

TecnetSOC vs. Action1

Action1 is a tool your team configures. TecnetSOC is an agentic SOC that runs your entire security.

With Action1, there's no EDR or SIEM, and its own guide suggests adding a managed detection and response (MDR) service; your team defines approvals, stages, and timelines, and is accountable for meeting them. **With TecnetSOC, the same SOC that patches also monitors, investigates, and responds 24/7.**



42

capabilities where TecnetSOC goes further

8

capabilities where we match

0

capabilities where Action1 outperforms TecnetSOC

Of the 50: 42 where we go further and 8 where we match

Same list of 50 capabilities and same criteria for TecnetSOC and Action1: 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

Action1 is a patching and vulnerability 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 Action1 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
Patches, but doesn't detect attacks

WITH ACTION1
The platform doesn't include EDR, SIEM, or incident response; its own guide suggests deploying EDR or XDR, or hiring an MDR provider. [1]

WITH TECNETSOC
The most complete offering includes EDR/XDR, SIEM with MITRE ATT&CK, and incident response with forensic analysis, operated 24/7 by in-house analysts.

02
You run the patching

WITH ACTION1
Your team configures approvals, deployment stages, schedules, restarts, and remediation timelines, and is accountable for meeting them; the platform executes whatever you define. [2]

WITH TECNETSOC
The SOC runs patching: it prioritizes by KEV and EPSS, validates in a pilot group, and installs critical patches within 48 h as a target.

03
Alerts to a single email address

WITH ACTION1
Each alert rule notifies a single console user by email and is silenced if it exceeds 10 per hour on a device. [3]

WITH TECNETSOC
AI agents investigate, correlate, and enrich every alert, and a person approves every critical action before it runs.

04
English-language support during business hours

WITH ACTION1
Its policy lists English as the support language for Latin America, and standard support is available Monday through Friday, 8 a.m. to 8 p.m. [4]

WITH TECNETSOC
Analysts in your time zone, in native Spanish and with multilingual support, run your security 24/7.

05
Technical reports, not executive ones

WITH ACTION1
Vulnerability reports list CVEs, CVSS, KEV, and affected devices, exportable as CSV or HTML; translating them into business risk is left to your team. [5]

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

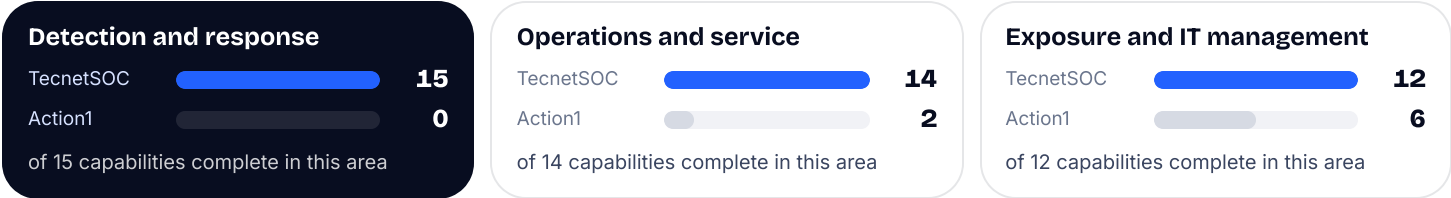
06
Free for up to 200 devices, without vendor support

WITH ACTION1
The free edition for up to 200 devices advertises community support on Discord (the community forum); opening cases with its technical support is for subscription customers. [6]

WITH TECNETSOC
Starting with the 30-day Response trial in your real environment, TectnetOne's own analysts run your service 24/7.

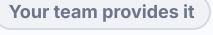
— WHERE THE DIFFERENCE LIES

The three areas with the biggest gap



— CAPABILITY BY CAPABILITY

TectnetSOC and Action1, side by side

Capability	TectnetSOC	Action1 Patching	Evidence on Action1
 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	2 complete  +2 partial	
24/7 security operations center (SOC) with human analysts			Self-service tool; no SOC or provider analysts [7]
AI agents that investigate and filter alerts before passing them to an analyst			No AI agents that investigate alerts; does not handle security alerts [7]
Human Gate: a person approves every critical action before it runs			Not applicable: the administrator defines and runs the policies [7]

Capability	TecnetSOC	Action1 Patching	Evidence on Action1
☒ 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			
AI investigation assistant in the portal that cites its sources	☒ Neo	☐	No public evidence of an AI investigation assistant in the console [7]
Operations in LATAM, the US, and Europe, with analysts in your time zone	☒	Your team provides it	No operations or office in LATAM; headquartered in Houston [7]
Analysts, support, and portal in native Spanish	☒	☐	Its support policy lists English as the language for Latin America [7]
Leadership reports in Spanish and in business language	☒	☐	Technical patch reports; user reviews point out a lack of reports for leadership [8]
Published notification and investigation start times by severity	☒ Critical: 30 min (target)	Your team provides it	No published notification or response SLA [7]
Executive summary every morning: what happened in the last 24 hours	☒ 7:30 a.m.	Your team provides it	No daily executive summary [7]
Automated weekly, monthly, quarterly, and annual reports	☒	☒	Patch and remediation reports; no periodic executive reports delivered [5]
Assigned technical account manager (TAM) and quarterly reviews	☒	Your team provides it	IT provider program with assigned dedicated support; no published TAM or quarterly reviews [9]
24/7 contact with support or security staff	☒	☒	With an active subscription, cases can be opened by email, phone, or web 24×7×365; standard support is Monday through Friday, 8 a.m. to 8 p.m., with priority for Severity 1 [4]
Independent certification of operations (ISO 27001 or SOC 2 Type II)	☒ ISO/IEC 27001:2022	☒	ISO 27001, SOC 2 Type II, and TX-RAMP declared [10]
Fast start with a software agent: your devices' activity, visible within hours	☒ Typical: 2 to 4 hours	☒	Cloud native, lightweight agent, up and running in minutes [7]
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 [7]
Advanced protection on every device (EDR/XDR): malware, ransomware, and vulnerability exploitation	☒	☐	No EDR/XDR [7]
Web filtering on the device	☒	☐	No web filtering [7]
Intrusion detection (IDS/IPS)	☒	☐	No IDS/IPS [7]
Threat detection on the internal network (NDR)	☒	☐	No NDR [7]
Documented investigations enriched with threat intelligence	☒	☐	Enriches vulnerabilities (VulnCheck), not incident investigations [11]
Incident management with a case log and response time measured per case	☒	☐	No incident management [7]
Response with device isolation and IP address blocking	☒	☐	No device isolation or IP blocking as a response [7]
Incident response with root cause analysis	☒	Your team provides it	No incident response or forensics [7]
Identity posture: MFA, privileged accounts, and conditional access	☒	☐	No identity posture [7]
Zero Trust: secure DNS, application access, and control of unauthorized applications (shadow IT)	☒	☐	No Zero Trust capabilities [7]
Cloud security: alerts and posture	☒	☐	No cloud security [7]
Email security: spam, phishing, malware, and impersonation fraud (BEC)	☒	☐	No email security [7]

Capability	TecnetSOC	Action1 Patching	Evidence on Action1
☒ 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			
Security awareness: phishing simulations and training with metrics	☒	☐	No security awareness or phishing simulations [7]
Prioritized security recommendations with an approval workflow	☒	☒	Vulnerability prioritization and compensating controls; limited to patches and configuration [5]
Exposure and IT management	12 of 12	6 complete	
		+1 partial	
Unified asset and software inventory	☒	☒	Hardware and software inventory included [7]
Vulnerabilities prioritized by severity and likelihood of exploitation (CVSS, EPSS)	☒	☒	Real-time vulnerability assessment with CVSS and exploitation intelligence [5]
Priority for flaws already being exploited (CISA KEV catalog)	☒	☒	CISA KEV attribute and ransomware use on every vulnerability [12]
Operating system and third-party application patching	☒	☒	Windows, macOS, Linux, and more than 630 third-party applications [13]
Provider-operated patching, with published timelines by severity	☒ Critical: 48 h (target)	Your team provides it	The customer or IT provider carries it out; remediation timelines are set by the customer [5]
Closure verification: the scanner confirms the vulnerability is gone	☒	☒	The report links each CVE to the patch that closed it, with a date [5]
Patch validation in a pilot group before rollout	☒	☒	Update Rings for phased deployment [10]
External attack surface: what your company exposes on the internet, with a risk score	☒ Score from 0 to 100	☐	No external attack surface [7]
Alerts for domains that imitate your brand and for exposed credentials or keys	☒	☐	No detection of lookalike domains or exposed secrets [7]
Annual penetration test (pentest)	☒ Annual	Your team provides it	No pentesting [7]
Remote monitoring and management (RMM)	☒	☒	Remote access, scripts, and software deployment; not a full RMM [7]
Uptime monitoring (NOC)	☒	☐	No uptime monitoring or NOC [7]
Backup and continuity	3 of 3	0 complete	
		+0 partial	
Backup for servers, files, databases, virtual machines, and Microsoft 365	☒ Add-on	☐	No backup [7]
Immutable backup vault (cannot be altered or deleted), isolated per customer	☒ Add-on	☐	No immutable vault [7]
Disaster recovery with drills and measured recovery time (RTO)	☒ Add-on Measured RTO	☐	No disaster recovery [7]
Compliance	6 of 6	0 complete	
		+1 partial	
Monthly evidence ready for auditors and insurers	☒ Monthly	☒	Patch and remediation compliance reports; not managed monthly evidence [5]
Readiness for ISO 27001, SOC 2, and PCI DSS with shared controls	☒ Add-on	☐	No GRC platform; only CIS, NIST, and STIG baselines (separate module) [14]
Mexican regulatory readiness: CNBV Fintech, data protection (LFPDPPP), and NOM-024	☒ Add-on	☐	No Mexican regulations [7]
Risk management, controls, statement of applicability, and internal audits	☒ Add-on	☐	No risk management, statement of applicability, or internal audits [7]
Auditor portal with an evidence room and a public trust page (trust center)	☒ Add-on	☐	No auditor portal or Trust Center for the customer [7]
Business continuity, vendor risk, and data breach management	☒ Add-on	☐	No business continuity or vendor management [7]

Capability	TecnetSOC	Action1 Patching	Evidence on Action1
✓ 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, but a single plan; extra modules licensed separately [15]
Free plan to get started	✓ Up to 10 devices	✓ Up to 200 devices	Permanent free edition for up to 200 devices, with all features [10]
Free trial in your real environment	✓ 30 days	✓	Free tier works as a permanent trial in a real environment [10]
Available under your IT provider's brand	✓	✗	Resale by IT providers allowed, but without the IT provider's brand [9]
Full coverage	50	8 +5 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 Action1: Action1, Autonomous Endpoint Management platform at its highest tier (Enterprise for IT providers, with the Configuration Management and Enrollment and Provisioning 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. www.action1.com/blog/endpoint-management/endpoint-security-management/ (Differences you notice day to day)
2. www.action1.com/documentation/review-and-approve-updates/ (Differences you notice day to day)
3. www.action1.com/documentation/alerts/ (Differences you notice day to day)
4. www.action1.com/legal/support-policy/ (Differences you notice day to day)
5. www.action1.com/documentation/vulnerability-management/ (Differences you notice day to day)
6. www.action1.com/pricing/ (Differences you notice day to day)
7. ifeeltech.com/blog/action1-review-free-patch-management (24/7 security operations center (SOC) with human analysts)
8. www.capterra.com/p/180609/Action1-RMM/reviews/ (Leadership reports in Spanish and in business...)
9. www.prnewswire.com/news-releases/action1-unveils-msp-partner-progra... (Assigned technical account manager (TAM) and...)
10. www.prnewswire.com/news-releases/action1-expands-its-free-offering-... (Independent certification of operations (ISO 27001...))
11. www.prnewswire.com/news-releases/action1-expands-vulnerability-inte... (Documented investigations enriched...)
12. www.action1.com/blog/kev-catalog-integration-enhancing-vulnerabilit... (Priority for flaws already being...)
13. www.prnewswire.com/news-releases/action1-expands-to-linux-deliverin... (Operating system and third-party application patching)
14. www.prnewswire.com/news-releases/action1-expands-endpoint-managemen... (Readiness for ISO 27001, SOC 2, and PCI...)
15. mspcompared.com/action1/pricing/ (Per-device pricing, with plans that stack)

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.](#)