

TecnetSOC vs. Sophos

Sophos protects your devices and alerts you. TecnetSOC delivers the case resolved, in your language and with everything included.

With Sophos, MDR excludes restoring systems, patching is out of scope, and NDR is licensed separately. With TecnetSOC, the SOC handles patching, detection on your network is included, and you can add immutable backup and disaster recovery with TecnetProtect.



31

capabilities where TecnetSOC goes further

19

capabilities where we match

0

capabilities where Sophos outperforms TecnetSOC

Of the 50: 31 where we go further and 19 where we match

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

Sophos combines its protection products with its MDR service; email, firewall, network, and identity 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
Patching stays on your side

WITH SOPHOS
Managed Risk scans and prioritizes vulnerabilities, but patching is outside the service: your team installs every patch and is accountable for the result. [1]

WITH TECNETSOC
The SOC patches based on real-world exploitation (KEV and EPSS), validates in a pilot group, and considers it closed only when the scanner confirms.

02
Recovering your operations is separate

WITH SOPHOS
MDR incident response excludes restoring or recovering systems: getting back up and running after the attack is in your hands. [2]

WITH TECNETSOC
You can add TecnetProtect (at an additional cost): backup in an immutable vault per customer and disaster recovery with drills.

03
NDR, retention, and integrations, licensed separately

WITH SOPHOS
MDR keeps 90 days of data; one year of retention, NDR, and integrating third-party firewall, email, or cloud require additional licenses. [3]

WITH TECNETSOC
The most complete offering already includes SIEM, internal network detection (NDR), identity, cloud, and email in a single service.

04
Sixty days to get covered

WITH SOPHOS
MDR onboarding is a phased 60-day plan: your team installs the agent until 90% of devices are covered. [4]

WITH TECNETSOC
You install one agent, the rest deploys on its own, and you typically see activity in 2 to 4 hours; full operations typically in under 7 days.

05
No direct line for LATAM

WITH SOPHOS
MDR phone lines cover EMEA, APAC, and North America; from LATAM, you're asked to contact the nearest operations center. [5]

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

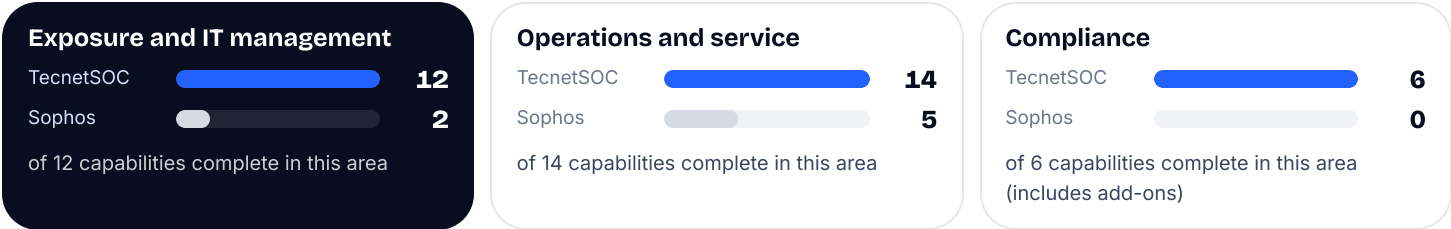
06
No executive summary every morning

WITH SOPHOS
MDR generates automated weekly and monthly reports for console administrators; it doesn't document a daily executive summary or quarterly reports. [6]

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

— WHERE THE DIFFERENCE LIES

The three areas with the biggest gap



— CAPABILITY BY CAPABILITY

TecnetSOC and Sophos, side by side

Capability	TecnetSOC	Sophos EDR and MDR	Evidence on Sophos
 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	
		 +7 partial	
24/7 security operations center (SOC) with human analysts			24/7/365 monitoring, investigation, and response by the MDR Ops team [2]
AI agents that investigate and filter alerts before passing them to an analyst			Triage Agent and Case Investigation Agent filter and analyze before the analyst [7]
Human Gate: a person approves every critical action before it runs			Collaborate mode requires your consent; in Authorize mode it acts without consulting you [8]

Capability	TecnetSOC	Sophos EDR and MDR	Evidence on Sophos
 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 Assistant investigates in natural language; doesn't document source citations; English only [9]
Operations in LATAM, the US, and Europe, with analysts in your time zone			Nine regional teams; phone lines only for EMEA, APAC, and North America, none for LATAM [5]
Analysts, support, and portal in native Spanish			Console in Spanish; AI in English only; analyst support in Spanish subject to availability or through third-party translation [10]
Leadership reports in Spanish and in business language			Monthly technical reports; no evidence of an executive report in Spanish [11]
Published notification and investigation start times by severity	 Critical: 30 min (target)		Publishes case in 2 min, action in 30 min, and a 60-min SLA; not by severity [2]
Executive summary every morning: what happened in the last 24 hours	 7:30 a.m.		No evidence of a daily executive summary [6]
Automated weekly, monthly, quarterly, and annual reports			Automated weekly and monthly reports; no quarterly or annual reports [12]
Assigned technical account manager (TAM) and quarterly reviews			Named TAM with quarterly reviews, a paid add-on on top of Enhanced Plus [13]
24/7 contact with support or security staff			24/7/365 direct line with Sophos to review incidents [2]
Independent certification of operations (ISO 27001 or SOC 2 Type II)	 ISO/IEC 27001:2022		ISO 27001:2022 and SOC 2 published in its Trust Center [14]
Fast start with a software agent: your devices' activity, visible within hours	 Typical: 2 to 4 hours		Phased 60-day onboarding; no commitment to activity data within hours [4]
Detection and response	15 of 15	12 complete +3 partial	
Continuous monitoring and event correlation (SIEM), aligned with MITRE ATT&CK (a reference framework of attack techniques)			XDR with data lake, correlation, MITRE ATT&CK, and its own Next-Gen SIEM [15]
Advanced protection on every device (EDR/XDR): malware, ransomware, and vulnerability exploitation			Sophos Endpoint (Intercept X) with EDR/XDR against malware, vulnerability exploitation, and ransomware [16]
Web filtering on the device			DNS Protection and web control on the device against malicious content [17]
Intrusion detection (IDS/IPS)			Its own Sophos Firewall with deep inspection and intrusion prevention [18]
Threat detection on the internal network (NDR)			Its own Sophos NDR monitors internal traffic, IoT/OT, and unauthorized devices [19]
Documented investigations enriched with threat intelligence			Enrichment with Sophos X-Ops; documented verdict with IoCs and a timeline [7]
Incident management with a case log and response time measured per case			Cases tracked in Fusion; SLA measured monthly, not per case [2]
Response with device isolation and IP address blocking			Device isolation, indicator blocking, and Active Threat Response on the firewall [2]
Incident response with root cause analysis			MDR Plus: full response with no hour cap and root cause analysis [20]
Identity posture: MFA, privileged accounts, and conditional access			ITDR: more than 160 posture checks in Entra ID and Active Directory [21]
Zero Trust: secure DNS, application access, and control of unauthorized applications (shadow IT)			Workspace Protection: ZTNA, DNS Protection, and shadow IT control [17]
Cloud security: alerts and posture			Workload protection and cloud alerts; Cloud Optix CSPM reaches end of life Sep 30, 2026 [22]
Email security: spam, phishing, malware, and impersonation fraud (BEC)			Sophos Email: spam, phishing, malware, BEC, and impersonation, integrated with MDR [23]

Capability	TecnetSOC	Sophos EDR and MDR	Evidence on Sophos
Offers it Offers it as an add-on Partial, limited, or requires another contract No public evidence Not part of its published offering			
Security awareness: phishing simulations and training with metrics			Phish Threat: simulations, more than 30 training modules, nine languages [24]
Prioritized security recommendations with an approval workflow			Account Health Check prioritizes and fixes after you confirm; Sophos configuration only [25]
Exposure and IT management	12 of 12	2 complete	
		+5 partial	
Unified asset and software inventory			Managed Risk discovers assets; software inventory only through XDR queries [26]
Vulnerabilities prioritized by severity and likelihood of exploitation (CVSS, EPSS)			Prioritizes with Tenable VPR; CVSS and EPSS not explicit [26]
Priority for flaws already being exploited (CISA KEV catalog)			Scans when newly exploited vulnerabilities appear; use of the KEV catalog not documented [27]
Operating system and third-party application patching			No patching of its own; Managed Risk leaves remediation to the customer [1]
Provider-operated patching, with published timelines by severity	 Critical: 48 h (target)		Patching and remediation outside the scope of the service [1]
Closure verification: the scanner confirms the vulnerability is gone			Weekly scans reflect closure; no formal remediation verification [1]
Patch validation in a pilot group before rollout			No evidence of a pilot group for patches [1]
External attack surface: what your company exposes on the internet, with a risk score	 Score from 0 to 100		Managed Risk: weekly inventory of external assets and risk prioritization [1]
Alerts for domains that imitate your brand and for exposed credentials or keys			ITDR searches for leaked credentials on the dark web; no lookalike domain alerts [21]
Annual penetration test (pentest)	 Annual		Advisory Services: external, internal, wireless, and web application pentests [28]
Remote monitoring and management (RMM)			No RMM in the Sophos Fusion portfolio [15]
Uptime monitoring (NOC)			No evidence of uptime monitoring (NOC) [15]
Backup and continuity	3 of 3	0 complete	
		+0 partial	
Backup for servers, files, databases, virtual machines, and Microsoft 365	Add-on		No backup product in the Sophos Fusion portfolio [15]
Immutable backup vault (cannot be altered or deleted), isolated per customer	Add-on		No evidence of a backup vault [15]
Disaster recovery with drills and measured recovery time (RTO)	Add-on Measured RTO		Incident response excludes restoring or recovering systems [2]
Compliance	6 of 6	0 complete	
		+3 partial	
Monthly evidence ready for auditors and insurers	 Monthly		CISO Advantage stores evidence for audits and insurance; rollout by region [29]
Readiness for ISO 27001, SOC 2, and PCI DSS with shared controls	Add-on		CISO Advantage maps to NIST and CIS; ISO 27001, SOC 2, and PCI not documented [29]
Mexican regulatory readiness: CNBV Fintech, data protection (LFPDPPP), and NOM-024	Add-on		No evidence of Mexican regulations [29]
Risk management, controls, statement of applicability, and internal audits	Add-on		CISO Advantage: risk assessment and roadmap; no SoA or internal audit [29]
Auditor portal with an evidence room and a public trust page (trust center)	Add-on		No evidence of an auditor portal or trust page for the customer [29]
Business continuity, vendor risk, and data breach management	Add-on		No evidence of continuity, vendor risk, or breach management [29]

Capability	TecnetSOC		Sophos EDR and MDR	Evidence on Sophos
✓ Offers it ✗ Not part of its published offering	+ Offers it as an add-on ⓘ Partial, limited, or requires another contract	? No public evidence		
How it's purchased	Not counted			
Per-device pricing, with plans that stack	✓ Per device	ⓘ	Per-user and per-server pricing; two MDR tiers plus add-ons [16]	
Free plan to get started	✓ Up to 10 devices	?	No free business plan; only free tools and trials [30]	
Free trial in your real environment	✓ 30 days	ⓘ	Free trials of XDR, Email, Firewall, and more; no trial of the MDR service [31]	
Available under your IT provider's brand	✓	ⓘ	Co-branding with the partner's logo in the portal and reports; service under the Sophos brand [32]	
Full coverage	50	19 +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 Sophos: Sophos MDR, most complete offering (Sophos MDR Plus, formerly MDR Complete, with Sophos XDR and a 24/7 SOC, plus its own add-ons: NDR, ITDR, Email, Phish Threat, Firewall, Workspace Protection with ZTNA and DNS Protection, Managed Risk with Tenable, Advisory Services, TAM, and CISO Advantage, all in the Sophos Fusion console, formerly Sophos Central), 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.sophos.com/en-us/legal/managed-risk-description (Differences you notice day to day)

2. www.sophos.com/en-us/legal/mdr-description (Differences you notice day to day)

3. docs.sophos.com/central/customer/help/en-us/ManageYourProducts/MDR/... (Differences you notice day to day)

4. docs.sophos.com/central/customer/help/en-us/GettingStarted/onboardi... (Differences you notice day to day)

5. docs.sophos.com/central/customer/help/en-us/ManageYourProducts/MDR/... (Differences you notice day to day)

6. docs.sophos.com/central/customer/help/en-us/ManageYourProducts/MDR/... (Differences you notice day to day)

7. www.sophos.com/en-us/blog/sophos-ai-agents-accelerating-mdr-and-pow... (AI agents that investigate and filter alerts...)

8. docs.sophos.com/central/customer/help/en-us/ManageYourProducts/MDR/... (Human Gate: a person approves every...)
9. docs.sophos.com/central/customer/help/en-us/AI/AIfeatures/index.html (AI investigation assistant in the portal that...)
10. docs.sophos.com/central/customer/help/en-us/ManageYourAccount/Langu... (Analysts, support, and portal in native Spanish)
11. docs.sophos.com/central/customer/help/en-us/ManageYourProducts/MDR/... (Leadership reports in Spanish and in business...)
12. docs.sophos.com/central/enterprise/help/en-us/MDR/MDRreporthisstory/... (Automated weekly, monthly, quarterly, and...)
13. docs.sophos.com/support/help/en-us/services-guide/tam/ (Assigned technical account manager (TAM) and...)
14. www.sophos.com/en-us/trust/business-certifications (Independent certification of operations (ISO 27001...))
15. www.sophos.com/en-us/press/press-releases/2026/07/sophos-fusion-ai-... (Continuous monitoring and event correlation...)
16. www.sophos.com/en-us/products/endpoint-security/how-to-buy (Advanced protection on every device (EDR/XDR)...))
17. www.sophos.com/en-us/products/workspace-protection (Web filtering on the device)
18. www.sophos.com/en-us/products/next-gen-firewall (Intrusion detection (IDS/IPS))
19. www.sophos.com/en-us/products/network-detection-and-response (Threat detection on the internal network (NDR))
20. www.sophos.com/en-us/services/managed-detection-and-response (Incident response with root cause analysis)
21. www.sophos.com/en-us/products/identity-threat-detection-and-response (Identity posture: MFA, privileged accounts...)
22. community.sophos.com/sophos-cloud-optix/b/blog/posts/sophos-cloud-o-... (Cloud security: alerts and posture)
23. www.sophos.com/en-us/products/sophos-email (Email security: spam, phishing, malware, and...)
24. www.sophos.com/en-us/products/phish-threat (Security awareness: phishing...)
25. docs.sophos.com/central/customer/help/en-us/ManageYourProducts/Acco... (Prioritized security recommendations with an...)
26. www.sophos.com/en-us/products/managed-risk (Unified asset and software inventory)
27. www.sophos.com/en-us/services/managed-risk (Priority for flaws already being...)
28. www.sophos.com/en-us/products/advisory-services/security-testing (Annual penetration test (pentest))
29. www.sophos.com/en-us/products/ciso-advantage (Monthly evidence ready for auditors and insurers)
30. www.sophos.com/en-us/free-tools (Free plan to get started)
31. www.sophos.com/en-us/free-trials (Free trial in your real environment)
32. docs.sophos.com/central/partner/help/en-us/Help/GlobalSettings/Plat... (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.](#)