

TecnetSOC vs. eSentire

eSentire gives you a SOC. TecnetSOC gives you the case resolved: AI investigates, a person decides, and your team doesn't have to run it.

With eSentire, EDR and the scanner come from partner vendors licensed separately, your team applies the patches, and its SOC's operate from Canada and Ireland. With TecnetSOC, the same SOC operates EDR/XDR, SIEM, and patching, on your schedule.



35

capabilities where TecnetSOC goes further

15

capabilities where we match

0

capabilities where eSentire outperforms TecnetSOC

Of the 50: 35 where we go further and 15 where we match

Same list of 50 capabilities and same criteria for TecnetSOC and eSentire: 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

eSentire is a managed SOC service, like TecnetSOC. Here we compare each one's most complete published offering, capability by capability.

— WHAT SETS US APART

Differences you notice day to day

01

No SOC in LATAM and no support in Spanish

WITH ESENTIRE
Its SOC's are in Canada and Ireland, its support lines cover North America, Europe, the Middle East, Africa, and Asia-Pacific, and it doesn't publish support in Spanish. [\[1\]](#)

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

02

Your team applies the patches

WITH ESENTIRE
Atlas tells you what to patch, but your security team deploys the patch from Atlas or from your current tool, with no published patching timelines. [\[2\]](#)

WITH TECNETSOC
The SOC patches for you: it validates in a pilot group, installs critical patches within 48 h as a target, and closes when the scanner confirms it.

03

Tools from other vendors, at your cost

WITH ESENTIRE
Endpoint, cloud, and vulnerabilities rely on partner vendors such as CrowdStrike, SentinelOne, or Tenable, and the price varies based on your investment in that technology. [\[3\]](#)

WITH TECNETSOC
The most complete offering already includes EDR/XDR, web filtering, IDS/IPS, NDR, and email security, operated by the same SOC.

04

Identity, cloud, and forensics, separately

WITH ESENTIRE
Identity, cloud, an incident response retainer, dark web monitoring, and offensive security are purchased as add-ons separate from the MDR package. [\[3\]](#)

WITH TECNETSOC
The most complete offering includes identity posture, cloud security, incident response with forensics, external attack surface, and annual pentesting.

05

Reports depend on the package you pay for

WITH ESENTIRE
Essentials gets an annual report, Advanced a quarterly one, and only Complete adds the in-depth monthly review and the named risk advisor. [\[3\]](#)

WITH TECNETSOC
You get an executive summary every morning at 7:30 a.m. and weekly, monthly, quarterly, and annual reports in business language.

06

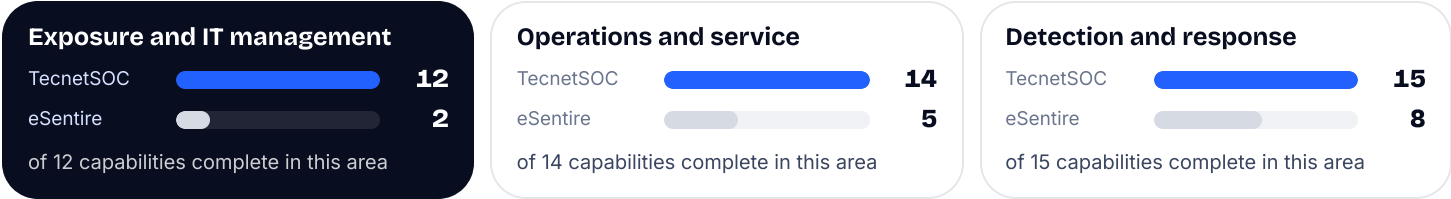
Security only, IT is separate

WITH ESENTIRE
The service focuses on detection and response; remote monitoring and management, uptime monitoring, and an IT help desk are purchased from another provider. [\[4\]](#)

WITH TECNETSOC
The most complete offering adds remote monitoring and management (RMM), uptime monitoring (NOC), and a 24/7 help desk.

— WHERE THE DIFFERENCE LIES

The three areas with the biggest gap



— CAPABILITY BY CAPABILITY

TecnetSOC and eSentire, side by side

Capability	TecnetSOC	eSentire SOC	Evidence on eSentire
 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  +6 partial	
24/7 security operations center (SOC) with human analysts			24/7 SOC with analysts averaging six years of tenure [5]
AI agents that investigate and filter alerts before passing them to an analyst			Agentic AI Operatives investigate with 30+ steps before the analyst [5]
Human Gate: a person approves every critical action before it runs			No action or isolation without an analyst's review and approval [5]

Capability	TecnetSOC	eSentire SOC	Evidence on eSentire
Offers it Offers it as an add-on Partial, limited, or requires another contract No public evidence Not part of its published offering			
AI investigation assistant in the portal that cites its sources	Neo		AI investigates and recommends; no evidence of an on-demand assistant that cites sources [5]
Operations in LATAM, the US, and Europe, with analysts in your time zone			SOCs in Waterloo and Cork; no operations in LATAM [6]
Analysts, support, and portal in native Spanish			No evidence of Spanish-speaking analysts or support [4]
Leadership reports in Spanish and in business language			Reports in English; no Spanish version [3]
Published notification and investigation start times by severity	Critical: 30 min (target)		Mean time to contain of 15 minutes as its own metric, not as a contractual commitment by severity [3]
Executive summary every morning: what happened in the last 24 hours	7:30 a.m.		No evidence of a daily executive summary [3]
Automated weekly, monthly, quarterly, and annual reports			Monthly reviews, quarterly reports, and an annual report in Complete; no weekly report [3]
Assigned technical account manager (TAM) and quarterly reviews			Named Cyber Risk Advisor or TAM and periodic reviews in Complete [3]
24/7 contact with support or security staff			24/7 direct line to the SOC, but no IT help desk [1]
Independent certification of operations (ISO 27001 or SOC 2 Type II)	ISO/IEC 27001:2022		ISO 27001, SOC 2 Type II, and PCI DSS certified [1]
Fast start with a software agent: your devices' activity, visible within hours	Typical: 2 to 4 hours		Value within hours without replacing tools, but it depends on the customer's EDR [5]
Detection and response	15 of 15	8 complete +5 partial	
Continuous monitoring and event correlation (SIEM), aligned with MITRE ATT&CK (a reference framework of attack techniques)			Unlimited event logging and multi-signal correlation in Atlas in all packages [3]
Advanced protection on every device (EDR/XDR): malware, ransomware, and vulnerability exploitation			No EDR of its own; uses the customer's CrowdStrike, SentinelOne, or Defender [5]
Web filtering on the device			No native web filtering on the device [7]
Intrusion detection (IDS/IPS)			Network signal included, relying on third-party firewalls; its own IDS not confirmed [5]
Threat detection on the internal network (NDR)			Network monitoring included in all MDR packages [3]
Documented investigations enriched with threat intelligence			Its own Threat Response Unit enriches investigations; auditable actions [7]
Incident management with a case log and response time measured per case			Unlimited incident handling with per-incident reports [3]
Response with device isolation and IP address blocking			Isolates hosts, suspends users, and cuts TCP connections [5]
Incident response with root cause analysis			Its own digital forensics and incident response (DFIR), through a retainer [8]
Identity posture: MFA, privileged accounts, and conditional access			Identity monitoring and response as an add-on; no published posture management [3]
Zero Trust: secure DNS, application access, and control of unauthorized applications (shadow IT)			No secure DNS, Zero Trust access, or shadow IT control [5]
Cloud security: alerts and posture			Cloud add-on with posture and workload protection (CSPM, CWPP, and CNAPP) [3]
Email security: spam, phishing, malware, and impersonation fraud (BEC)			Email through a partnership with Sublime Security (another vendor) [2]
Security awareness: phishing simulations and training with metrics			Its own Managed Phishing and Security Awareness Training [8]

Capability	TecnetSOC	eSentire SOC	Evidence on eSentire
✓ Offers it + Offers it as an add-on ● Partial, limited, or requires another contract ? No public evidence ✗ Not part of its published offering			
Prioritized security recommendations with an approval workflow	✓	●	vCISO and advisory reports; no evidenced approval workflow for recommendations [8]
Exposure and IT management	12 of 12	2 complete +5 partial	
Unified asset and software inventory	✓	●	Multi-scanner asset correlation; its own software inventory not evidenced [8]
Vulnerabilities prioritized by severity and likelihood of exploitation (CVSS, EPSS)	✓	✓	Managed Vulnerability Service included in Complete, on top of third-party scanners [3]
Priority for flaws already being exploited (CISA KEV catalog)	✓	●	Prioritizes by exposure and attacker behavior; use of KEV not confirmed [2]
Operating system and third-party application patching	✓	●	Patching from Atlas (Jul 2026) or via the customer's infrastructure; recently launched [2]
Provider-operated patching, with published timelines by severity	✓ Critical: 48 h (target)	✗	No published patching SLA or clarity on who operates the patch [2]
Closure verification: the scanner confirms the vulnerability is gone	✓	✗	No published closure verification [2]
Patch validation in a pilot group before rollout	✓	✗	No patch validation in a pilot group [2]
External attack surface: what your company exposes on the internet, with a risk score	✓ Score from 0 to 100	●	CTEM and Preempt cover external reconnaissance; no published exposure score [9]
Alerts for domains that imitate your brand and for exposed credentials or keys	✓	●	Dark web monitoring for credentials; typosquatting and secrets not evidenced [8]
Annual penetration test (pentest)	✓ Annual	✓	Continuous autonomous pentesting (Preempt) and offensive security services [9]
Remote monitoring and management (RMM)	✓	✗	No RMM [4]
Uptime monitoring (NOC)	✓	✗	No NOC or uptime monitoring [4]
Backup and continuity	3 of 3	0 complete +0 partial	
Backup for servers, files, databases, virtual machines, and Microsoft 365	+ Add-on	✗	No backup [4]
Immutable backup vault (cannot be altered or deleted), isolated per customer	+ Add-on	✗	No immutable vault [4]
Disaster recovery with drills and measured recovery time (RTO)	+ Add-on Measured RTO	✗	No disaster recovery [4]
Compliance	6 of 6	0 complete +1 partial	
Monthly evidence ready for auditors and insurers	✓ Monthly	?	No monthly evidence for auditors or insurers [3]
Readiness for ISO 27001, SOC 2, and PCI DSS with shared controls	+ Add-on	✗	No GRC platform for the customer [4]
Mexican regulatory readiness: CNBV Fintech, data protection (LFPDPPP), and NOM-024	+ Add-on	✗	No Mexican regulations [4]
Risk management, controls, statement of applicability, and internal audits	+ Add-on	●	Its virtual CISO assesses program maturity; no risk platform, statement of applicability, or audits [8]
Auditor portal with an evidence room and a public trust page (trust center)	+ Add-on	✗	No auditor portal or Trust Center for the customer [4]
Business continuity, vendor risk, and data breach management	+ Add-on	✗	No business continuity or vendor management [4]

Capability	TecnetSOC	eSentire SOC	Evidence on eSentire
✓ Offers it + Offers it as an add-on ⦿ Partial, limited, or requires another contract ? No public evidence ✗ Not part of its published offering			
How it's purchased	Not counted		
Per-device pricing, with plans that stack	✓ Per device	⦿	Per device with tiered packages; no public pricing, custom quote [3]
Free plan to get started	✓ Up to 10 devices	✗	No permanent free plan [3]
Free trial in your real environment	✓ 30 days	✓	Free 30-day Atlas deployment in the real environment [7]
Available under your IT provider's brand	✓	⦿	Resale under the eSentire brand; own branding only if the partner runs its own SOC [10]
Full coverage	50	15 +17 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 eSentire: eSentire MDR Complete package plus add-ons (identity, cloud, IR, dark web, CTM) and the Atlas platform (Response, Preempt, AIDR, email, patching), 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.

- [www.esentire.com/what-we-do/security-operations-center](#) (Differences you notice day to day)
- [www.esentire.com/news-releases/esentire-unifies-detection-response-...](#) (Differences you notice day to day)
- [www.esentire.com/how-we-do-it/mdr-pricing-packaging](#) (Differences you notice day to day)
- [www.esentire.com/](#) (Differences you notice day to day)
- [www.esentire.com/what-we-do/security-operations-platform](#) (24/7 security operations center (SOC) with human analysts)
- [mdrproviders.io/providers/esentire](#) (Operations in LATAM, the US, and Europe, with analysts...)
- [www.esentire.com/what-we-do/xdr-extended-detection-and-response](#) (Web filtering on the device)
- [www.esentire.com/what-we-do/exposure-vulnerability-and-risk-management](#) (Incident response with root cause analysis)
- [www.businesswire.com/news/home/20260618356205/en/eSentire-Launches-...](#) (External attack surface: what your company exposes...)

10. www.esentire.com/partners (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.](#)