THREATQUOTIENT™

McAfee™

THREATQ™ AND MCAFEE®

ThreatQ's integration with McAfee Active Response (MAR) enables security operations teams to accelerate investigations into potential threats and malicious activity.

The ThreatQ integration with McAfee Active Response allows analysts to query for malicious activity across the endpoints in their environment based on the intelligence in their Threat Library™.

THREATQ BY THREATQUOTIENT™

ThreatQuotient's solutions make security operations more efficient and effective. The ThreatQ open and extensible platform integrates disparate security technologies into a single security infrastructure, automating actions and workflows so that tools and people can work in unison. Empowered with continuous prioritization based on their organization's unique risk profile, security teams can focus resources on the most relevant threats, and collaboratively investigate and respond with the aim of taking the right actions faster.

MCAFEE ACTIVE RESPONSE

Security-conscious entities today face a threat landscape that is changing at a dramatic pace. Attacks are created and propagated at ever faster rates. "Designer" attacks target individual organizations by using focused knowledge to improve their effectiveness and minimize detection. Attackers are more frequently penetrating preventive technologies. Forward-looking organizations are demanding easy-to-use, integrated tools that help better detect attackers' presence and then allow rapid investigation and remediation. The best detection and response solutions increase security efficiency even as they capture increasingly more information from a growing number of systems. By providing superior out-of-the-box capabilities, automated interaction with existing security management solutions, and user-customization, McAfee Active Response greatly narrows the window of opportunity for attackers to damage your computing assets and corporate brand.

INTEGRATION HIGHLIGHTS

Query environment-wide endpoints that have had a MAR agent installed to see if a file has been deployed on that endpoint and capture its current status.

Capture any netflow information for a source or destination IP address supplied by ThreatQ by querying environment-wide endpoints with MAR agents.

INTEGRATION USE CASE

ThreatQ brings in threat data from many different sources (ISACs, open source, DHS-AIS, etc.). This threat data is deduplicated and scored in the system and considered relevant enough to send to infrastructure products, like McAfee Endpoint Security or McAfee Active Response (MAR), to hunt and determine whether that indicator has been found on the customer network.
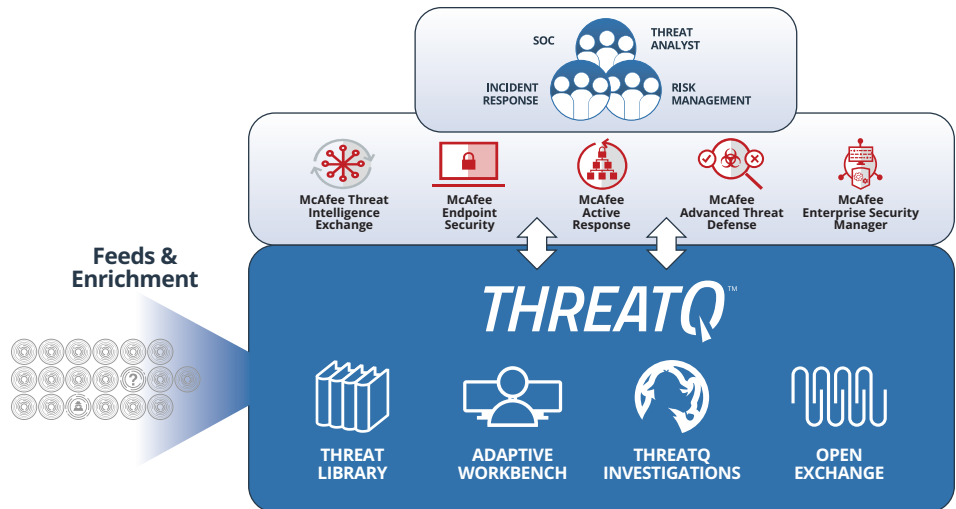
OPEN EXCHANGE ARCHITECTURE

ThreatQ's Open Exchange™ provides an extensible and flexible environment for analysts to achieve the optimal balance between system automation and expert analysis. Because no single security solution provides a silver bullet against attacks, ThreatQ's Open Exchange architecture supports standard interfaces for ingestion and exporting, including STIX/TAXII, XML, JSON, PDF, email and other formats of structured and unstructured data, along with an SDK and APIs for custom connections.
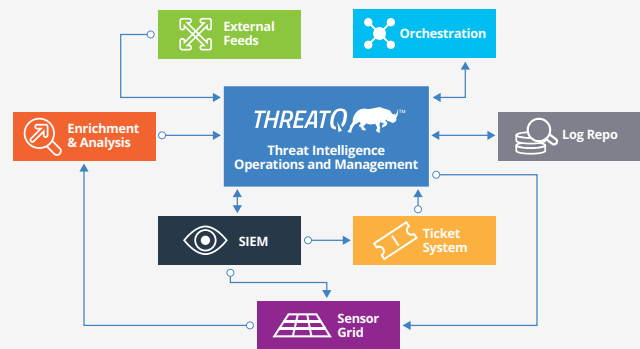
ABOUT THREATQUOTIENT™

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. ThreatQuotient is headquartered in Northern Virginia with international operations based out of Europe and APAC.

For additional information, please visit threatquotient.com.

ABOUT MCAFEE®

McAfee is the device-to-cloud cybersecurity company. Inspired by the power of working together, McAfee creates business and consumer solutions that make our world a safer place.

McAfee technologies' features and benefits depend on system configuration and may require enabled hardware, software, or service activation. No computer system can be absolutely secure. McAfee® and the McAfee logo are trademarks of McAfee, LLC or its subsidiaries in the United States and other countries. Other marks and brands may be claimed as the property of others.

For more information, visit www.mcafee.com.

TQ_ThreatQ-McAfee-MAR-Solution-Overview_Rev1