

# SentinelOne Vigilance

24x7 MDR and DFIR Services

While the number of emergent threats grows exponentially in speed and scope, global organizations face a shortage of experienced cybersecurity professionals to mitigate their risk. As the threat landscape continues to evolve, security operation centers and enterprise security teams are turning to experienced threat services teams, backed by autonomous cybersecurity to accelerate their threat investigation and response capabilities.

SentinelOne Vigilance is a 24x7 Managed Detection and Response (MDR) service, designed to supplement our autonomous Singularity™ Platform.

Vigilance Respond enables security teams to offload threat investigation and response to a global team of SentinelOne cybersecurity experts, allowing your team to focus on more strategic initiatives. Security teams can also add Digital Forensics and Incident Response (DFIR) onto their standard MDR services with Vigilance Respond Pro.

✓ **Expert Staff**

Never Outsourced

✓ **Trusted**

By the World's Largest Organizations

✓ **Value**

MDR & DFIR Reduce SOC Workload

## On Average, Incidents are Resolved in 20 Minutes or Less

Vigilance achieves ground-breaking speed, powered by patented Storyline technology, prioritization tech, and a team of non-outsourced Tier 1, 2, and 3 analysts.

## Need More Info?

Platform: [s1.ai/platform](https://s1.ai/platform)


Vigilance: [s1.ai/services](https://s1.ai/services)


## Vigilance Respond


Vigilance Respond augments your security organization by giving them...

- + Time to focus on your business' needs with 24x7 monitoring.
- + Expertise with a team of elite breach responders and security researchers that act as an extension of your SO to review, act on, and document threats for you.
- + Peace of mind, by keeping your dashboards clean, and only escalating to you for urgent matters.


 24x7x365 Follow-the-Sun


 Triage & Event Prioritization

 Fewer Alerts, More Context

 Accelerated Threat Resolution

 Clean Dashboards

 Proactive Notifications

 Executive Reporting


 Emerging Threat Response


## Vigilance Respond Pro

Vigilance Respond Pro adds digital forensics and incident response onto your MDR, giving you all Vigilance Respond MDR features and...

- + Direct access to forensic experts for incident management, containment, and consultation.
- + Incident response retainer hours for malware analysis and Proactive Services for remaining retainer hours.


 2x Faster SLA


 Incident-Driven Threat Hunting

 Annual Retainer Hours

 Digital Forensics & Malware Reversing

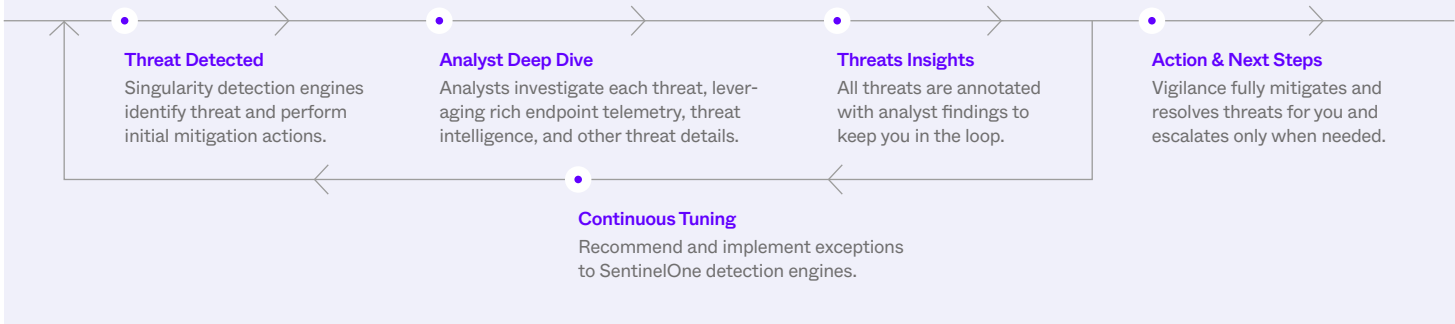
 IR Case Managers

 Containment & Eradication

 Root Cause Analysis

 Post Mortem Consultation

# How Vigilance MDR Works



	Respond	Respond Pro	What's Included
24x7 MDR	✓	✓	<ul style="list-style-type: none"> <li>Every console threat is reviewed, acted upon, and documented               <ul style="list-style-type: none"> <li>+ Full response capabilities</li> <li>+ Proactive notifications</li> </ul> </li> <li>Emerging threat response</li> </ul>
Watchtower	+	+	<ul style="list-style-type: none"> <li>Active campaign threat hunting for attacker techniques, global APT campaigns, and emerging cyber crimes</li> <li>Threat bulletins &amp; alerting if/when threats are detected in your environment</li> </ul>
Watchtower Pro	+	+	<ul style="list-style-type: none"> <li>Twice yearly deep-dive threat hunts and compromise assessments</li> <li>Unrestricted access to Signal Hunting Library that saves custom and pre-built hunting queries</li> </ul>
Threat Investigation	✓	✓	<ul style="list-style-type: none"> <li>Console indicator and dynamic analysis</li> </ul>
DFIR Investigation		✓	<ul style="list-style-type: none"> <li>RCA infection vector, exfil/breach determination, intel-driven hunting, threat intel enrichment &amp; contextualization, malware reversing, memory analysis and code extraction, malicious code deobfuscation</li> </ul>
IR Retainer		✓	<ul style="list-style-type: none"> <li>On-demand investigations</li> <li>Preset # of retainer hours (use or lose)</li> <li>Investigation → Active Containment → Eradication → Reporting</li> <li>Assigned IR case managers</li> <li>4-Hrs min charge per incident</li> </ul>
Response Readiness Review		✓	<ul style="list-style-type: none"> <li>Dynamic quarterly reporting for configuration hardening (agent health, policy and configuration, hardening recommendations)</li> <li>Threat/actor trends</li> </ul>

Legend: ✓ Included    + Add-on

**Gartner Peer Insights™**

“

Vigilance Respond has given our global organization much value, quickly.

**IT Security and Risk Management Role**  
SERVICES, 50M-250M USD

“

Excellent service, in terms of availability, detection, prevention capabilities, (and) SLA adherence.

**Infrastructure and Operations Role**  
MEDIA FIRM, 500M - 1B USD

**Vigilance Supports FedRAMP Moderate Organizations**

## Innovative. Trusted. Recognized.



A Leader in the 2023 Magic Quadrant for Endpoint Protection Platforms



Record Breaking ATT&CK Evaluation  
+ 100% Protection. 100% Detection  
+ Outstanding Analytic Coverage, 4 Years Running  
+ 100% Real-time with Zero Delays



96% of Gartner Peer Insights™ EDR Reviewers Recommend SentinelOne Singularity



### About SentinelOne

SentinelOne is the world's most advanced cybersecurity platform. The SentinelOne Singularity™ Platform detects, prevents, and responds to cyber-attacks at machine speed, empowering organizations to secure endpoints, cloud workloads, containers, identities, and mobile and network-connected devices with intelligence, speed, accuracy, and simplicity. Over 11,500 customers—including Fortune 10, Fortune 500, and Global 2000 companies, as well as prominent governments—all trust SentinelOne to Secure Tomorrow.

sentinelone.com  
sales@sentinelone.com  
+1 855 868 3733