RELIAQUEST

SOLUTION BRIEF

RELIAQUEST FOR SENTINELONE

SentinelOne is a leading Endpoint Detection and Response (EDR) technology that has a flexible cloud, on-premises, or hybrid model, depending on the customer's deployment preference. It offers the ability to deploy, scale, and upgrade its platform on a single agent. Though it is a foremost EDR solution and effective in protecting the endpoint, the product is sophisticated, and many find it challenging to keep it optimized for uninterrupted value. For one, the detection rules need to be curated and constantly updated in a changing and complex threat landscape. It requires dedicated support to ensure continued effectiveness and high fidelity. Additionally, since it is endpoint-focused, it does not provide a holistic view of threats across the enterprise.

ReliaQuest helps customers extend the power of SentinelOne by optimizing and continuously unifying its telemetry with other security technologies and unique log sources to accelerate threat detection, investigation, and response.

Drive Maximum Value from Your EDR Investments with ReliaQuest

SentinelOne requires a sophisticated skillset to manage. For it to be effective, teams must keep it operational and tuned for specific use cases and environments. Additionally, it is critical to continuously develop and deploy new detection rules to keep up with the dynamic threat landscape and IT environment.

ReliaQuest detection architects specialize in building detection content configured to the customer organization, tune existing ones and adding detected IOCs for highest fidelity. Using its cloud-native platform, GreyMatter, data from SentinelOne is unified with other sources such as SIEM, CASBs, threat intelligence and any other technologies to provide context and enrich investigations and drive fast response for proactive protection.

ReliaQuest continuously monitors tools under management to ensure events are received and parsed properly and system performance is within utilization ranges and responsiveness. Customers save time and maximize their investments with complete management of these tools, including software upgrades, performance tuning, and troubleshooting.

BENEFITS:

- Reduce noise and identify emerging threats with continuously built and optimized detection content
- Ensure optimal performance with managed integration and by continuously monitoring for health and system performance
- Drive faster insights by enhancing alerts with contextual telemetry from other security tools, log sources and threat intelligence
- Leverage early warnings from learnings from our global customer base to proactively protect your organization
- Enhance protection with automated response actions and controls validation

Key Capabilities

24/7/365 monitoring: Leveraging its cloud-native GreyMatter platform, ReliaQuest offers continuous monitorin g of SentinelOne tools for real-time situational awareness, improving alerts prioritization and support for higher-fidelity investigations.

Comprehensive threat protection and response: Leverage ReliaQuest MDR services and Open XDR technology to centralize alerts, reduce false positives, drive fast response, and stay ahead of evolving threats.

Continuous tuning and development of detection rules: Customize and automate detection rules specific to your environment with Storyline Active-Response (STAR), plus get continuous updates based on nonstop research and learning from across a growing customer environment.

Monitor for health and system performance: Detect and rectify any outages and degradations by continuously monitoring technology for optimal operations, responsiveness, and systems performance.

Save time with managed integrations: Keep your SentinelOne up to date and effective with timely patching, performance tuning, troubleshooting for any core components, software updates, and maintenance, including installation and testing of vendor product upgrades.

Lifecycle automation: Achieve faster time to value and higher adoption with a diverse set of customizable, automated actions.

MITRE ATT&CK framework mapping: Mappings to MITRE ATT&CK framework and Kill Chain stages help plot coverage and uncover areas for focus to improve security posture.

Industry peer benchmarking: Know how you are doing against your peers when it comes to visibility, team performance, and tool fidelity.

Customer success focus: Gain a dedicated customer success manager who gives you personalized attention, ensuring our services are curated to your needs and exceed your expectations

Sample Threat Types and Use Cases

SAMPLE THREAT TYPES	EXAMPLE USE CASES	
Execution: Detects techniques threat actors leverage to execute controlled code on a local or remote system.	• Named pipe creation • File encryption from unsigned process • Suspicious invocation of shell commands	• Removable drive followed by execution • Execution bypass via LOLBIN
Persistence: Detects techniques threat actors leverage to maintain access to systems across restarts, credential changes, etc.	• Kernel module modification • Cron job from a service account • PowerShell scheduled task creatio	
Privilege escalation: Detects techniques threat actors leverage to gain higher-privileged permissions on a system or network.	• Reconnaissance of SUID executables • SSP DLL injection	• Sudo file modification • Modification of Windows login screen
Defense evasion: Detects techniques threat actors leverage to avoid detection throughout their compromise.	• Nonstandard process executing Windows process • PowerShell execution policy modifications	• Shell history modification • Secure file deletion • Deletion of shadow copies
Credential access: Detects techniques threat actors leverage to steal credentials such as account names and passwords.	• Credential harvesting (access of files with credentials) • Allowing of credentials stored in plaintext	• Credential dumping (e.g., Mimikatz/LSASS)