

TecnetSOC vs. Blackpoint

Blackpoint acts on its own in your network. With TecnetSOC, AI investigates and a person approves every critical action.

With Blackpoint, its SOC can isolate devices without asking for prior approval, and applying patches remains in your team's hands. **With TecnetSOC, AI investigates, a person who knows your business approves critical actions, and the SOC patches.**



43

capabilities where TecnetSOC goes further

7

capabilities where we match

0

capabilities where Blackpoint 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 Blackpoint: 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

Blackpoint is a managed SOC service sold through IT providers. Here we compare each one's most complete published offering, capability by capability.

— WHAT SETS US APART

Differences you notice day to day

01
You apply the patches

WITH BLACKPOINT
Its vulnerability module identifies and prioritizes; applying the patch, testing it, and confirming closure remain in the hands of your team or your IT provider. [1]

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

02
They isolate first and tell you later

WITH BLACKPOINT
Its SOC acts first and notifies later: it can isolate a device or disable an account without prior approval, and it doesn't document an option to require it. [2]

WITH TECNETSOC
AI investigates and correlates every alert, and a person approves every critical action before it runs (Human Gate).

03
No documented operations in LATAM

WITH BLACKPOINT
Its published phone numbers are in North America, Australia, and the United Kingdom; it doesn't document Spanish-speaking analysts or operations in LATAM. [3]

WITH TECNETSOC
You get analysts in your time zone and in native Spanish, with ISO/IEC 27001:2022 certified operations in LATAM, the US, and Europe.

04
Only through an IT provider, with no free trial

WITH BLACKPOINT
It can't be purchased directly: it's available only through a partner IT provider, with no free plan or published free trial; the website only offers to schedule a demo. [4]

WITH TECNETSOC
You purchase directly or through your IT provider; Visibility is free for up to 10 devices, and you can try Response for 30 days in your environment.

05
Email and phishing, through another provider

WITH BLACKPOINT
Its SOC detects account takeover and suspicious sending in Microsoft 365, but its published packages don't include spam and malware filtering or phishing simulations. [5]

WITH TECNETSOC
The most complete offering includes email security (spam, phishing, malware, and BEC) and security awareness with phishing simulations.

06
Pentesting and look-alike domains, another contract

WITH BLACKPOINT
Its SOC watches for exposed credentials on the dark web, but it doesn't document pentesting or monitoring of domains that imitate your brand to impersonate you. [1]

WITH TECNETSOC
The most complete offering includes annual pentesting, alerts for domains that imitate your brand, and external attack surface with a score from 0 to 100.

— WHERE THE DIFFERENCE LIES

The three areas with the biggest gap

Operations and service

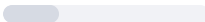
TecnetSOC  **14**

Blackpoint  **2**

of 14 capabilities complete in this area

Detection and response

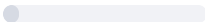
TecnetSOC  **15**

Blackpoint  **4**

of 15 capabilities complete in this area

Exposure and IT management

TecnetSOC  **12**

Blackpoint  **1**

of 12 capabilities complete in this area

— CAPABILITY BY CAPABILITY

TecnetSOC and Blackpoint, side by side

Capability	TecnetSOC	Blackpoint SOC for IT providers	Evidence on Blackpoint
 Offers it  Offers it as an add-on  Partial, limited, or requires another contract  No public evidence  Not part of its published offering			
Operations and service	14 of 14	2 complete  +6 partial	
24/7 security operations center (SOC) with human analysts			Its own 24/7/365 SOC with threat hunters and remediators [3]
AI agents that investigate and filter alerts before passing them to an analyst			"AI-enhanced" alerts; doesn't document AI agents that investigate every alert [6]
Human Gate: a person approves every critical action before it runs			Contains without prior approval from the IT provider; no approval mode, according to an independent directory [4]

Capability	TecnetSOC	Blackpoint SOC for IT providers	Evidence on Blackpoint
Offers it Offers it as an add-on Partial, limited, or requires another contract No public evidence Not part of its published offering			
AI investigation assistant in the portal that cites its sources	Neo		No evidence of a conversational AI analyst in the portal [5]
Operations in LATAM, the US, and Europe, with analysts in your time zone			No documented presence or SOC in LATAM; phone numbers in North America, Australia, and the UK [3]
Analysts, support, and portal in native Spanish			No evidence of Spanish-speaking analysts or support [3]
Leadership reports in Spanish and in business language			No evidence of reports in Spanish [5]
Published notification and investigation start times by severity	Critical: 30 min (target)		No published SLA; only self-reported averages (under 2 minutes for identity) [7]
Executive summary every morning: what happened in the last 24 hours	7:30 a.m.		No evidence of a daily executive summary [5]
Automated weekly, monthly, quarterly, and annual reports			Forensic reports and 180-day history; automated frequency not documented [7]
Assigned technical account manager (TAM) and quarterly reviews			Dedicated account team and quarterly plan for the IT provider, depending on its billing tier [8]
24/7 contact with support or security staff			24/7 SOC confirmed; a 24/7 help desk as such is not documented [3]
Independent certification of operations (ISO 27001 or SOC 2 Type II)	ISO/IEC 27001:2022		Publishes an annual SOC 2 Type II; does not list ISO/IEC 27001 [9]
Fast start with a software agent: your devices' activity, visible within hours	Typical: 2 to 4 hours		Easy deployment according to reviews; no published onboarding time [10]
Detection and response	15 of 15	4 complete +7 partial	
Continuous monitoring and event correlation (SIEM), aligned with MITRE ATT&CK (a reference framework of attack techniques)			SIEM in the Standard package with 365-day retention; MITRE ATT&CK mapping [5]
Advanced protection on every device (EDR/XDR): malware, ransomware, and vulnerability exploitation			Its own EDR agent with MDR and application control; Windows and macOS, no Linux [11]
Web filtering on the device			No evidence of web filtering on the device [5]
Intrusion detection (IDS/IPS)			No evidence of IDS/IPS [5]
Threat detection on the internal network (NDR)			No documented NDR or detection of devices without an agent [5]
Documented investigations enriched with threat intelligence			Contextual intelligence and its own adversary tracking team [6]
Incident management with a case log and response time measured per case			Prioritized incident response; case log and MTTR per incident not documented [6]
Response with device isolation and IP address blocking			Isolates devices and contains at the network level; automatic blocking by geography and VPN [4]
Incident response with root cause analysis			Identity forensic reports and recovery support; no documented full forensics [7]
Identity posture: MFA, privileged accounts, and conditional access			M365 and Google Workspace ITDR, admin MFA; no service accounts or conditional access [12]
Zero Trust: secure DNS, application access, and control of unauthorized applications (shadow IT)			Application control operated by its SOC; no secure DNS or Zero Trust application access [13]
Cloud security: alerts and posture			Posture for Microsoft 365 only; doesn't document Azure [12]
Email security: spam, phishing, malware, and impersonation fraud (BEC)			Detects BEC and suspicious sending in M365; no anti-spam or quarantine [7]

Capability	TecnetSOC	Blackpoint SOC for IT providers	Evidence on Blackpoint
☒ Offers it ☒ Offers it as an add-on ☐ Partial, limited, or requires another contract ☐ No public evidence ☐ Not part of its published offering			
Security awareness: phishing simulations and training with metrics	☒	☐	No evidence of phishing simulations or training [5]
Prioritized security recommendations with an approval workflow	☒	☐	Prioritized remediation backlog and posture rating; no approval workflow [1]
Exposure and IT management	12 of 12	1 complete +4 partial	
Unified asset and software inventory	☒	☒	Inventory of devices, identities, applications, and SaaS accounts in all packages [5]
Vulnerabilities prioritized by severity and likelihood of exploitation (CVSS, EPSS)	☒	☐	Vulnerabilities by risk and exploitability; use of CVSS and EPSS not documented [1]
Priority for flaws already being exploited (CISA KEV catalog)	☒	☐	Prioritizes by exploitability; doesn't mention the CISA KEV catalog [1]
Operating system and third-party application patching	☒	☐	Identifies and prioritizes; doesn't offer patching, the IT provider does it [1]
Provider-operated patching, with published timelines by severity	☒ Critical: 48 h (target)	☐	No operated patching or published timelines [1]
Closure verification: the scanner confirms the vulnerability is gone	☒	☐	No documented closure verification [1]
Patch validation in a pilot group before rollout	☒	☐	No patching, and therefore no pilot group [1]
External attack surface: what your company exposes on the internet, with a risk score	☒ Score from 0 to 100	☐	Network and cloud scanning plus posture rating; no documented external attack surface management (EASM) [1]
Alerts for domains that imitate your brand and for exposed credentials or keys	☒	☐	Dark web monitoring for credentials; no alerts for domains that imitate your brand or for exposed code [1]
Annual penetration test (pentest)	☒ Annual	☐	No evidence of pentesting [5]
Remote monitoring and management (RMM)	☒	☐	No RMM of its own; the IT provider uses its own [5]
Uptime monitoring (NOC)	☒	☐	No evidence of uptime monitoring or a NOC [5]
Backup and continuity	3 of 3	0 complete +0 partial	
Backup for servers, files, databases, virtual machines, and Microsoft 365	☒ Add-on	☐	No backup of its own [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 [5]
Compliance	6 of 6	0 complete +1 partial	
Monthly evidence ready for auditors and insurers	☒ Monthly	☐	Continuous evidence for insurers, limited to M365 and SIEM logs [12]
Readiness for ISO 27001, SOC 2, and PCI DSS with shared controls	☒ Add-on	☐	No GRC platform or cross-framework mapping [5]
Mexican regulatory readiness: CNBV Fintech, data protection (LFPDPPP), and NOM-024	☒ Add-on	☐	No Mexican regulations [5]
Risk management, controls, statement of applicability, and internal audits	☒ Add-on	☐	No risk management, SoA, or internal audits [5]
Auditor portal with an evidence room and a public trust page (trust center)	☒ Add-on	☐	The provider's own Trust Center, not for customers; no evidence room for the auditor [9]
Business continuity, vendor risk, and data breach management	☒ Add-on	☐	No continuity, vendor, or breach modules [5]

Capability	TecnetSOC	Blackpoint SOC for IT providers	Evidence on Blackpoint
✔ Offers it ✗ Not part of its published offering	⊕ Offers it as an add-on ⓪ Partial, limited, or requires another contract	❓ No public evidence	
How it's purchased	Not counted		
Per-device pricing, with plans that stack	✔ Per device	✔	Billed per device per month; stackable Essentials, Core, and Standard packages; price not public [5]
Free plan to get started	✔ Up to 10 devices	✗	No free plan [5]
Free trial in your real environment	✔ 30 days	✗	No published trial; demo request only [5]
Available under your IT provider's brand	✔	⓪	Only through IT providers, co-branded with Blackpoint [8]
Full coverage	50	7 +18 partial	

— NEXT STEP

See it in your own operations

Try it in a real environment, without changing what already works for you.

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 Blackpoint: Blackpoint Cyber, CompassOne Standard package (ITDR + MDR + vulnerabilities + cloud posture + application control + SIEM) plus Managed EDR and Dark Web Monitoring, 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. [blackpointcyber.com/platform/vulnerability-management/](#) (Differences you notice day to day)

2. [blackpointcyber.com/why-blackpoint/security-operations-center/](#) (Differences you notice day to day)

3. [blackpointcyber.com/frequently-asked-questions/](#) (Differences you notice day to day)

4. [www.flamingo.run/blog/blackpoint-cyber-review](#) (Differences you notice day to day)

5. [blackpointcyber.com/platform/](#) (Differences you notice day to day)

6. [blackpointcyber.com/platform/managed-detection-and-response/](#) (AI agents that investigate and filter alerts...)

7. [www.globenewswire.com/news-release/2026/09/10/3359559/0/en/new-blac...](#) (Published notification and investigation...)

8. [blackpointcyber.com/wp-content/uploads/2025/08/Blackpoint-Cyber-Par...](#) (Assigned technical account manager (TAM) and...)

9. blackpointcyber.com/company/trust-center/ (Independent certification of operations (ISO 27001...))
10. capterra.com/p/212884/Blackpoint-MDR/ (Fast start with a software agent: your...)
11. blackpointcyber.com/solutions/blackpoint-response/ (Advanced protection on every device (EDR/XDR)...)
 12. blackpointcyber.com/platform/cloud-posture/ (Identity posture: MFA, privileged accounts...)
13. blackpointcyber.com/resources/blog/introducing-managed-application-... (Zero Trust: secure DNS, application access, and...)

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.](#)