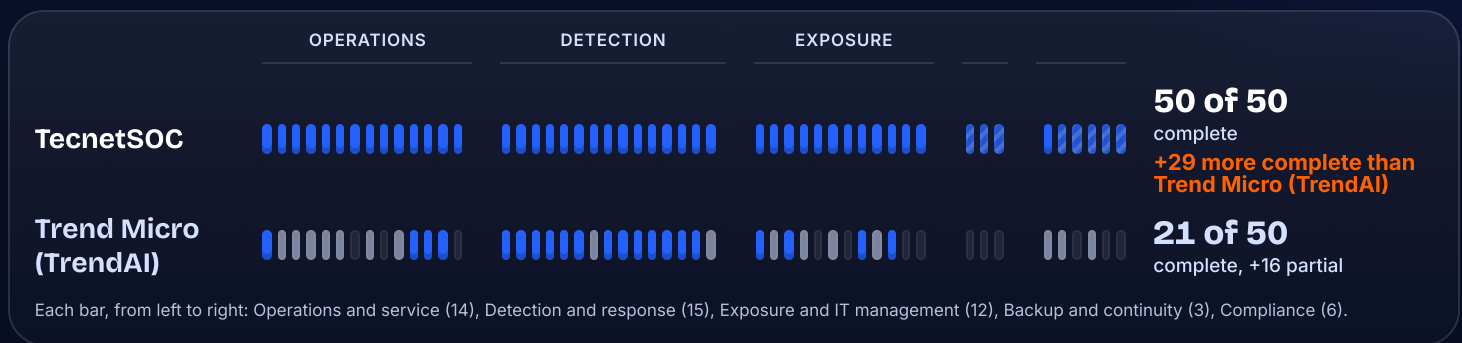


TecnetSOC vs. Trend Micro (TrendAI)

Trend Micro gives you the platform and the MDR. TecnetSOC gives you the complete service, operated in your language and in your time zone.

With Trend Micro, the SIEM consumes credits for every GB ingested and retained, and its patching is virtual: you install the official patch yourself. TecnetSOC charges per device, not per gigabyte, and its SOC installs the patches.



29

capabilities where TecnetSOC goes further

21

capabilities where we match

0

capabilities where Trend Micro (TrendAI) outperforms TecnetSOC

Of the 50: 29 where we go further and 21 where we match

Same list of 50 capabilities and same criteria for TecnetSOC and Trend Micro (TrendAI): 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

Trend Micro (TrendAI) offers a security platform with an MDR service; its modules are licensed separately. Here we compare its most complete service with its own add-ons, capability by capability.

— WHAT SETS US APART

Differences you notice day to day

01

Its operations centers, far from LATAM

WITH TREND MICRO (TRENDAl)

The MDR is operated from security operations centers (SOCs) in Dallas, Cork, Manila, and Singapore; none are in Latin America. [1]

WITH TECNETSOC

In-house analysts support you in your time zone and in native Spanish, with 24/7 operations in LATAM, the US, and Europe.

02

The SIEM charges per gigabyte, not per device

WITH TREND MICRO (TRENDAl)

The SIEM consumes credits for every GB of third-party data it ingests and, on top of that, every month for every GB retained. [2]

WITH TECNETSOC

You pay a per-device price, not per gigabyte, with stackable plans and Visibility free for up to 10 devices.

03

Virtual patching; the real patch is on you

WITH TREND MICRO (TRENDAl)

Patching is virtual (it blocks the attack on the network without fixing the software); the vendor says the official patch is still the definitive fix and doesn't document installing it for you. [3]

WITH TECNETSOC

The SOC installs patches prioritized by KEV and EPSS, validates them in a pilot group, and closes only when the scanner confirms the fix.

04

Recommends auto-approving all actions

WITH TREND MICRO (TRENDAl)

The MDR can act without your prior approval, and the vendor recommends turning on auto-approval for all actions. [4]

WITH TECNETSOC

AI agents investigate every alert, and a person approves every critical action before it runs (Human Gate).

05

Service terms, behind a password

WITH TREND MICRO (TRENDAl)

The MDR service descriptions are password-protected; before buying, you have to request the password from your account executive. [5]

WITH TECNETSOC

Times are published: for a critical incident, notification and investigation start within 30 minutes, as a target.

06

No RMM or NOC monitoring

WITH TREND MICRO (TRENDAl)

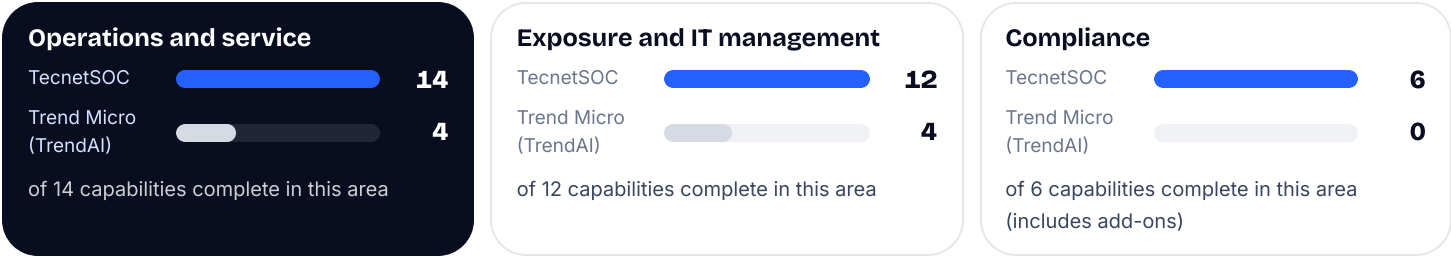
The platform doesn't include remote monitoring and management (RMM) or uptime monitoring; you purchase and operate those separately. [6]

WITH TECNETSOC

Remote monitoring and management (RMM) and uptime monitoring (NOC) come with the most complete offering.

— WHERE THE DIFFERENCE LIES

The three areas with the biggest gap



— CAPABILITY BY CAPABILITY

TecnetSOC and Trend Micro (TrendAl), side by side

Capability	TecnetSOC	Trend Micro (TrendAl) XDR and MDR	Evidence on Trend Micro (TrendAl)
 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	4 complete  +7 partial	
24/7 security operations center (SOC) with human analysts			24/7/365 MDR with human analysts; SOC's in Dallas, Cork, Manila, and Singapore [1]
AI agents that investigate and filter alerts before passing them to an analyst			MDR teams already use AI triage agents to support analysts; scope not detailed [7]

Capability	TecnetSOC	Trend Micro (TrendAI) XDR and MDR	Evidence on Trend Micro (TrendAI)
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			Manual approval per action, configurable by the customer; the provider recommends auto-approval [4]
AI investigation assistant in the portal that cites its sources	 Neo		Companion explains alerts and suggests steps; no evidence that it cites its sources [8]
Operations in LATAM, the US, and Europe, with analysts in your time zone			SOCs in the US, Ireland, the Philippines, and Singapore (follow the sun); none in LATAM [1]
Analysts, support, and portal in native Spanish			Spanish-language website and office in Mexico; no evidence of MDR analysts or a console in Spanish [9]
Leadership reports in Spanish and in business language			Monthly executive summaries; no evidence that they are delivered in Spanish [10]
Published notification and investigation start times by severity	 Critical: 30 min (target)		Publishes objectives (SLOs), not service level agreements (SLAs); times are in password-protected descriptions [5]
Executive summary every morning: what happened in the last 24 hours	 7:30 a.m.		No evidence of a daily executive summary [11]
Automated weekly, monthly, quarterly, and annual reports			Monthly executive summary and quarterly service review; no published weekly or annual reports [10]
Assigned technical account manager (TAM) and quarterly reviews			Named TAM, designated service manager, and quarterly business reviews in Complete [12]
24/7 contact with support or security staff			24/7/365 support by phone, email, and case portal [12]
Independent certification of operations (ISO 27001 or SOC 2 Type II)	 ISO/IEC 27001:2022		Vision One certified for ISO 27001, ISO 27017, and SOC 2 Type II [13]
Fast start with a software agent: your devices' activity, visible within hours	 Typical: 2 to 4 hours		No public evidence of onboarding time until activity data is visible [11]
Detection and response	15 of 15	13 complete +2 partial	
Continuous monitoring and event correlation (SIEM), aligned with MITRE ATT&CK (a reference framework of attack techniques)			Agentic SIEM and XDR correlate layers; observed techniques mapped to MITRE ATT&CK [14]
Advanced protection on every device (EDR/XDR): malware, ransomware, and vulnerability exploitation			Its own EDR/XDR with anti-ransomware and vulnerability exploit protection [15]
Web filtering on the device			Web filtering included in endpoint protection [15]
Intrusion detection (IDS/IPS)			Its own network IPS (TippingPoint, ZDI filters) and host IPS [16]
Threat detection on the internal network (NDR)			Its own AI-powered NDR with analysis of hundreds of protocols [16]
Documented investigations enriched with threat intelligence			Investigation with its own threat intelligence (ZDI) and detailed incident reports [11]
Incident management with a case log and response time measured per case			Case Management with priority and owner; no evidence of time measured per case [17]
Response with device isolation and IP address blocking			Endpoint isolation and IP blocking as response actions [18]
Incident response with root cause analysis			Root cause analysis in MDR and 40 hours of incident response in Complete [12]
Identity posture: MFA, privileged accounts, and conditional access			ITDR and identity posture: MFA, privileged accounts; Entra ID, AD, Okta [19]
Zero Trust: secure DNS, application access, and control of unauthorized applications (shadow IT)			Zero Trust Secure Access: application access (ZTNA), secure web gateway, and control of unauthorized apps; secure DNS not explicit [20]
Cloud security: alerts and posture			Its own Cloud Security (CNAPP, CSPM) with multicloud alerts and posture [21]

Capability	TecnetSOC	Trend Micro (TrendAI) XDR and MDR	Evidence on Trend Micro (TrendAI)
✓ Offers it ✚ Offers it as an add-on ⦿ Partial, limited, or requires another contract ? No public evidence ✗ Not part of its published offering			
Email security: spam, phishing, malware, and impersonation fraud (BEC)	✓	✓	Email and Collaboration Security: phishing, malware, ransomware, and BEC by writing style [22]
Security awareness: phishing simulations and training with metrics	✓	✓	Security awareness training with realistic phishing simulations within CREM [23]
Prioritized security recommendations with an approval workflow	✓	⦿	CREM provides prioritized recommendations and playbooks; no evidence of an approval workflow [23]
Exposure and IT management	12 of 12	4 complete +4 partial	
Unified asset and software inventory	✓	✓	CREM discovers devices, identities, applications, cloud, and unmanaged assets [23]
Vulnerabilities prioritized by severity and likelihood of exploitation (CVSS, EPSS)	✓	⦿	CVSS v3.1 plus its own exploitation potential rating; no explicit EPSS [24]
Priority for flaws already being exploited (CISA KEV catalog)	✓	✓	Checks KEV status and filters actively exploited vulnerabilities [24]
Operating system and third-party application patching	✓	⦿	Virtual patching only (host and network IPS); no documented patch deployment of its own [3]
Provider-operated patching, with published timelines by severity	✓ Critical: 48 h (target)	?	No evidence of provider-operated patching with timelines [11]
Closure verification: the scanner confirms the vulnerability is gone	✓	⦿	Continuous vulnerability assessment; no explicit closure verification workflow [23]
Patch validation in a pilot group before rollout	✓	?	No evidence of patch validation in a pilot group [19]
External attack surface: what your company exposes on the internet, with a risk score	✓ Score from 0 to 100	✓	Its own EASM with an organizational risk score and benchmarking [23]
Alerts for domains that imitate your brand and for exposed credentials or keys	✓	⦿	Dark web leak monitoring by domain; no evidence of lookalike domain alerts [25]
Annual penetration test (pentest)	✓ Annual	✓	Red and purple teaming with penetration testing as its own service [10]
Remote monitoring and management (RMM)	✓	?	No evidence of its own RMM [6]
Uptime monitoring (NOC)	✓	?	No evidence of uptime monitoring (NOC) [26]
Backup and continuity	3 of 3	0 complete +0 partial	
Backup for servers, files, databases, virtual machines, and Microsoft 365	✚ Add-on	?	No evidence of its own server or Microsoft 365 backup [6]
Immutable backup vault (cannot be altered or deleted), isolated per customer	✚ Add-on	?	No evidence of an immutable vault [6]
Disaster recovery with drills and measured recovery time (RTO)	✚ Add-on Measured RTO	?	No evidence of disaster recovery with measured RTO [26]
Compliance	6 of 6	0 complete +3 partial	
Monthly evidence ready for auditors and insurers	✓ Monthly	⦿	Auditor-ready compliance reports on demand; no published monthly delivery [23]
Readiness for ISO 27001, SOC 2, and PCI DSS with shared controls	✚ Add-on	⦿	Mapping to NIST, FedRAMP, GDPR, and CSPM frameworks; not full ISO/SOC 2 readiness [23]
Mexican regulatory readiness: CNBV Fintech, data protection (LFPDPPP), and NOM-024	✚ Add-on	?	No evidence of Mexican regulatory readiness [19]
Risk management, controls, statement of applicability, and internal audits	✚ Add-on	⦿	Risk quantification and automated controls; no statement of applicability or internal audit [23]
Auditor portal with an evidence room and a public trust page (trust center)	✚ Add-on	?	No evidence of an auditor portal or a public trust page for the customer [19]

Capability	TecnetSOC	Trend Micro (TrendAI) XDR and MDR	Evidence on Trend Micro (TrendAI)
✓ Offers it ✗ Not part of its published offering	ⓘ Offers it as an add-on ⓘ Partial, limited, or requires another contract	? No public evidence	
Business continuity, vendor risk, and data breach management	+ Add-on	?	No evidence of continuity, vendor risk, or breach management modules [19]
How it's purchased	Not counted		
Per-device pricing, with plans that stack	✓ Per device	ⓘ	Credit-based model; MDR by user tiers, minimum 251 [27]
Free plan to get started	✓ Up to 10 devices	?	No evidence of a permanent free plan [28]
Free trial in your real environment	✓ 30 days	✓	30-day free trial of the platform [28]
Available under your IT provider's brand	✓	ⓘ	Multi-tenant Vision One for Service Providers; no evidence of white labeling [28]
Full coverage	50	21 +16 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 Trend Micro (TrendAI): Trend Micro (TrendAI since Mar 2026): TrendAI Vision One with TrendAI Vision One Services Complete (MDR, incident response, premium support with a TAM) plus its own CREM, Endpoint, Email, Network, Cloud, Identity, and Zero Trust Secure Access modules, 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. success.trendmicro.com/en-US/solution/ka-0019617 (Differences you notice day to day)

2. docs.trendmicro.com/en-us/documentation/article/trend-vision-one-cr... (Differences you notice day to day)

3. www.trendaisecurity.com/en-us/resources-insights/deep-research/secu... (Differences you notice day to day)

4. success.trendmicro.com/en-US/solution/KA-0019492 (Differences you notice day to day)

5. success.trendmicro.com/en-US/solution/KA-0008963 (Differences you notice day to day)

6. www.trendaisecurity.com/en/platform (Differences you notice day to day)

7. newsroom.trendmicro.com (AI agents that investigate and filter alerts...)

8. www.trendmicro.com/en_us/business/ai/companion.html (AI investigation assistant in the portal that...)
9. www.trendmicro.com/es_mx/business/services/support-services.html (Analysts, support, and portal in native Spanish)
10. www.trendmicro.com/content/dam/trendmicro/global/en/core/docs/solut... (Leadership reports in Spanish and in business...)
11. www.trendmicro.com/en/business/services/managed-xdr.html (Executive summary every morning: what happened...)
12. www.trendmicro.com/en/business/services/service-one.html (Assigned technical account manager (TAM) and...)
13. www.trendmicro.com/en_us/about/trust-center/compliance.html (Independent certification of operations (ISO 27001...))
14. www.docs.trendmicro.com/en-us/enterprise/trend-vision-one/xdr-part/... (Continuous monitoring and event correlation...)
15. www.trendaisecurity.com/en/platform/endpoint-security (Advanced protection on every device (EDR/XDR)...))
16. www.trendaisecurity.com/en/platform/network-security (Intrusion detection (IDS/IPS))
17. docs.trendmicro.com/en-us/documentation/article/trend-vision-one-ca... (Incident management with a case log and response time...)
18. www.trendaisecurity.com/en/platform/security-operations (Response with device isolation and IP...)
19. www.trendaisecurity.com/en/platform/cyber-risk-exposure-management (Identity posture: MFA, privileged accounts...)
20. www.trendmicro.com/en_us/business/products/network/zero-trust-secu... (Zero Trust: secure DNS, application access, and...)
21. www.trendaisecurity.com/en/platform/cloud-security (Cloud security: alerts and posture)
22. www.trendaisecurity.com/en/platform/email-security (Email security: spam, phishing, malware, and...)
23. www.trendmicro.com/content/dam/trendmicro/global/en/core/docs/solut... (Security awareness: phishing...)
24. docs.trendmicro.com/en-us/documentation/article/trend-vision-one-TI... (Vulnerabilities prioritized by severity...)
25. docs.trendmicro.com/en-us/documentation/article/trend-vision-one-da... (Alerts for domains that imitate your brand...)
26. www.trendaisecurity.com/en/services (Uptime monitoring (NOC))
27. mdrproviders.io/providers/trend-micro (Per-device pricing, with plans that stack)
28. www.trendmicro.com/en_us/partners/service-providers.html (Free plan to get started)

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.