SOLUTION BRIEF

ThreatQuotient and McAfee Advanced Threat Defense Integration

Prioritize threat intelligence to accelerate security operations

The ThreatQuotient and McAfee® Advanced Threat Defense joint solution allows users to submit files for analysis and to store resulting data in the ThreatQuotient Library. With this integration, customers can aggregate, prioritize, and act upon the most relevant threats facing their organization.

McAfee Compatible Solution

- ThreatQ and McAfee Advanced Threat Defense

Connect With Us

The Business Problem

The volume of available threat data has increased dramatically over the last decade, making it challenging for security professionals to separate relevant data from the noise. Mature security organizations are racing to develop tools, teams, and processes to turn threat data into timely and useful threat intelligence. Once this is accomplished, the intelligence must be distributed to existing security tools across networks that may be isolated from one another, and the intelligence team must get feedback from internal sightings.

Through their McAfee® Security Innovation Alliance partnership, McAfee and ThreatQuotient have developed integrations and use cases that help solve these problems.

McAfee and ThreatQuotient Joint Solution

ThreatQuotient's integration with McAfee Advanced Threat Defense provides analysts with tools that enable them to easily send malware or URLs for detonation. The resulting threat data set will immediately be added to the Threat Library, where it is evaluated or reevaluated for relevance. From there, actionable intelligence is distributed to other McAfee products, such as McAfee® Enterprise Security Manager and McAfee® Threat Intelligence Exchange. This seamless workflow allows a security team to move from sample research to analysis and enforcement, all manageable from within a single-pane-of-glass console.

Features and Benefits

- Provide feed of analysis results from McAfee Advanced Threat Defense.
- ThreatQ Operation enables user to submit files to McAfee Advanced Threat Defense for analysis.
- Enables analysts to make better, more informed decisions by providing context and situational understanding of threats.

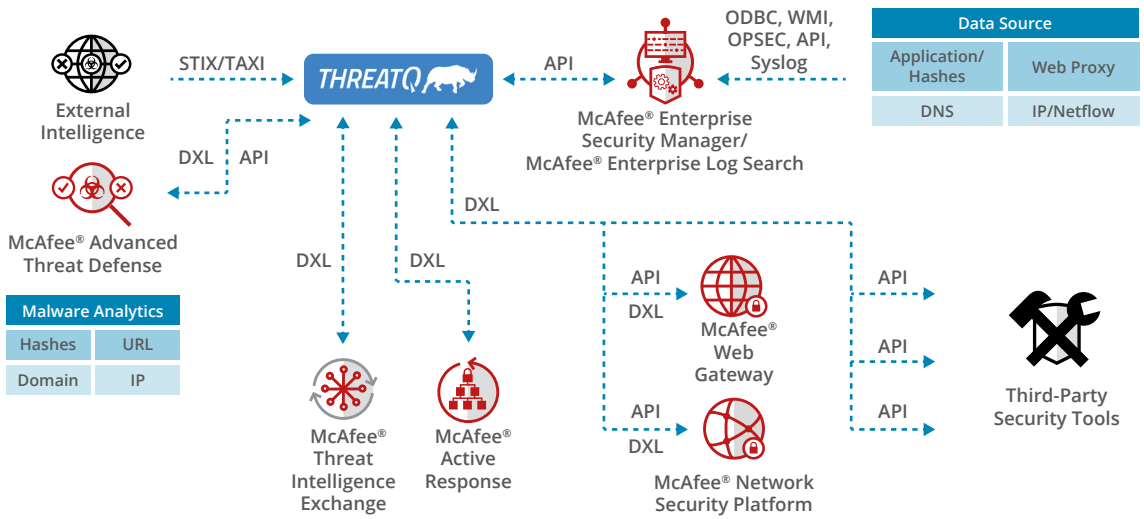

Figure 1. The power of McAfee and ThreatQuotient.

McAfee and ThreatQuotient Use Cases

McAfee Advanced Threat Defense publishes analysis results onto the Data Exchange Layer (DXL) messaging fabric. ThreatQuotient captures any new messages and creates an event within the Threat Library. Threat data that is associated with the ThreatQuotient event is then scored and sent to infrastructure products in a mixed vendor environment.

The analysis report and (optionally) malware samples are also captured and related to the relevant pieces of threat data within the Threat Library. This information may be used to offer analyst and incident responses additional contextually relevant data from within the ThreatQuotient graphic user interface.

ThreatQuotient receives sample malware from an external feed source. Users may then leverage a ThreatQuotient operation to send files and URLs to McAfee Advanced Threat Defense for evaluation and detection. All results are published back onto the DXL messaging fabric and made visible to all technologies that have subscribed to the McAfee Advanced Threat Defense DXL topic. This includes passing data that scores above a user-defined threshold back to ThreatQuotient.

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 Advanced Threat Defense

McAfee Advanced Threat Defense enables organizations to detect advanced, evasive malware and convert threat information into immediate action and protection. Unlike traditional sandboxes, it includes additional inspection capabilities that broaden detection and expose evasive threats. Tight integration between security solutions—from network and endpoint to investigation—enables instant sharing of threat information across the environment, enhancing protection and investigation. Flexible deployment options support every network.

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