Business Brief

Increase the Effectiveness of Existing Cybersecurity Tools

Enterprises have invested a fortune in cybersecurity tools developed by some of the best minds in technology. Yet more than five million data records are lost or stolen every day.[1]

The problem is not that today's cybersecurity tools are badly designed or missing features. It's not that IT organizations are lazy or apathetic about security. On the contrary. Most often the problem is that surging volumes of network traffic overwhelm security tools, causing administrators to use sampling or disable advanced features in order to preserve application performance. Another common problem is that security tools and IT staff don't get all the data they need to detect and respond to outside attacks and insider incidents, because they are faced with "blind spots" in data collection.

To solve these problems without buying more security tools or adding staff, Gigamon offers the GigaSECURE® Security Delivery Platform, a next-generation network packet broker purpose-built for security. The GigaSECURE Security Delivery Platform makes existing security tools more effective by preventing them from being overwhelmed by network traffic and by providing pervasive visibility into data in motion.

Use Traffic Intelligence and Load Balancing to Keep Performance High

When traffic volume climbs, administrators often turn off SSL decryption, deep packet inspection and other important security features. They do this to prevent devices from becoming bottlenecks that choke off network and application performance.

GigaSECURE Security Delivery Platform uses Traffic Intelligence to filter out unnecessary traffic to each security tool, for example routing traffic containing emails only to email security products and packets containing video streams only to tools designed to inspect video. GigaSECURE Security Delivery Platform also provides dynamic load balancing, which optimizes the use of capacity across multiple devices. Administrators can keep security tools at full effectiveness without degrading network performance.

Decrypt Once, Share with All Tools

According to the Electronic Frontier Foundation, more than half of web traffic is encrypted by HTTPS and other variants of SSL.[2] Yet some security tools can't decrypt SSL traffic. Other tools find decryption so "expensive" that administrators choose to let SSL traffic enter the organization uninspected.[3] These limitations allow hackers to conceal malware and command and control communications in encrypted traffic, knowing that they probably won't be detected.

GigaSECURE Security Delivery Platform very efficiently decrypts and re-encrypts SSL traffic as needed, no matter where it enters the enterprise.[4] The decrypted traffic is provided for inspection to all the required security tools in the enterprise and then re-encrypted for inline prevention tools such as intrusion prevention systems (IPS). Malware and command-and-control traffic can no longer use SSL encryption to hide from security tools.

Eliminate Network Blind Spots

Most security tools only have access to data in motion that traverses the network segment where they are located. This makes it extremely difficult to correlate all the data needed to identify advanced attacks. Perimeter security tools are particularly handicapped, because they have little visibility into "East-West" traffic within a data center and traffic between application services running on virtual machines.

GigaSECURE Security Delivery Platform provides "pervasive visibility" by acquiring network traffic moving between conventional servers, virtual machines in virtualized server farms and network devices such as switches and routers, and delivering

[1] Breach Level Index, January 2018

[2] We're Halfway to Encrypting the Entire Web.

[3] A study by NSS Labs of eight leading next-generation firewalls found that scanning SSL traffic degraded the performance of the firewalls by as much as 80 percent.

[4] Data such as personally identifiable information (PII) can remain encrypted or be masked to meet regulatory requirements.

that traffic to all the organization's security tools. Security information and event management systems (SIEMs) and security analytics tools get visibility into all the indicators of advanced attacks anywhere on the network. Products such as anti-malware tools, firewalls, intrusion detection systems and data leak protection tools obtain all the data they need to detect malware, spot lateral movement and communications from outside attackers and track suspicious actions by rogue insiders.

Simplify Management to Reduce Errors

As networks grow and become more segmented, most enterprises are compelled to buy more security devices. Not only is this expensive, it makes the security infrastructure more complex and harder to manage. Complexity leads to more errors and makes it harder to capture and analyze data from across the enterprise.

But GigaSECURE Security Delivery Platform allows organizations to protect themselves with as few as one-quarter of the security tools that would otherwise be needed.[5] It accomplishes this by techniques such as offloading processor-intensive tasks, filtering traffic to each tool and load balancing traffic across tools.

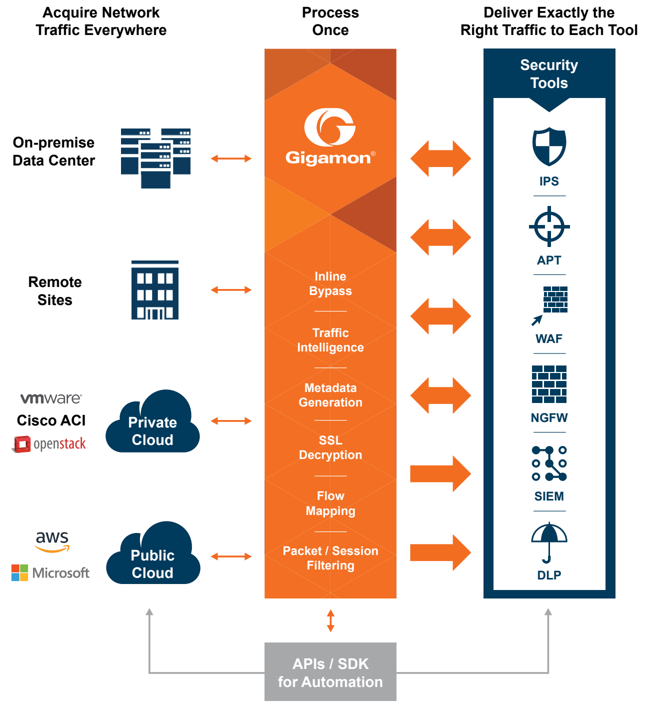
Fewer tools mean less complexity and easier management, leading to more accurate configurations, more reliable updates, better collection of security data and other improvements that increase the effectiveness of existing security tools.

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

The GigaSECURE Security Delivery Platform

As illustrated in the diagram, the GigaSECURE 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 response to infrastructure changes, events and other early indicators of compromise.



The GigaSECURE 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

[5] A Gigamon customer interviewed by industry analysts from Forrester, Inc. estimated that his company would require four times as many appliances if it didn't have Gigamon technology. Cited in the study The Total Economic Impact™ of Gigamon: Cost Savings and Business Benefits.