SentinelOne
The future of endpoint security

SentinelOne Vigilance

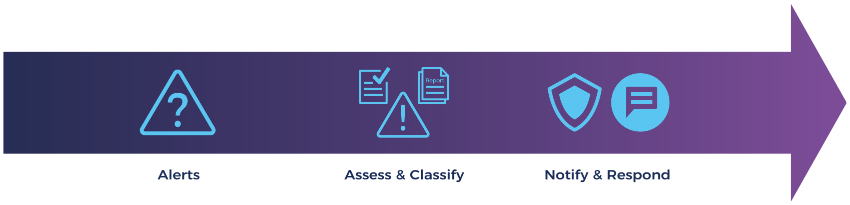
Security breaches are increasingly becoming commonplace and their impact echoes across industries. Today's attackers are adept at finding weaknesses in traditional security products—and finding ways to exploit them. Technologies adopted by organizations to safeguard assets generate thousands of alerts on a weekly basis, which increases staff workload, creates operational inefficiencies, and causes employee burnout. And with the rising shortage of trained security personnel[1], this also escalates the risk to your organization.

SentinelOne Vigilance

SentinelOne Vigilance provides a turnkey solution to augment your security and IT teams by accelerating the detection, prioritization, and response to advanced cyber threats and reducing your risk of missing a critical alert that goes undetected.

Vigilance Cyber Security Analysts assess the suspicious alerts, review raw data on threats, process operations, and network connections, analyze samples, as needed, correlate the information with threat intelligence feeds, analyze low level log-data, and collaborate with security researchers to identify and prioritize events. Vigilance security analysts will also notify security personnel and execute applicable policy-driven actions to limit the impact of any threat to your organization.

Figure 1: SentinelOne Vigilance Workflow



SentinelOne is recognized as a Visionary on the 2017 Gartner MQ for Endpoint Protection Platforms.

CYBER SentinelOne WARRANTY

SentinelOne covers customers up to $1,000/ endpoint (up to $1M total) to recover files in the event of an undetected ransomware attack.[2]

[1] http://www.csoonline.com/article/3177374/security/cybersecurity-skills-shortage-holding-steady.html
[2] Refer to SentinelOne Cyber Warranty for program details.

SentinelOne Vigilance can coexist with your Managed Security Service Provider (MSSP) to augment their efforts to secure your organization. In such deployments, the Vigilance service managers will work with the MSSP counterparts to operationalize the workflow from detection, response, and remediation.

Vigilance Capabilities & Benefits

Continuous supervision

24 x 7 follow-the-sun model to ensure always-on visibility, monitoring and analysis.

Stronger security

Deployment validation, alert monitoring, prioritization and response to reduce risk of security incidents.

Expedited response

Accelerated mitigation, quarantine and rollback to minimize threat impact.

Operational efficiency

False-positive reduction to reduce workflow overheads and enable security staff to focus on critical issues.

Threat insights

Threat summarization and insights on severity and impact to aid risk analysis and threat hunting.

Executive insights

Quarterly or monthly reporting to aid executives understand system risks and security.

Vigilance: Tiers of Service

	Active Monitoring	Active Response
ONBOARDING		
Onboarding & Setup	✓	✓
Coverage	24/7	24/7
DETECTION & RESPONSE		
Threat Classification	✓	✓
Alert Validation & Incident Prioritization	✓	✓
Customer Notification	Email, Console	Email, Console
Expert Consultation		✓
Threat Response		✓
FORENSICS & REPORTING		
Executive Reporting	Quarterly	Monthly
On-Demand Deep Sample Forensics		✓
Threat Hunting		✓

SentinelOne is a certified AV replacement for Windows and MacOS.

For more information about SentinelOne Next-Generation Endpoint Protection Platform and the future of endpoint protection,
please visit: sentinelone.com