SOLUTION BRIEF

McAfee
Together is power.

ThreatQuotient and McAfee Enterprise Security Manager Integration

Prioritize threat intelligence to accelerate security operations

The ThreatQuotient and McAfee® Enterprise Security Manager joint solution provides integrated workflows that optimize time and the user experience for intelligence and security analysts. With this integration, you can aggregate, prioritize, and act upon the most relevant threats facing an organization.

McAfee Compatible Solution

- ThreatQ and McAfee Enterprise Security Manager

McAfee COMPATIBLE

THREATQUOTIENT

Connect With Us

The Business Problem

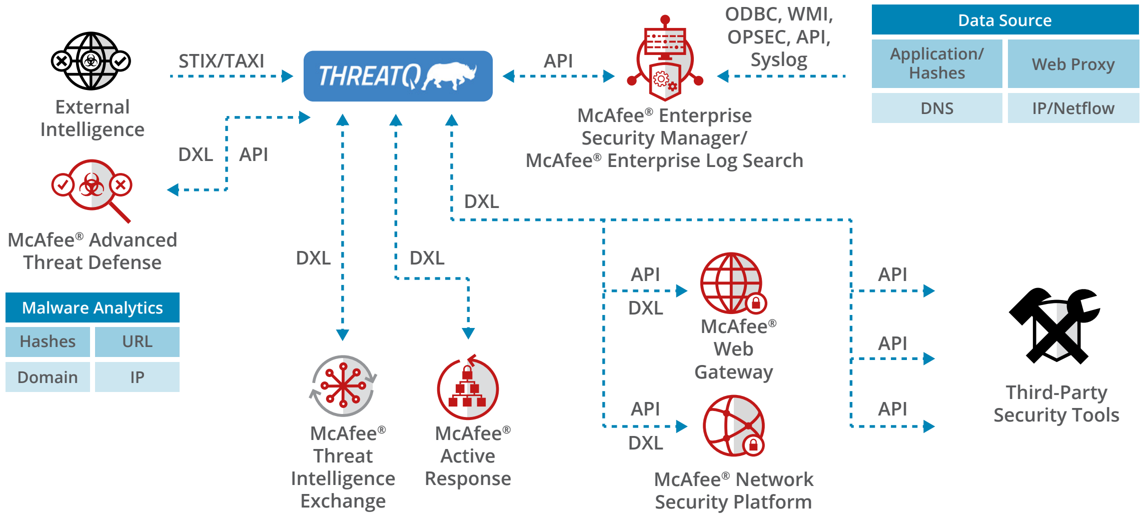
Security operators struggle with managing, prioritizing, and acting on the threat data available to them both internally and externally. Once prioritized threat intelligence is produced, there is the additional hurdle of rapidly publishing it to the security operators' tools, such as security information and event management (SIEM) solutions. Lastly, there is the final challenge of reporting any resulting SIEM sightings on indicators back to the intelligence team and their tool set for additional awareness.

McAfee and ThreatQuotient Joint Solution

The integration of McAfee Enterprise Security Manager and ThreatQuotient helps organizations accelerate detection and response. You can reduce noise and minimize false positives by quickly identifying relevant threat data. ThreatQuotient provides a bi-directional integration with McAfee Enterprise Security Manager to add contextual threat intelligence to the Threat Library.

Features and Benefits

- Accelerate event triage by providing a searchable and single source of threat knowledge.
- Automatically consume sightings in ThreatQuotient to deliver customer-specific scoring, allowing for the identification of relevant threats.
- Understand the details and context behind indicators and their associated events.
- Enable analysts to make better, more informed decisions by providing context and situational understanding of threats.
- Deliver qualified and contextual threat data to automate searching for relevant threats in McAfee Enterprise Security Manager.


External Intelligence
STIX/TAXI
THREATQ
API
McAfee® Enterprise Security Manager/ McAfee® Enterprise Log Search
ODBC, WMI, OPSEC, API, Syslog
DXL
API
McAfee® Advanced Threat Defense
DXL
DXL
DXL
McAfee® Threat Intelligence Exchange
McAfee® Active Response
API
DXL
McAfee® Web Gateway
API
DXL
McAfee® Network Security Platform
API
API
API
Third-Party Security Tools

Data Source	
Application/ Hashes	Web Proxy
DNS	IP/Netflow

Malware Analytics	
Hashes	URL
Domain	IP

Figure 1. The power of McAfee and ThreatQuotient.

McAfee and ThreatQuotient Use Cases

ThreatQuotient's integration with McAfee Enterprise Security Manager allows the threat intelligence team to publish relevant, targeted indicators to multiple McAfee Enterprise Security Manager instances. Each McAfee Enterprise Security Manager instance will then have curated watchlists based on the latest expertise of the threat intelligence team.

In the event an item on a watchlist, such as an IP address or a file hash is seen by McAfee Enterprise Security Manager, an alarm will be generated and an event created in the ThreatQuotient Threat Library. The event in the Threat Library will include important context, such as any additional and relevant indicators.

The additional context McAfee Enterprise Security Manager returns can be used in the ThreatQuotient customizable scoring policy. The threat intelligence team is therefore able to automatically re-evaluate the relevance of certain features to the organization based on external reports and internal sightings.

Additionally, ThreatQuotient is able to use the backtrace functionality provided in McAfee Enterprise Security Manager. This capability enables the analyst in ThreatQuotient to look back over the events that have occurred in a given time period (user-definable) to identify any matches that may have been missed or previously unknown.

ThreatQuotient brings in threat data from many different sources (ISACs, open source, DHS-AIS, and others). After threat data is deduplicated and scored, high-relevance indicators are sent to McAfee Enterprise Security Manager watchlists. The integration is bidirectional, meaning that a sighting by McAfee Enterprise Security Manager will be reflected in the threat library as an additional source. The score is then edged higher, and the indicator is pushed to the infrastructure products, like McAfee Endpoint Security or McAfee Active Response, to automatically block this particular indicator.

An analyst can pivot on the indicator within ThreatQuotient and correlate it to a particular adversary. The scoring algorithm is adjusted to automatically increase the score of any indicator associated with this adversary. Based on the new scoring policy, the system recalculates all the indicators associated with that adversary and, as a result, new indicators exceed the threshold for export and are sent to McAfee Enterprise Security Manager and other enforcement infrastructure for blocking.

About ThreatQuotient

ThreatQuotient understands that the foundation of intelligence-drive security is people. The company's open and extensible threat intelligence platform, ThreatQ, and cybersecurity situation room solution, ThreatQ Investigations, empower security teams with the context, customization, and prioritization needed to make better decisions, accelerate detection, and response and advance team collaboration. Leading global companies use ThreatQuotient solutions as the cornerstone of their security operations and threat management system. ThreatQuotient is headquartered in Northern Virginia with international operations based in Europe and Asia-Pacific. For more information, visit **threatquotient.com**.

About McAfee Enterprise Security Manager

McAfee Enterprise Security Manager—the foundation of the SIEM solution family from McAfee—delivers the performance, actionable intelligence, and real-time situational awareness at the speed and scale required for security organizations to identify, understand, and respond to stealthy threats, while the embedded compliance framework simplifies compliance.

Learn More

For more information, contact your McAfee representative or channel partner, or visit **www.mcafee.com**.

McAfee™
Together is power.

2821 Mission College Blvd.
Santa Clara, CA 95054
888.847.8766
www.mcafee.com