

FortiSIEM es un SIEM que tu equipo opera. TecnetSOC es un SOC agéntico que lo opera por ti, 24/7.

Con FortiSIEM, tu equipo instala y mantiene servidores, afina detecciones, licencia aparte los eventos extra y responde a toda hora; el SOC 24/7 es otro servicio. Con TecnetSOC, analistas de TecnetOne operan la correlación MITRE ATT&CK por ti.



43

capacidades donde TecnetSOC va más allá

7

capacidades en las que coincidimos

0

capacidades donde FortiSIEM supera a TecnetSOC

De las 50: 43 donde vamos más allá y 7 en las que coincidimos

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

FortiSIEM es una plataforma SIEM que tu equipo instala, configura y vigila; no es un servicio de SOC administrado. Lo que FortiSIEM no cubre se completa con otros productos de Fortinet, cada uno con su licencia y su operación. Este comparativo muestra, capacidad por capacidad, qué parte de lo que incluye TecnetSOC cubre FortiSIEM por sí sola y qué tendrías que sumar en productos, contratos y personal.

Diferencias que se notan en el día a día

01

Tu equipo vigila y responde

CON FORTISIAM

Compras la plataforma y tu equipo vigila, investiga y responde a toda hora; si no tienes turnos 24/7, contratas un proveedor aparte. [\[1\]](#)

CON TECNETSOC

Analistas propios de TecnetOne vigilan, investigan y responden 24/7, en tu zona horaria y en español nativo.

02

Servidores y almacenamiento a tu cargo

CON FORTISIAM

Si lo hospedas tú, instalas y mantienes sus componentes (Supervisor, Workers y Collectors) y su almacenamiento; en su nube, licencias cómputo y almacenamiento por separado. [\[1\]](#)

CON TECNETSOC

Instalas un agente y el resto se despliega solo: actividad visible en 2 a 4 horas, sin servidores que mantener.

03

Tu equipo administra las detecciones

CON FORTISIAM

Tu equipo administra sus más de 2800 reglas y las detecciones SIGMA o de ML que agregue; Fortinet forma administradores en un curso de 15 horas. [\[2\]](#)

CON TECNETSOC

No contratas ni capacitas especialistas en SIEM: analistas de TecnetOne operan la correlación MITRE ATT&CK por ti.

04

Cada evento extra se licencia

CON FORTISIAM

Cada dispositivo licenciado trae 10 eventos por segundo; los eventos por segundo (EPS) adicionales, el análisis de comportamiento de usuarios (UEBA), los agentes avanzados, el servicio IOC y la automatización se licencian aparte. [\[1\]](#)

CON TECNETSOC

Pagas por dispositivo con planes acumulativos; Visibility es gratis hasta 10 dispositivos y Response se prueba 30 días en tu entorno real.

05

Recolecta eventos, no protege equipos

CON FORTISIAM

Su agente recolecta eventos, integridad de archivos y consultas Osquery; bloquear amenazas en equipos, correo o red exige FortiEDR, FortiMail, FortiGate u otros productos. [\[1\]](#)

CON TECNETSOC

La oferta más completa incluye protección avanzada en cada equipo (EDR/XDR), filtrado web, IDS/IPS, NDR y seguridad de correo.

06

Ve parches, no los instala

CON FORTISIAM

Ves los parches instalados e ingieres tus escáneres, pero no parchea: escanear, instalar y confirmar el cierre queda en otros productos y tu equipo. [\[1\]](#)

CON TECNETSOC

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

Las tres áreas con más diferencia

Operación y servicio

TecnetSOC 14

FortiSIEM 2

de 14 capacidades completas en esta área

Detección y respuesta

TecnetSOC 15

FortiSIEM 3

de 15 capacidades completas en esta área

Exposición y gestión de TI

TecnetSOC 12

FortiSIEM 2

de 12 capacidades completas en esta área

TecnetSOC y FortiSIEM, lado a lado

Capacidad	TecnetSOC	FortiSIEM SIEM	Evidencia sobre FortiSIEM
✓ 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	2 completas +3 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	✓	Ⓜ	FortiAI-Assist con agentes para análisis de eventos e incidentes; no filtra toda alerta automáticamente [1]
Compuerta Humana: una persona aprueba cada acción crítica antes de ejecutarse	✓	✗	Playbooks basados en FortiSOAR; no hay compuerta humana obligatoria documentada en la ficha [1]

Capacidad	TecnetSOC	FortiSIEM SIEM	Evidencia sobre FortiSIEM
☒ 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	
Asistente de investigación con IA en el portal, que cita sus fuentes	☒ Neo	☐	FortiAI-Assist GenAI guía investigación y búsquedas; sin evidencia de citas con fecha [1]
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	☒	☐	FortiCare publica un teléfono global de soporte en inglés y español; sin evidencia de analistas de seguridad ni portal en español [4]
Reportes para dirección en español y en lenguaje de negocio	☒	☐	Más de 1300 reportes de cumplimiento técnicos; sin evidencia de reportes ejecutivos en español [1]
Tiempos de notificación e inicio de investigación publicados por severidad	☒ Crítico: 30 min (objetivo)	Lo pone tu equipo	Sin SLA en el producto; el SOCaaS, servicio aparte, publica notificación en un máximo de 15 minutos [3]
Resumen ejecutivo cada mañana: lo que pasó en las últimas 24 horas	☒ 07:30	Lo pone tu equipo	Sin resumen ejecutivo diario; solo reportes programados que el cliente configura [1]
Reportes automáticos semanales, mensuales, trimestrales y anuales	☒	☒	Reportes programables con entrega por correo a interesados [1]
Gerente técnico de cuenta (TAM) asignado y revisiones trimestrales	☒	Lo pone tu equipo	TAM solo con FortiCare Advanced Support Pro, contrato aparte [5]
Contacto 24/7 con personas de soporte o seguridad	☒	☒	Contrato FortiCare 24x7 incluido o vendido con la licencia [1]
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 [6]
Arranque rápido con un agente de software: la actividad de tus dispositivos, visible en horas	☒ Típico: 2 a 4 horas	☐	Arquitectura Supervisor, Workers y Collectors; requiere proyecto de implementación [1]
Detección y respuesta	15 de 15	3 completas +4 parciales	
Monitoreo continuo y correlación de eventos (SIEM), alineado con MITRE ATT&CK (marco de referencia de técnicas de ataque)	☒	☒	Más de 2800 reglas de correlación, UEBA, mapeo MITRE ATT&CK [7]
Protección avanzada en cada equipo (EDR/XDR): malware, ransomware y explotación de vulnerabilidades	☒	☐	No incluye EDR; FortiEDR es producto aparte. Su agente solo recolecta eventos, integridad de archivos (FIM) y consultas Osquery [8]
Filtrado web en el equipo	☒	☐	No filtra web; solo ingiere logs. Filtrado en FortiClient o FortiProxy, aparte [9]
Detección de intrusos (IDS/IPS)	☒	☐	No es IDS/IPS; ingiere eventos de IPS. IPS en FortiGate, aparte [10]
Detección de amenazas en la red interna (NDR)	☒	☐	Análisis de NetFlow y descubrimiento sin agente; la detección en red completa (NDR) es FortiNDR, producto aparte [11]
Investigaciones documentadas y enriquecidas con inteligencia de amenazas	☒	☒	Enriquecimiento automático con FortiGuard y fuentes externas de inteligencia; servicio IOC como complemento propio [1]
Gestión de incidentes con bitácora y tiempo de atención medido por caso	☒	☒	Gestión de casos integrada, Incident Explorer y ciclo de vida del incidente [1]
Respuesta con aislamiento de equipos y bloqueo de direcciones IP	☒	☐	Scripts y playbooks de remediación; ejecución depende de firewall o EDR de terceros [1]
Respuesta a incidentes con análisis de causa raíz	☒	Lo pone tu equipo	Osquery da detalle forense del equipo; respuesta forense es servicio FortiGuard IR aparte [12]
Postura de identidad: MFA, cuentas privilegiadas y acceso condicional	☒	☐	UEBA y eventos de identidad (AD, Okta); sin evaluación de postura de identidad [1]
Zero Trust: DNS seguro, acceso a aplicaciones y control de aplicaciones no autorizadas (shadow IT)	☒	☐	Sin Zero Trust propio; ZTNA, DNS y shadow IT en FortiSASE, aparte [13]
Seguridad en la nube: alertas y postura	☒	☐	Ingiere logs de nube y se despliega en Azure; sin postura de Azure [1]
Seguridad de correo: spam, phishing, malware y fraude por suplantación (BEC)	☒	☐	Sin seguridad de correo propia; FortiMail es producto aparte [14]

Capacidad	TecnetSOC	FortiSIEM SIEM	Evidencia sobre FortiSIEM
✓ 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			
Concientización: simulaciones de phishing y entrenamiento con métricas	✓	✗	Sin concientización; servicio Fortinet Security Awareness aparte [15]
Recomendaciones de seguridad priorizadas con flujo de aprobación	✓	✗	Puntuación de riesgo por usuario y host; sin recomendaciones con flujo de aprobación [1]
Exposición y gestión de TI	12 de 12	2 completas +1 parcial	
Inventario unificado de activos y de software	✓	✓	CMDB con descubrimiento automático, configuración, software instalado y parches [1]
Vulnerabilidades priorizadas por gravedad y probabilidad de explotación (CVSS, EPSS)	✓	○	Integra escáneres de vulnerabilidades para riesgo; no escanea por sí mismo ni usa EPSS [1]
Prioridad a las fallas que ya se están explotando (catálogo KEV de CISA)	✓	?	Sin evidencia de priorización por catálogo KEV de CISA [1]
Parcheo de sistema operativo y aplicaciones de terceros	✓	✗	Sin parcheo en FortiSIEM; parcheo de vulnerabilidades en FortiClient EMS, aparte [9]
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 [7]
Verificación de cierre: el escáner confirma que la vulnerabilidad desapareció	✓	✗	Sin verificación de cierre de vulnerabilidades documentada [1]
Validación de parches en grupo piloto antes del despliegue	✓	✗	Sin validación de parches en grupo piloto [1]
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 en el producto [7]
Gestión remota de equipos (RMM)	✓	✗	Monitorea desempeño, pero no gestiona equipos de forma remota (no es RMM) [1]
Monitoreo de disponibilidad (NOC)	✓	✓	Monitoreo de disponibilidad, desempeño, transacciones sintéticas y cálculo de SLA [1]
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 [7]
Bóveda de respaldo inmutable (no se puede alterar ni borrar), aislada por cliente	Complemento	✗	Sin bóveda inmutable de respaldo [7]
Recuperación ante desastres con simulacros y tiempo de recuperación (RTO) medido	Complemento RTO medido	✗	Alta disponibilidad y recuperación solo del propio SIEM, no de tus sistemas [1]
Cumplimiento	6 de 6	0 completas +2 parciales	
Evidencia mensual lista para auditores y aseguradoras	✓ Mensual	○	Reportes de cumplimiento listos; no entrega paquete mensual de evidencia [1]
Preparación para ISO 27001, SOC 2 y PCI DSS con controles compartidos	Complemento	○	Reportes para ISO 27001, PCI, HIPAA, NIST; no es plataforma GRC ni mapea SOC 2 [1]
Preparación normativa mexicana: CNBV Fintech, protección de datos (LFPDPPP) y NOM-024	Complemento	✗	Sin normativa mexicana (CNBV, LFPDPPP, NOM-024) [1]

Capacidad	TecnetSOC	FortiSIEM SIEM	Evidencia sobre FortiSIEM
☒ 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 registro de riesgos, SoA ni auditorías internas [1]
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 [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	☒	Licencia por dispositivo y EPS, pero sin planes acumulativos [1]
Plan gratuito para empezar	☒ Hasta 10 dispositivos	☒	Sin plan gratuito permanente [1]
Prueba gratuita en tu entorno real	☒ 30 días	☒	La página ofrece prueba gratuita; duración y condiciones no publicadas [7]
Disponible con la marca de tu proveedor de TI	☒	☒	Multiinquilino para proveedor de seguridad administrada, con permisos por cliente y logo propio [1]
Cobertura completa	50	7 +10 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 FortiSIEM: Fortinet FortiSIEM (software, VM, appliance o FortiSIEM Cloud SaaS; licencia por dispositivo + EPS, GB/día o FCU en la nube, suscripción o perpetua; complementos propios UEBA, Advanced Agent, IOC Service y Automation Service; 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/FortiSIEM.pdf (Diferencias que se notan en el día a día)
2. training.fortinet.com/local/staticpage/view.php (Diferencias que se notan en el día a día)
3. www.fortinet.com/products/soc/soc (Centro de operaciones (SOC) 24/7 con analistas humanos)
4. www.fortinet.com/support/contact (Analistas, soporte y portal en español nativo)
5. www.fortinet.com/support/advanced-support (Gerente técnico de cuenta (TAM) asignado y revisiones...)
6. www.fortinet.com/corporate/about-us/product-certifications/iso27001... (Certificación independiente de la operación (ISO 27001...))
7. www.fortinet.com/products/siem/fortisiem (Monitoreo continuo y correlación de eventos (SIEM),...)
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...)

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.