

TecnetSOC vs. SentinelOne

# SentinelOne stops and rolls back attacks on the device; its 24/7 monitoring is purchased separately. TecnetSOC runs your security, with each case resolved in your language.

With SentinelOne, email, automatic patching, and detection on your network come from other vendors, and there is no backup of its own. With TecnetSOC, the SOC handles patching, email protection is included, and you can add immutable backup with TecnetProtect.



33

capabilities where TecnetSOC goes further

17

capabilities where we match

0

capabilities where SentinelOne outperforms TecnetSOC

Of the 50: 33 where we go further and 17 where we match

Same list of 50 capabilities and same criteria for TecnetSOC and SentinelOne: 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](https://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 October 13, 2026. Version 2026.09. Informational comparison prepared by TecnetOne, not affiliated with the brands mentioned.

## — BEFORE YOU COMPARE

SentinelOne is a device protection platform (EDR/XDR) purchased in bundles and modules; with Wayfinder MDR, its managed service at an additional cost, its analysts monitor and respond 24/7. Email, automatic patching, and network detection come from other vendors integrated into Singularity. Here we compare the platform, Wayfinder MDR, and its own modules with what TecnetSOC includes, capability by capability.

— WHAT SETS US APART

Differences you notice day to day

**01**

**Another tool installs the patch**

**WITH SENTINELONE**  
Vulnerability Management scans and prioritizes, but doesn't publish patching of its own: its marketplace offers automatic patching from other vendors, such as Adapiva. [1]

**WITH TECNETSOC**  
The SOC patches based on real-world exploitation (KEV and EPSS), with target timelines by severity, validates in a pilot group, and considers it closed only when the scanner confirms.

**02**

**Another vendor protects your email**

**WITH SENTINELONE**  
There is no email security of its own: its XDR receives signals from other vendors' email products, such as Proofpoint, to respond on the device. [2]

**WITH TECNETSOC**  
Protection against spam, phishing, malware, and impersonation (BEC) is part of the same service, with self-service quarantine.

**03**

**Rollback is not a substitute for backup**

**WITH SENTINELONE**  
Rollback undoes an attack's changes on the device, but its published portfolio doesn't include server backup, an immutable vault, or disaster recovery. [3]

**WITH TECNETSOC**  
You can add TecnetProtect (at an additional cost): backup in an immutable vault per customer and disaster recovery with drills and measured RTO.

**04**

**Threats on your network, with another vendor's sensors**

**WITH SENTINELONE**  
Detection of threats on your internal network (NDR) and of intruders comes from integrating other vendors' products, such as Vectra or ExtraHop, into its XDR. [4]

**WITH TECNETSOC**  
Internal network detection (NDR) and IDS/IPS are included in the most complete offering, with a sensor on a mirror port.

**05**

**Compliance: its certificates, not your audits**

**WITH SENTINELONE**  
Its compliance page shows its own platform's certifications and a third-party document on how it supports PCI DSS; it doesn't publish tools to prepare for your audits. [5]

**WITH TECNETSOC**  
You receive monthly evidence for auditors and insurers and, with TecnetGRC (at an additional cost), you prepare for ISO 27001, SOC 2, PCI DSS, and Mexican regulations.

**06**

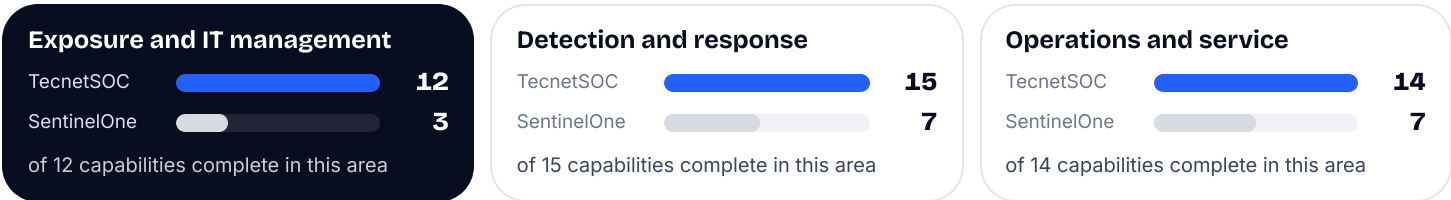
**Your staff, without phishing drills**

**WITH SENTINELONE**  
Its published bundles don't include phishing simulations or security awareness training for your staff. [6]

**WITH TECNETSOC**  
The most complete offering includes phishing simulations and training with per-user metrics, along with email protection.

— WHERE THE DIFFERENCE LIES

The three areas with the biggest gap



— CAPABILITY BY CAPABILITY

TecnetSOC and SentinelOne, side by side

| Capability                                                                                                                         | TecnetSOC                                                                           | SentinelOne<br>EDR/XDR and MDR                                                                                      | Evidence on SentinelOne                                                                                              |
|------------------------------------------------------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------|
|  Offers it                                      |                                                                                     |                                                                                                                     |                                                                                                                      |
|  Offers it as an add-on                         |                                                                                     |                                                                                                                     |                                                                                                                      |
|  Partial, limited, or requires another contract |                                                                                     |                                                                                                                     |                                                                                                                      |
|  Not part of its published offering             |                                                                                     |                                                                                                                     |  No public evidence              |
| <b>Operations and service</b>                                                                                                      | <b>14 of 14</b>                                                                     | <b>7 complete</b><br> +5 partial |                                                                                                                      |
| 24/7 security operations center (SOC) with human analysts                                                                          |  |                                  | Wayfinder MDR: certified analysts monitor, investigate, and contain threats 24/7/365 [7]                             |
| AI agents that investigate and filter alerts before passing them to an analyst                                                     |  |                                  | Purple AI enriches the context of each alert; certified analysts confirm severity and filter out false positives [7] |

| Capability                                                                                                                                                                        | TecnetSOC                     | SentinelOne<br>EDR/XDR and MDR      | Evidence on SentinelOne                                                                                                                  |
|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------------------------------|-------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------|
| Offers it            Offers it as an add-on            Partial, limited, or requires another contract            No public evidence            Not part of its published offering |                               |                                     |                                                                                                                                          |
| Human Gate: a person approves every critical action before it runs                                                                                                                |                               |                                     | Contains threats according to the response policy you configure; case-by-case approval not documented <a href="#">[7]</a>                |
| AI investigation assistant in the portal that cites its sources                                                                                                                   | <br>Neo                       |                                     | Purple AI investigates in natural language and explains each verdict with a rationale <a href="#">[8]</a>                                |
| Operations in LATAM, the US, and Europe, with analysts in your time zone                                                                                                          |                               |                                     | Experts in 16 countries with 24/7 operations; doesn't publish locations or operations in LATAM <a href="#">[9]</a>                       |
| Analysts, support, and portal in native Spanish                                                                                                                                   |                               |                                     | Spanish-language website and support line in Mexico; language of analysts and console not published <a href="#">[10]</a>                 |
| Leadership reports in Spanish and in business language                                                                                                                            |                               |                                     | MDR Elite assigns a threat advisor with operational reviews; executive reports in Spanish not documented <a href="#">[9]</a>             |
| Published notification and investigation start times by severity                                                                                                                  | <br>Critical: 30 min (target) |                                     | No times by severity; publishes a mean time to detect of 3.3 minutes <a href="#">[7]</a>                                                 |
| Executive summary every morning: what happened in the last 24 hours                                                                                                               | <br>7:30 a.m.                 |                                     | No evidence of a daily executive summary <a href="#">[7]</a>                                                                             |
| Automated weekly, monthly, quarterly, and annual reports                                                                                                                          |                               |                                     | Quarterly health reviews with the TAM; no documented automatic weekly to annual reports <a href="#">[11]</a>                             |
| Assigned technical account manager (TAM) and quarterly reviews                                                                                                                    |                               |                                     | Technical account manager (TAM, at an additional cost) with quarterly health reviews <a href="#">[11]</a>                                |
| 24/7 contact with support or security staff                                                                                                                                       |                               |                                     | 24/7/365 access to incident response specialists and a breach hotline <a href="#">[12]</a>                                               |
| Independent certification of operations (ISO 27001 or SOC 2 Type II)                                                                                                              | <br>ISO/IEC 27001:2022        |                                     | ISO/IEC 27001:2022 and SOC 2 Type 2 examination of its platform <a href="#">[5]</a>                                                      |
| Fast start with a software agent: your devices' activity, visible within hours                                                                                                    | <br>Typical: 2 to 4 hours     |                                     | A single lightweight agent with automated deployment for devices, identity, and cloud <a href="#">[3]</a>                                |
| <b>Detection and response</b>                                                                                                                                                     | <b>15 of 15</b><br>           | <b>7 complete</b><br><br>+6 partial |                                                                                                                                          |
| Continuous monitoring and event correlation (SIEM), aligned with MITRE ATT&CK (a reference framework of attack techniques)                                                        |                               |                                     | XDR correlates activity data from devices, cloud, and identity; threat hunting with MITRE ATT&CK techniques <a href="#">[3]</a>          |
| Advanced protection on every device (EDR/XDR): malware, ransomware, and vulnerability exploitation                                                                                |                               |                                     | Autonomous containment of ransomware, zero-day attacks, and fileless malware on every device <a href="#">[13]</a>                        |
| Web filtering on the device                                                                                                                                                       |                               |                                     | Firewall and USB device control on the device; category-based web filtering not documented <a href="#">[14]</a>                          |
| Intrusion detection (IDS/IPS)                                                                                                                                                     |                               |                                     | No IDS/IPS of its own; integrates other vendors' firewalls and network sensors into its XDR <a href="#">[4]</a>                          |
| Threat detection on the internal network (NDR)                                                                                                                                    |                               |                                     | Network threat detection with other vendors' NDR (Vectra, ExtraHop) integrated into its XDR <a href="#">[4]</a>                          |
| Documented investigations enriched with threat intelligence                                                                                                                       |                               |                                     | Investigations enriched with threat intelligence: indicators, actor attribution, and campaigns <a href="#">[7]</a>                       |
| Incident management with a case log and response time measured per case                                                                                                           |                               |                                     | Purple AI documents each investigation in notebooks; handling time per case not published <a href="#">[8]</a>                            |
| Response with device isolation and IP address blocking                                                                                                                            |                               |                                     | Isolates devices, stops processes, rolls back changes, and blocks inbound and outbound network traffic <a href="#">[3]</a>               |
| Incident response with root cause analysis                                                                                                                                        |                               |                                     | Forensics specialists (DFIR) contain, investigate, and analyze the root cause; hours come with a retainer <a href="#">[12]</a>           |
| Identity posture: MFA, privileged accounts, and conditional access                                                                                                                |                               |                                     | Singularity Identity: Active Directory, Entra ID, and Okta, conditional access, and MFA re-authentication by policy <a href="#">[15]</a> |

| Capability                                                                                                                                                                        | TecnetSOC                   | SentinelOne<br>EDR/XDR and MDR  | Evidence on SentinelOne                                                                                                                         |
|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-----------------------------|---------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------|
| Offers it            Offers it as an add-on            Partial, limited, or requires another contract            No public evidence            Not part of its published offering |                             |                                 |                                                                                                                                                 |
| Zero Trust: secure DNS, application access, and control of unauthorized applications (shadow IT)                                                                                  |                             |                                 | Prompt Security controls unauthorized AI tools (shadow AI); no documented secure DNS <a href="#">[16]</a>                                       |
| Cloud security: alerts and posture                                                                                                                                                |                             |                                 | Singularity Cloud: posture, runtime workload protection, and data in your cloud <a href="#">[17]</a>                                            |
| Email security: spam, phishing, malware, and impersonation fraud (BEC)                                                                                                            |                             |                                 | No email security of its own; its XDR receives data from Proofpoint to respond on the device <a href="#">[2]</a>                                |
| Security awareness: phishing simulations and training with metrics                                                                                                                |                             |                                 | No phishing simulations or user training in its published bundles <a href="#">[6]</a>                                                           |
| Prioritized security recommendations with an approval workflow                                                                                                                    |                             |                                 | Hyperautomation runs responses with human approval when required; prioritized recommendations with approval not documented <a href="#">[18]</a> |
| <b>Exposure and IT management</b>                                                                                                                                                 | <b>12 of 12</b>             | <b>3 complete</b><br>+6 partial |                                                                                                                                                 |
| Unified asset and software inventory                                                                                                                                              |                             |                                 | Discovers managed and unmanaged devices (IoT, personal) and assesses applications and the operating system <a href="#">[19]</a>                 |
| Vulnerabilities prioritized by severity and likelihood of exploitation (CVSS, EPSS)                                                                                               |                             |                                 | Prioritizes with EPSS, the CISA KEV catalog, and its own risk score, not just CVSS <a href="#">[19]</a>                                         |
| Priority for flaws already being exploited (CISA KEV catalog)                                                                                                                     |                             |                                 | Uses CISA KEV catalog signals to prioritize what is already being exploited <a href="#">[19]</a>                                                |
| Operating system and third-party application patching                                                                                                                             |                             |                                 | No published patching of its own; its marketplace offers automatic patching from other vendors, such as Adaptiva <a href="#">[1]</a>            |
| Provider-operated patching, with published timelines by severity                                                                                                                  | <br>Critical: 48 h (target) |                                 | No evidence that SentinelOne installs patches or of timelines by severity <a href="#">[19]</a>                                                  |
| Closure verification: the scanner confirms the vulnerability is gone                                                                                                              |                             |                                 | Scheduled and on-demand scans reflect status; formal closure verification not documented <a href="#">[19]</a>                                   |
| Patch validation in a pilot group before rollout                                                                                                                                  |                             |                                 | No evidence of patch validation in a pilot group <a href="#">[19]</a>                                                                           |
| External attack surface: what your company exposes on the internet, with a risk score                                                                                             | <br>Score from 0 to 100     |                                 | Validates which of your cloud exposures are exploitable; no documented monitoring of what you expose on the internet <a href="#">[20]</a>       |
| Alerts for domains that imitate your brand and for exposed credentials or keys                                                                                                    |                             |                                 | Detects stolen credentials exposed on the dark web; alerts for domains that imitate your brand not documented <a href="#">[15]</a>              |
| Annual penetration test (pentest)                                                                                                                                                 | <br>Annual                  |                                 | Purple team exercises and compromise assessments; pentesting not published as its own service <a href="#">[12]</a>                              |
| Remote monitoring and management (RMM)                                                                                                                                            |                             |                                 | RemoteOps runs scripts and installs, updates, or removes software on devices; not presented as an RMM <a href="#">[21]</a>                      |
| Uptime monitoring (NOC)                                                                                                                                                           |                             |                                 | No evidence of uptime monitoring (NOC) <a href="#">[13]</a>                                                                                     |
| <b>Backup and continuity</b>                                                                                                                                                      | <b>3 of 3</b>               | <b>0 complete</b><br>+0 partial |                                                                                                                                                 |
| Backup for servers, files, databases, virtual machines, and Microsoft 365                                                                                                         | Add-on                      |                                 | No backup of its own; rollback undoes an attack's changes on the device and is not backup <a href="#">[3]</a>                                   |
| Immutable backup vault (cannot be altered or deleted), isolated per customer                                                                                                      | Add-on                      |                                 | No backup vault of its own <a href="#">[13]</a>                                                                                                 |
| Disaster recovery with drills and measured recovery time (RTO)                                                                                                                    | Add-on<br>Measured RTO      |                                 | No disaster recovery or drills in its published portfolio <a href="#">[13]</a>                                                                  |

| Capability                                                                                                                                                                                                                       | TecnetSOC                     | SentinelOne<br>EDR/XDR and MDR | Evidence on SentinelOne                                                                                                  |
|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------------------------------|--------------------------------|--------------------------------------------------------------------------------------------------------------------------|
| <div> <div>✓</div> Offers it <div>+</div> Offers it as an add-on <div>⦿</div> Partial, limited, or requires another contract <div>?</div> No public evidence </div> <div> <div>✗</div> Not part of its published offering </div> |                               |                                |                                                                                                                          |
| Compliance                                                                                                                                                                                                                       | 6 of 6                        | 0 complete<br>+1 partial       |                                                                                                                          |
| Monthly evidence ready for auditors and insurers                                                                                                                                                                                 | <div>✓</div> Monthly          | <div>?</div>                   | No documented monthly evidence for your auditors; shares the SOC 2 report for its own platform <a href="#">[5]</a>       |
| Readiness for ISO 27001, SOC 2, and PCI DSS with shared controls                                                                                                                                                                 | <div>+</div> Add-on           | <div>⦿</div>                   | A third-party document explains how it supports PCI DSS; ISO 27001 or SOC 2 readiness not documented <a href="#">[5]</a> |
| Mexican regulatory readiness: CNBV Fintech, data protection (LFPDPPP), and NOM-024                                                                                                                                               | <div>+</div> Add-on           | <div>?</div>                   | No evidence of Mexican regulations <a href="#">[5]</a>                                                                   |
| Risk management, controls, statement of applicability, and internal audits                                                                                                                                                       | <div>+</div> Add-on           | <div>?</div>                   | No risk management, controls, or internal audits for your company <a href="#">[5]</a>                                    |
| Auditor portal with an evidence room and a public trust page (trust center)                                                                                                                                                      | <div>+</div> Add-on           | <div>?</div>                   | Its trust center is SentinelOne's own; no portal for your auditor or trust page of your own <a href="#">[5]</a>          |
| Business continuity, vendor risk, and data breach management                                                                                                                                                                     | <div>+</div> Add-on           | <div>?</div>                   | No evidence of business continuity, vendor risk, or breach management <a href="#">[5]</a>                                |
| How it's purchased                                                                                                                                                                                                               | Not counted                   |                                |                                                                                                                          |
| Per-device pricing, with plans that stack                                                                                                                                                                                        | <div>✓</div> Per device       | <div>✓</div>                   | Annual bundles per device (Complete, Commercial); Enterprise and MDR by quote <a href="#">[6]</a>                        |
| Free plan to get started                                                                                                                                                                                                         | <div>✓</div> Up to 10 devices | <div>?</div>                   | No published free plan <a href="#">[6]</a>                                                                               |
| Free trial in your real environment                                                                                                                                                                                              | <div>✓</div> 30 days          | <div>⦿</div>                   | 30-day free trial of Singularity Control announced in 2024 for SMBs; no published MDR trial <a href="#">[22]</a>         |
| Available under your IT provider's brand                                                                                                                                                                                         | <div>✓</div>                  | <div>⦿</div>                   | MSSP program with a multi-tenant platform; white labeling or co-branding not documented <a href="#">[23]</a>             |
| Full coverage                                                                                                                                                                                                                    | 50                            | 17<br>+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.

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

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

TecnetSOC vs. SentinelOne · Comparison 2026.09

tecnetone.com/en/services/soc-as-a-service · Page 5 of 6

## 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 October 13, 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 SentinelOne:** SentinelOne, most complete published offering for a midsize company (the Singularity platform in its Enterprise bundle plus Wayfinder MDR Elite, a 24/7 service operated by SentinelOne that succeeds Vigilance Respond Pro and WatchTower, with a dedicated threat advisor, an incident response retainer, and access to forensics; plus its own modules at an additional cost: Purple AI, Singularity AI SIEM, Singularity Identity, Singularity Cloud Security, Singularity Vulnerability Management and Network Discovery, Hyperautomation, RemoteOps, Singularity Mobile, Prompt Security, Wayfinder Threat Hunting, and support with a TAM), reviewed Oct 13, 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](https://soc.catalogo.tecnetone.com) and [tecnetone.com/servicios/soc-as-a-service](https://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.sentinelone.com/partners/singularity-marketplace/](https://www.sentinelone.com/partners/singularity-marketplace/) (Differences you notice day to day)
2. [www.sentinelone.com/press/sentinelone-integrates-with-proofpoint-fo...](https://www.sentinelone.com/press/sentinelone-integrates-with-proofpoint-fo...) (Differences you notice day to day)
3. [www.sentinelone.com/platform/singularity-complete/](https://www.sentinelone.com/platform/singularity-complete/) (Differences you notice day to day)
4. [www.sentinelone.com/press/sentinelone-expands-firewall-and-ndr-capabilities](https://www.sentinelone.com/press/sentinelone-expands-firewall-and-ndr-capabilities) (Differences you notice day to day)
5. [www.sentinelone.com/security-compliance/](https://www.sentinelone.com/security-compliance/) (Differences you notice day to day)
6. [www.sentinelone.com/pricing/](https://www.sentinelone.com/pricing/) (Differences you notice day to day)
7. [www.sentinelone.com/global-services/managed-detection-and-response/](https://www.sentinelone.com/global-services/managed-detection-and-response/) (24/7 security operations center (SOC) with human analysts)
8. [www.sentinelone.com/platform/purple/](https://www.sentinelone.com/platform/purple/) (AI investigation assistant in the portal that...)
9. [www.sentinelone.com/blog/managed-defense-reimagined-introducing-way...](https://www.sentinelone.com/blog/managed-defense-reimagined-introducing-way...) (Operations in LATAM, the US, and Europe, with analysts...)
10. [www.sentinelone.com/global-services/get-support-now/](https://www.sentinelone.com/global-services/get-support-now/) (Analysts, support, and portal in native Spanish)
11. [www.sentinelone.com/global-services/technical-account-management/](https://www.sentinelone.com/global-services/technical-account-management/) (Automated weekly, monthly, quarterly, and...)
12. [www.sentinelone.com/global-services/incident-readiness-and-response/](https://www.sentinelone.com/global-services/incident-readiness-and-response/) (24/7 contact with support or security staff)
13. [www.sentinelone.com/platform/](https://www.sentinelone.com/platform/) (Advanced protection on every device (EDR/XDR)...)
14. [www.sentinelone.com/platform/singularity-control/](https://www.sentinelone.com/platform/singularity-control/) (Web filtering on the device)
15. [www.sentinelone.com/platform/identity/](https://www.sentinelone.com/platform/identity/) (Identity posture: MFA, privileged accounts...)
16. [www.sentinelone.com/platform/securing-ai-prompt/](https://www.sentinelone.com/platform/securing-ai-prompt/) (Zero Trust: secure DNS, application access, and...)
17. [www.sentinelone.com/platform/cloud-security/](https://www.sentinelone.com/platform/cloud-security/) (Cloud security: alerts and posture)
18. [www.sentinelone.com/platform/singularity-hyperautomation/](https://www.sentinelone.com/platform/singularity-hyperautomation/) (Prioritized security recommendations with an...)
19. [www.sentinelone.com/platform/singularity-vulnerability-management/](https://www.sentinelone.com/platform/singularity-vulnerability-management/) (Unified asset and software inventory)
20. [www.sentinelone.com/platform/singularity-cloud-native-security/](https://www.sentinelone.com/platform/singularity-cloud-native-security/) (External attack surface: what your company exposes...)
21. [www.sentinelone.com/press/sentinelone-remote-script-orchestration-r...](https://www.sentinelone.com/press/sentinelone-remote-script-orchestration-r...) (Remote monitoring and management (RMM))
22. [www.sentinelone.com/press/sentinelone-delivers-leading-cyber-threat...](https://www.sentinelone.com/press/sentinelone-delivers-leading-cyber-threat...) (Free trial in your real environment)
23. [www.sentinelone.com/partners/mssp-partners/](https://www.sentinelone.com/partners/mssp-partners/) (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 October 13, 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.