

Arctic Wolf detecta y te avisa. TecnetSOC opera tu seguridad completa por ti, en tu idioma y en tu zona horaria.

Con Arctic Wolf, el análisis forense dentro de tu entorno se contrata aparte, con una bolsa de horas pagada por adelantado (retainer), y el parche del sistema operativo lo aplica tu equipo. En TecnetSOC, la respuesta con análisis forense y el parcheo ya van incluidos.



35

capacidades donde TecnetSOC va más allá

15

capacidades en las que coincidimos

0

capacidades donde Arctic Wolf supera a TecnetSOC

De las 50: 35 donde vamos más allá y 15 en las que coincidimos

Misma lista de 50 capacidades y mismo criterio para TecnetSOC y Arctic Wolf: 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

Arctic Wolf es un servicio de SOC administrado, como TecnetSOC. Aquí comparamos la oferta más completa publicada de cada uno, capacidad por capacidad.

— LO QUE NOS HACE DISTINTOS

Diferencias que se notan en el día a día

01

La respuesta con análisis forense, en otro contrato

CON ARCTIC WOLF
Su servicio de detección y respuesta (MDR) detecta, contiene y guía la remediación; la respuesta con análisis forense dentro de tu entorno es un servicio aparte, por bolsa de horas prepagada (retainer) o por hora. [\[1\]](#)

CON TECNETSOC
La respuesta a incidentes con análisis forense va en la oferta más completa, y una persona aprueba cada acción crítica.

02

Parcheo solo de aplicaciones compatibles

CON ARCTIC WOLF
Su licencia Resolve parchea solo aplicaciones de terceros compatibles que no requieren reinicio; no documenta parches del sistema operativo ni plazos. [\[2\]](#)

CON TECNETSOC
El SOC prioriza el parcheo según lo que ya se explota en el mundo real (KEV y EPSS), lo valida en un grupo piloto y cierra solo cuando el escáner confirma la corrección.

03

Seguridad sí, operación de TI no

CON ARCTIC WOLF
Su portafolio no incluye RMM, monitoreo de disponibilidad ni mesa de soporte de TI, y para pentesting puede referirte a terceros: otro contrato. [\[3\]](#)

CON TECNETSOC
La oferta más completa incluye RMM, monitoreo de disponibilidad (NOC), mesa de soporte 24/7, TAM y pentesting anual.

04

Cada fuente de datos, otra licencia

CON ARCTIC WOLF
Su lista de precios para sector público cobra licencias por separado para usuarios, servidores, cada nube y cada aplicación, como Microsoft 365 o Google Workspace. [\[4\]](#)

CON TECNETSOC
Pagas por dispositivo con planes acumulativos; Visibility es gratis hasta 10 dispositivos y Response se prueba 30 días.

05

Sin operación en Latinoamérica

CON ARCTIC WOLF
Sus SOC publicados están en Norteamérica, Europa y Asia Pacífico, ninguno en Latinoamérica, y su documentación técnica no tiene versión en español. [\[5\]](#)

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

06

Cumplimiento sin normativa mexicana

CON ARCTIC WOLF
Sus reportes de cumplimiento cubren marcos como NIST, PCI DSS, HIPAA o GDPR, sin normativa mexicana ni plataforma GRC para tu auditoría. [\[6\]](#)

CON TECNETSOC
Sumas TecnetGRC como complemento con CNBV, LFPDPPP, NOM-024, ISO 27001 y portal del auditor; cada marco normativo se contrata por separado.

— DÓNDE ESTÁ LA DIFERENCIA

Las tres áreas con más diferencia

Exposición y gestión de TI

TecnetSOC **12**

Arctic Wolf **2**

de 12 capacidades completas en esta área

Operación y servicio

TecnetSOC **14**

Arctic Wolf **5**

de 14 capacidades completas en esta área

Detección y respuesta

TecnetSOC **15**

Arctic Wolf **8**

de 15 capacidades completas en esta área

— CAPACIDAD POR CAPACIDAD

TecnetSOC y Arctic Wolf, lado a lado

Capacidad		TecnetSOC	Arctic Wolf SOC	Evidencia sobre Arctic Wolf
✓ 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	5 completas	
			+6 parciales	
Centro de operaciones (SOC) 24/7 con analistas humanos	✓	✓	Monitoreo 24×7 con Concierge Security Team asignado [7]	
Agentes de IA que investigan y filtran las alertas antes de pasarlas a un analista	✓	✓	Aurora Agentic SOC: Triage Agent e Investigation Agent analizan y priorizan alertas [8]	
Compuerta Humana: una persona aprueba cada acción crítica antes de ejecutarse	✓	🕒	Humanos aprueban acciones de alto impacto o baja confianza; otras se ejecutan solas [8]	

Capacidad	TecnetSOC	Arctic Wolf SOC	Evidencia sobre Arctic Wolf
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		Cipher / Aurora Security Assistant responde bajo demanda; no se documenta cita de fuentes con fecha [9]
Operación en LATAM, EE.UU. y Europa, con analistas en tu zona horaria			Sin SOC ni oficina en LATAM; SOC en Norteamérica, Europa y Asia Pacífico [10]
Analistas, soporte y portal en español nativo			Sin evidencia pública de analistas ni soporte en español para la región; su portal se ofrece en inglés, japonés, alemán y francés, sin español [11]
Reportes para dirección en español y en lenguaje de negocio			Reportes ejecutivos existen; sin evidencia de versión en español [12]
Tiempos de notificación e inicio de investigación publicados por severidad	 Crítico: 30 min (objetivo)		No publica tiempos de notificación por severidad; las cifras disponibles provienen de terceros [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			Reportes detallados y tableros bajo demanda; no publica reportes automáticos periódicos [7]
Gerente técnico de cuenta (TAM) asignado y revisiones trimestrales			Concierge Security Team nombrado con revisiones estratégicas periódicas [7]
Contacto 24/7 con personas de soporte o seguridad			Equipo Concierge y SOC disponibles 24x7 [7]
Certificación independiente de la operación (ISO 27001 o SOC 2 Tipo II)	 ISO/IEC 27001:2022		Arctic Wolf certificada ISO 27001 y con reporte SOC 2 Tipo II [13]
Arranque rápido con un agente de software: la actividad de tus dispositivos, visible en horas	 Típico: 2 a 4 horas		Despliegue típico de unos 10 días; MDR Connect para proveedor de TI "en horas" [14]
Detección y respuesta	15 de 15	8 completas +4 parciales	
Monitoreo continuo y correlación de eventos (SIEM), alineado con MITRE ATT&CK (marco de referencia de técnicas de ataque)			Plataforma propia de ingesta, correlación y búsqueda de logs, más de 250 integraciones [8]
Protección avanzada en cada equipo (EDR/XDR): malware, ransomware y explotación de vulnerabilidades			Aurora Protect y Endpoint Defense (Cylance) contra malware y ransomware [15]
Filtrado web en el equipo			Sin evidencia de filtrado web en el agente de endpoint [15]
Detección de intrusos (IDS/IPS)			Monitorea IDS/IPS del cliente y tráfico con sensor; no vende IPS propio [7]
Detección de amenazas en la red interna (NDR)			Sensor de red físico o virtual detecta amenazas en red interna, incluye equipos sin agente [7]
Investigaciones documentadas y enriquecidas con inteligencia de amenazas			Investigaciones con Threat Intelligence y Threat Intelligence Plus propios [16]
Gestión de incidentes con bitácora y tiempo de atención medido por caso			Crea el incidente con ticket y guía; tiempo de atención por incidente no documentado [7]
Respuesta con aislamiento de equipos y bloqueo de direcciones IP			Managed Containment aísla a nivel red y host; Dynamic Block Lists [7]
Respuesta a incidentes con análisis de causa raíz			Incident360 e IR JumpStart Retainer: respuesta y análisis forense, contratados aparte [1]
Postura de identidad: MFA, cuentas privilegiadas y acceso condicional			Monitoreo de identidad M365/Google e integraciones; postura de identidad no detallada [16]
Zero Trust: DNS seguro, acceso a aplicaciones y control de aplicaciones no autorizadas (shadow IT)			Sin DNS seguro, ZTNA ni control de shadow IT propios [15]
Seguridad en la nube: alertas y postura			Módulos MDR y CSPM para Azure, AWS y GCP [4]
Seguridad de correo: spam, phishing, malware y fraude por suplantación (BEC)			Solo monitorea buzones M365/Google; sin gateway antispam ni cuarentena propios [4]

Capacidad	TecnetSOC	Arctic Wolf SOC	Evidencia sobre Arctic Wolf
Lo ofrece Lo ofrece como complemento Parcial, limitado o requiere otro contrato Sin evidencia pública No forma parte de su oferta publicada			
Concientización: simulaciones de phishing y entrenamiento con métricas			Managed Security Awareness y Plus con phishing simulado [4]
Recomendaciones de seguridad priorizadas con flujo de aprobación			Guía de remediación con IA e integración ITSM; sin flujo de aprobación documentado [17]
Exposición y gestión de TI	12 de 12	2 completas +4 parciales	
Inventario unificado de activos y de software			Inventario continuo de activos (tecnología Sevco) en Attack Surface Management [12]
Vulnerabilidades priorizadas por gravedad y probabilidad de explotación (CVSS, EPSS)			Escaneo interno y externo con probabilidad de explotación; EPSS no explícito [17]
Prioridad a las fallas que ya se están explotando (catálogo KEV de CISA)			Prioriza con inteligencia de explotación; uso de KEV no documentado en producto [18]
Parcheo de sistema operativo y aplicaciones de terceros			Resuelve parchea solo software de terceros compatible, no sistema operativo [2]
Parcheo operado por el proveedor, con plazos publicados por severidad	 Críticos: 48 h (objetivo)		No publica parcheo operado por el proveedor ni tiempos publicados [2]
Verificación de cierre: el escáner confirma que la vulnerabilidad desapareció			Menciona seguimiento de verificación de remediación; mecánica por reescaneo no detallada [12]
Validación de parches en grupo piloto antes del despliegue			Sin evidencia de grupo piloto antes del despliegue de parches [2]
Superficie de ataque externa: lo que tu empresa expone en Internet, con puntaje de riesgo	 Puntaje 0 a 100		Escaneo externo y Aurora Attack Surface Management con priorización de riesgo [12]
Alertas de dominios que imitan tu marca y de credenciales o claves expuestas			Sin evidencia de detección de typosquatting ni de secretos expuestos [17]
Prueba de penetración (pentest) anual	 Anual		Sin evidencia de servicio de pentesting propio [12]
Gestión remota de equipos (RMM)			No ofrece RMM [19]
Monitoreo de disponibilidad (NOC)			No ofrece NOC ni monitoreo de disponibilidad [19]
Respaldo y continuidad	3 de 3	0 completas +0 parciales	
Respaldo de servidores, archivos, bases de datos, máquinas virtuales y Microsoft 365	 Complemento		Sin oferta de respaldo [19]
Bóveda de respaldo inmutable (no se puede alterar ni borrar), aislada por cliente	 Complemento		Sin bóveda de respaldo [19]
Recuperación ante desastres con simulacros y tiempo de recuperación (RTO) medido	 Complemento RTO medido		Sin recuperación ante desastres; su garantía financiera no sustituye un plan de recuperación [20]
Cumplimiento	6 de 6	0 completas +2 parciales	
Evidencia mensual lista para auditores y aseguradoras	 Mensual		Su equipo Concierge ofrece apoyo en auditorías y reportes; sin paquete mensual de evidencia [7]
Preparación para ISO 27001, SOC 2 y PCI DSS con controles compartidos	 Complemento		Reportes de cumplimiento por marco; no es plataforma GRC con mapeo [6]
Preparación normativa mexicana: CNBV Fintech, protección de datos (LFPDPPP) y NOM-024	 Complemento		Sin cobertura de normativa mexicana [6]

Capacidad	TecnetSOC	Arctic Wolf SOC	Evidencia sobre Arctic Wolf
✓ Lo ofrece + Lo ofrece como complemento ⓪ Parcial, limitado o requiere otro contrato ? Sin evidencia pública ✗ No forma parte de su oferta publicada			
Gestión de riesgos, controles, declaración de aplicabilidad y auditorías internas	+ Complemento	✗	Sin gestión de riesgos, SoA ni auditorías internas para el cliente [6]
Portal para tu auditor con sala de evidencias y página pública de confianza (trust center)	+ Complemento	✗	Trust Center propio, no ofrecido al cliente [21]
Continuidad de negocio, riesgo de proveedores y gestión de brechas de datos	+ Complemento	✗	Sin módulos de continuidad, proveedores o brechas [6]
Cómo se contrata	No suma al conteo		
Precio por dispositivo, con planes que se suman	✓ Por dispositivo	⓪	Cobra por usuario o servidor más una cuota base; el módulo de protección de equipos sí se cobra por dispositivo; niveles Silver a Platinum [4]
Plan gratuito para empezar	✓ Hasta 10 dispositivos	✗	Sin plan gratuito; cuota base con precio publicado por el fabricante [4]
Prueba gratuita en tu entorno real	✓ 30 días	⓪	Solo una evaluación de 30 días de su módulo de superficie de ataque, a través de sus socios de canal; sin prueba gratuita del SOC [22]
Disponible con la marca de tu proveedor de TI	✓	✗	Venta por canal con material de marketing de marca compartida; el servicio conserva la marca Arctic Wolf [23]
Cobertura completa	50	15 +16 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 Arctic Wolf · 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 Arctic Wolf: Arctic Wolf, oferta más completa (Aurora MDR "Total" Platinum + Aurora Endpoint Security + Exposure Management con Resolve + Awareness Plus + Incident360 + Threat Intelligence Plus), 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.

- arcticwolf.com/solutions/incident-response-retainer/ (Diferencias que se notan en el día a día)
- docs.arcticwolf.com/en/arctic-wolf-unified-portal/unified-portal/au... (Diferencias que se notan en el día a día)
- arcticwolf.com/resources/blog-uk/an-in-depth-guide-to-pen-tests/ (Diferencias que se notan en el día a día)
- www.freeitdata.com/wp-content/uploads/2025/01/AW-Public-Sector-Pric... (Diferencias que se notan en el día a día)
- arcticwolf.com/resources/press-releases/arctic-wolf-security-operat... (Diferencias que se notan en el día a día)
- arcticwolf.com/compliance/ (Diferencias que se notan en el día a día)
- arcticwolf.com/solutions/managed-detection-and-response/faq/ (Centro de operaciones (SOC) 24/7 con analistas humanos)
- arcticwolf.com/aurora-soc/ (Agentes de IA que investigan y filtran las alertas...)
- www.globenewswire.com/news-release/2025/04/28/3069280/0/en/Arctic-W... (Asistente de investigación con IA en el portal, que...)
- arcticwolf.com/company/overview/ (Operación en LATAM, EE.UU. y Europa, con analistas en...)
- arcticwolf.com/es/ (Analistas, soporte y portal en español nativo)
- arcticwolf.com/solutions/exposure-management/ (Reportes para dirección en español y en lenguaje de...)
- arcticwolf.com/information-security/ (Certificación independiente de la operación (ISO 27001...))
- arcticwolf.com/resources/press-releases/arctic-wolf-launches-aurora... (Arranque rápido con un agente de software: la actividad...)
- docs.arcticwolf.com/en/aurora-endpoint-security/overview-and-archit... (Protección avanzada en cada equipo (EDR/XDR): malware,...)
- arcticwolf.com/resources/blog/arctic-wolf-product-updates-may-2026/ (Investigaciones documentadas y enriquecidas con...)
- arcticwolf.com/solutions/exposure-management/faq/ (Recomendaciones de seguridad priorizadas con flujo de...)
- arcticwolf.com/resources/blog/vulnerability-prioritization-requires... (Prioridad a las fallas que ya se están explotando...)
- arcticwolf.com/partners/ (Gestión remota de equipos (RMM))
- arcticwolf.com/why-arctic-wolf/security-operations-warranty/ (Recuperación ante desastres con simulacros y tiempo de...)
- trust.arcticwolf.com/ (Portal para tu auditor con sala de evidencias y página...)
- www.channelinsider.com/security/arctic-wolf-new-partner-program-cyb... (Prueba gratuita en tu entorno real)
- arcticwolf.com/resources/press-releases/arctic-wolf-launches-new-an... (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.