FireEye and Gigamon®

Real-Time Threat Protection with Enhanced Traffic Visibility

SOLUTION BRIEF

INTEGRATED SOLUTION HIGHLIGHTS

- **Offers scalable threat protection:** Distributes traffic from multiple 1G/10G/40G/100G networks across several FireEye platforms.
- **Provides comprehensive, adaptable traffic visibility:** Ensure all physical and virtual network traffic is available to FireEye platform for swift analysis and action.
- **Inspects encrypted traffic:** Decrypt SSL traffic for out-of-band inspection and analysis.
- **Protects against network outages:** Inline bypass protection maintains traffic continuity and minimizes maintenance windows.

OVERVIEW

The next generation of cyber attacks has changed radically and are targeted to get something valuable—sensitive, personal information, intellectual property, authentication credentials, and insider information. 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 because legacy solutions cannot stop advanced persistent threat (APT) attacks. There is no single, static, technical answer.

A fast, robust, and adaptable solution is needed. This solution must have 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 needs to be deployed wherever it is required inline or out-of-band. 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 CHALLENGE

Advanced persistent threats (APTs) easily evade traditional and legacy security models and tools. Multi-stage attacks that move laterally through the data center require a pervasive, flexible, and scalable architecture. Adversaries will get into the network. The challenge is to detect, mitigate, and stop their threat.

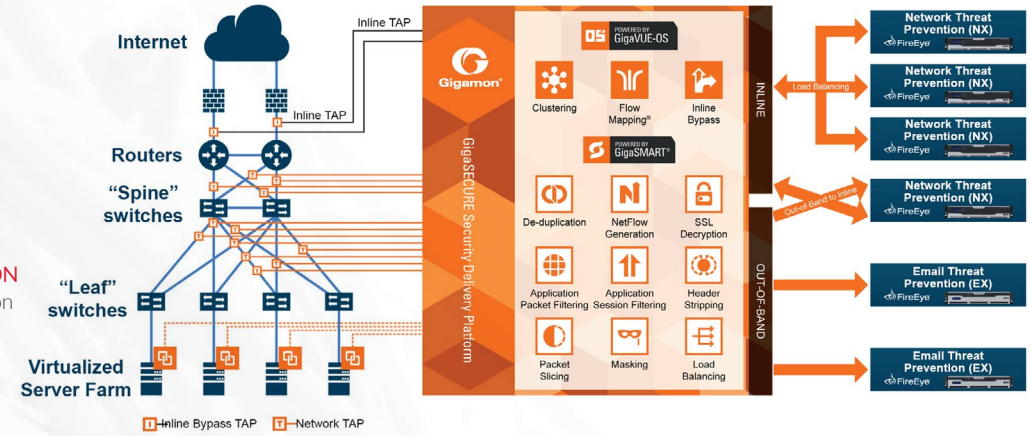
The dilemma for data center security managers is finding solutions that leverage the capabilities of other security products rather than having multiple, isolated products whose functionality operates in a silo and limit their deployment flexibility. In other words, achieving integration among deployed security products is a challenge that security managers must address.

A robust solution needs to have comprehensive visibility across the network to all traffic to protect valuable assets, keep malware away, and ensure security tools are used to their full potential. The right solution needs the flexibility to deploy wherever it is required in-line or out-of-band. The FireEye and Gigamon joint solution offers customers flexible deployment options and scalability up to 100 GB of traffic throughput for optimal threat protection.

THE INTEGRATED SOLUTION

The FireEye Network Threat Prevention Platform (NX Series) and FireEye Email Threat Prevention Platform (EX Series) combined with the GigaSECURE Security Delivery Platform offer 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 contained quickly and efficiently.

FireEye and Gigamon have collaborated to offer customers one of the most flexible deployment options coupled with robust performance. The combination of the FireEye platform and the Gigamon Visibility Fabric™ architecture ensures traffic is analyzed, and threats are detected in real time, allowing administrators to quarantine or delete harmful data before it gets inside the network.



FIREEYE PRODUCT AND VERSION

FireEye Network Threat Prevention Platform (NX Series) 7.5 and later versions

FireEye Email Threat Prevention Platform (EX Series) 7.6 and later versions

GIGAMON® PRODUCT

GigaSECURE® Security Delivery Platform

FireEye and Gigamon have collaborated to offer customers one of the most flexible deployment options coupled with robust performance. The combination of the FireEye platform and the Gigamon Visibility Fabric™ architecture ensures traffic is analyzed and threats are detected in real time, allowing administrators to quarantine or delete harmful data before it gets inside the network.

HOW THE JOINT SOLUTION WORKS TOGETHER

The joint solution supports two models of deployment for flexibility and adaptability:

Out-of-band Deployment

- Utilizes GigaSECURE Security Delivery Platform to aggregate and forward specific traffic flows at line rate without data loss.
- Extends visibility and malware detection from network edge to core including East-West traffic between virtual machines.
- Distributes the flows across multiple FireEye Network Threat Prevention Platform (NX Series) and FireEye Email Threat Prevention Platform (EX Series), allowing FireEye to scale as network speeds increase.
- Decrypts SSL traffic for inspection, preventing malware from hiding in SSL sessions.

Inline Deployment

- Bypass protection in both hardware and software ensures network integrity.
- GigaSECURE distributes live production traffic to multiple inline FireEye Network Threat Prevention Platform (NX Series) and FireEye Email Threat Prevention Platform (EX Series) platforms.
- FireEye platforms in active mode take action (quarantine, block, etc.).
- Switches between out-of-band and inline deployments with a single software command and without recabling.

THE VALUE OF THIS PARTNERSHIP

- **Lower total cost of ownership:** Ensures optimal performance and longevity of devices through load balancing across multiple FireEye devices, link consolidation, and filtering.
- **Reduced noise:** Filtering out traffic that doesn't need inspection provides greater efficiency from your FireEye appliances.
- **Avoid SPAN port contention:** Gigamon can replicate a feed from the SPAN port or a tap to multiple tools while also filtering feeds to just relevant traffic for that tool.

ABOUT FIREEYE

FireEye protects the most valuable assets in the world from today's cyber attackers. Our combination of technology, intelligence, and expertise — reinforced with an aggressive incident response team — helps eliminate the impact of breaches. The FireEye Global Defense Community includes 3,700 customers across 67 countries, including 675 of the Forbes Global 2000.

ABOUT GIGAMON

Gigamon provides the GigaSECURE Security Delivery Platform to enable the management of increasingly complex networks. Gigamon technology empowers infrastructure architects, managers and operators with pervasive visibility and control of traffic across both physical and virtual environments without affecting the performance or stability of the production network.

For more information contact CSC@fireeye.com.

FireEye, Inc. | 1440 McCarthy Blvd. Milpitas, CA 95035 | 408.321.6300 | 877.FIREEYE (347.3393) | info@fireeye.com | **www.fireeye.com**