

TecnetSOC vs. FortiSOAR

FortiSOAR automates what your team designs. TecnetSOC investigates, decides, and responds for you, with a person on critical calls.

With FortiSOAR, you purchase SIEM, EDR, and email security separately, your team operates cases and automations, and onboarding is quoted as a separate project. TecnetSOC already comes with the platform and 24/7 analysts, and it's operational in less than 7 days.



44

capabilities where TecnetSOC goes further

6

capabilities where we match

0

capabilities where FortiSOAR 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 FortiSOAR: 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

FortiSOAR is a security orchestration, automation, and response platform: it doesn't detect threats on its own, and it isn't a managed SOC service. The SIEM, EDR, and other tools it coordinates are products that are purchased and operated separately. This comparison shows, capability by capability, how much of what TecnetSOC includes FortiSOAR 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
Your team has to operate it

WITH FORTISOAR
You buy a platform for your SOC to operate: your team handles cases and playbooks, and the 24/7 shift is covered by you or a separate service. [\[1\]](#)

WITH TECNETSOC
TecnetOne's own analysts run your security 24/7, in your time zone and in native Spanish.

02
Orchestrates tools you buy separately

WITH FORTISOAR
It doesn't come with its own SIEM, EDR, firewall, or email security: it coordinates the ones you've already bought and license separately. [\[1\]](#)

WITH TECNETSOC
The most complete offering already includes SIEM, EDR/XDR, IDS/IPS, NDR, web filtering, and email security.

03
AI with a monthly usage cap

WITH FORTISOAR
Agentic AI includes 5 million tokens per month per instance, about 60 investigations according to Fortinet; for more, you buy additional token packs. [\[1\]](#)

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

04
Shows vulnerabilities, but doesn't patch them

WITH FORTISOAR
The vulnerability view comes from external scanners that you integrate and license separately, and patching depends on your team and other tools. [\[2\]](#)

WITH TECNETSOC
The SOC prioritizes patching by real-world exploitation (KEV and EPSS), validates in a pilot group, and considers each vulnerability closed only when the scanner confirms it.

05
Onboarding with separate professional services

WITH FORTISOAR
You choose deployment, size, add-ons, and training, and Fortinet separately offers Quick-Start, defined-scope projects (SOW) billed per day, or a Resident Engineer for 6 to 12 months. [\[1\]](#)

WITH TECNETSOC
You install an agent, see activity in 2 to 4 hours, and are operational in less than 7 days, with no implementation project or project management office.

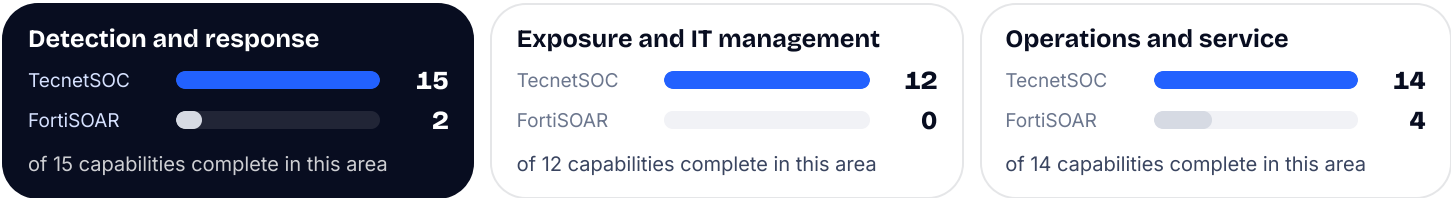
06
Servers you size

WITH FORTISOAR
You install and maintain RHEL or Rocky Linux servers starting at 8 vCPUs and 24 GB of RAM, or choose its hosted cloud, which your team still operates. [\[2\]](#)

WITH TECNETSOC
The platform is a cloud service operated by TecnetOne: you don't install or maintain servers.

— WHERE THE DIFFERENCE LIES

The three areas with the biggest gap



— CAPABILITY BY CAPABILITY

TecnetSOC and FortiSOAR, side by side

Capability	TecnetSOC	FortiSOAR Orchestration	Evidence on FortiSOAR
✓ 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
Operations and service	14 of 14	4 complete +2 partial	
24/7 security operations center (SOC) with human analysts	✓	Your team provides it	The product does not include a SOC; 24/7 SOC only with FortiGuard SOCaaS, a separate service [3]
AI agents that investigate and filter alerts before passing them to an analyst	✓	✓	19 AI agents; automatic triage closes routine alerts and groups priority ones [2]
Human Gate: a person approves every critical action before it runs	✓	✓	Configurable "in-the-loop" workflows with manual intervention in playbooks [4]

Capability	TecnetSOC	FortiSOAR Orchestration	Evidence on FortiSOAR
☒ 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	☒	FortiAI assistant in every case, with context and intelligence; no evidence of dated citations [2]
Operations in LATAM, the US, and Europe, with analysts in your time zone	☒	Your team provides it	Software operated by the customer; Fortinet's SOCaaS operates from North America, EMEA, and APAC [3]
Analysts, support, and portal in native Spanish	☒	☒	Fortinet's FortiCare support, with published phone support in English and Spanish; does not include security analysts [5]
Leadership reports in Spanish and in business language	☒	☐	Configurable dashboards and reports; no evidence of executive reports in Spanish [2]
Published notification and investigation start times by severity	☒ Critical: 30 min (target)	Your team provides it	No provider SLA; it measures the customer team's SLA. The separate SOCaaS notifies within 15 min [3]
Executive summary every morning: what happened in the last 24 hours	☒ 7:30 a.m.	Your team provides it	No daily executive summary [2]
Automated weekly, monthly, quarterly, and annual reports	☒	☒	Reports scheduled hourly, daily, weekly, monthly, or yearly, emailed to a list of recipients [6]
Assigned technical account manager (TAM) and quarterly reviews	☒	Your team provides it	Resident Engineer or TAM from FortiCare Advanced Support, separate contracts [1]
24/7 contact with support or security staff	☒	☒	FortiCare Premium 24x7 included in the subscription [2]
Independent certification of operations (ISO 27001 or SOC 2 Type II)	☒ ISO/IEC 27001:2022	☒	ISO 27001 covers FortiGuard and FortiCloud; when self-hosted, operations are the customer's responsibility [7]
Fast start with a software agent: your devices' activity, visible within hours	☒ Typical: 2 to 4 hours	☒	Requires sizing nodes, integrating connectors, and onboarding services (Quick-Start) [1]
Detection and response	15 of 15	2 complete +5 partial	
Continuous monitoring and event correlation (SIEM), aligned with MITRE ATT&CK (a reference framework of attack techniques)	☒	☒	Not a SIEM; receives and correlates alerts with MITRE ATT&CK. The SIEM is FortiSIEM, purchased separately [2]
Advanced protection on every device (EDR/XDR): malware, ransomware, and vulnerability exploitation	☒	☒	No EDR of its own; orchestrates FortiEDR or other EDRs purchased separately [8]
Web filtering on the device	☒	☒	No web filtering; FortiClient or FortiProxy, purchased separately [9]
Intrusion detection (IDS/IPS)	☒	☒	No IDS/IPS; orchestrates FortiGate or other firewalls, purchased separately [10]
Threat detection on the internal network (NDR)	☒	☒	No NDR; connector to FortiNDR, a separate product [11]
Documented investigations enriched with threat intelligence	☒	☒	Automatic enrichment and a TIM module with FortiGuard as its own add-on [2]
Incident management with a case log and response time measured per case	☒	☒	Full case management, war room, forensic activity log, and SLA [2]
Response with device isolation and IP address blocking	☒	☒	Blocks indicators and isolates via connectors; depends on a firewall or EDR purchased separately [2]
Incident response with root cause analysis	☒	Your team provides it	War room forensic log; forensic analysis is FortiGuard IR, a separate service [12]
Identity posture: MFA, privileged accounts, and conditional access	☒	☒	No identity posture; only actions via IdP connectors [2]
Zero Trust: secure DNS, application access, and control of unauthorized applications (shadow IT)	☒	☒	No Zero Trust of its own; FortiSASE is a separate product [13]
Cloud security: alerts and posture	☒	☒	Automates cloud operations via connectors; no cloud posture of its own [2]

Capability	TecnetSOC	FortiSOAR Orchestration	Evidence on FortiSOAR
☒ 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		
Email security: spam, phishing, malware, and impersonation fraud (BEC)	☒	☐	No email security; orchestrates FortiMail, a separate product [14]
Security awareness: phishing simulations and training with metrics	☒	☐	No security awareness; Fortinet Security Awareness is a separate service [15]
Prioritized security recommendations with an approval workflow	☒	☒	ML and GenAI response recommendations; no posture approval workflow [2]
Exposure and IT management	12 of 12	0 complete +3 partial	
Unified asset and software inventory	☒	☒	Asset profiles from integrated systems; doesn't discover assets or software on its own [2]
Vulnerabilities prioritized by severity and likelihood of exploitation (CVSS, EPSS)	☒	☒	Vulnerability management based on external scanners (Qualys, Tenable, Rapid7) [2]
Priority for flaws already being exploited (CISA KEV catalog)	☒	☐	No evidence of prioritization by the CISA KEV catalog [2]
Operating system and third-party application patching	☒	☒	Automates updates via playbooks; actual patching in FortiClient EMS or others, purchased separately [2]
Provider-operated patching, with published timelines by severity	☒ Critical: 48 h (target)	Your team provides it	No Fortinet-operated patching with published timelines [4]
Closure verification: the scanner confirms the vulnerability is gone	☒	☐	No documented closure verification [2]
Patch validation in a pilot group before rollout	☒	☐	No patch validation in a pilot group [2]
External attack surface: what your company exposes on the internet, with a risk score	☒ Score from 0 to 100	☐	No native EASM; FortiRecon is a separate product [16]
Alerts for domains that imitate your brand and for exposed credentials or keys	☒	☐	Brand and leak protection in FortiRecon, a separate product [16]
Annual penetration test (pentest)	☒ Annual	Your team provides it	No pentesting included [4]
Remote monitoring and management (RMM)	☒	☐	Not an RMM; only automates tasks via connectors [2]
Uptime monitoring (NOC)	☒	☐	No uptime monitoring of its own; FortiSIEM does it, purchased separately [2]
Backup and continuity	3 of 3	0 complete +0 partial	
Backup for servers, files, databases, virtual machines, and Microsoft 365	☒ Add-on	☐	No backup for servers, VMs, or Microsoft 365 [4]
Immutable backup vault (cannot be altered or deleted), isolated per customer	☒ Add-on	☐	No immutable backup vault [4]
Disaster recovery with drills and measured recovery time (RTO)	☒ Add-on Measured RTO	☐	High availability and recovery only for the platform itself, not for the customer's systems [1]
Compliance	6 of 6	0 complete +2 partial	
Monthly evidence ready for auditors and insurers	☒ Monthly	☒	Compliance dashboards and reports; does not deliver a monthly evidence package [2]
Readiness for ISO 27001, SOC 2, and PCI DSS with shared controls	☒ Add-on	☒	Mapping to NIST CSF, ISO 27001, GDPR, and SOC 2; not a complete GRC platform [2]
Mexican regulatory readiness: CNBV Fintech, data protection (LFPDPPP), and NOM-024	☒ Add-on	☐	No Mexican regulations (CNBV, LFPDPPP, NOM-024) [2]
Risk management, controls, statement of applicability, and internal audits	☒ Add-on	☐	Compliance workflows, but no risk register, statement of applicability, or internal audits [2]
Auditor portal with an evidence room and a public trust page (trust center)	☒ Add-on	☐	No auditor portal or Trust Center for the customer [4]

Capability	TecnetSOC	FortiSOAR Orchestration	Evidence on FortiSOAR
✔ 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	
Business continuity, vendor risk, and data breach management	⊕ Add-on	✗	No business continuity or vendor management [4]
How it's purchased	Not counted		
Per-device pricing, with plans that stack	✔ Per device	✗	Licensed by edition, node, and concurrent user, not per device [1]
Free plan to get started	✔ Up to 10 devices	👁	Non-expiring trial license: 2 users and 1,000 actions per day [17]
Free trial in your real environment	✔ 30 days	✔	Trial license from FortiCare, installable in your own environment [17]
Available under your IT provider's brand	✔	✔	Multi-tenant edition for managed security service providers with configurable custom branding [1]
Full coverage	50	6 +12 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 FortiSOAR: Fortinet FortiSOAR 8.0 (self-hosted VM or FortiSOAR Cloud PaaS; subscription or FortiFlex by Starter, Enterprise, or multi-tenant edition, by nodes and concurrent users, 2 included; its own TIM add-on with FortiGuard; includes 5 million FortiAI tokens per month; operated by the customer's team or its managed security service provider, not Fortinet), 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.fortinet.com/content/dam/fortinet/assets/data-sheets/og-fortisoar... (Differences you notice day to day)

2. www.fortinet.com/content/dam/fortinet/assets/data-sheets/fortisoar.pdf (Differences you notice day to day)

3. www.fortinet.com/products/socaas (24/7 security operations center (SOC) with human analysts)

4. www.fortinet.com/products/fortisoar (Human Gate: a person approves every...)

5. www.fortinet.com/support/contact (Analysts, support, and portal in native Spanish)

6. docs.fortinet.com/document/fortisoar/7.0.0/user-guide/292560/report... (Automated weekly, monthly, quarterly, and...)
7. www.fortinet.com/corporate/about-us/product-certifications/iso27001... (Independent certification of operations (ISO 27001...))

8. www.fortinet.com/products/endpoint-security/fortiedr (Advanced protection on every device (EDR/XDR)...)

9. www.fortinet.com/products/endpoint-security/forticlient (Web filtering on the device)

10. www.fortinet.com/products/next-generation-firewall (Intrusion detection (IDS/IPS))

11. www.fortinet.com/products/network-detection-and-response (Threat detection on the internal network (NDR))
12. www.fortinet.com/support/support-services/fortiguard-security-subsc... (Incident response with root cause analysis)

13. www.fortinet.com/products/sase (Zero Trust: secure DNS, application access, and...)

14. www.fortinet.com/products/email-security/fortimail (Email security: spam, phishing, malware, and...)

15. www.fortinet.com/training/security-awareness-training (Security awareness: phishing...)

16. www.fortinet.com/products/fortirecon (External attack surface: what your company exposes...)

17. docs.fortinet.com/document/fortisoar/7.6.5/deployment-guide/223944/... (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.](#)