

TecnetSOC vs. Heimdal

Heimdal sells you the platform. TecnetSOC delivers the service: security run by people and AI, 24/7.

With Heimdal, what its SOC can do is set when you sign and covers only the modules you license. With TecnetSOC, analysts respond 24/7 across every layer of your plan, and a person approves every critical action.



41

capabilities where TecnetSOC goes further

9

capabilities where we match

0

capabilities where Heimdal 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 Heimdal: 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

Heimdal is a security platform with a SOC service; each module is licensed separately. Here we compare each one's most complete published offering, capability by capability.

— WHAT SETS US APART

Differences you notice day to day

01

If it only notifies, containment is up to you

WITH HEIMDAL
What its SOC can do is agreed in advance in MXDR Adapt: if you only authorize it to notify or advise, containment is up to you. [1]

WITH TECNETSOC
TecnetOne's own analysts investigate and respond 24/7; a person approves every critical action before it runs, case by case.

02

The SOC sees only what is licensed

WITH HEIMDAL
The SOC only monitors and contains within the modules you license and deploy; each module is paid for separately. [1]

WITH TECNETSOC
You pay per device with stackable plans: each plan adds layers to the previous one, and the SOC runs every layer in your plan 24/7.

03

Other layers, other providers

WITH HEIMDAL
Its catalog doesn't include phishing simulations, external attack surface, pentesting, uptime monitoring, or backup: each one is another provider and another contract. [2]

WITH TECNETSOC
The most complete offering adds simulated phishing, external attack surface, annual pentesting, and NOC; immutable backup is a separate add-on.

04

A delivered patch is not a closed vulnerability

WITH HEIMDAL
Its 4 hours measure how long the vendor's patch takes to reach your device; it doesn't publish prioritization based on real-world exploitation (KEV or EPSS). [3]

WITH TECNETSOC
The SOC prioritizes by KEV and EPSS, validates in a pilot group, and considers the vulnerability closed only when the scanner confirms the fix.

05

SOC in Europe, distributor in LATAM

WITH HEIMDAL
Its SOC operates from Europe, and in LATAM the business relationship goes through a distributor, not the team that monitors your devices. [4]

WITH TECNETSOC
We operate in LATAM, the US, and Europe with analysts in your time zone, in native Spanish, and with multilingual support.

06

No Mexican regulations or compliance platform

WITH HEIMDAL
Compliance reports map to frameworks such as NIS2, DORA, and ISO 27001; it doesn't include a GRC platform or Mexican regulations such as CNBV or NOM-024. [5]

WITH TECNETSOC
You can add TecnetGRC, at an additional cost per standard: ISO 27001, SOC 2, PCI DSS, CNBV, LFPDPPP, NOM-024, and an auditor portal.

— WHERE THE DIFFERENCE LIES

The three areas with the biggest gap

Operations and service

TecnetSOC 14

Heimdal 3

of 14 capabilities complete in this area

Detection and response

TecnetSOC 15

Heimdal 4

of 15 capabilities complete in this area

Exposure and IT management

TecnetSOC 12

Heimdal 2

of 12 capabilities complete in this area

— CAPABILITY BY CAPABILITY

TecnetSOC and Heimdal, side by side

Capability		TecnetSOC	Heimdal Platform and SOC	Evidence on Heimdal
✓ Offers it ✗ Not part of its published offering	⊕ Offers it as an add-on ⦿ Partial, limited, or requires another contract	? No public evidence		
Operations and service		14 of 14	3 complete +8 partial	
24/7 security operations center (SOC) with human analysts	✓	✓	MXDR includes its own 24/7 SOC with analysts, operated from Europe [5]	
AI agents that investigate and filter alerts before passing them to an analyst	✓	⦿	AI Wingman Triage announced Apr 2026, phased release; no evidence that it filters every alert [6]	
Human Gate: a person approves every critical action before it runs	✓	⦿	MXDR Adapt sets by contract whether the SOC notifies, advises, or acts; no per-action approval [7]	

Capability	TecnetSOC	Heimdal Platform and SOC	Evidence on Heimdal
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		AI Wingman Assist guides in the console; in phased rollout, no evidence that it cites sources [6]
Operations in LATAM, the US, and Europe, with analysts in your time zone			SOC in Europe; LATAM only through the distributor Aufiero, no local SOC operations [4]
Analysts, support, and portal in native Spanish			Spanish support via the distributor Aufiero; no evidence of Spanish-speaking SOC analysts [8]
Leadership reports in Spanish and in business language			Compliance reports in English; no evidence of executive reports in Spanish [5]
Published notification and investigation start times by severity	Critical: 30 min (target)		Its blog states that it doesn't publish a SOC SLA [4]
Executive summary every morning: what happened in the last 24 hours	7:30 a.m.		No public evidence of a daily executive summary [5]
Automated weekly, monthly, quarterly, and annual reports			Centralized reports in a multi-tenant console; no evidence of a weekly to annual cadence [9]
Assigned technical account manager (TAM) and quarterly reviews			Dedicated account managers for partners; no evidence of a TAM or quarterly reviews [9]
24/7 contact with support or security staff			Its official MXDR data sheet includes 24x7 customer support as a key service, separate from continuous monitoring [10]
Independent certification of operations (ISO 27001 or SOC 2 Type II)	ISO/IEC 27001:2022		SOC 2 Type II certified (ISAE 3000); no published ISO 27001 of its own [11]
Fast start with a software agent: your devices' activity, visible within hours	Typical: 2 to 4 hours		A single cloud agent; doesn't publish time to first activity data [2]
Detection and response	15 of 15	4 complete +10 partial	
Continuous monitoring and event correlation (SIEM), aligned with MITRE ATT&CK (a reference framework of attack techniques)			XDR correlates activity data and maps to MITRE ATT&CK; it is not a log SIEM of its own [12]
Advanced protection on every device (EDR/XDR): malware, ransomware, and vulnerability exploitation			Its own Next-Gen Antivirus, EDR/XDR, and Ransomware Encryption Protection [2]
Web filtering on the device			DNS Security Endpoint filters web traffic on the device [2]
Intrusion detection (IDS/IPS)			Firewall in the antivirus module; no published dedicated IDS/IPS [2]
Threat detection on the internal network (NDR)			DNS Security Network covers the network at the DNS level; it is not traffic NDR [2]
Documented investigations enriched with threat intelligence			XDR with threat intelligence, activity data, and forensic details [12]
Incident management with a case log and response time measured per case			Threat Hunting & Action Center manages cases; no evidence of MTTR per incident [12]
Response with device isolation and IP address blocking			The SOC can isolate devices; IP blocking only via integrated firewalls (Meraki, Palo Alto) [7]
Incident response with root cause analysis			MXDR mentions forensic analysis; no defined forensic incident response service [5]
Identity posture: MFA, privileged accounts, and conditional access			ITDR detects suspicious sign-ins in M365, and PASM manages privileged accounts; no MFA posture [5]
Zero Trust: secure DNS, application access, and control of unauthorized applications (shadow IT)			Secure DNS and containment of third-party AI; no Zero Trust access to applications [6]
Cloud security: alerts and posture			Covers M365 and Google Workspace; no evidence of Azure posture or alerts [12]
Email security: spam, phishing, malware, and impersonation fraud (BEC)			Its own email security: anti-spam, anti-phishing, advanced malware filtering, and impersonation fraud prevention (BEC) [13]

Capability	TecnetSOC	Heimdal Platform and SOC	Evidence on Heimdal
✓ Offers it + Offers it as an add-on 0 Partial, limited, or requires another contract ? No public evidence ✗ Not part of its published offering			
Security awareness: phishing simulations and training with metrics	✓	✗	No phishing simulations or security awareness training in its catalog [2]
Prioritized security recommendations with an approval workflow	✓	0	AI Wingman Assist suggests best-practice configurations; no approval workflow [6]
Exposure and IT management	12 of 12	2 complete +4 partial	
Unified asset and software inventory	✓	✓	Patch & Asset Management with asset and software inventory [3]
Vulnerabilities prioritized by severity and likelihood of exploitation (CVSS, EPSS)	✓	0	Vulnerabilities by severity and CVE within patching; no EPSS or standalone scanner [3]
Priority for flaws already being exploited (CISA KEV catalog)	✓	?	No evidence of prioritization by the CISA KEV catalog [3]
Operating system and third-party application patching	✓	✓	Windows, macOS, Linux, and 350+ third-party applications; Infinity for in-house apps [3]
Provider-operated patching, with published timelines by severity	✓ Critical: 48 h (target)	0	MXDR lists patching and vulnerability remediation among its use cases; the customer configures patching, and it doesn't publish timelines by severity [10]
Closure verification: the scanner confirms the vulnerability is gone	✓	0	Its vulnerability management process includes a verification stage, without stating that the scanner performs it [10]
Patch validation in a pilot group before rollout	✓	✗	Configurable schedules, but no published pilot group workflow [3]
External attack surface: what your company exposes on the internet, with a risk score	✓ Score from 0 to 100	✗	No external attack surface (EASM) offering [2]
Alerts for domains that imitate your brand and for exposed credentials or keys	✓	✗	No detection of typosquatting or exposed secrets or code [2]
Annual penetration test (pentest)	✓ Annual	✗	No pentesting offering [2]
Remote monitoring and management (RMM)	✓	0	Remote desktop, patching, and inventory; not a full RMM, integrates ConnectWise RMM [2]
Uptime monitoring (NOC)	✓	✗	No uptime monitoring or NOC [2]
Backup and continuity	3 of 3	0 complete +0 partial	
Backup for servers, files, databases, virtual machines, and Microsoft 365	+ Add-on	✗	Does not offer backup [2]
Immutable backup vault (cannot be altered or deleted), isolated per customer	+ Add-on	✗	Does not offer an immutable vault [2]
Disaster recovery with drills and measured recovery time (RTO)	+ Add-on Measured RTO	✗	Does not offer disaster recovery [2]
Compliance	6 of 6	0 complete +1 partial	
Monthly evidence ready for auditors and insurers	✓ Monthly	0	Compliance reports mapped to NIS2, ISO 27001, and others; no formal monthly evidence [5]
Readiness for ISO 27001, SOC 2, and PCI DSS with shared controls	+ Add-on	✗	Maps controls in reports; doesn't offer a GRC platform [5]
Mexican regulatory readiness: CNBV Fintech, data protection (LFPDPPP), and NOM-024	+ Add-on	✗	No coverage of Mexican regulations [2]
Risk management, controls, statement of applicability, and internal audits	+ Add-on	✗	No risk management, SoA, 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 [2]
Business continuity, vendor risk, and data breach management	+ Add-on	✗	No continuity, vendor, or breach management modules [2]

Capability	TecnetSOC	Heimdal Platform and SOC	Evidence on Heimdal
✓ Offers it ✗ Not part of its published offering	ⓘ Offers it as an add-on ⓘ 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 year, but each module is licensed separately, not stackable [14]
Free plan to get started	✓ Up to 10 devices	✗	No published permanent free plan [14]
Free trial in your real environment	✓ 30 days	✓	30-day free trial with no card required, according to the XDR data sheet [12]
Available under your IT provider's brand	✓	ⓘ	NEXUS program for IT providers with co-branding; the product and SOC remain Heimdal [9]
Full coverage	50	9 +23 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 Heimdal: Heimdal Security (Heimdal), full platform with all of its modules plus the MXDR service (24/7 SOC), 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. [heimdalsecurity.com/wp-content/themes/heimdal/product-sheets/Heimda...](#) (Differences you notice day to day)

2. [heimdalsecurity.com/](#) (Differences you notice day to day)

3. [heimdalsecurity.com/enterprise-security/products/patch-management-s...](#) (Differences you notice day to day)

4. [heimdalsecurity.com/blog/best-managed-edr-services/](#) (Differences you notice day to day)

5. [heimdalsecurity.com/enterprise-security/products/managed-extended-d...](#) (Differences you notice day to day)

6. [heimdalsecurity.com/blog/heimdal-expands-ai-strategy-with-ai-wingma...](#) (AI agents that investigate and filter alerts...)

7. [heimdalsecurity.com/blog/heimdals-mxdr-adapt-worlds-first-tailored-...](#) (Human Gate: a person approves every...)

8. [www.heimdalsecurity-la.com/en/heimdal-security-businesses-msps/](#) (Analysts, support, and portal in native Spanish)

9. [heimdalsecurity.com/channel-partners](#) (Automated weekly, monthly, quarterly, and...)

10. support.heimdalsecurity.com/hc/en-us/articles/10792316864669-Manage... (24/7 contact with support or security staff)

11. heimdalsecurity.com/blog/category/heimdal-announcements/ (Independent certification of operations (ISO 27001...))
12. heimdalsecurity.com/enterprise-security/products/extended-detection... (Continuous monitoring and event correlation...)

13. support.heimdalsecurity.com/hc/en-us/articles/360007435238-Email-Se... (Email security: spam, phishing, malware, and...)
14. heimdalsecurity.com/enterprise/request-pricing (Per-device pricing, with plans that stack)

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.](#)