

FortiSIEM is a SIEM your team operates. TecnetSOC is an agentic SOC that operates it for you, 24/7.

With FortiSIEM, your team installs and maintains servers, tunes detections, licenses extra events separately, and responds around the clock; a 24/7 SOC is another service. **With TecnetSOC, TecnetOne analysts run MITRE ATT&CK correlation for you.**



43

capabilities where TecnetSOC goes further

7

capabilities where we match

0

capabilities where FortiSIEM outperforms TecnetSOC

Of the 50: 43 where we go further and 7 where we match

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

FortiSIEM is a SIEM platform that your team installs, configures, and monitors; it is not a managed SOC service. What FortiSIEM doesn't cover is filled in with other Fortinet products, each with its own license and operation. This comparison shows, capability by capability, how much of what TecnetSOC includes FortiSIEM 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 monitors and responds

WITH FORTISIEM
You buy the platform, and your team monitors, investigates, and responds around the clock; if you don't have 24/7 shifts, you hire a separate provider. [\[1\]](#)

WITH TECNETSOC
TecnetOne's own analysts monitor, investigate, and respond 24/7, in your time zone and in native Spanish.

02
Servers and storage are on you

WITH FORTISIEM
If you host it yourself, you install and maintain its components (Supervisor, Workers, and Collectors) and their storage; in its cloud, you license compute and storage separately. [\[1\]](#)

WITH TECNETSOC
You install an agent and the rest deploys on its own: activity visible in 2 to 4 hours, with no servers to maintain.

03
Your team manages the detections

WITH FORTISIEM
Your team manages its more than 2,800 rules and any SIGMA or ML detections it adds; Fortinet trains administrators in a 15-hour course. [\[2\]](#)

WITH TECNETSOC
You don't hire or train SIEM specialists: TecnetOne analysts run MITRE ATT&CK correlation for you.

04
Every extra event is licensed

WITH FORTISIEM
Each licensed device comes with 10 events per second; additional events per second (EPS), user behavior analytics (UEBA), advanced agents, the IOC service, and automation are licensed separately. [\[1\]](#)

WITH TECNETSOC
You pay per device with stackable plans; Visibility is free for up to 10 devices, and Response comes with a 30-day trial in your real environment.

05
Collects events, doesn't protect devices

WITH FORTISIEM
Its agent collects events, file integrity data, and Osquery queries; blocking threats on devices, email, or the network requires FortiEDR, FortiMail, FortiGate, or other products. [\[1\]](#)

WITH TECNETSOC
The most complete offering includes advanced protection on every device (EDR/XDR), web filtering, IDS/IPS, NDR, and email security.

06
Sees patches, doesn't install them

WITH FORTISIEM
You see installed patches and ingest your scanners, but it doesn't patch: scanning, installing, and confirming closure are left to other products and your team. [\[1\]](#)

WITH TECNETSOC
The SOC prioritizes by real-world exploitation (KEV and EPSS), validates in a pilot group, installs, and closes when the scanner confirms the fix.

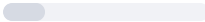
— WHERE THE DIFFERENCE LIES

The three areas with the biggest gap

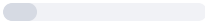
Operations and service

TecnetSOC  **14**
FortiSIEM  **2**
of 14 capabilities complete in this area

Detection and response

TecnetSOC  **15**
FortiSIEM  **3**
of 15 capabilities complete in this area

Exposure and IT management

TecnetSOC  **12**
FortiSIEM  **2**
of 12 capabilities complete in this area

— CAPABILITY BY CAPABILITY

TecnetSOC and FortiSIEM, side by side

Capability	TecnetSOC	FortiSIEM SIEM	Evidence on FortiSIEM
 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  +3 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			FortiAI-Assist with agents for event and incident analysis; doesn't automatically filter every alert [1]
Human Gate: a person approves every critical action before it runs			Playbooks based on FortiSOAR; no mandatory human gate documented in the data sheet [1]

Capability	TecnetSOC	FortiSIEM SIEM	Evidence on FortiSIEM
☒ 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-Assist GenAI guides investigations and searches; no evidence of dated citations [1]
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	☒	☒	FortiCare publishes a global support phone line in English and Spanish; no evidence of security analysts or a portal in Spanish [4]
Leadership reports in Spanish and in business language	☒	☐	More than 1,300 technical compliance reports; no evidence of executive reports in Spanish [1]
Published notification and investigation start times by severity	☒ Critical: 30 min (target)	Your team provides it	No SLA in the product; the SOCaaS, a separate service, publishes notification within 15 minutes at most [3]
Executive summary every morning: what happened in the last 24 hours	☒ 7:30 a.m.	Your team provides it	No daily executive summary; only scheduled reports that the customer configures [1]
Automated weekly, monthly, quarterly, and annual reports	☒	☒	Schedulable reports with email delivery to stakeholders [1]
Assigned technical account manager (TAM) and quarterly reviews	☒	Your team provides it	TAM only with FortiCare Advanced Support Pro, a separate contract [5]
24/7 contact with support or security staff	☒	☒	FortiCare 24x7 contract included or sold with the license [1]
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 [6]
Fast start with a software agent: your devices' activity, visible within hours	☒ Typical: 2 to 4 hours	☐	Supervisor, Workers, and Collectors architecture; requires an implementation project [1]
Detection and response	15 of 15	3 complete + 4 partial	
Continuous monitoring and event correlation (SIEM), aligned with MITRE ATT&CK (a reference framework of attack techniques)	☒	☒	More than 2,800 correlation rules, UEBA, MITRE ATT&CK mapping [7]
Advanced protection on every device (EDR/XDR): malware, ransomware, and vulnerability exploitation	☒	☐	Does not include EDR; FortiEDR is a separate product. Its agent only collects events, file integrity (FIM), and Osquery queries [8]
Web filtering on the device	☒	☐	Does not filter web traffic; it only ingests logs. Filtering in FortiClient or FortiProxy, purchased separately [9]
Intrusion detection (IDS/IPS)	☒	☐	Not an IDS/IPS; it ingests IPS events. IPS in FortiGate, purchased separately [10]
Threat detection on the internal network (NDR)	☒	☒	NetFlow analysis and agentless discovery; full network detection (NDR) is FortiNDR, a separate product [11]
Documented investigations enriched with threat intelligence	☒	☒	Automatic enrichment with FortiGuard and external intelligence sources; IOC service as its own add-on [1]
Incident management with a case log and response time measured per case	☒	☒	Integrated case management, Incident Explorer, and incident lifecycle [1]
Response with device isolation and IP address blocking	☒	☒	Remediation scripts and playbooks; execution depends on a third-party firewall or EDR [1]
Incident response with root cause analysis	☒	Your team provides it	Osquery provides device forensic detail; forensic response is FortiGuard IR, a separate service [12]
Identity posture: MFA, privileged accounts, and conditional access	☒	☒	UEBA and identity events (AD, Okta); no identity posture assessment [1]
Zero Trust: secure DNS, application access, and control of unauthorized applications (shadow IT)	☒	☐	No Zero Trust of its own; ZTNA, DNS, and shadow IT in FortiSASE, purchased separately [13]

Capability	TecnetSOC	FortiSIEM SIEM	Evidence on FortiSIEM
☒ 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			
Cloud security: alerts and posture	☒	☒	Ingests cloud logs and deploys on Azure; no Azure posture [1]
Email security: spam, phishing, malware, and impersonation fraud (BEC)	☒	☒	No email security of its own; FortiMail is 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	☒	☒	Risk scoring per user and host; no recommendations with an approval workflow [1]
Exposure and IT management	12 of 12	2 complete +1 partial	
Unified asset and software inventory	☒	☒	CMDB with automatic discovery, configuration, installed software, and patches [1]
Vulnerabilities prioritized by severity and likelihood of exploitation (CVSS, EPSS)	☒	☒	Integrates vulnerability scanners for risk; doesn't scan on its own or use EPSS [1]
Priority for flaws already being exploited (CISA KEV catalog)	☒	☐	No evidence of prioritization by the CISA KEV catalog [1]
Operating system and third-party application patching	☒	☒	No patching in FortiSIEM; vulnerability patching in FortiClient EMS, purchased separately [9]
Provider-operated patching, with published timelines by severity	☒ Critical: 48 h (target)	Your team provides it	No Fortinet-operated patching with published timelines [7]
Closure verification: the scanner confirms the vulnerability is gone	☒	☒	No documented vulnerability closure verification [1]
Patch validation in a pilot group before rollout	☒	☒	No patch validation in a pilot group [1]
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 in the product [7]
Remote monitoring and management (RMM)	☒	☒	Monitors performance, but doesn't manage devices remotely (not an RMM) [1]
Uptime monitoring (NOC)	☒	☒	Uptime, performance, and synthetic transaction monitoring, and SLA calculation [1]
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 [7]
Immutable backup vault (cannot be altered or deleted), isolated per customer	☒ Add-on	☒	No immutable backup vault [7]
Disaster recovery with drills and measured recovery time (RTO)	☒ Add-on Measured RTO	☒	High availability and recovery only for the SIEM itself, not for your systems [1]
Compliance	6 of 6	0 complete +2 partial	
Monthly evidence ready for auditors and insurers	☒ Monthly	☒	Ready-made compliance reports; does not deliver a monthly evidence package [1]
Readiness for ISO 27001, SOC 2, and PCI DSS with shared controls	☒ Add-on	☒	Reports for ISO 27001, PCI, HIPAA, and NIST; not a GRC platform and doesn't map SOC 2 [1]
Mexican regulatory readiness: CNBV Fintech, data protection (LFPDPPP), and NOM-024	☒ Add-on	☒	No Mexican regulations (CNBV, LFPDPPP, NOM-024) [1]
Risk management, controls, statement of applicability, and internal audits	☒ Add-on	☒	No risk register, SoA, or internal audits [1]

Capability	TecnetSOC	FortiSIEM SIEM	Evidence on FortiSIEM
✔ 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	
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]
How it's purchased	Not counted		
Per-device pricing, with plans that stack	✔ Per device	⦿	Licensed per device and EPS, but without stackable plans [1]
Free plan to get started	✔ Up to 10 devices	✗	No permanent free plan [1]
Free trial in your real environment	✔ 30 days	⦿	The page offers a free trial; duration and terms not published [7]
Available under your IT provider's brand	✔	✔	Multi-tenant for managed security service providers, with per-customer permissions and their own logo [1]
Full coverage	50	7 +10 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 FortiSIEM: Fortinet FortiSIEM (software, VM, appliance, or FortiSIEM Cloud SaaS; licensed per device + EPS, GB/day, or FCU in the cloud, subscription or perpetual; its own UEBA, Advanced Agent, IOC Service, and Automation Service add-ons; 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/FortiSIEM.pdf (Differences you notice day to day)

2. training.fortinet.com/local/staticpage/view.php (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/support/contact (Analysts, support, and portal in native Spanish)

5. www.fortinet.com/support/advanced-support (Assigned technical account manager (TAM) and...)

6. www.fortinet.com/corporate/about-us/product-certifications/iso27001... (Independent certification of operations (ISO 27001...))
7. www.fortinet.com/products/siem/fortisiem (Continuous monitoring and event correlation...)

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...)

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.](#)