

TecnetSOC vs. ManageEngine

ManageEngine gives you tools for your team to operate. TecnetSOC is the service that operates them for you.

ManageEngine is software: your analysts cover nights and weekends, you install and update the server, and storing logs in its cloud is charged per GB. With TecnetSOC, one agent and TecnetOne analysts 24/7, with no servers of your own.



32

capabilities where TecnetSOC goes further

18

capabilities where we match

0

capabilities where ManageEngine outperforms TecnetSOC

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

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

ManageEngine is a suite of IT management and security tools that your team installs and operates; it is not a managed SOC service. They are products that are purchased and operated separately, and not all of them integrate natively with each other. This comparison shows, capability by capability, how much of what TecnetSOC includes ManageEngine 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

You provide the analysts

WITH MANAGEENGINE
Log360 is built to equip your own SOC: your analysts monitor, investigate, and respond to every alert, at night and on weekends too. [\[1\]](#)

WITH TECNETSOC
TecnetOne's own analysts run your security 24/7, in your time zone and in native Spanish; you don't have to build a SOC.

02

You install and update the server

WITH MANAGEENGINE
With ManageEngine on your own servers (on-premises), you install, size, and update the central server; when the vendor issues a critical advisory, the emergency update is on you. [\[2\]](#)

WITH TECNETSOC
You install an agent and the rest deploys on its own; TecnetOne operates the platform in the cloud, with no servers to maintain.

03

Storing logs is paid per GB

WITH MANAGEENGINE LOG360 CLOUD
Log storage is charged separately per GB per year, for search and for archiving; more retention means a bigger bill. [\[3\]](#)

WITH TECNETSOC
SIEM with MITRE ATT&CK correlation is part of the cloud service that TecnetOne operates; you don't size your own storage.

04

Your technician runs the patching

WITH MANAGEENGINE
Your team configures, approves, and tracks every patch deployment; the tool automates, but no one is accountable for closure timelines. [\[4\]](#)

WITH TECNETSOC
The SOC prioritizes by real-world exploitation, validates in a pilot group, and installs critical patches within 48 h as a target; it closes when the scanner confirms.

05

SIEM and EDR, separately

WITH MANAGEENGINE
The SIEM (Log360) is licensed separately from Endpoint Central, and EDR, anti-malware, and anti-ransomware are add-ons, each with its own price. [\[5\]](#)

WITH TECNETSOC
One per-device price; the most complete plan already brings together SIEM, EDR/XDR, web filtering, RMM, and patching, operated by the SOC.

06

Email and phishing, through another provider

WITH MANAGEENGINE
Log360 audits and reports on Microsoft 365, but doesn't filter spam, phishing, or BEC in your email; phishing simulations, external attack surface, and pentesting are separate. [\[6\]](#)

WITH TECNETSOC
The most complete offering adds email security against phishing and BEC, phishing simulations, external attack surface, and annual pentesting.

— WHERE THE DIFFERENCE LIES

The three areas with the biggest gap

Operations and service

TecnetSOC 14

ManageEngine 4

of 14 capabilities complete in this area

Detection and response

TecnetSOC 15

ManageEngine 7

of 15 capabilities complete in this area

Compliance

TecnetSOC 6

ManageEngine 0

of 6 capabilities complete in this area (includes add-ons)

— CAPABILITY BY CAPABILITY

TecnetSOC and ManageEngine, side by side

Capability	TecnetSOC	ManageEngine IT management	Evidence on ManageEngine
✓ 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	4 complete +5 partial	
24/7 security operations center (SOC) with human analysts	✓	Your team provides it	Software operated by the customer or IT provider; no SOC of its own [1]
AI agents that investigate and filter alerts before passing them to an analyst	✓	⦿	Zia agents correlate alerts in Log360 Cloud Enterprise; the customer operates them [7]

Capability	TecnetSOC	ManageEngine IT management	Evidence on ManageEngine
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			
Human Gate: a person approves every critical action before it runs			Native SOAR included in Log360 Cloud Enterprise; its playbooks can require approval before running actions, configured and operated by your team [8]
AI investigation assistant in the portal that cites its sources	 Neo		Zia Insights and AI Investigation provide context; no analyst who explains findings with sources [9]
Operations in LATAM, the US, and Europe, with analysts in your time zone		Your team provides it	Sales offices in Mexico and Colombia; does not operate the customer's security [10]
Analysts, support, and portal in native Spanish			Spanish-language support for IT providers; no security analysts [11]
Leadership reports in Spanish and in business language			Technical and compliance reports; not written for leadership [1]
Published notification and investigation start times by severity	 Critical: 30 min (target)	Your team provides it	No notification or response SLA; it's not a service [12]
Executive summary every morning: what happened in the last 24 hours	 7:30 a.m.	Your team provides it	No daily executive summary [1]
Automated weekly, monthly, quarterly, and annual reports			Schedulable reports in Endpoint Central and Log360 [1]
Assigned technical account manager (TAM) and quarterly reviews		Your team provides it	Premium Support, paid: dedicated account manager and periodic health reviews [13]
24/7 contact with support or security staff			24/7 multichannel Premium Support; basic support is during business hours [13]
Independent certification of operations (ISO 27001 or SOC 2 Type II)	 ISO/IEC 27001:2022		Zoho, ManageEngine's parent company, is ISO/IEC 27001 certified for its cloud services [14]
Fast start with a software agent: your devices' activity, visible within hours	 Typical: 2 to 4 hours		Cloud with an agent is fast; on-premises requires a server and a project [15]
Detection and response	15 of 15	7 complete +3 partial	
Continuous monitoring and event correlation (SIEM), aligned with MITRE ATT&CK (a reference framework of attack techniques)			Log360: SIEM with more than 2,000 detections mapped to MITRE ATT&CK [1]
Advanced protection on every device (EDR/XDR): malware, ransomware, and vulnerability exploitation			Its own add-ons for EDR, next-generation antivirus, and anti-ransomware [16]
Web filtering on the device			Endpoint Central Security includes browser security with web filtering [5]
Intrusion detection (IDS/IPS)			No IDS/IPS of its own; Log360 only ingests IDS/IPS logs [1]
Threat detection on the internal network (NDR)			No NDR in the products evaluated [1]
Documented investigations enriched with threat intelligence			Log360 cross-references events with threat intelligence [1]
Incident management with a case log and response time measured per case			Log360 incident console with MTTD and MTTR metrics [17]
Response with device isolation and IP address blocking			EDR isolates devices; Log360 SOAR runs blocks [18]
Incident response with root cause analysis		Your team provides it	Log forensic analysis tools; no response service [1]
Identity posture: MFA, privileged accounts, and conditional access			Audits Active Directory and Entra ID; no comprehensive posture or Google Workspace [6]
Zero Trust: secure DNS, application access, and control of unauthorized applications (shadow IT)			Private Access (ZTNA) add-on from March 2026; no secure DNS or shadow IT control [18]
Cloud security: alerts and posture			Cloud Security Plus in Log360 monitors Azure and AWS [19]

Capability	TecnetSOC	ManageEngine IT management	Evidence on ManageEngine
☒ 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)	☒	☐	Audits Exchange; no anti-spam, anti-phishing, or quarantine [6]
Security awareness: phishing simulations and training with metrics	☒	☐	No phishing simulations or training [1]
Prioritized security recommendations with an approval workflow	☒	☒	Secure configuration recommendations; approval only for patches [20]
Exposure and IT management	12 of 12	7 complete +1 partial	
Unified asset and software inventory	☒	☒	Hardware and software inventory in Endpoint Central [5]
Vulnerabilities prioritized by severity and likelihood of exploitation (CVSS, EPSS)	☒	☒	Vulnerability Manager Plus with CVSS and EPSS [21]
Priority for flaws already being exploited (CISA KEV catalog)	☒	☒	Flags inclusion in the CISA KEV catalog and due dates [21]
Operating system and third-party application patching	☒	☒	Windows, macOS, Linux, and more than 1,000 third-party applications [4]
Provider-operated patching, with published timelines by severity	☒ Critical: 48 h (target)	Your team provides it	The customer or IT provider runs it; no published timelines [4]
Closure verification: the scanner confirms the vulnerability is gone	☒	☒	Continuous scans reflect vulnerabilities remediated per device [20]
Patch validation in a pilot group before rollout	☒	☒	Enterprise: patch testing and approval before rollout [4]
External attack surface: what your company exposes on the internet, with a risk score	☒ Score from 0 to 100	☐	No EASM in the products evaluated [22]
Alerts for domains that imitate your brand and for exposed credentials or keys	☒	☐	No typosquatting or exposed secrets detection [22]
Annual penetration test (pentest)	☒ Annual	Your team provides it	No pentesting [22]
Remote monitoring and management (RMM)	☒	☒	Endpoint Central and Endpoint Central MSP: remote control and management [11]
Uptime monitoring (NOC)	☒	☒	MSP Central monitors servers and network; there is no NOC as a service [23]
Backup and continuity	3 of 3	0 complete +0 partial	
Backup for servers, files, databases, virtual machines, and Microsoft 365	☒ Add-on	☐	No backup in the products evaluated [5]
Immutable backup vault (cannot be altered or deleted), isolated per customer	☒ Add-on	☐	No immutable vault [5]
Disaster recovery with drills and measured recovery time (RTO)	☒ Add-on Measured RTO	☐	No disaster recovery with testing [5]
Compliance	6 of 6	0 complete +2 partial	
Monthly evidence ready for auditors and insurers	☒ Monthly	☒	Log360 generates compliance reports; no prepared monthly evidence [1]
Readiness for ISO 27001, SOC 2, and PCI DSS with shared controls	☒ Add-on	☒	Reports by framework (PCI, ISO, HIPAA); not a GRC platform with mapping [1]
Mexican regulatory readiness: CNBV Fintech, data protection (LFPDPPP), and NOM-024	☒ Add-on	☐	No Mexican regulations [24]
Risk management, controls, statement of applicability, and internal audits	☒ Add-on	☐	No risk management, SoA, or internal audits [1]
Auditor portal with an evidence room and a public trust page (trust center)	☒ Add-on	☐	No auditor portal or Trust Center for the customer [1]

Capability	TecnetSOC	ManageEngine IT management	Evidence on ManageEngine
☒ 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			
Business continuity, vendor risk, and data breach management	☒ Add-on	☒	No continuity, vendor, or breach management [1]
How it's purchased	Not counted		
Per-device pricing, with plans that stack	☒ Per device	☒	Public per-device pricing with tiered editions; MSP edition per endpoint per month [23]
Free plan to get started	☒ Up to 10 devices	☒ Up to 25 devices	Permanent free editions: Patch Manager Plus for 20 devices and Endpoint Central for 25 [25]
Free trial in your real environment	☒ 30 days	☒	30-day trial for most products [23]
Available under your IT provider's brand	☒	☒	Endpoint Central MSP under the IT provider's brand [11]
Full coverage	50	18 +11 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.

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

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

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 ManageEngine: ManageEngine (Endpoint Central Security or MSP with EDR, Malware Protection, and Private Access add-ons; Patch Manager Plus Enterprise; Vulnerability Manager Plus Enterprise; Log360 Cloud Enterprise; Premium Support), 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.manageengine.com/log-management/integrated-log-management-and-s... (Differences you notice day to day)	9. blogs.manageengine.com/it-security/manageengine-log360-launches-zia... (AI investigation assistant in the portal that...)	17. www.manageengine.com/log-management/soar-incident-management.html (Incident management with a case log and response time...)
2. www.manageengine.com/products/desktop-central/cve-2021-44515-authen... (Differences you notice day to day)	10. mobiletime.la/noticias/04/06/2025/manageengine-en-latam/ (Operations in LATAM, the US, and Europe, with analysts...)	18. securitymea.com/2026/03/18/manageengine-adds-edr-and-secure-private... (Response with device isolation and IP...)
3. www.manageengine.com/cloud-siem/pricing-details.html (Differences you notice day to day)	11. www.manageengine.com/desktop-management-msp/ (Analysts, support, and portal in native Spanish)	19. www.manageengine.com/log-management/cloud/features-new.html (Cloud security: alerts and posture)
4. www.manageengine.com/patch-management/edition-comparison.html (Differences you notice day to day)	12. www.manageengine.com/products/desktop-central/support.html (Published notification and investigation...)	20. www.manageengine.com/vulnerability-management/help/vulnerability-ma... (Prioritized security recommendations with an...)
5. www.manageengine.com/products/desktop-central/pricing.html (Differences you notice day to day)	13. www.manageengine.com/products/desktop-central/premium-support.html (Assigned technical account manager (TAM) and...)	21. www.manageengine.com/products/desktop-central/help/vulnerability-re... (Vulnerabilities prioritized by severity...)
6. www.manageengine.com/log-management/office-365-administration-repor... (Differences you notice day to day)	14. www.zoho.com/compliance.html (Independent certification of operations (ISO 27001...))	22. www.manageengine.com/vulnerability-management/pricing.html (External attack surface: what your company exposes...)
7. www.manageengine.com/log-management/ai-security/ai-agents-for-secur... (AI agents that investigate and filter alerts...)	15. www.manageengine.com/products/desktop-central/faq.html (Fast start with a software agent: your...)	23. www.manageengine.com/msp-central/pricing.html (Uptime monitoring (NOC))
8. www.manageengine.com/log-management/soar/what-is-security-automatio... (Human Gate: a person approves every...)	16. www.manageengine.com/products/desktop-central/endpoint-detection-an... (Advanced protection on every device (EDR/XDR)...)	24. www.manageengine.com/latam/partners.html (Mexican regulatory readiness: CNBV...)
		25. www.manageengine.com/patch-management/pricing.html (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.](#)