SentinelOne

SOLUTION BRIEF

Threat-Centric Endpoint Protection, Investigation and Response

SentinelOne & ThreatQuotient Joint Solution Brief

Market Challenges

With an ever-evolving threat landscape, security teams often lack a clear understanding of how to operationalize threat intelligence and proactively secure their endpoints. Large enterprises need to navigate the explosion of threat data and noise to better understand which attacks are relevant to their environment, quickly detect attack behavior, and better defend their network.

Organizations now, more than ever, need contextualized threat data from internal and external sources to allow for automation and extended protection to their endpoints and cloud workloads.

Joint Solution

SentinelOne and ThreatQuotient unite to make threat intelligence prioritized and actionable, giving security teams greater context when performing endpoint investigations. The API-enabled integration between SentinelOne and ThreatQuotient provides security teams the upper hand when preventing, detecting, and responding to endpoint threat activity.

SentinelOne ingests prioritized threat intelligence from ThreatQuotient data collections into blocklists, which improve defenses by preventing known malicious indicators of compromise from executing across the entire endpoint fleet. Vulnerabilities identified by SentinelOne are sent to ThreatQuotient to track and aggregate potential exploits.

SentinelOne incidents triaged within ThreatQuotient are automatically enriched with context about the campaign's motivation, attackers, and intent. While an analyst investigation is taking place, affected SentinelOne endpoints can be quarantined from ThreatQuotient to stem further infection. Analysts can quickly pivot from an endpoint investigation in ThreatQuotient to a Deep Visibility threat hunt to look for additional indicators or affected endpoints. When an incident is confirmed, mitigation can be triggered from ThreatQuotient to automatically remediate or roll back the affected endpoints.

How It Works

The integration between SentinelOne and ThreatQuotient consists of three components within the ThreatQuotient solution:

The **SentinelOne Custom Connector for ThreatQ** enables the automatic blocking of indicators from a data collection.

The **SentinelOne Operation for ThreatQ** enables endpoint triage actions to be executed directly from ThreatQ to mitigate and respond to threats.

THREATQUOTIENT™

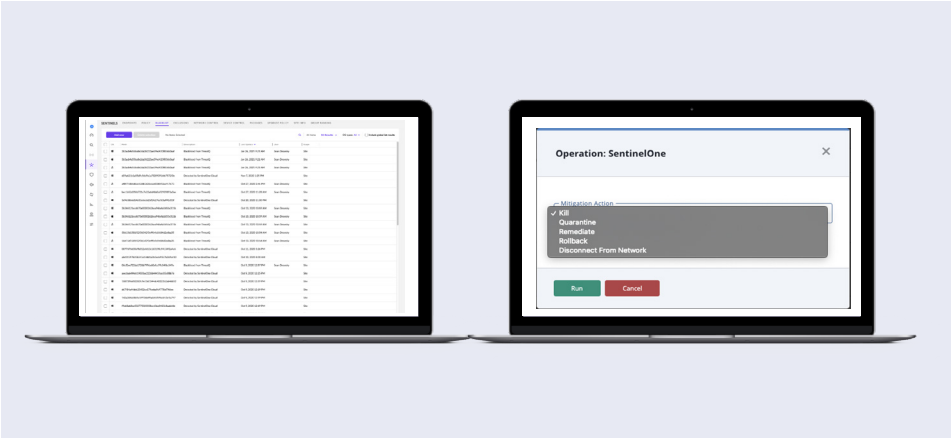
JOINT SOLUTION HIGHLIGHTS

+ Infuse endpoint protection with contextualized, prioritized threat intelligence
+ Triage and respond to endpoint threats with adversary context
+ One-click pivot from attack indicators to Deep Visibility threat hunting

INTEGRATION BENEFITS

- **Improve Defenses**
- **Accelerate Response**
- **Informed Threat Hunting**

The **SentinelOne CDF for ThreatQ** enables application vulnerabilities to be automatically ingested into ThreatQ for tracking and reporting.



Use Cases

01 | Threat-Centric Operations

Provide an intelligence-driven, customer-specific threat dataset that can be used to detect, track and prevent as required across company assets.

02 | Incident response

Respond to endpoint security alerts with speed and accuracy.

03 | Automation

Automatically contextualize, prioritize, and disseminate threat intelligence to SentinelOne to block threats before they can cause damage.

Conclusion/Summary

The joint solution of SentinelOne and ThreatQuotient is a potent combination that provides the intelligence and automation to improve defenses, reduce mean-time-to-respond (MTTR) and accelerate threat hunting activities across endpoints and cloud workloads.

JOINT SOLUTION BENEFITS

Improve Defenses

Infuse endpoint prevention with contextualized, prioritized threat intelligence

Accelerate Response

Triage and respond to endpoint threats with adversary context

Informed Threat Hunting

One-click pivot from attack indicators to Deep Visibility hunting

READY FOR A DEMO?

Visit the SentinelOne website for more details.

SentinelOne is a Customer First Company

Continual measurement and improvement drives us to exceed customer expectations.

Gartner peerinsights customers' choice

97% Of Gartner Peer Insights™ 'Voice of the Customer' Reviewers recommend SentinelOne

97% Customer Satisfaction (CSAT)

FedRAMP | ISO 27001 CERTIFIED by schellman | EU GDPR COMPLIANT | AAA | TEVORA PCI DSS Attestation HIPAA Attestation | Gartner peerinsights 4.9

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?

About ThreatQuotient

ThreatQuotient's mission is to improve the efficiency and effectiveness of security operations through a threat-centric platform. By integrating an organization's existing processes and technologies into a single security architecture, ThreatQuotient accelerates and simplifies investigations and collaboration within and across teams and tools. Through automation, prioritization and visualization, ThreatQuotient's solutions reduce noise and highlight top priority threats to provide greater focus and decision support for limited resources. For more information, visit www.threatquotient.com..

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