FIREEYE™

SOLUTION BRIEF

Intelligence-Based Enhancement of Email Security

A collaboration between ThreatQ and FireEye Email Security

INTEGRATION HIGHLIGHTS

- Offers comprehensive email security against malicious attachments, phishing URLs, supply chain impersonation, zero-day and multi-stage attacks
- Extensively examines email for threats hidden in password protected files, encrypted attachments, and URLs
- Acquires real-time threat intelligence from the FireEye DTI Cloud
- Prioritizes and contains threats by providing insights for alerts
- Deploys on-premises or virtual via AWS

By combining FireEye Email Security–Server Edition (EX series) with the ThreatQ platform, organizations can minimize the risk of costly breaches caused by advanced email attacks. Deployed on premises or virtually on AWS, FireEye Email Security leads the industry in identifying, isolating and immediately stopping advanced email attacks before they enter an organization's environment.

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.

FireEye Email Security—Server Edition Overview

Email is the most vulnerable vector for cyber attacks because it is the highest volume data ingress point. Organizations face an ever-increasing number of security challenges from email-based advanced threats. Most advanced threats use email to deliver URLs linked to credential phishing sites and weaponized file attachments. Because it is highly targetable and customizable, email is the primary medium for cyber crime.

THREATQUOTIENT

Email Security combines intelligence-led context and detection plug-ins to unearth malicious and benign phishing URLs on a big data, scalable platform. The signatureless Multi-Vector Virtual Execution™ (MVX) engine analyzes email attachments and URLs linked to downloadable content against a comprehensive cross-matrix of operating systems, applications and web browsers. FireEye collects extensive threat intelligence on adversaries through firsthand breach investigations and millions of sensors. Email Security draws on both concrete evidence and contextual intelligence about attacks and attackers to prioritize alerts and block threats in real time. This includes:

- Credential phishing and impersonation email—also known as business email compromise (BEC)
- More than 140 attachment types
- Password-protected and encrypted attachments
- Password-protected attachments with password sent via image, URLs embedded in emails, docs, zip files, etc.
- Files downloaded through URLs and FTP links
- Obfuscated, spoofed, shortened and dynamically redirected URLs
- Credential-phishing and typosquatting URLs

Integration Use Cases

- **Yara Rules Enable Customization:** Email Security enables analysts to specify and test custom rules to analyze email attachments for threats targeting their organization.
- **Data Enrichment:** Using these YARA rules, analysts are able to correlate information from other ThreatQ sources to malicious email attachments such as active campaigns.
- **Gain Context:** Build out investigations into specific email campaigns through the use of ThreatQ Investigations.

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 , APAC and MENA. For more information, visit **www.threatquotient.com**.

To learn more about FireEye Email Security, visit:
www.FireEye.com/products/email-security.html

FireEye, Inc.
601 McCarthy Blvd. Milpitas, CA 95035
408.321.6300/877.FIREEYE (347.3393)
info@FireEye.com

About FireEye

FireEye is the intelligence-led security company. Working as a seamless, scalable extension of customer security operations, FireEye offers a single platform that blends innovative security technologies, nation-state grade threat intelligence, and world-renowned Mandiant® consulting. With this approach, FireEye eliminates the complexity and burden of cyber security for organizations struggling to prepare for, prevent and respond to cyber attacks.

FIREEYE™