

Blackpoint actúa solo en tu red. En TecnetSOC la IA investiga y una persona aprueba cada acción crítica.

Con Blackpoint, su SOC puede aislar equipos sin pedir aprobación previa, y aplicar el parche sigue en manos de tu equipo. En TecnetSOC, la IA investiga, una persona aprueba lo crítico conociendo tu negocio y el SOC parchea.



43

capacidades donde TecnetSOC va más allá

7

capacidades en las que coincidimos

0

capacidades donde Blackpoint 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 Blackpoint: 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

Blackpoint es un servicio de SOC administrado que se vende a través de proveedores de TI. Aquí comparamos la oferta más completa publicada de cada uno, capacidad por capacidad.

Diferencias que se notan en el día a día

01
El parche lo aplicas tú

CON BLACKPOINT
Su módulo de vulnerabilidades identifica y prioriza; aplicar el parche, probarlo y confirmar el cierre queda en manos de tu equipo o de tu proveedor de TI. [1]

CON TECNETSOC
El SOC parchea: prioriza por explotación real (KEV y EPSS), valida en grupo piloto y cierra solo cuando el escáner lo confirma.

02
Aíslan primero, te avisan después

CON BLACKPOINT
Su SOC actúa primero y avisa después: puede aislar un equipo o deshabilitar una cuenta sin aprobación previa, y no documenta opción para exigirla. [2]

CON TECNETSOC
La IA investiga y correlaciona cada alerta, y una persona aprueba toda acción crítica antes de ejecutarla (Compuerta Humana).

03
Sin operación documentada en LATAM

CON BLACKPOINT
Sus teléfonos publicados son de Norteamérica, Australia y Reino Unido; no documenta analistas en español ni operación en LATAM. [3]

CON TECNETSOC
Tienes analistas en tu zona horaria y en español nativo, con operación en LATAM, EE.UU. y Europa certificada ISO/IEC 27001:2022.

04
Solo a través de un proveedor de TI, sin prueba gratuita

CON BLACKPOINT
No se contrata directo: llega solo a través de un proveedor de TI (proveedor de TI) asociado, sin plan gratuito ni prueba gratuita publicada; el sitio solo ofrece agendar una demo. [4]

CON TECNETSOC
Contratas directo o con tu proveedor de TI; Visibility es gratis hasta 10 dispositivos y pruebas Response 30 días en tu entorno.

05
Correo y phishing, con otro proveedor

CON BLACKPOINT
Su SOC detecta toma de cuentas y envíos sospechosos en Microsoft 365, pero sus paquetes publicados no incluyen filtrado de spam y malware ni simulaciones de phishing. [5]

CON TECNETSOC
La oferta más completa incluye seguridad de correo (spam, phishing, malware, BEC) y concientización con simulaciones de phishing.

06
Pentest y dominios que imitan tu marca, otro contrato

CON BLACKPOINT
Su SOC vigila credenciales expuestas en la dark web, pero no documenta pentesting ni monitoreo de dominios que imitan tu marca para suplantarle. [1]

CON TECNETSOC
La oferta más completa incluye pentesting anual, alertas de dominios que imitan tu marca y superficie de ataque externa con puntaje de 0 a 100.

Las tres áreas con más diferencia

Operación y servicio

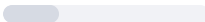
TecnetSOC  **14**

Blackpoint  **2**

de 14 capacidades completas en esta área

Detección y respuesta

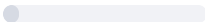
TecnetSOC  **15**

Blackpoint  **4**

de 15 capacidades completas en esta área

Exposición y gestión de TI

TecnetSOC  **12**

Blackpoint  **1**

de 12 capacidades completas en esta área

TecnetSOC y Blackpoint, lado a lado

Capacidad	TecnetSOC	Blackpoint SOC para proveedores de TI	Evidencia sobre Blackpoint
 Lo ofrece  Lo ofrece como complemento  Parcial, limitado o requiere otro contrato  Sin evidencia pública  No forma parte de su oferta publicada			
Operación y servicio	14 de 14	2 completas  +6 parciales	
Centro de operaciones (SOC) 24/7 con analistas humanos			SOC propio 24/7/365 con cazadores de amenazas y remediadores [3]
Agentes de IA que investigan y filtran las alertas antes de pasarlas a un analista			Alertas "mejoradas con IA"; no documenta agentes de IA que investiguen cada alerta [6]

Capacidad	TecnetSOC	Blackpoint SOC para proveedores de TI	Evidencia sobre Blackpoint
Lo ofrece Lo ofrece como complemento Parcial, limitado o requiere otro contrato Sin evidencia pública No forma parte de su oferta publicada			
Compuerta Humana: una persona aprueba cada acción crítica antes de ejecutarse			Contiene sin aprobación previa del proveedor de TI; sin modo de aprobación, según un directorio independiente [4]
Asistente de investigación con IA en el portal, que cita sus fuentes	 Neo		Sin evidencia de analista de IA conversacional en el portal [5]
Operación en LATAM, EE.UU. y Europa, con analistas en tu zona horaria			Sin presencia ni SOC documentado en LATAM; teléfonos NA, Australia, Reino Unido [3]
Analistas, soporte y portal en español nativo			Sin evidencia de analistas o soporte en español [3]
Reportes para dirección en español y en lenguaje de negocio			Sin evidencia de reportes en español [5]
Tiempos de notificación e inicio de investigación publicados por severidad	 Crítico: 30 min (objetivo)		Sin SLA publicado; solo promedios autodeclarados (menos de 2 minutos en identidad) [7]
Resumen ejecutivo cada mañana: lo que pasó en las últimas 24 horas	 07:30		Sin evidencia de resumen ejecutivo diario [5]
Reportes automáticos semanales, mensuales, trimestrales y anuales			Reportes forenses e histórico de 180 días; periodicidad automática no documentada [7]
Gerente técnico de cuenta (TAM) asignado y revisiones trimestrales			Equipo de cuenta dedicado y plan trimestral para el proveedor de TI, según su nivel de facturación [8]
Contacto 24/7 con personas de soporte o seguridad			SOC 24/7 confirmado; mesa de soporte 24/7 como tal no documentada [3]
Certificación independiente de la operación (ISO 27001 o SOC 2 Tipo II)	 ISO/IEC 27001:2022		Publica SOC 2 Tipo II anual; no lista ISO/IEC 27001 [9]
Arranque rápido con un agente de software: la actividad de tus dispositivos, visible en horas	 Típico: 2 a 4 horas		Despliegue fácil según reseñas; sin tiempo de arranque publicado [10]
Detección y respuesta	15 de 15	4 completas +7 parciales	
Monitoreo continuo y correlación de eventos (SIEM), alineado con MITRE ATT&CK (marco de referencia de técnicas de ataque)			SIEM en paquete Standard con 365 días de retención; mapeo MITRE ATT&CK [5]
Protección avanzada en cada equipo (EDR/XDR): malware, ransomware y explotación de vulnerabilidades			Agente EDR propio con MDR y control de aplicaciones; Windows y macOS, sin Linux [11]
Filtrado web en el equipo			Sin evidencia de filtrado web en el equipo [5]
Detección de intrusos (IDS/IPS)			Sin evidencia de IDS/IPS [5]
Detección de amenazas en la red interna (NDR)			Sin NDR documentado ni detección de equipos sin agente [5]
Investigaciones documentadas y enriquecidas con inteligencia de amenazas			Inteligencia contextual y equipo propio de seguimiento de adversarios [6]
Gestión de incidentes con bitácora y tiempo de atención medido por caso			Respuesta a incidentes priorizada; bitácora y MTTR por incidente no documentados [6]
Respuesta con aislamiento de equipos y bloqueo de direcciones IP			Aísla equipos y contiene en red; bloqueo automático por geografía y VPN [4]
Respuesta a incidentes con análisis de causa raíz			Reportes forenses de identidad y soporte de recuperación; sin forense completo documentado [7]
Postura de identidad: MFA, cuentas privilegiadas y acceso condicional			ITDR M365 y Google Workspace, MFA de administradores; sin cuentas de servicio ni acceso condicional [12]
Zero Trust: DNS seguro, acceso a aplicaciones y control de aplicaciones no autorizadas (shadow IT)			Control de aplicaciones operado por su SOC; sin DNS seguro ni acceso Zero Trust a aplicaciones [13]
Seguridad en la nube: alertas y postura			Postura solo de Microsoft 365; no documenta Azure [12]

Capacidad	TecnetSOC	Blackpoint SOC para proveedores de TI	Evidencia sobre Blackpoint
Lo ofrece Lo ofrece como complemento Parcial, limitado o requiere otro contrato Sin evidencia pública No forma parte de su oferta publicada			
Seguridad de correo: spam, phishing, malware y fraude por suplantación (BEC)			Detecta BEC y envíos sospechosos en M365; sin antispam ni cuarentena [7]
Concientización: simulaciones de phishing y entrenamiento con métricas			Sin evidencia de simulaciones de phishing ni entrenamiento [5]
Recomendaciones de seguridad priorizadas con flujo de aprobación			Backlog de remediación priorizado y calificación de postura; sin flujo de aprobación [1]
Exposición y gestión de TI	12 de 12	1 completa +4 parciales	
Inventario unificado de activos y de software			Inventario de dispositivos, identidades, aplicaciones y cuentas SaaS en todos los paquetes [5]
Vulnerabilidades priorizadas por gravedad y probabilidad de explotación (CVSS, EPSS)			Vulnerabilidades por riesgo y explotabilidad; uso de CVSS y EPSS no documentado [1]
Prioridad a las fallas que ya se están explotando (catálogo KEV de CISA)			Prioriza por explotabilidad; no menciona el catálogo KEV de CISA [1]
Parcheo de sistema operativo y aplicaciones de terceros			Identifica y prioriza; no ofrece parcheo, lo hace el proveedor de TI [1]
Parcheo operado por el proveedor, con plazos publicados por severidad	 Críticos: 48 h (objetivo)		Sin parcheo operado ni tiempos publicados [1]
Verificación de cierre: el escáner confirma que la vulnerabilidad desapareció			Sin verificación de cierre documentada [1]
Validación de parches en grupo piloto antes del despliegue			Sin parcheo, por tanto sin grupo piloto [1]
Superficie de ataque externa: lo que tu empresa expone en Internet, con puntaje de riesgo	 Puntaje 0 a 100		Escaneo de red y nube más calificación de postura; sin superficie de ataque externa (EASM) documentada [1]
Alertas de dominios que imitan tu marca y de credenciales o claves expuestas			Monitoreo de dark web por credenciales; sin alertas de dominios que imitan tu marca ni de código expuesto [1]
Prueba de penetración (pentest) anual	 Anual		Sin evidencia de pentesting [5]
Gestión remota de equipos (RMM)			Sin RMM propio; el proveedor de TI usa el suyo [5]
Monitoreo de disponibilidad (NOC)			Sin evidencia de monitoreo de disponibilidad ni NOC [5]
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 [5]
Bóveda de respaldo inmutable (no se puede alterar ni borrar), aislada por cliente	 Complemento		Sin bóveda inmutable [5]
Recuperación ante desastres con simulacros y tiempo de recuperación (RTO) medido	 Complemento RTO medido		Sin recuperación ante desastres [5]
Cumplimiento	6 de 6	0 completas +1 parcial	
Evidencia mensual lista para auditores y aseguradoras	 Mensual		Evidencia continua para aseguradoras, limitada a M365 y bitácoras SIEM [12]
Preparación para ISO 27001, SOC 2 y PCI DSS con controles compartidos	 Complemento		Sin plataforma GRC ni mapeo entre marcos [5]

Capacidad	TecnetSOC	Blackpoint SOC para proveedores de TI	Evidencia sobre Blackpoint
✓ Lo ofrece + Lo ofrece como complemento ✗ No forma parte de su oferta publicada	⌚ Parcial, limitado o requiere otro contrato	? Sin evidencia pública	
Preparación normativa mexicana: CNBV Fintech, protección de datos (LFPDPPP) y NOM-024	+ Complemento	✗	Sin normativa mexicana [5]
Gestión de riesgos, controles, declaración de aplicabilidad y auditorías internas	+ Complemento	✗	Sin gestión de riesgos, SoA ni auditorías internas [5]
Portal para tu auditor con sala de evidencias y página pública de confianza (trust center)	+ Complemento	✗	Trust Center propio del proveedor, no para clientes; sin sala de evidencias para el auditor [9]
Continuidad de negocio, riesgo de proveedores y gestión de brechas de datos	+ Complemento	✗	Sin módulos de continuidad, proveedores ni brechas [5]
Cómo se contrata	No suma al conteo		
Precio por dispositivo, con planes que se suman	✓ Por dispositivo	✓	Cobro por equipo al mes; paquetes acumulativos Essentials, Core, Standard; precio no público [5]
Plan gratuito para empezar	✓ Hasta 10 dispositivos	✗	Sin plan gratuito [5]
Prueba gratuita en tu entorno real	✓ 30 días	✗	Sin prueba publicada; solo solicitud de demo [5]
Disponible con la marca de tu proveedor de TI	✓	⌚	Solo a través de proveedores de TI, con marca compartida junto a Blackpoint [8]
Cobertura completa	50	7 +18 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

TecnetSOC frente a Blackpoint · Comparativo 2026.09

tecnetone.com/servicios/soc-as-a-service · Pág. 5 de 6

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 Blackpoint: Blackpoint Cyber, CompassOne paquete Standard (ITDR + MDR + vulnerabilidades + postura de nube + control de aplicaciones + SIEM) más Managed EDR y Dark Web Monitoring, 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.

- blackpointcyber.com/platform/vulnerability-management/ (Diferencias que se notan en el día a día)
- blackpointcyber.com/why-blackpoint/security-operations-center/ (Diferencias que se notan en el día a día)
- blackpointcyber.com/frequently-asked-questions/ (Diferencias que se notan en el día a día)
- www.flamingo.run/blog/blackpoint-cyber-review (Diferencias que se notan en el día a día)
- blackpointcyber.com/platform/ (Diferencias que se notan en el día a día)
- blackpointcyber.com/platform/managed-detection-and-response/ (Agentes de IA que investigan y filtran las alertas...)
- www.globenewswire.com/news-release/2026/09/10/3359559/0/en/new-blackpoint-cyber-announces-new-managed-detection-and-response-service.html (Tiempos de notificación e inicio de investigación...)
- blackpointcyber.com/wp-content/uploads/2025/08/Blackpoint-Cyber-Parade-Report-2025.pdf (Gerente técnico de cuenta (TAM) asignado y revisiones...)
- blackpointcyber.com/company/trust-center/ (Certificación independiente de la operación (ISO 27001...))
- capterra.com/p/212884/Blackpoint-MDR/ (Arranque rápido con un agente de software: la actividad...)
- blackpointcyber.com/solutions/blackpoint-response/ (Protección avanzada en cada equipo (EDR/XDR): malware,...)
- blackpointcyber.com/platform/cloud-posture/ (Postura de identidad: MFA, cuentas privilegiadas y...)
- blackpointcyber.com/resources/blog/introducing-managed-application-security/ (Zero Trust: DNS seguro, acceso a aplicaciones y control...)

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.