

Vigilance Respond

SOC Augmentation MDR / Digital Forensics / Incident Response

SentinelOne's Vigilance Respond and Respond Pro Managed Detection & Response (MDR) service subscriptions are designed to supplement our endpoint security SaaS offerings.

The Vigilance MDR Team is the human side to our AI-based Singularity™ platform. We are a 100% in-house, non-outsourced Team of Tier-1, Tier-2, and Tier-3 cybersecurity experts monitoring millions of endpoints. Our mission is to augment customer security organizations. We provide a second set of eyes on the SentinelOne deployment and appropriate responses to contain threats. Vigilance Respond & Respond Pro empower customers to focus only on the incidents that matter making it the perfect endpoint add-on solution for overstretched IT/SOC Teams.



ON AVERAGE, INCIDENTS ARE RESOLVED IN 20 MINUTES OR LESS.

Vigilance MDR achieves ground breaking speed with AI-based Storyline automation and prioritization tech bolstered by multiple analyst tiers.



EXPERT STAFF
Never Outsourced



TRUSTED
By the World's
Largest Organizations



VALUE
MDR & DFIR Reduce
SOC Workload



WATCHTOWER
Includes Intel-Based
Threat Hunting

NEED MORE INFO?

Platform: s1.ai/platform
Vigilance: s1.ai/services

Vigilance Respond

Vigilance Respond MDR adds value by augmenting and reducing the load on security organizations.

- Clean dashboards and peace of mind
- Every threat is reviewed, acted upon, and documented to keep you in the loop
- Escalations to you for urgent matters only



24x7x365
Follow-the-Sun



Triage & Event
Prioritization



Fewer Alerts,
More Context



Accelerated Threat
Resolution



Clean
Dashboards



Proactive
Notifications



Executive
Reporting



Periodic
Cadence Calls

Vigilance Respond Pro

Vigilance Respond Pro builds on our Respond tier and adds Digital Forensics and Incident Response.

- All Respond MDR features plus...
- Direct access to forensic experts for incident management, containment, and consultation
- IR retainer hours for malware analysis and IR



2x Faster
SLA



Intel-driven
Hunting



Annual Retainer
Hours



Digital Forensics &
Malware Reversing



IR Case
Managers



Containment &
Eradication

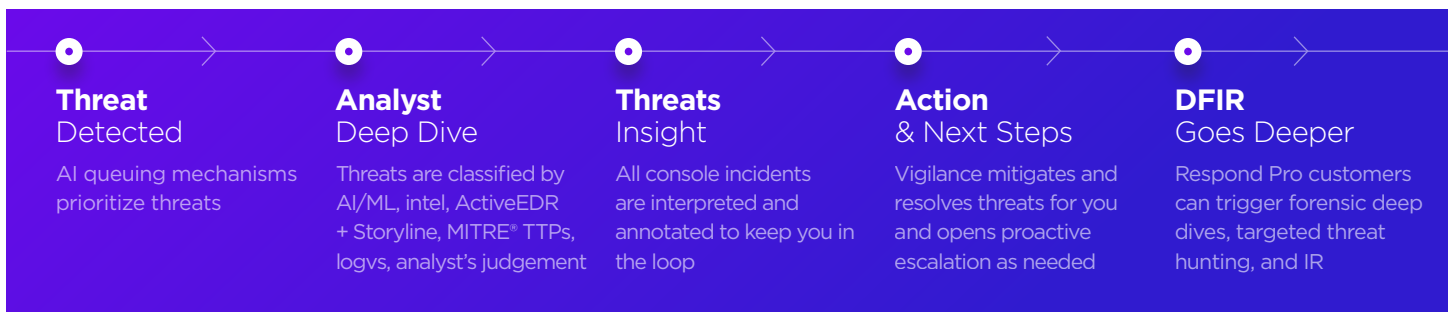


Root Cause
Analysis



Post Mortem
Consultation

How Vigilance MDR Works



	RESPOND	RESPOND PRO	WHAT'S INCLUDED?
24X7 MDR	✓	✓	<ul style="list-style-type: none"> Every console threat is, reviewed, acted upon, and documented Full response capabilities Proactive Notifications
WATCHTOWER	✓	✓	<ul style="list-style-type: none"> Intelligence-based hunting for attacker techniques, global APT campaigns, and emerging cyber crimes Threat bulletins & alerting if/when threats are detected in your environment
THREAT RESPONSE SLA	Standard 2-hour/4-hour own/investigate	Premium 1-hour/2-hour own/investigate	<ul style="list-style-type: none"> The fastest MDR on the planet Analyst triage, verdict, and initial actions
DIGITAL FORENSIC ANALYSIS	Triage	Full Investigation	<ul style="list-style-type: none"> Full Investigation: RCA infection vector, exfil/breach determination, intel-driven hunting, threat intel enrichment & contextualization, malware reversing, memory analysis and code extraction, malicious code deobfuscation Triage: Console indicator and dynamic analysis
IR RETAINER		✓	<ul style="list-style-type: none"> Preset # of retainer hours (use or lose) Investigation → Active Containment → Eradication → Reporting Assigned IR case managers 4-Hrs min charge per incident
QUARTERLY SECURITY REVIEW		✓	<ul style="list-style-type: none"> Consultation guiding long-term remediation and security architecture Agent version alignment & exclusions review Threat / actor trends



Fantastic experience from beginning to end



Security and Risk Management Role
Energy & Utilities, 500M - 1B USD



Very proactive, supportive and professional team



Infrastructure and Operations Role
Media Firm, 500M - 1B USD



Knowledgeable and highly responsive team



Security and Risk Management Role
Healthcare, 1B - 3B USD



Very useful add-on service



Security and Risk Management Role
Manufacturing, 1B - 3B USD

Innovative. Trusted. Recognized.



A Leader in the 2021 Magic Quadrant for Endpoint Protection Platforms

Highest Ranked in all Critical Capabilities Report Use Cases



Record Breaking ATT&CK Evaluation

- No missed detections. 100% visibility
- Most Analytic Detections 2 years running
- Zero Delays. Zero Config Changes



98% of Gartner Peer Insights™

Voice of the Customer Reviewers recommend SentinelOne



About SentinelOne

More Capability. Less Complexity. SentinelOne is pioneering the future of cybersecurity with autonomous, distributed endpoint intelligence aimed at simplifying the security stack without forgoing enterprise capabilities. Our technology is designed to scale people with automation and frictionless threat resolution. Are you ready?

sentinelone.com

sales@sentinelone.com
+1 855 868 3733