SOLUTION BRIEF

Real-time Threat Protection with Enhanced Traffic Visibility

A joint solution by Gigamon® and FireEye

INTEGRATED SOLUTION HIGHLIGHTS

- **Offers scalable threat protection:** Distributes traffic from multiple 1G/10G/40G/100G networks across several FireEye platforms.
  - Deploy FireEye in high capacity networks, like 100Gbps Networks. FireEye devices can be kept in-line with greater traffic volumes.
  - Increase efficiency and resiliency through load balancing traffic for inspection to and across multiple FireEye appliances
  - Easily move FireEye devices from detection to prevention modes (and vice-versa)
- **Provides comprehensive, adaptable traffic visibility:** Ensure all physical and virtual network traffic is available to FireEye platform for swift analysis and action.
  - Resolve asymmetric routing issues.
  - Full visibility enables FireEye appliances and SmartVision to see all north-south and east-west traffic.
  - Send copies of inline traffic to out-of-band FireEye devices
  - Provides data masking and splicing capabilities
- **Inspects encrypted traffic:** Selectively decrypt SSL traffic for out-of-band inspection and analysis.
  - Helps ensure that decrypted traffic can be forwarded to appropriate FireEye appliances to expose possible hidden threats with the Gigamon inline SSL solution.
- **Protects against network outages:** Inline bypass protection maintains traffic continuity and minimizes maintenance windows.
  - Reduce the need for network outages if moving FireEye appliances out of line or taking it down for upgrades and planned/unplanned maintenance.

Overview

New and expanding cyber attacks target valuable assets: sensitive personal information, intellectual property, authentication credentials and insider information. These multi-stage attacks breach systems, spread laterally through networks, call back to attackers, and extract high-value data.

Firewalls and intrusion prevention systems cannot stop these advanced persistent threat (APT) attacks.

An ideal solution needs comprehensive visibility across network traffic with the ability to go from alert to fix in minutes and scale service up or down as threats and needs evolve. The right solution needs to be deployed as needed, either inline or out-of-band. With increased vigilance and early detection, security teams can reduce breach impacts, which include costly fixes, disrupted business, stolen information and damaged reputations.

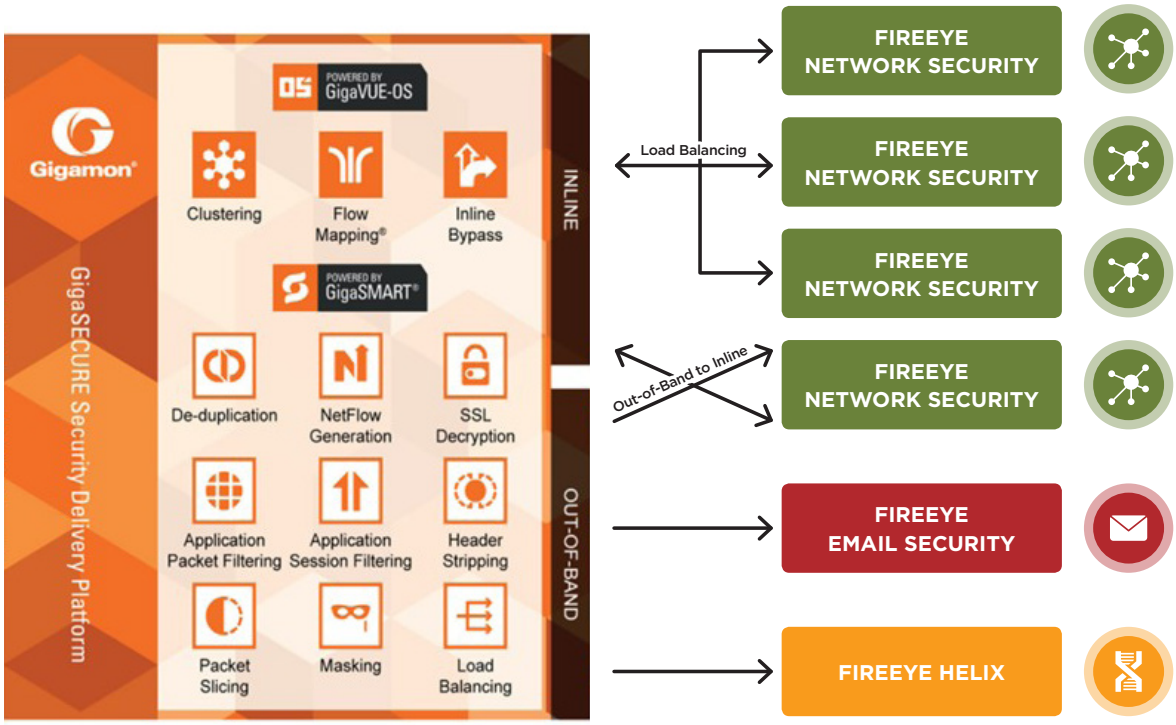
The Challenge

Advanced persistent threats (APTs) easily evade common security approaches. Multi-stage attacks that move laterally through the data center require a pervasive, flexible and scalable architecture.

To deal with advanced attacks, data center security managers often have multiple security products that work in isolation with limited deployment flexibility. Achieving integration among deployed security products is a significant challenge.

The ideal solution would have comprehensive visibility across all network traffic to protect valuable assets, block malware, and realize the full potential of existing security tools. It would also have the flexibility to deploy in-line or out-of-band, as a situation demands.

Figure 1. Gigamon® and FireEye joint solution.



The integrated solution

FireEye Network Security and FireEye Network Forensics 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.

The joint solution approach offers customers a more flexible deployment option with scalability up to 100 GB of traffic throughput for optimal threat protection. The combination of the FireEye platform and the Gigamon Visibility Fabric™ architecture ensures that traffic is efficiently 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 utilizing FireEye SmartVision.
- Distributes the flows across multiple FireEye Network Security (NX Series), FireEye Network Forensics (PX Series) and FireEye Email Security (EX Series) appliances, 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 Security and FireEye Network Forensics deployments, whether physical, cloud or hybrid
- 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 re-cabling.

Improved Production Network Reliability

- Taking FireEye devices offline does not cause link failures.
- FireEye devices can be moved inline or out-of-band without network outage.
- Patches to FireEye devices can be applied immediately without having to schedule an outage.

Improved Security Reliability

- Traffic can be distributed across multiple FireEye devices, sharing the load and increasing resilience.
- Heartbeat and link failure detection allow for redistribution of traffic to remaining active load balanced FireEye devices.
- FireEye devices can be kept inline with greater traffic volumes in high capacity networks.
- Inline SSL solution helps ensure decrypted traffic can be forwarded to FireEye appliances to expose possible hidden threats.

Greater Tool Efficiency

- GigaSECURE simplifies the incorporation of expanded traffic for FireEye SmartVision from north-south to include east-west traffic.
- Irrelevant traffic can be diverted around FireEye devices avoiding overload.
- FireEye device capacity can be matched to volume of traffic to be inspected not network interface speed.
- Ensure traffic flows in and out of the same FireEye devices, eliminating asymmetric routing issues.

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 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.

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 **GigamonPartner@Fireeye.com**

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

Gigamon®

FireEye®