

TecnetSOC vs. Automox

Automox automates one task. TecnetSOC runs all your security for you: AI that investigates and people who decide.

With Automox, even with Turnkey Results you approve and operate, you depend on another vendor's scanner, and attack detection lives in another tool. **With TecnetSOC, the SOC prioritizes by real-world exploitation, patches, and monitors 24/7.**



44

capabilities where TecnetSOC goes further

6

capabilities where we match

0

capabilities where Automox outperforms TecnetSOC

Of the 50: 44 where we go further and 6 where we match

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

Automox is a patch automation tool that your team configures; it's not a managed SOC service. Detection, response, and 24/7 monitoring are products and services that are purchased and operated separately. This comparison shows, capability by capability, how much of what TecnetSOC includes Automox covers on its own and what you would have to add in products, contracts, and staff.

— WHAT SETS US APART

Differences you notice day to day

01
Automox configures, you operate

WITH AUTOMOX
Even in its Turnkey Results program, Automox configures and you approve: patching decisions and day-to-day operations stay with your team. [1]

WITH TECNETSOC
Our SOC runs patching: it validates in a pilot group and installs critical patches within 48 h and important ones within 7 days, as a target.

02
Patches, but doesn't detect attacks

WITH AUTOMOX
Detection and response stay in another tool: it presents itself as a complement to CrowdStrike, so EDR, SIEM, and whoever monitors them are purchased separately. [2]

WITH TECNETSOC
EDR/XDR, SIEM with MITRE ATT&CK correlation, and in-house analysts monitoring 24/7 come with the most complete offering.

03
You need another vulnerability scanner

WITH AUTOMOX
To know which vulnerabilities you have, you depend on another vendor's scanner (CrowdStrike, Tenable, or Qualys) whose findings you import into the console. [3]

WITH TECNETSOC
We prioritize by real-world exploitation (CISA KEV and EPSS) and consider a vulnerability closed only when the scanner confirms it.

04
Support during US business hours

WITH AUTOMOX
You can open tickets at any time, but published support hours are 6 a.m. to 6 p.m. (US Mountain Time), Monday through Friday. [4]

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

05
Five tickets a month

WITH AUTOMOX
Standard support allows up to 5 tickets a month; unlimited tickets, custom onboarding, and quarterly service reviews are in higher support tiers. [5]

WITH TECNETSOC
The most complete offering includes a 24/7 help desk, a TAM, and quarterly reviews.

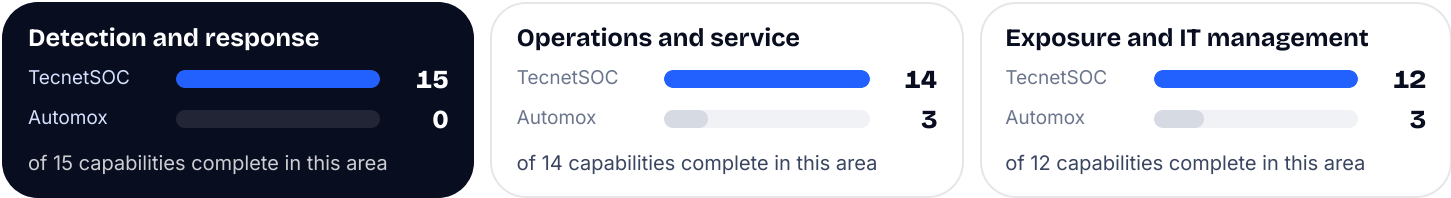
06
Everything else, with other providers

WITH AUTOMOX
The vendor itself states that its product is for those who already have RMM and backup separately; email, identity, and cloud also stay with other providers. [6]

WITH TECNETSOC
Email, identity, cloud, RMM, and NOC come with the most complete offering; immutable backup is a separate add-on.

— WHERE THE DIFFERENCE LIES

The three areas with the biggest gap



— CAPABILITY BY CAPABILITY

TecnetSOC and Automox, side by side

Capability	TecnetSOC	Automox Patching	Evidence on Automox
 Offers it	 Offers it as an add-on	 Partial, limited, or requires another contract	 No public evidence
 Not part of its published offering	 Your team provides it		
Operations and service	14 of 14	3 complete	
		 +2 partial	
24/7 security operations center (SOC) with human analysts		Your team provides it	A tool run by the customer or IT provider; no SOC or NOC [4]
AI agents that investigate and filter alerts before passing them to an analyst			AI generates scripts and mitigations; does not investigate alerts [7]
Human Gate: a person approves every critical action before it runs			Automox staff review AI mitigations before publishing them; not per action [7]
AI investigation assistant in the portal that cites its sources	 Neo		Otto AI only generates Worklets (automation scripts) from natural language; does not investigate cases [8]

Capability	TecnetSOC	Automox Patching	Evidence on Automox
☒ Offers it ☒ Offers it as an add-on ☒ Partial, limited, or requires another contract ☐ No public evidence			
☐ Not part of its published offering ☐ Your team provides it			
Operations in LATAM, the US, and Europe, with analysts in your time zone	☒	Your team provides it	No operations in LATAM; support during US Mountain Time hours [4]
Analysts, support, and portal in native Spanish	☒	☐	Support in English; LATAM only through resellers [4]
Leadership reports in Spanish and in business language	☒	☐	Technical reports; user reviews describe them as insufficient for audits [9]
Published notification and investigation start times by severity	☒ Critical: 30 min (target)	Your team provides it	No published notification or response SLA [4]
Executive summary every morning: what happened in the last 24 hours	☒ 7:30 a.m.	Your team provides it	No daily executive summary [4]
Automated weekly, monthly, quarterly, and annual reports	☒	☒	Analytics dashboards schedulable by minutes, hour, day, week, or month, sent as PDF, XLSX, or CSV to multiple recipients [10]
Assigned technical account manager (TAM) and quarterly reviews	☒	Your team provides it	Preferred and Turnkey support tiers at an additional cost; TAM not published [5]
24/7 contact with support or security staff	☒	☒	Standard support with 24/7 access to open up to 5 tickets a month; support hours Monday through Friday, 6 a.m. to 6 p.m., Mountain Time (US) [5]
Independent certification of operations (ISO 27001 or SOC 2 Type II)	☒ ISO/IEC 27001:2022	☒	Official site lists SOC 2 and CSA STAR; ISO 27001 only according to an independent directory [11]
Fast start with a software agent: your devices' activity, visible within hours	☒ Typical: 2 to 4 hours	☒	Cloud only, lightweight agent, no servers or VPN [4]
Detection and response	15 of 15 	0 complete +1 partial	
Continuous monitoring and event correlation (SIEM), aligned with MITRE ATT&CK (a reference framework of attack techniques)	☒	☐	No SIEM; integrates with Splunk [4]
Advanced protection on every device (EDR/XDR): malware, ransomware, and vulnerability exploitation	☒	☐	No EDR/XDR; integrates with CrowdStrike and SentinelOne [4]
Web filtering on the device	☒	☐	No web filtering [4]
Intrusion detection (IDS/IPS)	☒	☐	No IDS/IPS [4]
Threat detection on the internal network (NDR)	☒	☐	No NDR [4]
Documented investigations enriched with threat intelligence	☒	☐	No threat investigations [4]
Incident management with a case log and response time measured per case	☒	☐	No incident management [4]
Response with device isolation and IP address blocking	☒	☐	No native isolation; only scripts the customer writes [4]
Incident response with root cause analysis	☒	Your team provides it	No incident response or forensics [4]
Identity posture: MFA, privileged accounts, and conditional access	☒	☐	No identity posture [4]
Zero Trust: secure DNS, application access, and control of unauthorized applications (shadow IT)	☒	☐	No Zero Trust capabilities [4]
Cloud security: alerts and posture	☒	☐	No cloud security [4]
Email security: spam, phishing, malware, and impersonation fraud (BEC)	☒	☐	No email security [4]
Security awareness: phishing simulations and training with metrics	☒	☐	No security awareness [4]

Capability	TecnetSOC	Automox Patching	Evidence on Automox
☒ Offers it ☒ Offers it as an add-on ☒ Partial, limited, or requires another contract ☐ No public evidence			
☐ Not part of its published offering ☐ Your team provides it			
Prioritized security recommendations with an approval workflow	☒	☒	Vulnerability Sync turns external findings into approvable remediation tasks [12]
Exposure and IT management	12 of 12	3 complete +3 partial	
Unified asset and software inventory	☒	☒	Inventory of devices and installed software [5]
Vulnerabilities prioritized by severity and likelihood of exploitation (CVSS, EPSS)	☒	☒	Does not scan; imports findings from CrowdStrike, Tenable, Qualys, or Rapid7 [12]
Priority for flaws already being exploited (CISA KEV catalog)	☒	☐	No public evidence of its own KEV prioritization; depends on the external scanner [12]
Operating system and third-party application patching	☒	☒	Windows, macOS, Linux, and more than 630 third-party applications [5]
Provider-operated patching, with published timelines by severity	☒ Critical: 48 h (target)	Your team provides it	No patching SLA; responsibility lies with the customer [4]
Closure verification: the scanner confirms the vulnerability is gone	☒	☒	No scanner of its own; reports patch status, does not confirm the vulnerability is closed [12]
Patch validation in a pilot group before rollout	☒	☒	Pilot groups with ring-based staged policies [13]
External attack surface: what your company exposes on the internet, with a risk score	☒ Score from 0 to 100	☐	No external attack surface [4]
Alerts for domains that imitate your brand and for exposed credentials or keys	☒	☐	No detection of lookalike domains or exposed secrets [4]
Annual penetration test (pentest)	☒ Annual	Your team provides it	No pentesting [4]
Remote monitoring and management (RMM)	☒	☒	Basic remote control (Splashtop) and Worklets; not a full RMM [5]
Uptime monitoring (NOC)	☒	☐	No uptime monitoring or NOC [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	☒	Patch compliance reports; user reviews describe them as insufficient for audits [14]
Readiness for ISO 27001, SOC 2, and PCI DSS with shared controls	☒ Add-on	☐	No GRC platform [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	☐	No risk management, statement of applicability, or internal audits [4]
Auditor portal with an evidence room and a public trust page (trust center)	☒ Add-on	☐	No auditor portal for the customer [4]
Business continuity, vendor risk, and data breach management	☒ Add-on	☐	No business continuity or vendor management [4]

Capability	TecnetSOC	Automox Patching	Evidence on Automox
✓ Offers it ✗ Not part of its published offering	⊕ Offers it as an add-on ⦿ Your team provides it	⦿ 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 device with three stackable plans (Patch OS, Essentials, Enterprise) [5]
Free plan to get started	✓ Up to 10 devices	⦿	No free plan; after canceling, only free monitoring remains, without management [4]
Free trial in your real environment	✓ 30 days	⦿	Full platform trial; duration not published [5]
Available under your IT provider's brand	✓	✗	Multi-tenant for IT providers, but without the IT provider's brand [15]
Full coverage	50	6 +7 partial	

What your team would have to provide to run it 24/7: people, shifts, response times, a daily summary, incident response, and operated patching. TecnetSOC includes them in the service.

— NEXT STEP

From tool to service, with no implementation project

You install a single agent, see your devices' activity within hours, and our analysts operate 24/7 in your language.

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 Automox: Automox, Automate Enterprise plan (the highest) with a multi-organization IT provider program, 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.automox.com/solutions/turnkey-results (Differences you notice day to day)

2. www.automox.com/automox-and/crowdstrike (Differences you notice day to day)

3. www.automox.com/platform/vulnerability-remediation (Differences you notice day to day)

4. www.automox.com/faq (Differences you notice day to day)

5. www.automox.com/pricing (Differences you notice day to day)

6. www.automox.com/blog/automated-patching-solutions-compared-2026 (Differences you notice day to day)

7. www.globenewswire.com/news-release/2026/09/10/3359585/0/en/automox-... (AI agents that investigate and filter alerts...)

8. www.automox.com/resources/news/automox-launches-otto-ai (AI investigation assistant in the portal that...)

9. www.peerspot.com/products/automox-pros-and-cons (Leadership reports in Spanish and in business...)

10. docs.automox.com/product/Product_Documentation/Automox_Reports/Anal... (Automated weekly, monthly, quarterly, and...)

11. www.automox.com/platform/security (Independent certification of operations (ISO 27001...))

12. community.automox.com/automox-q-a-92/about-vulnerability-sync-1627 (Prioritized security recommendations with an...)

13. www.automox.com/blog/patch-management-best-practices (Patch validation in a pilot group...)

14. capterra.com/p/148872/Automox/reviews/ (Monthly evidence ready for auditors and insurers)

15. www.automox.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.](#)