JOINT SOLUTION BRIEF

Optimizing Security Operations With the Right Network Data

The Challenge

To protect against advanced threats, organizations need to integrate their security and apply the right expertise and processes. They need easy and complete access to the data flowing into and through their enterprise infrastructure and they need to be able to inspect, correlate, analyze and react to it rapidly.

The Solution

FireEye Helix is a cloud-hosted security operations platform that allows organizations to take control of any incident from alert to fix. It integrates disparate security tools and augments them with next generation SIEM, orchestration, and threat intelligence capabilities to capture the untapped potential of security investments.

Gigamon Application Metadata is deployed as part of the Gigamon platform and gives Helix users unique access to exactly the application specific data they require. Provided as metadata, this insight provides Helix the raw material for a host of extremely valuable security investigation and operational use-cases.

Joint Solution Benefits

- Helix acts as mission control for the Security operations center (SOC)
- Quickly identify breaches, vulnerabilities and potential misconfigurations
- No need to deploy stand-alone probes or collectors for network data
- Pre-built Helix rules provide workflows for standard security processes

Introduction

Today's enterprises realize that simply adding more technology and tools to their security infrastructure rarely yields the improved security posture they are seeking. To protect against advanced threats, organizations need to integrate their security and apply the right expertise and processes. FireEye Helix is a cloud-hosted security operations platform that allows organizations to take control of any incident from alert to fix. In order to do this, FireEye Helix integrates many disparate security tools and augments them with next generation SIEM, orchestration, and threat intelligence capabilities to capture the untapped potential of security investments.

To be effective as a security operations and response platform, FireEye Helix needs clear visibility into what is happening on all parts of the network as well as a clear understanding of the environment that organization is operating within. It needs to be able to use that information in conjunction with all the other contextual data is has to help determine what risks need investigation and how best to respond to them.

The Gigamon and FireEye Helix Joint Solution

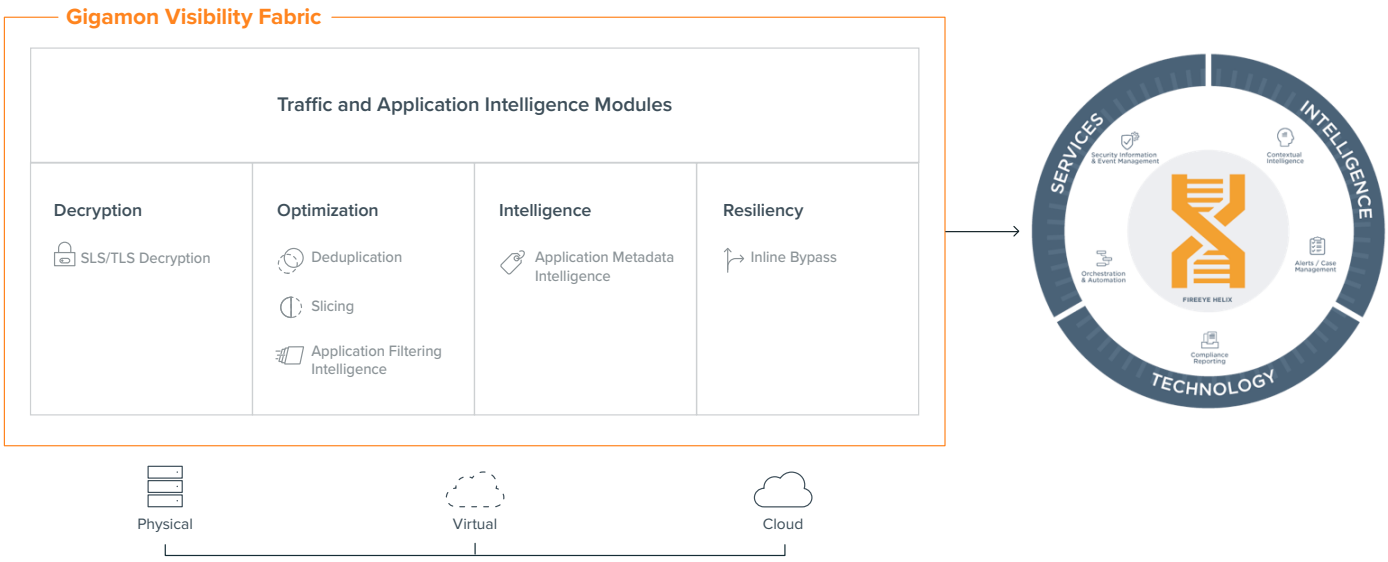
As two of the leaders in protecting our customer's businesses through efficient network security, Gigamon and FireEye have many shared customers using a variety of different product integrations to strengthen their security posture. With the release of Application Metadata Intelligence from Gigamon, FireEye Helix customers can now take advantage of rich, application specific metadata, made available within Helix, without the need to deploy and manage specific sensor devices or probes across their network. The Gigamon platform can be configured to inspect all traffic flowing across the network, capturing specific metadata attributes that feed a variety of security operations and threat hunting use-cases that can be run directly from the Helix platform.

Network Data Visibility is Essential

While server and other end-point logs will tell you what happened on the network, as long as bad actors haven't had the chance to modify those logs, information gathered directly from live traffic flowing over the network can tell you immediately what is happening right now. Of course, collecting and storing every packet can quickly become prohibitively challenging, both operationally and cost-wise. The answer is to selectively identify data attributes that can provide specific insights into known risks on the network, or can validate that specific protections are operating as desired, and collect that data in the form of metadata. The Gigamon platform does this and then sends that data to FireEye Helix where it can be utilized for stand-alone use-cases and combined with data from other sources for greater contextual awareness.

Example Use-Cases Enabled by This Solution:

- Analysis of HTTP User-Agent for malware and anomalies
- Detection of DNS traffic on non-standard ports
- Identification of vulnerable software
- Creation of an inventory of devices
- Identification of expired TLS certificates
- Validation of firewall rules changes are effective
- Identification of loose firewall rules based on network traffic and determination of possible routes for data exfiltration
- Identification of data exfiltration
- Identification of DNS tunneling from severs and endpoints not providing a DNS service



About FireEye, Inc.

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 has over 8,200 customers across 103 countries, including more than 50 percent of the Forbes Global 2000.

About Gigamon

Gigamon delivers network visibility and analytics for digital applications and services across physical, virtual and cloud infrastructure enabling organizations to run fast, stay secure and innovate. Only Gigamon offers a full-stack solution with a common architecture across an organization's complex hybrid infrastructure to address performance and security needs. Since 2004, Gigamon has been awarded over 75 technology patents and enjoys industry-leading customer satisfaction with more than 3,000 organizations, including over 80 percent of the Fortune 100 and the majority of the world's Top 10 banks, healthcare providers, technology companies, mobile operators and government agencies. Headquartered in Silicon Valley, Gigamon operates globally. For the full story on how Gigamon can help your organization, please visit www.gigamon.com.

For more information on Gigamon and FireEye Helix, visit:
www.gigamon.com and www.fireeye.com

Gigamon®
Worldwide Headquarters
3300 Olcott Street, Santa Clara, CA 95054 USA
+1 (408) 831-4000 | www.gigamon.com