

TecnetSOC vs. Acronis

Acronis backs up and protects your devices. TecnetSOC is the agentic SOC that runs all your security for you, 24/7.

With Acronis, 24/7 MDR is purchased separately from your backup, and its catalog doesn't include detection on your internal network. **With TecnetSOC, 24/7 monitoring is the service, with detection on your internal network and an executive summary every morning.**



32

capabilities where TecnetSOC goes further

18

capabilities where we match

1

capability where Acronis outperforms TecnetSOC
Included in the 18 where we match

Of the 50: 32 where we go further and 18 where we match

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

Acronis is a protection and backup platform sold through IT providers (MSPs); its SOC service is purchased and delivered through them, and each module is licensed 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
Your provider installs, configures, and fine-tunes

WITH ACRONIS
Your IT provider deploys the agents, configures the policies, chooses the critical devices, and resolves the exclusions the SOC asks for. [\[1\]](#)

WITH TECNETSOC
You install one agent, the rest of the platform deploys on its own, and TecnetOne analysts run it 24/7, with no implementation project.

02
24/7 monitoring is purchased separately

WITH ACRONIS
The 24/7 SOC (MDR) doesn't come with the platform: it's billed separately, just like security awareness, and your provider decides whether to purchase it. [\[2\]](#)

WITH TECNETSOC
24/7 SOC operations are the service itself: nothing is added separately; you pay per device with stackable plans.

03
Remediation depends on the tier purchased

WITH ACRONIS
In MDR Standard, the SOC recommends and your provider remediates, including rolling back changes (rollback); in Advanced, patching or running scripts requires a remote monitoring and management (RMM) license. [\[1\]](#)

WITH TECNETSOC
The SOC carries out response and patching, with RMM in the most complete offering, and a person approves every critical action.

04
Your internal network is left out

WITH ACRONIS
MDR starts from what its EDR/XDR agent detects; its catalog doesn't offer IDS/IPS or internal network detection (NDR). [\[1\]](#)

WITH TECNETSOC
The most complete offering adds IDS/IPS and internal network detection (NDR) to SIEM with MITRE ATT&CK, identity, cloud, and email.

05
Alerts go to your provider

WITH ACRONIS
The SOC notifies, calls, and requests approvals from the contacts your IT provider registers, and they are the ones who receive the monthly report. [\[1\]](#)

WITH TECNETSOC
You purchase it directly or through your provider, and every morning at 7:30 a.m. you get an executive summary in business language.

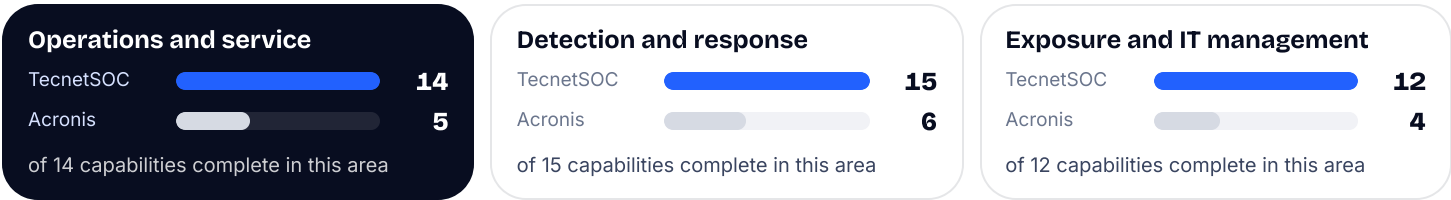
06
Vendor support in English only

WITH ACRONIS
Its technical support is available only in English and only to your IT provider; you have no direct channel with the vendor. [\[3\]](#)

WITH TECNETSOC
Operations and the 24/7 help desk are in native Spanish, with multilingual support and analysts in your time zone.

— WHERE THE DIFFERENCE LIES

The three areas with the biggest gap



— CAPABILITY BY CAPABILITY

TecnetSOC and Acronis, side by side

Capability	TecnetSOC	Acronis Platform and SOC through IT providers	Evidence on Acronis
 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  +9 partial	
24/7 security operations center (SOC) with human analysts			24/7 MDR run by the Acronis TRU SOC since April 2026, also by partners; purchased and delivered through the IT provider [4]
AI agents that investigate and filter alerts before passing them to an analyst			EDR prioritizes suspicious activity and summarizes incidents with AI; no agents filter each alert [5]

Capability	TecnetSOC	Acronis Platform and SOC through IT providers	Evidence on Acronis
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			IT provider approval only on critical devices; the rest are isolated without prior approval [1]
AI investigation assistant in the portal that cites its sources	 Neo		Acronis Copilot investigates in natural language, but is still in early access [5]
Operations in LATAM, the US, and Europe, with analysts in your time zone			No evidence of a SOC in LATAM; partner managed security providers cited in the United Kingdom, Australia, Asia, and Europe [4]
Analysts, support, and portal in native Spanish			Official support for service providers in English only; the platform portal is available in 26 languages [3]
Leadership reports in Spanish and in business language			Executive Summary report for the customer; no evidence of it being written in Spanish or in business language [6]
Published notification and investigation start times by severity	 Critical: 30 min (target)	 15 min, average	Average investigation start: 15 min for high and critical, 30 min for low and medium; alerts go to the IT provider [1]
Executive summary every morning: what happened in the last 24 hours	 7:30 a.m.		Daily schedulable reports in the portal; no daily executive summary of what happened [7]
Automated weekly, monthly, quarterly, and annual reports			Scheduled reports in the portal and a monthly MDR report; no documented quarterly or annual reports [1]
Assigned technical account manager (TAM) and quarterly reviews			Paid Technical Account Management service from Acronis Professional Services [8]
24/7 contact with support or security staff			24/7 contact in English for the IT provider only; the end customer has no direct channel with Acronis [9]
Independent certification of operations (ISO 27001 or SOC 2 Type II)	 ISO/IEC 27001:2022		Trust Center states ISO/IEC 27000 series, SOC 2, and PCI DSS [10]
Fast start with a software agent: your devices' activity, visible within hours	 Typical: 2 to 4 hours		A single agent and console; MDR is activated with one click on top of EDR or XDR [11]
Detection and response	15 of 15	6 complete +5 partial	
Continuous monitoring and event correlation (SIEM), aligned with MITRE ATT&CK (a reference framework of attack techniques)			XDR correlates events with MITRE ATT&CK; it's not a SIEM for third-party logs [5]
Advanced protection on every device (EDR/XDR): malware, ransomware, and vulnerability exploitation			EDR/XDR with behavioral detection, vulnerability exploit prevention, and anti-ransomware with rollback [12]
Web filtering on the device			URL filtering included in device protection [5]
Intrusion detection (IDS/IPS)			Does not offer network IDS/IPS [13]
Threat detection on the internal network (NDR)			No NDR; Device Sense only discovers devices without an agent [14]
Documented investigations enriched with threat intelligence			Real-time intelligence feed, IoC search, and enrichment in MDR [5]
Incident management with a case log and response time measured per case			Incidents with ticket, status, and resolution; MDR reports with MTTR and SLA [1]
Response with device isolation and IP address blocking			Isolation and quarantine included; no evidence of IP address blocking as a response action [12]
Incident response with root cause analysis			Forensic backup and root cause analysis in MDR Advanced [1]
Identity posture: MFA, privileged accounts, and conditional access			Microsoft 365 posture and actions in Entra ID; no Google Workspace posture [15]
Zero Trust: secure DNS, application access, and control of unauthorized applications (shadow IT)			No secure DNS or Zero Trust access; only GenAI usage control by URL [12]

Capability	TecnetSOC	Acronis Platform and SOC through IT providers	Evidence on Acronis
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			No Azure alert or posture monitoring; Azure only as a DR target [16]
Email security: spam, phishing, malware, and impersonation fraud (BEC)			Acronis-branded Email Security with a third-party engine; licensed per user separately from device protection [17]
Security awareness: phishing simulations and training with metrics			Its own SAT with phishing simulations, courses, and a multi-customer console [18]
Prioritized security recommendations with an approval workflow			M365 posture baselines and CyberFit Score; no documented approval workflow [15]
Exposure and IT management	12 of 12	4 complete +4 partial	
Unified asset and software inventory			Hardware and software inventory with RMM, plus Device Sense discovery [14]
Vulnerabilities prioritized by severity and likelihood of exploitation (CVSS, EPSS)			Operating system and third-party application vulnerability assessment; no documented EPSS prioritization [19]
Priority for flaws already being exploited (CISA KEV catalog)			No public evidence of prioritization by the CISA KEV catalog [19]
Operating system and third-party application patching			Operating system and third-party application patching with RMM [14]
Provider-operated patching, with published timelines by severity	 Critical: 48 h (target)		MDR Advanced can run patches as remediation; no published patching times [11]
Closure verification: the scanner confirms the vulnerability is gone			Scheduled scans reflect the status; no explicit closure verification [19]
Patch validation in a pilot group before rollout			Automatic patch approval with testing: if patches install successfully on the test devices, they roll out to the rest [20]
External attack surface: what your company exposes on the internet, with a risk score	 Score from 0 to 100		Does not offer EASM [13]
Alerts for domains that imitate your brand and for exposed credentials or keys			Does not detect typosquatting or exposed secrets [13]
Annual penetration test (pentest)	 Annual		Does not offer pentesting; professional services cover audits of its own solution [5]
Remote monitoring and management (RMM)			Its own RMM with remote desktop, scripting, and automation [14]
Uptime monitoring (NOC)			System and hardware monitoring with alerts; Acronis does not run a NOC [14]
Backup and continuity	3 of 3	3 complete +0 partial	
Backup for servers, files, databases, virtual machines, and Microsoft 365	Add-on		Backup for servers, VMs, applications, files, and Microsoft 365 [2]
Immutable backup vault (cannot be altered or deleted), isolated per customer	Add-on		Immutable storage in Acronis Cloud, isolated per customer tenant [21]
Disaster recovery with drills and measured recovery time (RTO)	Add-on Measured RTO		DR with runbooks and automated monthly failover tests [16]
Compliance	6 of 6	0 complete +1 partial	
Monthly evidence ready for auditors and insurers	 Monthly		M365 posture compliance reports and executive reports; not a monthly evidence package [15]
Readiness for ISO 27001, SOC 2, and PCI DSS with shared controls	Add-on		No GRC platform; only support guides for ISO 27001 [22]
Mexican regulatory readiness: CNBV Fintech, data protection (LFPDPPP), and NOM-024	Add-on		No Mexican frameworks (CNBV, LFPDPPP, NOM-024) [10]

Capability	TecnetSOC	Acronis Platform and SOC through IT providers	Evidence on Acronis
✓ Offers it + Offers it as an add-on ⓪ Partial, limited, or requires another contract ? No public evidence ✗ Not part of its published offering			
Risk management, controls, statement of applicability, and internal audits	+ Add-on	✗	Does not manage risks, SoA, or internal audits [13]
Auditor portal with an evidence room and a public trust page (trust center)	+ Add-on	✗	Trust Center belongs to Acronis, not to the end customer [23]
Business continuity, vendor risk, and data breach management	+ Add-on	✗	Technical DR yes, but no GRC modules for continuity, vendors, or breaches [13]
How it's purchased	Not counted		
Per-device pricing, with plans that stack	✓ Per device	⓪	Per workload, user, or GB depending on the service, or by bundle; no stackable per-device plans [2]
Free plan to get started	✓ Up to 10 devices	⓪	Essential security features at no cost, but within a contract with a minimum commitment [13]
Free trial in your real environment	✓ 30 days	✓	30-day free trial [24]
Available under your IT provider's brand	✓	✓	Sold only through service providers under their own brand (white label) [25]
Full coverage	50	18 +19 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 Acronis: Acronis Cyber Protect Cloud in its most complete offering (Ultimate Protection or individual services: EDR, XDR, MDR Advanced by Acronis TRU, Email Security, Collaboration Security, Security Posture Management, SAT, DLP, RMM, PSA, Backup, Backup M365, Disaster Recovery). Sold only to service providers (IT providers), licensed per workload, per user, or per GB with a minimum monthly commitment; the platform is run by the IT provider, and MDR is run by the Acronis SOC (TRU) or a partner managed security provider. 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.acronis.com/mdr-service-definition (Differences you notice day to day)	10. www.acronis.com/en/trust-center/compliance/ (Independent certification of operations (ISO 27001...))	18. www.acronis.com/en/products/cloud/cyber-protect/security-awareness-... (Security awareness: phishing...)
2. www.acronis.com/en/products/cloud/cyber-protect/pricing/ (Differences you notice day to day)	11. www.acronis.com/en/products/cloud/cyber-protect/managed-detection-a... (Fast start with a software agent: your...)	19. www.acronis.com/en/solutions/cloud/vulnerability-assessments/ (Vulnerabilities prioritized by severity...)
3. www.acronis.com/en/support/serviceproviderscope/ (Differences you notice day to day)	12. www.acronis.com/en/products/cloud/cyber-protect/security-edr/ (Advanced protection on every device (EDR/XDR)...)	20. www.acronis.com/en-us/support/documentation/CyberProtectionService/.. (Patch validation in a pilot group...)
4. www.acronis.com/en/pr/2026/acronis-launches-mdr-by-acronis-tru-to-p... (24/7 security operations center (SOC) with human analysts)	13. www.acronis.com/en/products/cloud/cyber-protect/ (Intrusion detection (IDS/IPS))	21. www.acronis.com/en/products/cloud/cyber-protect/backup/ (Immutable backup vault (cannot be altered or...))
5. www.acronis.com/en/products/cloud/cyber-protect/extended-detection-... (AI agents that investigate and filter alerts...)	14. www.acronis.com/en/products/cloud/cyber-protect/rmm-solution/ (Threat detection on the internal network (NDR))	22. www.acronis.com/en/compliance/iso-27001/ (Readiness for ISO 27001, SOC 2, and PCI...)
6. www.acronis.com/en/resource-center/resource/executive-summary-repor... (Leadership reports in Spanish and in business...)	15. www.acronis.com/en/solutions/cloud/microsoft-365-security-posture-m... (Identity posture: MFA, privileged accounts...)	23. www.acronis.com/en/trust-center/ (Auditor portal with an evidence room and a...)
7. www.acronis.com/en/support/documentation/AcronisCyberCloud/reportin... (Executive summary every morning: what happened...)	16. www.acronis.com/en/products/cloud/cyber-protect/disaster-recovery/ (Cloud security: alerts and posture)	24. www.acronis.com/en/products/cloud/trial/ (Free trial in your real environment)
8. www.acronis.com/en/services/technical-account-management/ (Assigned technical account manager (TAM) and...)	17. www.acronis.com/en/products/cloud/cyber-protect/email-security/ (Email security: spam, phishing, malware, and...)	25. www.acronis.com/en/partners/service-providers/ (Available under your IT provider's brand)
9. www.acronis.com/en/support/serviceproviderguidelines/ (24/7 contact with support or security staff)		

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.