SentinelOne®

DATA SHEET

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(TM) 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

WATCHTOWER
Active Campaign Threat Hunting

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
Vigilance: 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

Fewer Alerts, More Context

Clean Dashboards

Executive Reporting

Triage & Event Prioritization

Accelerated Threat Resolution

Proactive Notifications

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

Annual Retainer Hours

IR Case Managers

Root Cause Analysis

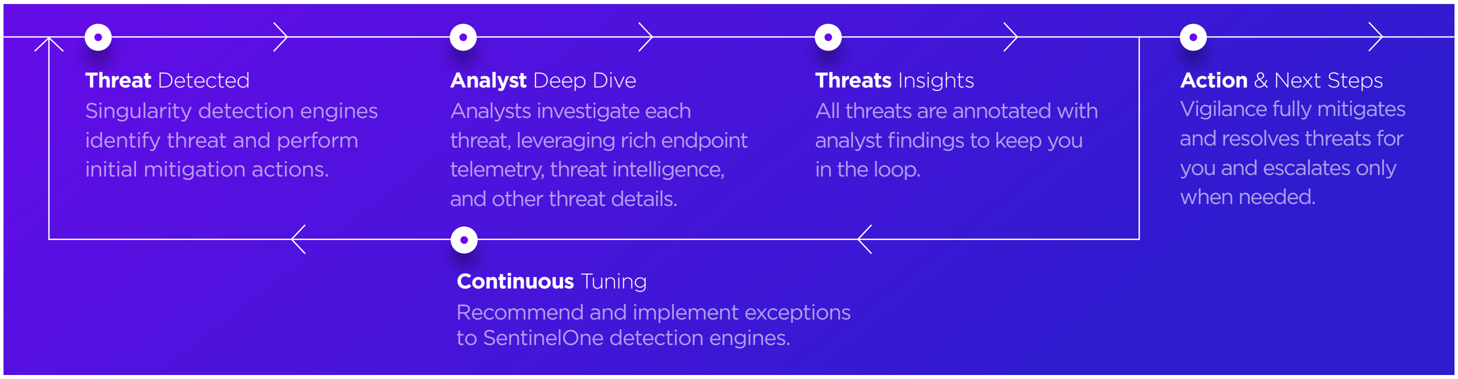
Incident-Driven Threat Hunting

Digital Forensics & Malware Reversing

Containment & Eradication

Post Mortem Consultation

How Vigilance MDR Works



Threat Detected
Singularity detection engines identify threat and perform initial mitigation actions.

Analyst Deep Dive
Analysts investigate each threat, leveraging rich endpoint telemetry, threat intelligence, and other threat details.

Threats Insights
All threats are annotated with analyst findings to keep you in the loop.

Action & Next Steps
Vigilance fully mitigates and resolves threats for you and escalates only when needed.

Continuous Tuning
Recommend and implement exceptions to SentinelOne detection engines.

	RESPOND	RESPOND PRO	WHAT'S INCLUDED
24X7 MDR	✓	✓	• Every console threat is, reviewed, acted upon, and documented • Full response capabilities • Proactive Notifications
WATCHTOWER	✓	✓	• Active campaign threat hunting for attacker techniques, global APT campaigns, and emerging cyber crimes • Threat bulletins & alerting if/when threats are detected in your environment
WATCHTOWER PRO	+	+	• Twice yearly deep-dive threat hunts and compromise assessments • Unrestricted access to Signal Hunting Library that saves custom and pre-built hunting queries
DIGITAL FORENSIC ANALYSIS	Triage	**Full Investigation**	• 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		✓	• Preset # of retainer hours (use or lose) • Investigation → Active Containment → Eradication → Reporting • Assigned IR case managers • 4-Hrs min charge per incident
SECURITY ASSESSMENT		✓	• Consultation guiding long-term remediation and security architecture • Agent version alignment & exclusions review • Threat / actor trends

Gartner Peer Insights

> “Vigilance Respond has given our global organization much value, quickly.
>
> ★★★★★
>
> **IT Security and Risk Management Role**
> Services, 50M-250M USD

Gartner Peer Insights

> “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

LEGEND ✓ Included + Add-on

Innovative. Trusted. Recognized.

Gartner

A Leader in the 2022 Magic Quadrant for Endpoint Protection Platforms

MITRE ENGENUITY

Record Breaking ATT&CK Evaluation

- 100% Protection. 100% Detection
- Top Analytic Coverage, 3 Years Running
- 100% Real-time with Zero Delays

Gartner Peer Insights

96% of Gartner Peer Insights™

EDR Reviewers Recommend SentinelOne Singularity

FedRAMP · TEVORA PCI DSS Attestation HIPAA Attestation · AICPA SOC · STAR LEVEL ONE · VB 100 VIRUS · SE Labs BEST Innovator WINNER 2021 · SE Labs AAA · Trusted Cloud Provider CSA

About SentinelOne

SentinelOne (NYSE:S) is pioneering autonomous cybersecurity to prevent, detect, and respond to cyber attacks at faster speed, greater scale and higher accuracy than human-powered technology alone. The Singularity Platform offers real-time visibility and intelligent AI-powered response. Achieve more capability with less complexity.

sentinelone.com

sales@sentinelone.com
+ 1 855 868 3733

© SentinelOne 2023