

CrowdStrike protege tus equipos; su vigilancia 24/7 se contrata aparte. TecnetSOC opera tu seguridad por ti, con el caso resuelto en tu idioma.

Con CrowdStrike, el correo y el respaldo vienen de otros fabricantes, y su parcheo por riesgo sigue anunciado como próximo. En TecnetSOC, el SOC parchea, la protección de correo va incluida y puedes sumar respaldo inmutable y recuperación ante desastres con TecnetProtect.



32

capacidades donde TecnetSOC va más allá

18

capacidades en las que coincidimos

0

capacidades donde CrowdStrike supera a TecnetSOC

De las 50: 32 donde vamos más allá y 18 en las que coincidimos

Misma lista de 50 capacidades y mismo criterio para TecnetSOC y CrowdStrike: 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)

— ANTES DE COMPARAR

CrowdStrike es una plataforma de protección de equipos (EDR/XDR) que se compra por paquetes y módulos; con Falcon Complete, su servicio administrado con costo aparte, sus analistas vigilan y responden 24/7. Correo, respaldo y detección en la red vienen de otros fabricantes integrados con Falcon. Aquí comparamos la plataforma, Falcon Complete y sus módulos propios con lo que incluye TecnetSOC, capacidad por capacidad.

— LO QUE NOS HACE DISTINTOS

Diferencias que se notan en el día a día

01

El parcheo queda de tu lado

CON CROWDSTRIKE

Exposure Management prioriza vulnerabilidades, pero el parcheo por riesgo de Falcon for IT sigue marcado como próximo y Falcon Complete no publica que su equipo instale parches. [1]

CON TECNETSOC

El SOC parchea por explotación real (KEV y EPSS), con plazos objetivo por severidad, válida en grupo piloto y da por cerrado solo cuando el escáner confirma.

02

Tu correo lo protege otro fabricante

CON CROWDSTRIKE

No hay seguridad de correo propia: Next-Gen SIEM analiza las señales de productos de correo de otros fabricantes, como Abnormal, Mimecast o Proofpoint. [2]

CON TECNETSOC

La protección contra spam, phishing, malware y suplantación (BEC) va dentro del mismo servicio, con cuarentena en autoservicio.

03

El respaldo viene de un aliado

CON CROWDSTRIKE

El respaldo no forma parte de su portafolio: su alianza con Rubrik suma el respaldo y la restauración de ese fabricante a la detección de Falcon. [3]

CON TECNETSOC

Puedes sumar TecnetProtect (costo aparte): respaldo en bóveda inmutable por cliente y recuperación ante desastres con simulacros y RTO medido.

04

La vigilancia de tu red interna, con sensores de otro fabricante

CON CROWDSTRIKE

La detección de intrusos y de amenazas en la red interna (IDS, NDR) llega con sensores de otros fabricantes, como Corelight, integrados en Next-Gen SIEM. [4]

CON TECNETSOC

La detección en la red interna (NDR) y el IDS/IPS van incluidos en la oferta más completa, con un sensor en puerto espejo.

05

Cumplimiento: herramientas, no solución

CON CROWDSTRIKE

Su propia página de cumplimiento aclara que sus productos y servicios no son soluciones de cumplimiento, sino herramientas que apoyan tu programa. [5]

CON TECNETSOC

Recibes evidencia mensual para auditores y aseguradoras y, con TecnetGRC (costo aparte), preparas ISO 27001, SOC 2, PCI DSS y normativa mexicana.

06

Sin analistas publicados en LATAM

CON CROWDSTRIKE

Falcon Complete no publica dónde están sus analistas ni en qué idioma atienden; el soporte en español que anunció lo dan distribuidores autorizados en Europa. [6]

CON TECNETSOC

Operamos en LATAM, EE.UU. y Europa, con analistas en tu zona horaria y atención en español nativo.

— DÓNDE ESTÁ LA DIFERENCIA

Las tres áreas con más diferencia

Detección y respuesta

TecnetSOC 15

CrowdStrike 7

de 15 capacidades completas en esta área

Exposición y gestión de TI

TecnetSOC 12

CrowdStrike 4

de 12 capacidades completas en esta área

Operación y servicio

TecnetSOC 14

CrowdStrike 7

de 14 capacidades completas en esta área

— CAPACIDAD POR CAPACIDAD

TecnetSOC y CrowdStrike, lado a lado

Capacidad		TecnetSOC	CrowdStrike EDR/XDR y MDR	Evidencia sobre CrowdStrike
✓ 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	7 completas	+5 parciales	
Centro de operaciones (SOC) 24/7 con analistas humanos	✓	✓	Falcon Complete: monitoreo, investigación y remediación 24/7 por analistas de CrowdStrike [7]	
Agentes de IA que investigan y filtran las alertas antes de pasarlas a un analista	✓	✓	MDR agéntico: agentes de IA investigan y responden; expertos de Falcon Complete validan las decisiones [7]	
Compuerta Humana: una persona aprueba cada acción crítica antes de ejecutarse	✓	●	Actúa en tu nombre dentro de contramedidas acordadas al inicio; aprobación caso por caso no documentada [8]	

Capacidad		TecnetSOC	CrowdStrike EDR/XDR y MDR	Evidencia sobre CrowdStrike
Lo ofrece	Lo ofrece como complemento	Parcial, limitado o requiere otro contrato	Sin evidencia pública	
No forma parte de su oferta publicada				
Asistente de investigación con IA en el portal, que cita sus fuentes	 Neo		Charlotte AI investiga en lenguaje natural y cada respuesta remite a sus datos; idiomas no publicados [9]	
Operación en LATAM, EE.UU. y Europa, con analistas en tu zona horaria			Equipos globales 24/7; no publica ubicación de sus analistas ni operación en LATAM [10]	
Analistas, soporte y portal en español nativo			Sitio en español; soporte en español anunciado vía distribuidores en Europa; idioma de analistas no publicado [6]	
Reportes para dirección en español y en lenguaje de negocio			Asesores de seguridad traducen la actividad en orientación ejecutiva; sin reportes en español documentados [10]	
Tiempos de notificación e inicio de investigación publicados por severidad	 Crítico: 30 min (objetivo)		Sin tiempos por severidad; publica una mediana de contención de 1 minuto, sujeta a variación [7]	
Resumen ejecutivo cada mañana: lo que pasó en las últimas 24 horas	 07:30		Sin evidencia de resumen ejecutivo diario [7]	
Reportes automáticos semanales, mensuales, trimestrales y anuales			Soporte de pago con revisiones de salud y reportes trimestrales; sin reportes semanales a anuales documentados [11]	
Gerente técnico de cuenta (TAM) asignado y revisiones trimestrales			Soporte Elite (costo aparte): TAM especialista en tu industria, revisiones mensuales y de operación [11]	
Contacto 24/7 con personas de soporte o seguridad			Soporte telefónico 24/7/365 en los planes de soporte de pago [11]	
Certificación independiente de la operación (ISO 27001 o SOC 2 Tipo II)	 ISO/IEC 27001:2022		ISO/IEC 27001:2022 y reporte SOC 2 Tipo 2 de la plataforma Falcon [5]	
Arranque rápido con un agente de software: la actividad de tus dispositivos, visible en horas	 Típico: 2 a 4 horas		Un sensor ligero que se despliega en minutos, administrado desde la consola web [12]	
Detección y respuesta	15 de 15	7 completas		
Monitoreo continuo y correlación de eventos (SIEM), alineado con MITRE ATT&CK (marco de referencia de técnicas de ataque)			XDR y Next-Gen SIEM correlacionan datos propios y de terceros; detecciones alineadas con MITRE ATT&CK [13]	
Protección avanzada en cada equipo (EDR/XDR): malware, ransomware y explotación de vulnerabilidades			Antivirus de nueva generación y EDR en los paquetes empresariales de Falcon [14]	
Filtrado web en el equipo			Falcon Secure Access protege la sesión del navegador; filtrado web por categorías no documentado [15]	
Detección de intrusos (IDS/IPS)			Sin IDS/IPS de red propio; se suma con sensores de terceros (por ejemplo, Corelight) en Next-Gen SIEM [4]	
Detección de amenazas en la red interna (NDR)			Detección en la red interna solo con sensores NDR de terceros integrados en Next-Gen SIEM [4]	
Investigaciones documentadas y enriquecidas con inteligencia de amenazas			Investigaciones con su inteligencia de adversarios, indicadores en tiempo real y monitoreo de la web oscura [16]	
Gestión de incidentes con bitácora y tiempo de atención medido por caso			Gestión de incidentes con IA en Next-Gen SIEM; tiempo de atención por caso no publicado [17]	
Respuesta con aislamiento de equipos y bloqueo de direcciones IP			Contención de red del equipo y restricción de IP con acciones de respuesta en tiempo real [13]	
Respuesta a incidentes con análisis de causa raíz			Remediación de punta a punta en Falcon Complete; causa raíz con su servicio de respuesta a incidentes [18]	
Postura de identidad: MFA, cuentas privilegiadas y acceso condicional			Next-Gen Identity Security: AD, Entra ID y Okta, MFA según riesgo y acceso justo a tiempo [19]	
Zero Trust: DNS seguro, acceso a aplicaciones y control de aplicaciones no autorizadas (shadow IT)			Falcon Shield detecta apps SaaS no autorizadas y Secure Access protege la navegación; sin DNS seguro documentado [20]	

Capacidad	TecnetSOC	CrowdStrike EDR/XDR y MDR	Evidencia sobre CrowdStrike
Lo ofrece Lo ofrece como complemento Parcial, limitado o requiere otro contrato Sin evidencia pública No forma parte de su oferta publicada			
Seguridad en la nube: alertas y postura			Falcon Cloud Security: postura y detecciones en tiempo real en AWS, Azure, GCP y OCI [21]
Seguridad de correo: spam, phishing, malware y fraude por suplantación (BEC)			Sin seguridad de correo propia; Next-Gen SIEM analiza datos de Abnormal, Mimecast o Proofpoint [2]
Concientización: simulaciones de phishing y entrenamiento con métricas			Sin simulaciones de phishing ni entrenamiento de usuarios en sus paquetes publicados [14]
Recomendaciones de seguridad priorizadas con flujo de aprobación			Prioriza exposiciones y orquesta la remediación con Falcon Fusion; flujo de aprobación no documentado [22]
Exposición y gestión de TI	12 de 12	4 completas +6 parciales	
Inventario unificado de activos y de software			Descubrimiento activo, pasivo y por API, con las aplicaciones instaladas en cada equipo [22]
Vulnerabilidades priorizadas por gravedad y probabilidad de explotación (CVSS, EPSS)			Prioriza con ExPRT.AI y contexto de adversarios frente a CVSS; EPSS no explícito [22]
Prioridad a las fallas que ya se están explotando (catálogo KEV de CISA)			Prioriza por explotación con inteligencia propia; uso del catálogo KEV no documentado [23]
Parcheo de sistema operativo y aplicaciones de terceros			Parcheo de emergencia de Windows con un clic; parcheo por riesgo de Falcon for IT marcado como próximo [1]
Parcheo operado por el proveedor, con plazos publicados por severidad	 Críticos: 48 h (objetivo)		Sin evidencia de que CrowdStrike instale los parches ni de plazos por severidad [7]
Verificación de cierre: el escáner confirma que la vulnerabilidad desapareció			La evaluación continua del sensor refleja el cierre; sin verificación formal de remediación documentada [22]
Validación de parches en grupo piloto antes del despliegue			Despliegue por anillos y oleadas progresivas anunciado para Falcon for IT, aún como función próxima [24]
Superficie de ataque externa: lo que tu empresa expone en Internet, con puntaje de riesgo	 Puntaje 0 a 100		EASM 24/7: descubre activos expuestos en Internet y los prioriza por riesgo [25]
Alertas de dominios que imitan tu marca y de credenciales o claves expuestas			Protección de marca: suplantación de dominios, credenciales expuestas y fugas de datos [16]
Prueba de penetración (pentest) anual	 Anual		Pentest externo, interno, de aplicaciones web y móviles, e inalámbrico [26]
Gestión remota de equipos (RMM)			Falcon for IT automatiza tareas y scripts en equipos; no se presenta como RMM [27]
Monitoreo de disponibilidad (NOC)			Sin evidencia de monitoreo de disponibilidad (NOC) [27]
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 propio; se integra con fabricantes de respaldo aliados, como Rubrik [3]
Bóveda de respaldo inmutable (no se puede alterar ni borrar), aislada por cliente	 Complemento		Sin bóveda de respaldo propia [3]
Recuperación ante desastres con simulacros y tiempo de recuperación (RTO) medido	 Complemento RTO medido		Sin recuperación ante desastres ni simulacros; la restauración de datos depende de aliados de respaldo [3]

Capacidad	TecnetSOC	CrowdStrike EDR/XDR y MDR	Evidencia sobre CrowdStrike
✓ Lo ofrece + Lo ofrece como complemento ⓧ No forma parte de su oferta publicada	● Parcial, limitado o requiere otro contrato	? Sin evidencia pública	
Cumplimiento	6 de 6	0 completas	+1 parcial
Evidencia mensual lista para auditores y aseguradoras	✓ Mensual	?	Sin evidencia mensual documentada para tus auditores; entrega el reporte SOC 2 de su propia plataforma [5]
Preparación para ISO 27001, SOC 2 y PCI DSS con controles compartidos	+ Complemento	●	Mapeos de la plataforma a PCI DSS y NIST hechos por un tercero; ISO 27001 y SOC 2 no documentados [5]
Preparación normativa mexicana: CNBV Fintech, protección de datos (LFPDPPP) y NOM-024	+ Complemento	?	Sin evidencia de normativa mexicana [5]
Gestión de riesgos, controles, declaración de aplicabilidad y auditorías internas	+ Complemento	ⓧ	CrowdStrike indica que sus productos y servicios no son soluciones de cumplimiento [5]
Portal para tu auditor con sala de evidencias y página pública de confianza (trust center)	+ Complemento	?	Sin portal para tu auditor ni página de confianza para tu empresa [5]
Continuidad de negocio, riesgo de proveedores y gestión de brechas de datos	+ Complemento	?	Sin evidencia de continuidad de negocio, riesgo de proveedores ni gestión de brechas [5]
Cómo se contrata	No suma al conteo		
Precio por dispositivo, con planes que se suman	✓ Por dispositivo	✓	Paquetes por dispositivo que se suman (Go, Pro, Enterprise); Falcon Complete y módulos, por cotización [14]
Plan gratuito para empezar	✓ Hasta 10 dispositivos	?	Sin plan gratuito; solo prueba de 15 días [14]
Prueba gratuita en tu entorno real	✓ 30 días	●	Prueba gratis de 15 días de la plataforma; sin prueba publicada de Falcon Complete [14]
Disponible con la marca de tu proveedor de TI	✓	✓	Falcon Complete for Service Providers permite marca blanca o marca compartida [28]
Cobertura completa	50	18	+19 parciales

— SIGUIENTE PASO

Compruébalo en tu operación

Pruébalo en un entorno real, sin cambiar lo que ya te funciona.
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 CrowdStrike: CrowdStrike, oferta más completa publicada para empresa mediana (plataforma Falcon en su paquete Enterprise más Falcon Complete Next-Gen MDR, servicio 24/7 operado por CrowdStrike, con sus módulos propios de costo aparte: Next-Gen SIEM, Next-Gen Identity Security, Cloud Security, Exposure Management, Falcon for IT, Falcon Shield, Falcon Secure Access, Charlotte AI, Adversary Intelligence, servicios de pentest y respuesta a incidentes, y soporte Elite), consulta 13 oct 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.crowdstrike.com/en-au/platform/falcon-for-it/ (Diferencias que se notan en el día a día)
2. www.crowdstrike.com/tech-hub/ng-siem/harnessing-email-data-to-stop-... (Diferencias que se notan en el día a día)
3. www.crowdstrike.com/en-us/press-releases/industry-leaders-crowdstri... (Diferencias que se notan en el día a día)
4. marketplace.crowdstrike.com/listings/corelight-ndr-for-falcon-next-... (Diferencias que se notan en el día a día)
5. www.crowdstrike.com/en-us/why-crowdstrike/crowdstrike-compliance-ce... (Diferencias que se notan en el día a día)
6. www.crowdstrike.com/en-us/press-releases/crowdstrike-expands-europe... (Diferencias que se notan en el día a día)
7. www.crowdstrike.com/en-us/services/falcon-complete-next-gen-mdr/ (Centro de operaciones (SOC) 24/7 con analistas humanos)
8. www.crowdstrike.com/en-us/blog/inside-mitre-attack-evaluation-how-c-... (Compuerta Humana: una persona aprueba cada acción...)
9. www.crowdstrike.com/en-us/platform/charlotte-ai/ (Asistente de investigación con IA en el portal, que...)
10. www.crowdstrike.com/en-us/services/falcon-complete-mdr/operating-mo... (Operación en LATAM, EE.UU. y Europa, con analistas en...)
11. assets.crowdstrike.com/is/content/crowdstrikeinc/crowdstrike-falcon... (Reportes automáticos semanales, mensuales, trimestrales...)
12. www.crowdstrike.com/en-us/products/faq/ (Arranque rápido con un agente de software: la actividad...)
13. www.crowdstrike.com/tech-hub/endpoint-security/falcon-insight-xdr-w... (Monitoreo continuo y correlación de eventos (SIEM),...)
14. www.crowdstrike.com/en-us/pricing/ (Protección avanzada en cada equipo (EDR/XDR): malware,...)
15. www.crowdstrike.com/en-us/platform/falcon-secure-access/ (Filtrado web en el equipo)
16. www.crowdstrike.com/en-us/platform/threat-intelligence/ (Investigaciones documentadas y enriquecidas con...)
17. www.crowdstrike.com/en-us/platform/next-gen-siem/ (Gestión de incidentes con bitácora y tiempo de atención...)
18. www.crowdstrike.com/en-us/services/incident-response/ (Respuesta a incidentes con análisis de causa raíz)
19. www.crowdstrike.com/en-us/platform/identity-protection/ (Postura de identidad: MFA, cuentas privilegiadas y...)
20. www.crowdstrike.com/en-us/platform/falcon-shield/ (Zero Trust: DNS seguro, acceso a aplicaciones y control...)
21. www.crowdstrike.com/en-us/platform/cloud-security/ (Seguridad en la nube: alertas y postura)
22. crowdstrike.com/wp-content/uploads/2024/09/falcon-exposure-manageme... (Recomendaciones de seguridad priorizadas con flujo de...)
23. crowdstrike.com/platform/exposure-management/risk-prioritization (Prioridad a las fallas que ya se están explotando...)
24. www.crowdstrike.com/en-us/blog/falcon-for-it-redefines-vulnerabilit... (Validación de parches en grupo piloto antes del...)
25. crowdstrike.com/platform/exposure-management/easm (Superficie de ataque externa: lo que tu empresa expone...)
26. www.crowdstrike.com/en-gb/services/prepare/penetration-testing-exer... (Prueba de penetración (pentest) anual)
27. www.crowdstrike.com/en-us/platform/falcon-for-it/ (Gestión remota de equipos (RMM))
28. www.crowdstrike.com/en-us/resources/data-sheets/falcon-complete-for-... (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.