

ConnectSecure shows you the flaws. TecnetSOC fixes them and watches your operations for you, 24/7.

With ConnectSecure you detect and prioritize, but the tool doesn't monitor or contain attacks; expert help is purchased by the hour, from 4 to 12 a month. **With TecnetSOC, the SOC monitors 24/7 and patches until the scanner confirms.**



41

capabilities where TecnetSOC goes further

9

capabilities where we match

0

capabilities where ConnectSecure outperforms TecnetSOC

Of the 50: 41 where we go further and 9 where we match

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

ConnectSecure is a vulnerability scanning and compliance tool for IT providers; it is not a managed SOC service. Everything else you would need (EDR, SIEM, RMM, and backup) is purchased and operated separately, and not all of it integrates natively. This comparison shows, capability by capability, how much of what TecnetSOC includes ConnectSecure 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
It identifies risks; it doesn't stop attacks

WITH CONNECTSECURE
Its own FAQ places it in the Identify function of the NIST framework (and in Protect, because of patching): it doesn't monitor, investigate, or contain an attack in progress. [1]

WITH TECNETSOC
Our own analysts monitor 24/7, AI agents investigate every alert, and we respond to incidents with forensic analysis.

02
It alerts you; your team fixes

WITH CONNECTSECURE
It alerts you to what's critical, but your team defines policies, schedules patches, and follows up on every ticket until it's closed. [2]

WITH TECNETSOC
Our SOC prioritizes by KEV and EPSS, validates in a pilot group, installs critical patches within 48 h (target), and closes when the scanner confirms.

03
EDR, SIEM, and RMM, separately

WITH CONNECTSECURE
You purchase and operate EDR, SIEM, and RMM with other vendors; its FAQ even asks you to add its agent to your EDR's allowlist. [1]

WITH TECNETSOC
The most complete offering includes EDR/XDR, SIEM with MITRE ATT&CK, RMM, web filtering, IDS/IPS, and NDR, operated by our SOC.

04
Expert help with limited hours

WITH CONNECTSECURE
For an expert to deploy agents or automate patching, you purchase Virtual Administrator: a separate recurring service capped at 4, 8, or 12 hours per month. [3]

WITH TECNETSOC
Our SOC handles 24/7 operations and patching; the most complete offering adds a TAM and quarterly reviews.

05
Ticket-based support, typical response in 12 hours

WITH CONNECTSECURE
Support is by ticket or email, with no published hours and a typical response time of 12 hours; its documentation is in English. [4]

WITH TECNETSOC
24/7 analysts in your time zone, in native Spanish; for a critical incident, notification and investigation start within 30 minutes as a target.

06
Pentesting, with another provider

WITH CONNECTSECURE
There is web application scanning, but it clarifies that it doesn't do human-led pentesting: you purchase and coordinate that with another provider. [5]

WITH TECNETSOC
Annual pentesting is part of the most complete offering, along with monitoring for domains that imitate your brand and exposed secrets.

— WHERE THE DIFFERENCE LIES

The three areas with the biggest gap

Detection and response

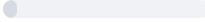
TecnetSOC  **15**

ConnectSecure  **1**

of 15 capabilities complete in this area

Operations and service

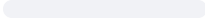
TecnetSOC  **14**

ConnectSecure  **1**

of 14 capabilities complete in this area

Compliance

TecnetSOC  **6**

ConnectSecure  **0**

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

— CAPABILITY BY CAPABILITY

TecnetSOC and ConnectSecure, side by side

Capability	TecnetSOC	ConnectSecure Vulnerability scanning	Evidence on ConnectSecure
 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	1 complete  +3 partial	
24/7 security operations center (SOC) with human analysts		Your team provides it	FAQ: does not provide managed services or security analysts [1]
AI agents that investigate and filter alerts before passing them to an analyst			AI only in reports and questionnaires; doesn't investigate alerts [6]

Capability	TecnetSOC	ConnectSecure Vulnerability scanning	Evidence on ConnectSecure
☒ 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	☒	☐	No provider approval gate; the IT provider decides and executes [1]
AI investigation assistant in the portal that cites its sources	☒ Neo	☐	No AI analyst; reports with AI-generated analysis [6]
Operations in LATAM, the US, and Europe, with analysts in your time zone	☒	Your team provides it	No operations in LATAM; headquartered in Tampa [1]
Analysts, support, and portal in native Spanish	☒	☐	Support and documentation in English [1]
Leadership reports in Spanish and in business language	☒	☒	AI reports in 5 languages with business impact; Spanish not officially confirmed [7]
Published notification and investigation start times by severity	☒ Critical: 30 min (target)	Your team provides it	No published SLAs [1]
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	☒	☒	More than 100 reports; automated executive frequency not officially confirmed [7]
Assigned technical account manager (TAM) and quarterly reviews	☒	Your team provides it	Virtual Administrator, its own paid service: consultant sessions every two weeks in Bronze and weekly in Silver [3]
24/7 contact with support or security staff	☒	☐	Support hours not published [1]
Independent certification of operations (ISO 27001 or SOC 2 Type II)	☒ ISO/IEC 27001:2022	☒	ISO/IEC 27001:2022 badge on its website; also SOC 2 [8]
Fast start with a software agent: your devices' activity, visible within hours	☒ Typical: 2 to 4 hours	☒	Lightweight agent and network probe; no published onboarding time [9]
Detection and response	15 of 15	1 complete +2 partial	
Continuous monitoring and event correlation (SIEM), aligned with MITRE ATT&CK (a reference framework of attack techniques)	☒	☐	No SIEM [1]
Advanced protection on every device (EDR/XDR): malware, ransomware, and vulnerability exploitation	☒	☐	No EDR/XDR [1]
Web filtering on the device	☒	☐	No web filtering [1]
Intrusion detection (IDS/IPS)	☒	☐	No IDS/IPS; reviews firewall configuration [7]
Threat detection on the internal network (NDR)	☒	☐	Probe scans vulnerabilities on devices without an agent; doesn't detect threats [9]
Documented investigations enriched with threat intelligence	☒	☐	No threat investigations [1]
Incident management with a case log and response time measured per case	☒	☐	No incident management; creates tickets in the PSA [1]
Response with device isolation and IP address blocking	☒	☐	No device isolation or IP blocking [1]
Incident response with root cause analysis	☒	Your team provides it	No incident response or forensics [1]
Identity posture: MFA, privileged accounts, and conditional access	☒	☒	AD, Entra ID, M365 (MFA, admins, and conditional access), and Google Workspace [10]
Zero Trust: secure DNS, application access, and control of unauthorized applications (shadow IT)	☒	☐	No Zero Trust capabilities [1]
Cloud security: alerts and posture	☒	☐	Assesses M365; no published Azure alerts or posture [7]

Capability	TecnetSOC	ConnectSecure Vulnerability scanning	Evidence on ConnectSecure
☒ 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 [1]
Security awareness: phishing simulations and training with metrics	☒	☒	AI training questionnaires; no phishing simulations [10]
Prioritized security recommendations with an approval workflow	☒	☒	EPSS, CVSS, and impact prioritization; optional M365 auto-remediation in report mode [10]
Exposure and IT management	12 of 12	7 complete +1 partial	
Unified asset and software inventory	☒	☒	Asset and software inventory (Silver) [7]
Vulnerabilities prioritized by severity and likelihood of exploitation (CVSS, EPSS)	☒	☒	Its own internal and external scanning with CVSS and EPSS [7]
Priority for flaws already being exploited (CISA KEV catalog)	☒	☒	Prioritization with CISA KEV, EPSS, and CVSS [5]
Operating system and third-party application patching	☒	☒	OS, more than 550 third-party apps, and Linux (Feb 2026) [11]
Provider-operated patching, with published timelines by severity	☒ Critical: 48 h (target)	Your team provides it	Virtual Administrator, its own recurring paid service: its experts deploy agents and automate patching, with a monthly hour cap [3]
Closure verification: the scanner confirms the vulnerability is gone	☒	☒	Its own continuous scanning reassesses after the patch [7]
Patch validation in a pilot group before rollout	☒	☒	Patch 360: pilot groups, testing, approval, and rollback [11]
External attack surface: what your company exposes on the internet, with a risk score	☒ Score from 0 to 100	☒	External scanning, subdomains, ports, surface map, and risk assessment [12]
Alerts for domains that imitate your brand and for exposed credentials or keys	☒	☒	Dark web credentials; no look-alike domains or secrets in code [12]
Annual penetration test (pentest)	☒ Annual	Your team provides it	No pentesting; web application scanning only [7]
Remote monitoring and management (RMM)	☒	☐	No RMM of its own; integrates with third-party RMM [1]
Uptime monitoring (NOC)	☒	☐	No uptime monitoring or NOC [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 [1]
Immutable backup vault (cannot be altered or deleted), isolated per customer	☒ Add-on	☐	No immutable vault [1]
Disaster recovery with drills and measured recovery time (RTO)	☒ Add-on Measured RTO	☐	No disaster recovery [1]
Compliance	6 of 6	0 complete +3 partial	
Monthly evidence ready for auditors and insurers	☒ Monthly	☒	Compliance and cyber insurance reports generated by the IT provider; no managed monthly delivery [7]
Readiness for ISO 27001, SOC 2, and PCI DSS with shared controls	☒ Add-on	☒	Control assessment across more than 20 frameworks; not a full GRC platform [8]
Mexican regulatory readiness: CNBV Fintech, data protection (LFPDPPP), and NOM-024	☒ Add-on	☐	No Mexican frameworks (LFPDPPP, CNBV) [8]
Risk management, controls, statement of applicability, and internal audits	☒ Add-on	☒	Risk and control assessment; no SoA 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; co-managed access for the customer [1]

Capability	TecnetSOC	ConnectSecure Vulnerability scanning	Evidence on ConnectSecure
☒ 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 business continuity or vendor management [1]
How it's purchased	Not counted		
Per-device pricing, with plans that stack	☒ Per device	☒	Per asset, stackable Bronze and Silver tiers; minimum purchase with a price published by the vendor [7]
Free plan to get started	☒ Up to 10 devices	☐	No free plan [7]
Free trial in your real environment	☒ 30 days	☒	Full 14-day trial, extendable [1]
Available under your IT provider's brand	☒	☒	Reports with the IT provider's brand; the console doesn't carry its brand [13]
Full coverage	50	9 +9 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

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

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

— 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 ConnectSecure: ConnectSecure, Silver license (the highest) with Patch 360 and M365 Auto Remediation, 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. [connectsecure.com/faq](#) (Differences you notice day to day)

2. [connectsecure.com/for-msps](#) (Differences you notice day to day)

3. [connectsecure.com/connectsecure-consulting](#) (Differences you notice day to day)

4. [connectsecure.com/support](#) (Differences you notice day to day)

5. [connectsecure.com/connectsecure-for-it-teams](#) (Differences you notice day to day)
6. [connectsecure.com/news/connectsecure-launches-groundbreaking-ai-pow...](#) (AI agents that investigate and filter alerts...)

7. [connectsecure.com/pricing](#) (Leadership reports in Spanish and in business...)

8. [connectsecure.com/platform](#) (Independent certification of operations (ISO 27001...))

9. [connectsecure.com/hubfs/ConnectSecure%20-%20Probes-Agents%20Overvie...](#) (Fast start with a software agent: your...)
10. [www.helpnetsecurity.com/2026/08/12/connectsecure-microsoft-365-auto...](#) (Identity posture: MFA, privileged accounts...)

11. [www.helpnetsecurity.com/2026/06/08/connectsecure-patch-360/](#) (Operating system and third-party application patching)

12. [connectsecure.com/attack-surface-scanning](#) (External attack surface: what your company exposes...)

13. [connectsecure.com/white-label-reports](#) (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.](#)