BUSINESS BRIEF

# Reduce the Cost of Cybersecurity Tools

Rising network traffic forces enterprises to add and upgrade their security tools. This drives up hardware and software budgets and also makes the cybersecurity infrastructure more complex and costly to manage. Then network traffic surges again and spending rises even higher. Is there any way to break this cycle?

A 2016 Total Economic Impact™ commissioned study conducted by Forrester Consulting on behalf of Gigamon estimated that by adopting the Gigamon Security Delivery Platform, a composite organization of 5,000 employees could save $1.1 million on security hardware and software and an additional $1.5 million on staffing over three years.[1]

The Gigamon Delivery Platform enables enterprises to get much better performance out of existing security devices and services. It offloads processor-intensive tasks and dramatically reduces the load on each device through traffic filtering, load balancing and de-duplication. It also improves security by providing better visibility into network traffic across the enterprise.

## Delivering Network Traffic to Every Security Tool While Offloading Processor-Intensive Tasks

Security tools such as firewalls, intrusion detection systems, antimalware and data leak protection each provide unique security capabilities. Unfortunately, they can also duplicate tasks. For example, many inline tools may decrypt and re-encrypt the same network traffic and multiple security tools might use processing power to extract metadata from the same stream of packets.

Some of these tasks are extremely processor intensive. One study of eight leading next-generation firewalls found that scanning SSL traffic degraded the performance of the firewalls by as much as 80 percent and reduced transactions per second by as much as 92 percent.[2]

A security delivery platform acquires network traffic from networks and devices throughout the enterprise, and then delivers that traffic to all of the organization's security tools. In between, it can perform tasks such as SSL decryption and metadata generation once, offloading these processor-intensive tasks from the individual security and network devices. This "perform once, share everywhere" capability frees up large amounts of capacity. With the Gigamon Security Delivery Platform, enterprises don't need to add and upgrade security tools every time network traffic expands.

## Using Traffic Intelligence to Send Security Tools Exactly the Information They Need – and No More

According to one forecast, IP video traffic will increase from 73 percent of all consumer internet traffic in 2016 to 82 percent in 2021.[3] Except for specialized products, most security tools can't interpret streaming video — or large image files, or VoiP, or teleconferences.

The Gigamon Security Delivery Platform uses traffic intelligence to distribute the right network traffic — and no more — to each security tool. Packets containing voice traffic and video streams can be routed only to tools that process voice and video. Application session filtering can be configured to send traffic containing emails only to email security tools. De-duplication can strip out redundant network packets, so tools don't waste cycles inspecting the same traffic twice. These capabilities allow the organization's existing tools to process far greater volumes of network traffic.

## Balancing Workloads to Eliminate Wasted Capacity and Reduce Upgrades

Most security tools and network devices are attached to one network segment. Their capacity can't be pooled or shared when traffic patterns change. As a result, expanding a network link often requires a so-called forklift upgrade to a more expensive security tool. In addition, every tool must be sized based on peak loads, even if most capacity is wasted during much of the day.

This issue becomes even more serious when enterprises move toward micro-segmentation. Adding devices to dozens of new network segments not only drives up hardware costs, it also requires new administrators.

[1]The Total Economic Impact™ of Gigamon, a commissioned study conducted by Forrester Consulting on behalf of Gigamon, April 2016.
[2]NSS Labs: SSL Performance Problems.
[3]Cisco Visual Networking Index: Forecast and Methodology, 2016–2021

The Gigamon Security Delivery Platform can load balance network traffic flows to security tools across the enterprise. If a network link is expanded, it is not necessary to forklift out the existing tools; old and new tools can share the load together. If a tool in one location is underused, it can offload traffic from another location that is overwhelmed. If the enterprise moves to micro-segmentation, a few large tools can scan the traffic from many network segments.

## Reducing Complexity to Lower Management Costs

Fewer security tools result in a less complex security infrastructure, which is easier to manage. That not only frees expensive network and security administrators for other tasks, it also reduces the chance of configuration errors and other mistakes that can undermine security.

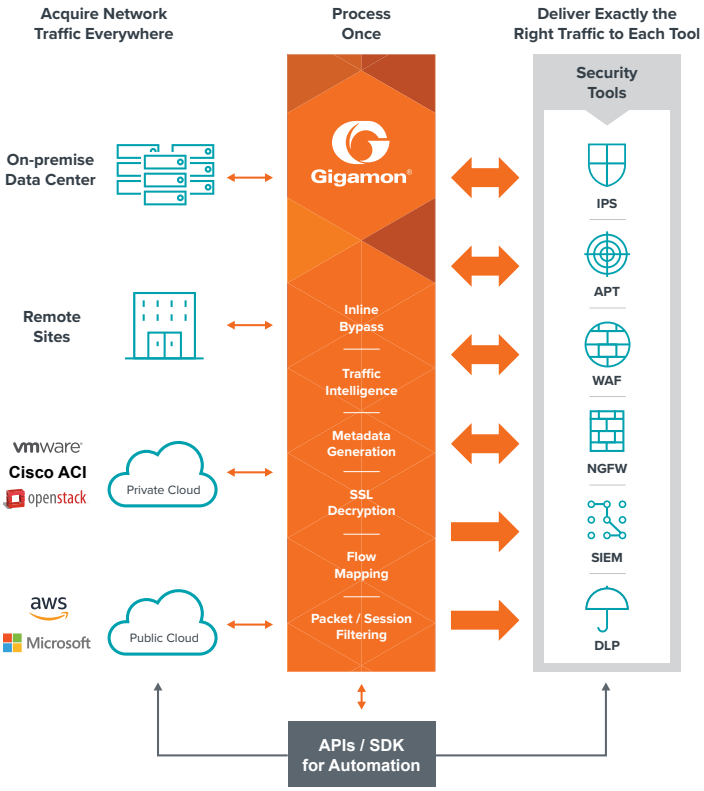
The impact of the Gigamon Security Delivery Platform can be dramatic. A Gigamon customer interviewed by Forrester Consulting estimated that his company would require four times as many appliances if it didn't have Gigamon technology, as cited in the commissioned study The Total Economic Impact of Gigamon: Cost Savings and Business Benefits, April 2016. As the study also indicated, the savings for even a medium-sized organization can add up to millions of dollars of hardware, software and administrative costs.

To find out how the Gigamon Security Delivery Platform can help you improve security and reduce costs, visit: www.gigamon.com.

## The Gigamon Security Delivery Platform

As illustrated in the diagram, the Gigamon Security Delivery Platform:

- Provides simplified access to network traffic across an enterprise
- Delivers selected traffic of interest required by individual security tools, both inline and out of band
- Offloads processor-intensive tasks such as SSL decryption and de-duplication from individual tools
- Uses traffic intelligence to optimize network traffic or extract metadata from network traffic and deliver to the appropriate security tool
- Provides a programmatic interface for integration with the security and infrastructure stack, enabling dynamic responses to infrastructure changes, events and other early indicators of compromise




The Gigamon Security Delivery Platform is a next-generation network packet broker purpose-built for security tools to work more efficiently across physical, virtual and cloud environments. For inline threat prevention tools, it strengthens security postures, simplifies IT and reduces costs. It also provides pervasive visibility into all the activity inside the perimeter of an enterprise so that all security tools can quickly detect, analyze and block cyberattacks. It eliminates partial visibility and blind spots by acquiring network traffic from anywhere in the enterprise and applying traffic intelligence before delivering precise data to specific security tools in and across the organization.



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