Joint Solution Brief
Real-Time Threat Protection with Enhanced Traffic Visibility

The Challenge
Advanced persistent threats (APT) easily evade traditional security models and tools. Detecting multi-stage attacks that move laterally through the data center requires a pervasive, flexible and scalable security architecture. Adversaries will get into the network; the challenge is to detect, mitigate and stop their threat as soon as possible.

Integrated Solution

Joint Solution Benefits
• Scalable threat protection: Distributes traffic from multiple network links across multiple FireEye appliances. Network upgrades don’t require tool upgrades.
• Comprehensive, adaptable traffic visibility: Helps ensure all physical, virtual and cloud network traffic is available to the FireEye appliances for swift analysis and action.
• Protect against network outages: Inline bypass protection maintains traffic continuity and minimizes maintenance windows.
• Decrypt SSL traffic once and send to multiple FireEye appliances for inspection and analysis.

Introduction
The next generation of cyber attacks has changed radically from previous approaches. Targeted to get something valuable — sensitive or personal information, intellectual property, authentication credentials or insider information — the attacks can combine social engineering with multi-pronged technical approaches that individually are hard to detect, but together can be devastating. Each attack is multi-staged with steps to get in, to call back from the compromised network, to spread laterally, and to get valuables out. It is not enough to simply put up a firewall or intrusion prevention system to stop these attacks at the perimeter because legacy solutions often cannot spot or stop advanced persistent threat (APT) attacks.

There is no single, static, technical answer. A fast, robust and adaptable solution is needed. A solution that has comprehensive visibility across the network traffic; that can go from alert to fix in minutes and then scale service up or down as threats and needs evolve. The right solution is deployed wherever it is required, inline or out-of-band. It needs to have comprehensive visibility across the network to all traffic to protect valuable assets, keep malware away and help ensure security tools are used to their full potential.

By being vigilant and catching an incident early, security teams can reduce the overall impact — costly fixes, disrupted business, stolen information and damaged reputations.

The Gigamon and FireEye Joint Solution
FireEye Network Security combined with the GigaSECURE® Security Delivery Platform offers customers flexible deployment options and scalability for optimal threat protection. With network-side visibility and options for both inline and out-of-band deployments, APTs can be spotted and contained quickly and efficiently.

FireEye and Gigamon have collaborated to offer customers the most flexible solution coupled with robust performance. The combination of FireEye Network Security and the Gigamon GigaSECURE Security Delivery Platform architecture helps ensure traffic is analyzed and threats are detected in real time, allowing administrators to quarantine or delete harmful data before it damages their business operations. By tapping into the key points of the network the GigaSECURE Security Delivery Platform efficiently delivers traffic to FireEye Network Security Appliances, providing the visibility those devices need to do their job and allowing them maximum performance by ensuring duplicate and unnecessary traffic is filtered out before being sent for analysis.

Joint Solution Benefits
• The GigaSECURE Security Delivery Platform provides visibility from physical, virtual and cloud environments to FireEye Network Security appliances for inspection.
Joint Solution Brief: Real-Time Threat Protection with Enhanced Traffic Visibility

Figure 1: Gigamon GigaSECURE Security Delivery Platform and FireEye Network Security Joint Solution

Figure 2: Scaling Threat Prevention Tools with GigaSECURE

- Move FireEye Network Security appliances between out-of-band and inline modes with a single software command and without re-cabling, reducing change orders, network outages and deployment time.
- Deploy FireEye Network Security appliances inline using the GigaSECURE Security Delivery Platform Inline Bypass functionality to provide physical bypass traffic protection in the event of power loss and logical bypass traffic protection in the event of an inline tool failure.
- Decrypt SSL traffic for inspection, helping to expose malware hiding in SSL sessions.

Signatureless, High-Accuracy Attack Detection with Low False Positive Rates
Purpose built for security, the FireEye MVX engine detects multiple attack types:
- Known and unknown
- Multiflow and multistage
- Alarms that matter with low false positive rates

Learn More
For more information on the FireEye and Gigamon solution, contact:

www.fireeye.com  www.gigamon.com