

TecnetSOC vs. CrowdStrike

# CrowdStrike protects your devices; its 24/7 monitoring is purchased separately. TecnetSOC runs your security for you, with the case resolved in your language.

With CrowdStrike, email security and backup come from other vendors, and its risk-based patching is still announced as coming soon. With TecnetSOC, the SOC handles patching, email protection is included, and you can add immutable backup and disaster recovery with TecnetProtect.



32

capabilities where TecnetSOC goes further

18

capabilities where we match

0

capabilities where CrowdStrike outperforms TecnetSOC

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

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

CrowdStrike is a device protection platform (EDR/XDR) that is purchased in bundles and modules; with Falcon Complete, its managed service at an additional cost, its analysts monitor and respond 24/7. Email security, backup, and network detection come from other vendors integrated with Falcon. Here we compare the platform, Falcon Complete, and its own modules with what TecnetSOC includes, capability by capability.

— WHAT SETS US APART

Differences you notice day to day

**01**  
**Patching stays on your side**

**WITH CROWDSTRIKE**  
Exposure Management prioritizes vulnerabilities, but risk-based patching in Falcon for IT is still marked as coming soon, and Falcon Complete doesn't publish that its team installs patches. [\[1\]](#)

**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 CROWDSTRIKE**  
There is no email security of its own: Next-Gen SIEM analyzes signals from other vendors' email products, such as Abnormal, Mimecast, or Proofpoint. [\[2\]](#)

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

**03**  
**Backup comes from a partner**

**WITH CROWDSTRIKE**  
Backup isn't part of its portfolio: its partnership with Rubrik adds that vendor's backup and restore to Falcon's detection. [\[3\]](#)

**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**  
**Monitoring your internal network, with another vendor's sensors**

**WITH CROWDSTRIKE**  
Intrusion and threat detection on the internal network (IDS, NDR) comes from other vendors' sensors, such as Corelight, integrated into Next-Gen SIEM. [\[4\]](#)

**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: tools, not a solution**

**WITH CROWDSTRIKE**  
Its own compliance page states that its products and services are not compliance solutions, but tools that support your program. [\[5\]](#)

**WITH TECNETSOC**  
You get 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.

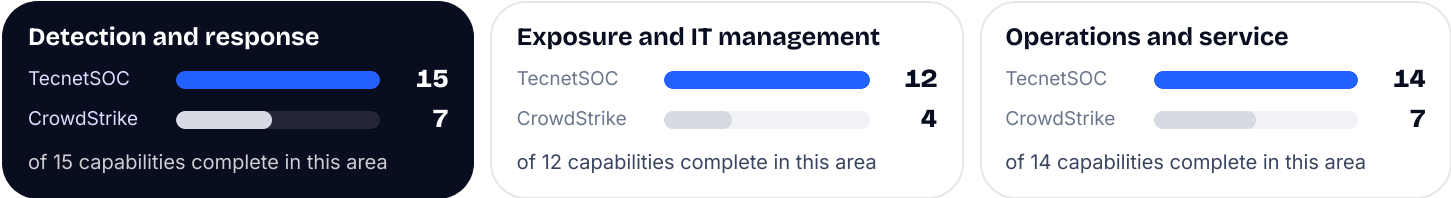
**06**  
**No published analysts in LATAM**

**WITH CROWDSTRIKE**  
Falcon Complete doesn't publish where its analysts are located or what language they work in; the Spanish-language support it announced is provided by authorized distributors in Europe. [\[6\]](#)

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

— WHERE THE DIFFERENCE LIES

The three areas with the biggest gap



— CAPABILITY BY CAPABILITY

TecnetSOC and CrowdStrike, side by side

| Capability                                                                                                                                                                                                                                                                                                                                                                                                                                          | TecnetSOC                                                                           | CrowdStrike<br>EDR/XDR and MDR                                                                                         | Evidence on CrowdStrike                                                                                            |
|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------|
|  Offers it  Offers it as an add-on  Partial, limited, or requires another contract  No public evidence |                                                                                     |                                                                                                                        |                                                                                                                    |
|  Not part of its published offering                                                                                                                                                                                                                                                                                                                              |                                                                                     |                                                                                                                        |                                                                                                                    |
| <b>Operations and service</b>                                                                                                                                                                                                                                                                                                                                                                                                                       | <b>14 of 14</b>                                                                     | <b>7 complete</b><br><br>+5 partial |                                                                                                                    |
| 24/7 security operations center (SOC) with human analysts                                                                                                                                                                                                                                                                                                                                                                                           |  |                                     | Falcon Complete: 24/7 monitoring, investigation, and remediation by CrowdStrike analysts <a href="#">[7]</a>       |
| AI agents that investigate and filter alerts before passing them to an analyst                                                                                                                                                                                                                                                                                                                                                                      |  |                                     | Agentic MDR: AI agents investigate and respond; Falcon Complete experts validate the decisions <a href="#">[7]</a> |

| Capability                                                                                                                                                                        | TecnetSOC                     | CrowdStrike<br>EDR/XDR and MDR      | Evidence on CrowdStrike                                                                                                                           |
|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------------------------------|-------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------|
| 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                                                                                                                |                               |                                     | Acts on your behalf within countermeasures agreed on at the start; case-by-case approval not documented <a href="#">[8]</a>                       |
| AI investigation assistant in the portal that cites its sources                                                                                                                   | <br>Neo                       |                                     | Charlotte AI investigates in natural language and every answer points back to its data; languages not published <a href="#">[9]</a>               |
| Operations in LATAM, the US, and Europe, with analysts in your time zone                                                                                                          |                               |                                     | Global 24/7 teams; doesn't publish where its analysts are located or any operations in LATAM <a href="#">[10]</a>                                 |
| Analysts, support, and portal in native Spanish                                                                                                                                   |                               |                                     | Spanish-language website; Spanish-language support announced through distributors in Europe; analysts' language not published <a href="#">[6]</a> |
| Leadership reports in Spanish and in business language                                                                                                                            |                               |                                     | Security advisors translate activity into executive guidance; no documented reports in Spanish <a href="#">[10]</a>                               |
| Published notification and investigation start times by severity                                                                                                                  | <br>Critical: 30 min (target) |                                     | No times by severity; publishes a median containment time of 1 minute, subject to variation <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                                                                                                                          |                               |                                     | Paid support with health checks and quarterly reports; no documented weekly to annual reports <a href="#">[11]</a>                                |
| Assigned technical account manager (TAM) and quarterly reviews                                                                                                                    |                               |                                     | Elite support (at an additional cost): a TAM specialized in your industry, plus monthly and operational reviews <a href="#">[11]</a>              |
| 24/7 contact with support or security staff                                                                                                                                       |                               |                                     | 24/7/365 phone support in paid support plans <a href="#">[11]</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 report for the Falcon platform <a href="#">[5]</a>                                                            |
| Fast start with a software agent: your devices' activity, visible within hours                                                                                                    | <br>Typical: 2 to 4 hours     |                                     | A lightweight sensor that deploys in minutes, managed from the web console <a href="#">[12]</a>                                                   |
| <b>Detection and response</b>                                                                                                                                                     | <b>15 of 15</b>               | <b>7 complete</b><br><br>+7 partial |                                                                                                                                                   |
| Continuous monitoring and event correlation (SIEM), aligned with MITRE ATT&CK (a reference framework of attack techniques)                                                        |                               |                                     | XDR and Next-Gen SIEM correlate first-party and third-party data; detections aligned with MITRE ATT&CK <a href="#">[13]</a>                       |
| Advanced protection on every device (EDR/XDR): malware, ransomware, and vulnerability exploitation                                                                                |                               |                                     | Next-generation antivirus and EDR in Falcon's business bundles <a href="#">[14]</a>                                                               |
| Web filtering on the device                                                                                                                                                       |                               |                                     | Falcon Secure Access protects the browser session; category-based web filtering not documented <a href="#">[15]</a>                               |
| Intrusion detection (IDS/IPS)                                                                                                                                                     |                               |                                     | No network IDS/IPS of its own; added with third-party sensors (for example, Corelight) in Next-Gen SIEM <a href="#">[4]</a>                       |
| Threat detection on the internal network (NDR)                                                                                                                                    |                               |                                     | Internal network detection only with third-party NDR sensors integrated into Next-Gen SIEM <a href="#">[4]</a>                                    |
| Documented investigations enriched with threat intelligence                                                                                                                       |                               |                                     | Investigations with its adversary intelligence, real-time indicators, and dark web monitoring <a href="#">[16]</a>                                |
| Incident management with a case log and response time measured per case                                                                                                           |                               |                                     | AI-powered incident management in Next-Gen SIEM; handling time per case not published <a href="#">[17]</a>                                        |
| Response with device isolation and IP address blocking                                                                                                                            |                               |                                     | Device network containment and IP restriction with real-time response actions <a href="#">[13]</a>                                                |
| Incident response with root cause analysis                                                                                                                                        |                               |                                     | End-to-end remediation in Falcon Complete; root cause through its incident response service <a href="#">[18]</a>                                  |
| Identity posture: MFA, privileged accounts, and conditional access                                                                                                                |                               |                                     | Next-Gen Identity Security: AD, Entra ID, and Okta, risk-based MFA, and just-in-time access <a href="#">[19]</a>                                  |
| Zero Trust: secure DNS, application access, and control of unauthorized applications (shadow IT)                                                                                  |                               |                                     | Falcon Shield detects unauthorized SaaS apps and Secure Access protects browsing; no documented secure DNS <a href="#">[20]</a>                   |

| Capability                                                                                                                                                                                                                   | TecnetSOC                                                      | CrowdStrike<br>EDR/XDR and MDR      | Evidence on CrowdStrike                                                                                                      |
|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|----------------------------------------------------------------|-------------------------------------|------------------------------------------------------------------------------------------------------------------------------|
| <input checked="" type="checkbox"/> Offers it <input checked="" type="checkbox"/> Offers it as an add-on <input type="checkbox"/> Partial, limited, or requires another contract <input type="checkbox"/> No public evidence |                                                                |                                     |                                                                                                                              |
| <input type="checkbox"/> Not part of its published offering                                                                                                                                                                  |                                                                |                                     |                                                                                                                              |
| Cloud security: alerts and posture                                                                                                                                                                                           | <input checked="" type="checkbox"/>                            | <input checked="" type="checkbox"/> | Falcon Cloud Security: posture and real-time detections on AWS, Azure, GCP, and OCI <a href="#">[21]</a>                     |
| Email security: spam, phishing, malware, and impersonation fraud (BEC)                                                                                                                                                       | <input checked="" type="checkbox"/>                            | <input type="checkbox"/>            | No email security of its own; Next-Gen SIEM analyzes data from Abnormal, Mimecast, or Proofpoint <a href="#">[2]</a>         |
| Security awareness: phishing simulations and training with metrics                                                                                                                                                           | <input checked="" type="checkbox"/>                            | <input type="checkbox"/>            | No phishing simulations or user training in its published bundles <a href="#">[14]</a>                                       |
| Prioritized security recommendations with an approval workflow                                                                                                                                                               | <input checked="" type="checkbox"/>                            | <input type="checkbox"/>            | Prioritizes exposures and orchestrates remediation with Falcon Fusion; approval workflow not documented <a href="#">[22]</a> |
| <b>Exposure and IT management</b>                                                                                                                                                                                            | <b>12 of 12</b>                                                | <b>4 complete</b><br>+6 partial     |                                                                                                                              |
| Unified asset and software inventory                                                                                                                                                                                         | <input checked="" type="checkbox"/>                            | <input checked="" type="checkbox"/> | Active, passive, and API-based discovery, including the applications installed on each device <a href="#">[22]</a>           |
| Vulnerabilities prioritized by severity and likelihood of exploitation (CVSS, EPSS)                                                                                                                                          | <input checked="" type="checkbox"/>                            | <input type="checkbox"/>            | Prioritizes with ExPRT.AI and adversary context rather than CVSS; EPSS not explicit <a href="#">[22]</a>                     |
| Priority for flaws already being exploited (CISA KEV catalog)                                                                                                                                                                | <input checked="" type="checkbox"/>                            | <input type="checkbox"/>            | Prioritizes by exploitation with its own intelligence; use of the KEV catalog not documented <a href="#">[23]</a>            |
| Operating system and third-party application patching                                                                                                                                                                        | <input checked="" type="checkbox"/>                            | <input type="checkbox"/>            | One-click emergency Windows patching; risk-based patching in Falcon for IT marked as coming soon <a href="#">[1]</a>         |
| Provider-operated patching, with published timelines by severity                                                                                                                                                             | <input checked="" type="checkbox"/><br>Critical: 48 h (target) | <input type="checkbox"/>            | No evidence that CrowdStrike installs the patches or of timelines by severity <a href="#">[7]</a>                            |
| Closure verification: the scanner confirms the vulnerability is gone                                                                                                                                                         | <input checked="" type="checkbox"/>                            | <input type="checkbox"/>            | The sensor's continuous assessment reflects the closure; no documented formal remediation verification <a href="#">[22]</a>  |
| Patch validation in a pilot group before rollout                                                                                                                                                                             | <input checked="" type="checkbox"/>                            | <input type="checkbox"/>            | Ring-based deployment in progressive waves announced for Falcon for IT, still as an upcoming feature <a href="#">[24]</a>    |
| External attack surface: what your company exposes on the internet, with a risk score                                                                                                                                        | <input checked="" type="checkbox"/><br>Score from 0 to 100     | <input checked="" type="checkbox"/> | 24/7 EASM: discovers internet-exposed assets and prioritizes them by risk <a href="#">[25]</a>                               |
| Alerts for domains that imitate your brand and for exposed credentials or keys                                                                                                                                               | <input checked="" type="checkbox"/>                            | <input checked="" type="checkbox"/> | Brand protection: domain impersonation, exposed credentials, and data leaks <a href="#">[16]</a>                             |
| Annual penetration test (pentest)                                                                                                                                                                                            | <input checked="" type="checkbox"/><br>Annual                  | <input checked="" type="checkbox"/> | External, internal, web and mobile application, and wireless pentesting <a href="#">[26]</a>                                 |
| Remote monitoring and management (RMM)                                                                                                                                                                                       | <input checked="" type="checkbox"/>                            | <input type="checkbox"/>            | Falcon for IT automates tasks and scripts on devices; it isn't positioned as an RMM <a href="#">[27]</a>                     |
| Uptime monitoring (NOC)                                                                                                                                                                                                      | <input checked="" type="checkbox"/>                            | <input type="checkbox"/>            | No evidence of uptime monitoring (NOC) <a href="#">[27]</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                                                                                                                                                    | <input checked="" type="checkbox"/> Add-on                     | <input type="checkbox"/>            | No backup of its own; integrates with partner backup vendors, such as Rubrik <a href="#">[3]</a>                             |
| Immutable backup vault (cannot be altered or deleted), isolated per customer                                                                                                                                                 | <input checked="" type="checkbox"/> Add-on                     | <input type="checkbox"/>            | No backup vault of its own <a href="#">[3]</a>                                                                               |
| Disaster recovery with drills and measured recovery time (RTO)                                                                                                                                                               | <input checked="" type="checkbox"/> Add-on<br>Measured RTO     | <input type="checkbox"/>            | No disaster recovery or drills; data restoration depends on backup partners <a href="#">[3]</a>                              |
| <b>Compliance</b>                                                                                                                                                                                                            | <b>6 of 6</b>                                                  | <b>0 complete</b><br>+1 partial     |                                                                                                                              |
| Monthly evidence ready for auditors and insurers                                                                                                                                                                             | <input checked="" type="checkbox"/><br>Monthly                 | <input type="checkbox"/>            | No documented monthly evidence for your auditors; provides the SOC 2 report for its own platform <a href="#">[5]</a>         |
| Readiness for ISO 27001, SOC 2, and PCI DSS with shared controls                                                                                                                                                             | <input checked="" type="checkbox"/> Add-on                     | <input type="checkbox"/>            | Platform mappings to PCI DSS and NIST done by a third party; ISO 27001 and SOC 2 not documented <a href="#">[5]</a>          |
| Mexican regulatory readiness: CNBV Fintech, data protection (LFPDPPP), and NOM-024                                                                                                                                           | <input checked="" type="checkbox"/> Add-on                     | <input type="checkbox"/>            | No evidence of Mexican regulations <a href="#">[5]</a>                                                                       |

| Capability                                                                                                                                                     | TecnetSOC                                                                             | CrowdStrike<br>EDR/XDR and MDR               | Evidence on CrowdStrike                                                                                       |
|----------------------------------------------------------------------------------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------|----------------------------------------------|---------------------------------------------------------------------------------------------------------------|
| <div> <div>✓</div> Offers it <div>+</div> Offers it as an add-on <div>ⓘ</div> </div> <div> <div>✗</div> Not part of its published offering <div>ⓘ</div> </div> | <div> <div>ⓘ</div> Partial, limited, or requires another contract <div>?</div> </div> | <div> <div>?</div> No public evidence </div> |                                                                                                               |
| Risk management, controls, statement of applicability, and internal audits                                                                                     | <div>+</div> Add-on                                                                   | <div>✗</div>                                 | CrowdStrike states that its products and services are not compliance solutions <a href="#">[5]</a>            |
| Auditor portal with an evidence room and a public trust page (trust center)                                                                                    | <div>+</div> Add-on                                                                   | <div>?</div>                                 | No portal for your auditor or trust page for your company <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>                                 | Stackable per-device bundles (Go, Pro, Enterprise); Falcon Complete and modules by quote <a href="#">[14]</a> |
| Free plan to get started                                                                                                                                       | <div>✓</div> Up to 10 devices                                                         | <div>?</div>                                 | No free plan; 15-day trial only <a href="#">[14]</a>                                                          |
| Free trial in your real environment                                                                                                                            | <div>✓</div> 30 days                                                                  | <div>ⓘ</div>                                 | 15-day free trial of the platform; no published trial of Falcon Complete <a href="#">[14]</a>                 |
| Available under your IT provider's brand                                                                                                                       | <div>✓</div>                                                                          | <div>✓</div>                                 | Falcon Complete for Service Providers allows white labeling or co-branding <a href="#">[28]</a>               |
| Full coverage                                                                                                                                                  | 50                                                                                    | 18<br>+19 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 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 CrowdStrike:** CrowdStrike, most complete published offering for a midsize company (Falcon platform in its Enterprise bundle plus Falcon Complete Next-Gen MDR, a 24/7 service operated by CrowdStrike, with its own modules at an additional cost: Next-Gen SIEM, Next-Gen Identity Security, Cloud Security, Exposure Management, Falcon for IT, Falcon Shield, Falcon Secure Access, Charlotte AI, Adversary Intelligence, pentest and incident response services, and Elite support), 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 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. <a href="https://www.crowdstrike.com/en-au/platform/falcon-for-it/">www.crowdstrike.com/en-au/platform/falcon-for-it/</a> (Differences you notice day to day)                                                       | 10. <a href="https://www.crowdstrike.com/en-us/services/falcon-complete-mdr/operating-mo...">www.crowdstrike.com/en-us/services/falcon-complete-mdr/operating-mo...</a> (Operations in LATAM, the US, and Europe, with analysts...) | 20. <a href="https://www.crowdstrike.com/en-us/platform/falcon-shield/">www.crowdstrike.com/en-us/platform/falcon-shield/</a> (Zero Trust: secure DNS, application access, and...)                                        |
| 2. <a href="https://www.crowdstrike.com/tech-hub/ng-siem/harnessing-email-data-to-stop-...">www.crowdstrike.com/tech-hub/ng-siem/harnessing-email-data-to-stop-...</a> (Differences you notice day to day)             | 11. <a href="https://assets.crowdstrike.com/is/content/crowdstrikeinc/crowdstrike-falcon...">assets.crowdstrike.com/is/content/crowdstrikeinc/crowdstrike-falcon...</a> (Automated weekly, monthly, quarterly, and...)              | 21. <a href="https://www.crowdstrike.com/en-us/platform/cloud-security/">www.crowdstrike.com/en-us/platform/cloud-security/</a> (Cloud security: alerts and posture)                                                      |
| 3. <a href="https://www.crowdstrike.com/en-us/press-releases/industry-leaders-crowdstri...">www.crowdstrike.com/en-us/press-releases/industry-leaders-crowdstri...</a> (Differences you notice day to day)             | 12. <a href="https://www.crowdstrike.com/en-us/products/faq/">www.crowdstrike.com/en-us/products/faq/</a> (Fast start with a software agent: your...)                                                                               | 22. <a href="https://crowdstrike.com/wp-content/uploads/2024/09/falcon-exposure-manageme...">crowdstrike.com/wp-content/uploads/2024/09/falcon-exposure-manageme...</a> (Prioritized security recommendations with an...) |
| 4. <a href="https://marketplace.crowdstrike.com/listings/corelight-ndr-for-falcon-next-...">marketplace.crowdstrike.com/listings/corelight-ndr-for-falcon-next-...</a> (Differences you notice day to day)             | 13. <a href="https://www.crowdstrike.com/tech-hub/endpoint-security/falcon-insight-xdr-w...">www.crowdstrike.com/tech-hub/endpoint-security/falcon-insight-xdr-w...</a> (Continuous monitoring and event correlation...)            | 23. <a href="https://crowdstrike.com/platform/exposure-management/risk-prioritization">crowdstrike.com/platform/exposure-management/risk-prioritization</a> (Priority for flaws already being...)                         |
| 5. <a href="https://www.crowdstrike.com/en-us/why-crowdstrike-compliance-ce...">www.crowdstrike.com/en-us/why-crowdstrike-compliance-ce...</a> (Differences you notice day to day)                                     | 14. <a href="https://www.crowdstrike.com/en-us/pricing/">www.crowdstrike.com/en-us/pricing/</a> (Advanced protection on every device (EDR/XDR)...) )                                                                                | 24. <a href="https://www.crowdstrike.com/en-us/blog/falcon-for-it-redefines-vulnerabilit...">www.crowdstrike.com/en-us/blog/falcon-for-it-redefines-vulnerabilit...</a> (Patch validation in a pilot group...)            |
| 6. <a href="https://www.crowdstrike.com/en-us/press-releases/crowdstrike-expands-europe...">www.crowdstrike.com/en-us/press-releases/crowdstrike-expands-europe...</a> (Differences you notice day to day)             | 15. <a href="https://www.crowdstrike.com/en-us/platform/falcon-secure-access/">www.crowdstrike.com/en-us/platform/falcon-secure-access/</a> (Web filtering on the device)                                                           | 25. <a href="https://crowdstrike.com/platform/exposure-management/easm">crowdstrike.com/platform/exposure-management/easm</a> (External attack surface: what your company exposes...)                                     |
| 7. <a href="https://www.crowdstrike.com/en-us/services/falcon-complete-next-gen-mdr/">www.crowdstrike.com/en-us/services/falcon-complete-next-gen-mdr/</a> (24/7 security operations center (SOC) with human analysts) | 16. <a href="https://www.crowdstrike.com/en-us/platform/threat-intelligence/">www.crowdstrike.com/en-us/platform/threat-intelligence/</a> (Documented investigations enriched...)                                                   | 26. <a href="https://www.crowdstrike.com/en-gb/services/prepare/penetration-testing-exer...">www.crowdstrike.com/en-gb/services/prepare/penetration-testing-exer...</a> (Annual penetration test (pentest))               |
| 8. <a href="https://www.crowdstrike.com/en-us/blog/inside-mitre-attack-evaluation-how-c-...">www.crowdstrike.com/en-us/blog/inside-mitre-attack-evaluation-how-c-...</a> (Human Gate: a person approves every...)      | 17. <a href="https://www.crowdstrike.com/en-us/platform/next-gen-siem/">www.crowdstrike.com/en-us/platform/next-gen-siem/</a> (Incident management with a case log and response time...)                                            | 27. <a href="https://www.crowdstrike.com/en-us/platform/falcon-for-it/">www.crowdstrike.com/en-us/platform/falcon-for-it/</a> (Remote monitoring and management (RMM))                                                    |
| 9. <a href="https://www.crowdstrike.com/en-us/platform/charlotte-ai/">www.crowdstrike.com/en-us/platform/charlotte-ai/</a> (AI investigation assistant in the portal that...)                                          | 18. <a href="https://www.crowdstrike.com/en-us/services/incident-response/">www.crowdstrike.com/en-us/services/incident-response/</a> (Incident response with root cause analysis)                                                  | 28. <a href="https://www.crowdstrike.com/en-us/resources/data-sheets/falcon-complete-for...">www.crowdstrike.com/en-us/resources/data-sheets/falcon-complete-for...</a> (Available under your IT provider's brand)        |
|                                                                                                                                                                                                                        | 19. <a href="https://www.crowdstrike.com/en-us/platform/identity-protection/">www.crowdstrike.com/en-us/platform/identity-protection/</a> (Identity posture: MFA, privileged accounts...)                                           |                                                                                                                                                                                                                           |

**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.](#)