

TecnetSOC vs. Huntress

Huntress watches your devices. TecnetSOC is an agentic SOC that runs all of your security for you, 24/7.

Huntress licenses EDR, identity, SIEM, and training separately, and its posture module flags missing patches without applying them. **With TecnetSOC, you pay per device, and the SOC patches, validates in a pilot group, and closes with a scanner.**



42

capabilities where TecnetSOC goes further

8

capabilities where we match

0

capabilities where Huntress outperforms TecnetSOC

Of the 50: 42 where we go further and 8 where we match

Same list of 50 capabilities and same criteria for TecnetSOC and Huntress: each one's most complete published offering, with the source for every data point. [How we did it](#)

[Request the 30-day Response trial](#)

[or start free with Visibility, up to 10 devices](#)

tecnetone.com/en/services/soc-as-a-service

- ✓ 24/7 agentic SOC in LATAM, the US, and Europe
- ✓ Native Spanish and multilingual support
- ✓ Human Gate on critical actions
- ✓ ISO/IEC 27001:2022 certified operations
- ✓ Critical: notification and investigation start within 30 min (target)

Public information reviewed as of September 29, 2026. Version 2026.09. Informational comparison prepared by TecnetOne, not affiliated with the brands mentioned.

— BEFORE YOU COMPARE

Huntress is a managed SOC service sold through IT providers, with modules that are purchased separately. Here we compare each one's most complete published offering, capability by capability.

— WHAT SETS US APART

Differences you notice day to day

01
It flags patches, it doesn't run them

WITH HUNTRESS
Its posture module (ESPM) is in Early Access, with general availability announced for 2027, and it flags missing patches using Microsoft Defender data; it doesn't publish patching times. [\[1\]](#)

WITH TECNETSOC
The SOC prioritizes patching based on what is already being exploited in the real world (KEV, EPSS), validates it in a pilot group, targets 48 h for critical patches, and closes only when the scanner confirms the fix.

02
One license for every module

WITH HUNTRESS
EDR, identity, SIEM, training, and posture are licensed separately, each with its own billing unit, and direct purchases require a minimum of 50 licenses per product. [\[2\]](#)

WITH TECNETSOC
You pay per device with stackable plans; Visibility is free for up to 10 devices, and you can try Response for 30 days in your environment.

03
You provide the antivirus

WITH HUNTRESS
Antivirus prevention comes from Microsoft Defender or another antivirus you already have, and the platform doesn't include web filtering or IDS/IPS. [\[3\]](#)

WITH TECNETSOC
Advanced protection on every device (EDR/XDR), web filtering, and IDS/IPS come in the most complete offering.

04
No network sensor or anti-spam

WITH HUNTRESS
The internal network is visible only through the firewall logs you send to its SIEM, and email is monitored in the mailbox, with no anti-spam. [\[4\]](#)

WITH TECNETSOC
The most complete offering includes internal network detection (NDR) and email security against spam, phishing, malware, and BEC.

05
RMM, NOC, and pentesting: another provider

WITH HUNTRESS
There is no RMM, uptime monitoring, pentesting, or backup; it connects to the RMM you already have, and you purchase the rest from other providers. [\[5\]](#)

WITH TECNETSOC
RMM, NOC, annual pentesting, a TAM, and a 24/7 help desk come in the most complete offering; immutable backup is an add-on.

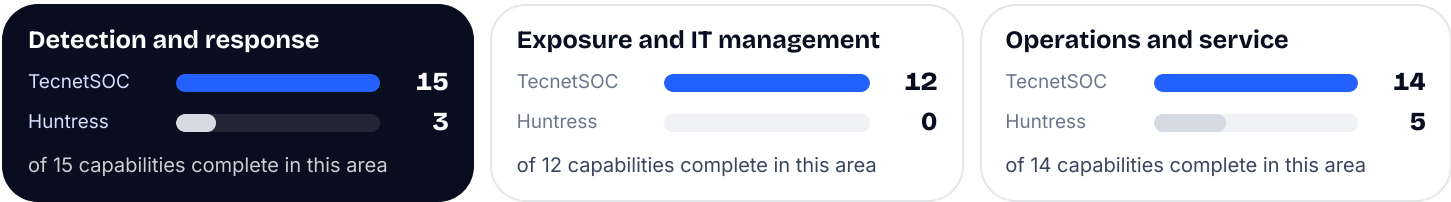
06
No operations in LATAM or support in Spanish

WITH HUNTRESS
Its channel announcements target the US, the UK, and the Europe, Middle East, and Africa (EMEA) region; it doesn't publish operations in LATAM or analysts who can support you in Spanish. [\[6\]](#)

WITH TECNETSOC
We operate in LATAM, the US, and Europe with analysts in your time zone, native Spanish, and multilingual support.

— WHERE THE DIFFERENCE LIES

The three areas with the biggest gap



— CAPABILITY BY CAPABILITY

TecnetSOC and Huntress, side by side

Capability	TecnetSOC	Huntress SOC for IT providers	Evidence on Huntress
 Offers it  Offers it as an add-on  Partial, limited, or requires another contract  No public evidence			
 Not part of its published offering			
Operations and service	14 of 14	5 complete  +5 partial	
24/7 security operations center (SOC) with human analysts			Its own 24/7 SOC, human-led and AI-assisted, included in all modules [2]
AI agents that investigate and filter alerts before passing them to an analyst			Athena: more than 40 AI agents investigate and render a verdict on every signal [7]

Capability	TecnetSOC	Huntress SOC for IT providers	Evidence on Huntress
Offers it Offers it as an add-on Partial, limited, or requires another contract No public evidence Not part of its published offering			
Human Gate: a person approves every critical action before it runs			A person reviews uncertain cases; high-confidence cases are reported without human review; isolation runs without prior approval [7]
AI investigation assistant in the portal that cites its sources	 Neo		Athena works inside the SOC; there is no on-demand assistant in the portal [7]
Operations in LATAM, the US, and Europe, with analysts in your time zone			Operations in the US; no office or operations in LATAM [6]
Analysts, support, and portal in native Spanish			No evidence of Spanish-speaking analysts or support [5]
Leadership reports in Spanish and in business language			Monthly and quarterly threat reports can be generated in Spanish from the branding settings, with a summary page [8]
Published notification and investigation start times by severity	 Critical: 30 min (target)		Publishes average response times, not notification times by severity [9]
Executive summary every morning: what happened in the last 24 hours	 7:30 a.m.		No evidence of a daily summary [10]
Automated weekly, monthly, quarterly, and annual reports			Weekly, monthly, and quarterly reports; no public evidence of an annual report [11]
Assigned technical account manager (TAM) and quarterly reviews			Its help center mentions an assigned channel account manager; it doesn't publish a technical account manager (TAM) or quarterly reviews [12]
24/7 contact with support or security staff			24/7 SOC included; 24/7 help desk hours not confirmed [2]
Independent certification of operations (ISO 27001 or SOC 2 Type II)	 ISO/IEC 27001:2022		Its trust center shows SOC 2 Type II, GDPR, and CCPA; no ISO 27001 [13]
Fast start with a software agent: your devices' activity, visible within hours	 Typical: 2 to 4 hours		Lightweight agent deployable via RMM, with no implementation project [5]
Detection and response	15 of 15	3 complete +8 partial	
Continuous monitoring and event correlation (SIEM), aligned with MITRE ATT&CK (a reference framework of attack techniques)			Managed SIEM with correlation rules; MITRE ATT&CK not explicitly mentioned [4]
Advanced protection on every device (EDR/XDR): malware, ransomware, and vulnerability exploitation			Its own detection EDR; antivirus prevention relies on Microsoft Defender [9]
Web filtering on the device			No web filtering on the device [9]
Intrusion detection (IDS/IPS)			No IDS/IPS of its own [9]
Threat detection on the internal network (NDR)			No NDR; only ingests firewall and DNS logs into the SIEM [4]
Documented investigations enriched with threat intelligence			Athena builds context, a timeline, and known malicious infrastructure [7]
Incident management with a case log and response time measured per case			Incident reports with a timeline; MTTR per incident not published [7]
Response with device isolation and IP address blocking			Device isolation yes; IP blocking not documented [14]
Incident response with root cause analysis			Investigation and remediation included; no public evidence of a forensic analysis service [9]
Identity posture: MFA, privileged accounts, and conditional access			ISPM covers MFA, privileges, and conditional access in M365 only, Early Access [15]
Zero Trust: secure DNS, application access, and control of unauthorized applications (shadow IT)			No secure DNS, ZTNA, or shadow IT control [2]

Capability	TecnetSOC	Huntress SOC for IT providers	Evidence on Huntress
Offers it Offers it as an add-on Partial, limited, or requires another contract No public evidence Not part of its published offering			
Cloud security: alerts and posture			SIEM ingests AWS CloudTrail; no Azure posture or alerts [4]
Email security: spam, phishing, malware, and impersonation fraud (BEC)			ITDR detects BEC and malicious rules; no anti-spam gateway or quarantine [16]
Security awareness: phishing simulations and training with metrics			Its own Managed SAT with phishing simulations and metrics [2]
Prioritized security recommendations with an approval workflow			ESPM and ISPM prioritize and fix posture, in Early Access [1]
Exposure and IT management	12 of 12	0 complete +4 partial	
Unified asset and software inventory			ESPM shows detected applications and RMM; in Early Access, with general availability announced for 2027 [1]
Vulnerabilities prioritized by severity and likelihood of exploitation (CVSS, EPSS)			Vulnerabilities via Defender for Endpoint data; CVSS/EPSS not mentioned [1]
Priority for flaws already being exploited (CISA KEV catalog)			Prioritizes what is exploited in the real world; KEV not cited; Early Access [17]
Operating system and third-party application patching			ESPM highlights missing patches but doesn't deploy them [1]
Provider-operated patching, with published timelines by severity	 Critical: 48 h (target)		Doesn't run patching or offer patching times [1]
Closure verification: the scanner confirms the vulnerability is gone			No scanner verification that vulnerabilities are closed [1]
Patch validation in a pilot group before rollout			No patch rollout, and therefore no pilot group [1]
External attack surface: what your company exposes on the internet, with a risk score	 Score from 0 to 100		External Recon detects open ports on devices; no external attack surface management or risk score [9]
Alerts for domains that imitate your brand and for exposed credentials or keys			No typosquatting or exposed secrets detection [2]
Annual penetration test (pentest)	 Annual		No pentesting in its offering [2]
Remote monitoring and management (RMM)			Doesn't offer RMM; integrates with third-party RMM [5]
Uptime monitoring (NOC)			No uptime monitoring or NOC [2]
Backup and continuity	3 of 3	0 complete +0 partial	
Backup for servers, files, databases, virtual machines, and Microsoft 365	Add-on		No backup [2]
Immutable backup vault (cannot be altered or deleted), isolated per customer	Add-on		No immutable vault [2]
Disaster recovery with drills and measured recovery time (RTO)	Add-on Measured RTO		No disaster recovery [2]
Compliance	6 of 6	0 complete +1 partial	
Monthly evidence ready for auditors and insurers	 Monthly		"Audit-ready" SIEM with retention of up to 7 years; no monthly evidence package [4]
Readiness for ISO 27001, SOC 2, and PCI DSS with shared controls	Add-on		No GRC platform; only security awareness courses geared to SOC 2 and ISO 27001 [18]
Mexican regulatory readiness: CNBV Fintech, data protection (LFPDPPP), and NOM-024	Add-on		No coverage of Mexican regulations [2]
Risk management, controls, statement of applicability, and internal audits	Add-on		No risk management, controls, or SoA [2]

Capability	TecnetSOC	Huntress SOC for IT providers	Evidence on Huntress
✓ Offers it ✗ Not part of its published offering	ⓘ Offers it as an add-on ⓘ Partial, limited, or requires another contract	? No public evidence	
Auditor portal with an evidence room and a public trust page (trust center)	+ Add-on	✗	Trust Center for its own company only, not for the customer [13]
Business continuity, vendor risk, and data breach management	+ Add-on	✗	No continuity, vendor, or breach modules [2]
How it's purchased	Not counted		
Per-device pricing, with plans that stack	✓ Per device	ⓘ	Pricing per unit and per module (endpoint, identity, source); no stackable plans [2]
Free plan to get started	✓ Up to 10 devices	✗	No permanent free plan [2]
Free trial in your real environment	✓ 30 days	✓	Full free trial with 24/7 SOC; duration not officially published [2]
Available under your IT provider's brand	✓	ⓘ	Co-branding: reports with the IT provider's logo; the platform and training show the Huntress brand [19]
Full coverage	50	8 +18 partial	

— NEXT STEP

See it in your own operations

Try it in a real environment, without changing what already works for you.

The first agentic SOC in Spanish: platform, analysts, and support.

Request the 30-day Response trial

Start free with Visibility (up to 10 devices)

Or talk to a specialist

tecnetone.com/en/services/soc-as-a-service

HOW THE RESPONSE TRIAL WORKS

1 You install a single agent

2 You get the executive summary every morning

3 You decide with data from your environment

— APPENDIX

Methodology and sources

Who prepared it and how

We prepared it at TecnetOne and show you the source for every data point. The list of capabilities is based on the TecnetSOC catalog. We evaluated each provider's most complete published offering, including its own add-ons, and ours with the same rigor. We used only public information (official websites, documentation, and press releases) reviewed as of September 29, 2026.

What each status means

Offers it: the provider delivers it, operates it, and is accountable for it within its service, wherever the technology comes from. Add-on: available at an additional cost. Partial: limited scope, or requires another contract or another operator. No public evidence: no public information confirms it at the time of review; this does not mean the provider doesn't offer it. Not part of its published offering: its documentation indicates it is not included. Your team provides it: with a tool, that capability depends on your staff, your shifts, and your response times, not on the provider. When in doubt between two values, we chose the more conservative one.

How we make corrections

A provider may offer something it doesn't publish: confirm it directly with them. If you see outdated or incorrect information, write to us through our contact form and we'll correct it in the next version. We review this comparison every quarter and whenever a provider's published offering or our catalog changes.

Evaluated for Huntress: Huntress, full platform (Managed EDR, ITDR, SIEM, SAT, ISPM, and ESPM in Early Access, with 24/7 SOC), reviewed Sep 29, 2026

Evaluated for TecnetSOC: TecnetSOC in its most complete offering (Compliance plan, with the TecnetProtect and TecnetGRC add-ons), platform catalog soc.catalogo.tecnetone.com and tecnetone.com/servicios/soc-as-a-service, reviewed Sep 29, 2026. Same standard as the others. Add-ons at an additional cost count as part of the offering, just like the other providers' own add-ons.

1. www.huntress.com/platform/managed-espm (Differences you notice day to day)

2. www.huntress.com/pricing (Differences you notice day to day)

3. www.huntress.com/platform/managed-edr/managed-microsoft-defender (Differences you notice day to day)

4. www.huntress.com/platform/siem (Differences you notice day to day)

5. www.huntress.com/partners/msps (Differences you notice day to day)

TecnetSOC vs. Huntress · Comparison 2026.09

tecnetone.com/en/services/soc-as-a-service · Page 5 of 6

6. www.huntress.com/press-release/huntress-expands-channel-ecosystem-w... (Differences you notice day to day)
7. www.huntress.com/use-cases/athena (AI agents that investigate and filter alerts...)
8. support.huntress.io/hc/en-us/articles/19223729361939-Huntress-Relea... (Leadership reports in Spanish and in business...)
9. www.huntress.com/platform/managed-edr (Published notification and investigation...)
10. support.huntress.io/hc/en-us/sections/22539292694547-Reports (Executive summary every morning: what happened...)
11. support.huntress.io/hc/en-us/articles/4404012804115-Monthly-and-Qua... (Automated weekly, monthly, quarterly, and...)
12. support.huntress.io/hc/en-us/articles/10962580083731-How-can-I-chan... (Assigned technical account manager (TAM) and...)
13. trust.huntress.com/ (Independent certification of operations (ISO 27001...))
14. support.huntress.io/hc/en-us/articles/4404960349459-Managed-Host-Is... (Response with device isolation and IP...)
15. www.huntress.com/platform/managed-ispn (Identity posture: MFA, privileged accounts...)
16. www.huntress.com/platform/managed-itdr (Email security: spam, phishing, malware, and...)
17. www.huntress.com/press-release/huntress-platform-expands-new-postur... (Priority for flaws already being...)
18. www.huntress.com/platform/security-awareness-training/compliance/is... (Readiness for ISO 27001, SOC 2, and PCI...)
19. support.huntress.io/hc/en-us/articles/4414363214995-Add-Your-Compan... (Available under your IT provider's brand)

Sources and date. This comparison is informational and is prepared by TecnetOne so you can compare, capability by capability, what TecnetSOC includes versus the most complete published offering of each provider mentioned. The list of capabilities is TecnetOne's own catalog and may not include every feature of each provider. We used only public information (official websites, technical documentation, and press releases) reviewed as of September 29, 2026; version 2026.09, reviewed quarterly. "No public evidence" means that no public

information confirms it at the time of review, not that the provider cannot offer it in another way: confirm every detail directly with them. The sources for each data point are in each provider's individual comparison, linked at the bottom of the table.

Trademarks. Third-party names and trademarks belong to their respective owners and are used only to identify them and for informational comparison. None of these providers is affiliated with TecnetOne or sponsors or endorses this document.

TecnetSOC scope. Backup and the compliance platform (TecnetGRC) are add-ons at an additional cost. Our times are service targets for notification and investigation start, not for resolution (critical: 30 minutes, as a target). Patching is subject to the maintenance windows agreed with you and to the applications included in your profile. Compliance is delivered as readiness and evidence, not as certification. TecnetSOC is a TecnetOne service, with ISO/IEC 27001:2022 certified operations, available directly or through your IT provider.



A SOC that speaks your language.

See outdated or inaccurate information? [Write to us and we'll correct it.](#)