de 14 capacidades completas en esta área

— CAPACIDAD POR CAPACIDAD

TecnetSOC y FortiSOAR, lado a lado

Capacidad	TecnetSOC	FortiSOAR Orquestación	Evidencia sobre FortiSOAR
✓ Lo ofrece ✗ No forma parte de su oferta publicada + Lo ofrece como complemento ● Lo pone tu equipo ○ Parcial, limitado o requiere otro contrato ? Sin evidencia pública			
Operación y servicio	14 de 14	4 completas +2 parciales	
Centro de operaciones (SOC) 24/7 con analistas humanos	✓	Lo pone tu equipo	El producto no incluye SOC; SOC 24/7 solo con FortiGuard SOCaaS, servicio aparte [3]
Agentes de IA que investigan y filtran las alertas antes de pasarlas a un analista	✓	✓	19 agentes de IA; triaje automático cierra alertas rutinarias y agrupa las prioritarias [2]
Compuerta Humana: una persona aprueba cada acción crítica antes de ejecutarse	✓	✓	Flujos "in-the-loop" con intervención manual configurables en playbooks [4]

Capacidad	TecnetSOC	FortiSOAR Orquestación	Evidencia sobre FortiSOAR
☒ 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			
Asistente de investigación con IA en el portal, que cita sus fuentes	☒ Neo	☐	Asistente FortiAI en cada caso, con contexto e inteligencia; sin evidencia de citas fechadas [2]
Operación en LATAM, EE.UU. y Europa, con analistas en tu zona horaria	☒	Lo pone tu equipo	Software operado por el cliente; SOCaaS de Fortinet opera desde Norteamérica, EMEA y APAC [3]
Analistas, soporte y portal en español nativo	☒	☐	Soporte FortiCare de Fortinet, con atención telefónica publicada en inglés y español; no incluye analistas de seguridad [5]
Reportes para dirección en español y en lenguaje de negocio	☒	☐	Tableros y reportes configurables; sin evidencia de reportes ejecutivos en español [2]
Tiempos de notificación e inicio de investigación publicados por severidad	☒ Crítico: 30 min (objetivo)	Lo pone tu equipo	Sin SLA del proveedor; mide SLA del equipo del cliente. SOCaaS aparte notifica en 15 min [3]
Resumen ejecutivo cada mañana: lo que pasó en las últimas 24 horas	☒ 07:30	Lo pone tu equipo	Sin resumen ejecutivo diario [2]
Reportes automáticos semanales, mensuales, trimestrales y anuales	☒	☒	Reportes programados por hora, día, semana, mes o año, enviados por correo a una lista de destinatarios [6]
Gerente técnico de cuenta (TAM) asignado y revisiones trimestrales	☒	Lo pone tu equipo	Resident Engineer o TAM de FortiCare Advanced Support, contratos aparte [1]
Contacto 24/7 con personas de soporte o seguridad	☒	☒	FortiCare Premium 24x7 incluido en la suscripción [2]
Certificación independiente de la operación (ISO 27001 o SOC 2 Tipo II)	☒ ISO/IEC 27001:2022	☐	ISO 27001 cubre FortiGuard y FortiCloud; en autohospedado la operación es del cliente [7]
Arranque rápido con un agente de software: la actividad de tus dispositivos, visible en horas	☒ Típico: 2 a 4 horas	☐	Requiere dimensionar nodos, integrar conectores y servicios de arranque (Quick-Start) [1]
Detección y respuesta	15 de 15	2 completas +5 parciales	
Monitoreo continuo y correlación de eventos (SIEM), alineado con MITRE ATT&CK (marco de referencia de técnicas de ataque)	☒	☐	No es SIEM; recibe y correlaciona alertas con MITRE ATT&CK. SIEM es FortiSIEM, aparte [2]
Protección avanzada en cada equipo (EDR/XDR): malware, ransomware y explotación de vulnerabilidades	☒	☐	Sin EDR propio; orquesta FortiEDR u otros EDR comprados aparte [8]
Filtrado web en el equipo	☒	☐	Sin filtrado web; FortiClient o FortiProxy, aparte [9]
Detección de intrusos (IDS/IPS)	☒	☐	Sin IDS/IPS; orquesta FortiGate u otros firewalls, aparte [10]
Detección de amenazas en la red interna (NDR)	☒	☐	Sin NDR; conector a FortiNDR, producto aparte [11]
Investigaciones documentadas y enriquecidas con inteligencia de amenazas	☒	☒	Enriquecimiento automático y módulo TIM con FortiGuard como complemento propio [2]
Gestión de incidentes con bitácora y tiempo de atención medido por caso	☒	☒	Gestión completa de casos, sala de crisis (war room), bitácora forense de actividad y SLA [2]
Respuesta con aislamiento de equipos y bloqueo de direcciones IP	☒	☐	Bloquea indicadores y aísla vía conectores; depende de firewall o EDR aparte [2]
Respuesta a incidentes con análisis de causa raíz	☒	Lo pone tu equipo	Registro forense de la sala de crisis; el análisis forense es un servicio FortiGuard IR aparte [12]
Postura de identidad: MFA, cuentas privilegiadas y acceso condicional	☒	☐	Sin postura de identidad; solo acciones vía conectores a IdP [2]
Zero Trust: DNS seguro, acceso a aplicaciones y control de aplicaciones no autorizadas (shadow IT)	☒	☐	Sin Zero Trust propio; FortiSASE es producto aparte [13]
Seguridad en la nube: alertas y postura	☒	☐	Automatiza operaciones de nube vía conectores; sin postura de nube propia [2]
Seguridad de correo: spam, phishing, malware y fraude por suplantación (BEC)	☒	☐	Sin seguridad de correo; orquesta FortiMail, producto aparte [14]

Capacidad	TecnetSOC	FortiSOAR Orquestación	Evidencia sobre FortiSOAR
☒ 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			
Concientización: simulaciones de phishing y entrenamiento con métricas	☒	☐	Sin concientización; servicio Fortinet Security Awareness aparte [15]
Recomendaciones de seguridad priorizadas con flujo de aprobación	☒	☐	Recomendaciones de respuesta por ML y GenAI; sin flujo de aprobación de postura [2]
Exposición y gestión de TI	12 de 12	0 completas +3 parciales	
Inventario unificado de activos y de software	☒	☐	Perfiles de activos desde sistemas integrados; no descubre activos ni software por sí mismo [2]
Vulnerabilidades priorizadas por gravedad y probabilidad de explotación (CVSS, EPSS)	☒	☐	Gestión de vulnerabilidades a partir de escáneres externos (Qualys, Tenable, Rapid7) [2]
Prioridad a las fallas que ya se están explotando (catálogo KEV de CISA)	☒	☐	Sin evidencia de priorización por catálogo KEV de CISA [2]
Parcheo de sistema operativo y aplicaciones de terceros	☒	☐	Automatiza actualizaciones vía playbooks; parcheo real en FortiClient EMS u otros, aparte [2]
Parcheo operado por el proveedor, con plazos publicados por severidad	☒ Críticos: 48 h (objetivo)	Lo pone tu equipo	Sin parcheo operado por Fortinet con tiempos publicados [4]
Verificación de cierre: el escáner confirma que la vulnerabilidad desapareció	☒	☐	Sin verificación de cierre documentada [2]
Validación de parches en grupo piloto antes del despliegue	☒	☐	Sin validación de parches en grupo piloto [2]
Superficie de ataque externa: lo que tu empresa expone en Internet, con puntaje de riesgo	☒ Puntaje 0 a 100	☐	Sin EASM propio; FortiRecon es producto aparte [16]
Alertas de dominios que imitan tu marca y de credenciales o claves expuestas	☒	☐	Protección de marca y fugas en FortiRecon, producto aparte [16]
Prueba de penetración (pentest) anual	☒ Anual	Lo pone tu equipo	Sin pentesting incluido [4]
Gestión remota de equipos (RMM)	☒	☐	No es RMM; solo automatiza tareas vía conectores [2]
Monitoreo de disponibilidad (NOC)	☒	☐	Sin monitoreo de disponibilidad propio; FortiSIEM lo hace, aparte [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 de servidores, VMs ni Microsoft 365 [4]
Bóveda de respaldo inmutable (no se puede alterar ni borrar), aislada por cliente	☒ Complemento	☐	Sin bóveda inmutable de respaldo [4]
Recuperación ante desastres con simulacros y tiempo de recuperación (RTO) medido	☒ Complemento RTO medido	☐	Alta disponibilidad y recuperación solo de la propia plataforma, no de los sistemas del cliente [1]
Cumplimiento	6 de 6	0 completas +2 parciales	
Evidencia mensual lista para auditores y aseguradoras	☒ Mensual	☐	Tableros y reportes de cumplimiento; no entrega paquete mensual de evidencia [2]
Preparación para ISO 27001, SOC 2 y PCI DSS con controles compartidos	☒ Complemento	☐	Mapeo a NIST CSF, ISO 27001, GDPR y SOC 2; no es plataforma GRC completa [2]
Preparación normativa mexicana: CNBV Fintech, protección de datos (LFPDPPP) y NOM-024	☒ Complemento	☐	Sin normativa mexicana (CNBV, LFPDPPP, NOM-024) [2]

Capacidad	TecnetSOC	FortiSOAR Orquestación	Evidencia sobre FortiSOAR
☒ 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	☐	Flujos de cumplimiento, pero sin registro de riesgos, declaración de aplicabilidad ni auditorías internas [2]
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 [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	☐	Se licencia por edición, nodo y usuario concurrente, no por dispositivo [1]
Plan gratuito para empezar	☒ Hasta 10 dispositivos	☐	Licencia de prueba sin vencimiento: 2 usuarios y 1000 acciones por día [17]
Prueba gratuita en tu entorno real	☒ 30 días	☒	Licencia de prueba desde FortiCare, instalable en entorno propio [17]
Disponible con la marca de tu proveedor de TI	☒	☒	Edición multiempresa para proveedor de seguridad administrada con marca propia configurable [1]
Cobertura completa	50	6 +12 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 FortiSOAR: Fortinet FortiSOAR 8.0 (VM autohospedada o FortiSOAR Cloud PaaS; suscripción o FortiFlex por edición Starter, Enterprise o multiempresa, por nodos y usuarios concurrentes, 2 incluidos; complemento propio TIM con FortiGuard; incluye 5 millones de tokens FortiAI al mes; lo opera el equipo del cliente o su proveedor de seguridad administrada, no Fortinet), 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.fortinet.com/content/dam/fortinet/assets/data-sheets/og-fortisoar... (Diferencias que se notan en el día a día)
2. www.fortinet.com/content/dam/fortinet/assets/data-sheets/fortisoar.pdf (Diferencias que se notan en el día a día)
3. www.fortinet.com/products/socaas (Centro de operaciones (SOC) 24/7 con analistas humanos)
4. www.fortinet.com/products/fortisoar (Compuerta Humana: una persona aprueba cada acción...)
5. www.fortinet.com/support/contact (Analistas, soporte y portal en español nativo)
6. docs.fortinet.com/document/fortisoar/7.0.0/user-guide/292560/report... (Reportes automáticos semanales, mensuales, trimestrales...)
7. www.fortinet.com/corporate/about-us/product-certifications/iso27001... (Certificación independiente de la operación (ISO 27001...))
8. www.fortinet.com/products/endpoint-security/fortiedr (Protección avanzada en cada equipo (EDR/XDR): malware,...)
9. www.fortinet.com/products/endpoint-security/forticlient (Filtrado web en el equipo)
10. www.fortinet.com/products/next-generation-firewall (Detección de intrusos (IDS/IPS))
11. www.fortinet.com/products/network-detection-and-response (Detección de amenazas en la red interna (NDR))
12. www.fortinet.com/support/support-services/fortiguard-security-subsc... (Respuesta a incidentes con análisis de causa raíz)
13. www.fortinet.com/products/sase (Zero Trust: DNS seguro, acceso a aplicaciones y control...)
14. www.fortinet.com/products/email-security/fortimail (Seguridad de correo: spam, phishing, malware y fraude...)
15. www.fortinet.com/training/security-awareness-training (Concientización: simulaciones de phishing y...)
16. www.fortinet.com/products/fortirecon (Superficie de ataque externa: lo que tu empresa expone...)
17. docs.fortinet.com/document/fortisoar/7.6.5/deployment-guide/223944/... (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.