Whitepaper

Security at the Speed of Your Network

Introduction

As the volume and speed of network data increases, security tools are unable to keep up, resulting in security tool sprawl, performance degradation, inefficiencies and unnecessary expenditures. All of this leads to increased time to threat detection and response and a higher risk of a breach – despite massive spending on security tools.

The solution is to build an efficient network security architecture that copes with increasing network speeds today and in the future, improving the return on investment of security tools while reducing complexity, cost and tool overload across physical, virtual or cloud infrastructure. This is accomplished by using the architectural approach of a next-generation network packet broker designed for security to enable the deployment of a diverse set of security solutions as a centralized security tool farm – significantly reducing associated overhead, complexity and costs.

This white paper will examine the security issues introduced by more data over faster networks, how an architectural approach can solve those challenges and introduces the GigaSECURE® Security Delivery Platform, the leading next-generation network packet broker purpose-built for security tools to work more efficiently across physical, virtual and cloud environments. In fact, IHS Markit[1] has named Gigamon the market leader and the best-known vendor in the space with #1 market share in multiple industries – 36% overall and 59% in the government sector.

The Cost of More Data at Higher Speeds

As data in motion across on-premises and cloud environments continues to grow, organizations are responding by upgrading to higher-speed networks including running at 40Gb and 100Gb. While this helps scale their operations to meet market demand, there are some costly side effects to examine:

1. Worrisome Security Gaps

The growing volume of data on faster networks is surpassing the capacity and performance of monitoring and security tools, creating a major gap between the data flowing through an organization and the ability of security tools to process that data in a given time. For example, at 100Gb network speeds, the inter-packet gap of 6.7 nanoseconds is simply not enough time for many security tools to perform security analysis and threat prevention if they have to process all network traffic within that duration.

As a result, companies are forced to:

- Slow down their business by slowing down their networks in order for security tools to keep up.
- Turn off some of those security tools, such as IDS, IPS and Web Application Firewalls, in order to keep the business running at full capacity when the load is too high for the tools to manage.
- Sample traffic or run in detection-only mode, both of which are risky.

Any of these choices lead to less-than-optimal security coverage. Meanwhile, tools directly connected through taps or mirror/Switched Port Analyzer (SPAN) ports reach the limit of their processing capability, forcing traffic to be dropped and compromising organizational security in the process. Moreover, security tools that are connected into specific points of the network may not see traffic from other parts of the network or from users or applications that have moved to other parts of the network. This limited visibility creates contention for traffic across departments.

2. Escalating Costs

Companies have already invested huge sums into 10Gb and 40Gb capable tools (such as firewalls, IPS/IDS, DLP, etc.) and will continue to do so. Cybersecurity Ventures predicts global spending on cybersecurity products and services will exceed $1 trillion cumulatively over the next five years, from 2017 to 2021.[2]

[1] https://www.gigamon.com/content/dam/gated/AR-IHS-Technology-Gigamon-Market-Leader.pdf

[2] Steve Morgan, "Cybersecurity Market Report," Cybersecurity Ventures, May 30, 2017. https://cybersecurityventures.com/cybersecurity-market-report/

However, with the increased volumes in traffic that 100Gb networks bring, there is a mismatch between the capabilities of an organization's investment in current security tools and the amount of traffic that needs to be monitored and analyzed. This is further compounded by that fact that not all (or even the majority) of a company's security tools (especially the passive ones) are capable of operating at 100Gb and those that can are typically very expensive.

As companies purchase more and more security tools, upgrade them and replace them over time, networks become unwieldy and costs spiral.

3. Painful Compromises

As companies aim to secure higher traffic volumes so they can fully move to faster networks up to 40Gb and 100Gb without security tools becoming an issue, they are having to make trade-offs between security, performance and cost. Attempts to use slower security tools on faster networks require traffic sampling, which increases the risk of a breach. Or they allow the slower security tools to effectively throttle the network. Neither is an appealing option, so security tool vendors promote an expensive "rip and replace" approach to upgrade. Vendors that are unable to cope with higher loads promote multiple tools with a load balancer, another expensive and inefficient option. These approaches can add up to millions of dollars and do not help companies fully realize the benefits of upgrading their networks. Nor do they provide additional advantages, such as being able to easily add and remove inline tools and analyze more segments of the network without buying more tools.

To sum up, security teams face increased complexity, higher costs and increasing loss of control as volumes of data and network speeds increase. Security and management controls in high-performance networks demand a new approach.

An Architectural Approach to Security Solves the Speed and Volume Problem

To address the security gaps, escalating costs and compromise created by more data on faster networks, companies are turning to an architectural approach to help:

- Improve security posture.
- Reduce costs.
- Eliminate compromise.

This architectural approach enables the deployment of a diverse set of security solutions as a centralized security tool farm – significantly reducing associated overhead, complexity and costs. Such an approach is at the heart of a security delivery platform, which is able to load balance sessions against sets of lower capacity tools. This not only provides the capacity required but does so by utilizing the current security toolset, which decreases cost.

In addition, a security delivery platform improves network resilience by allowing N+1 over subscription for load balanced security tools such that if there is a failure, that security tool can be taken out of commission and be replaced with no down time and no reduction in security. Inline security tools can negatively impact network resiliency and performance because they

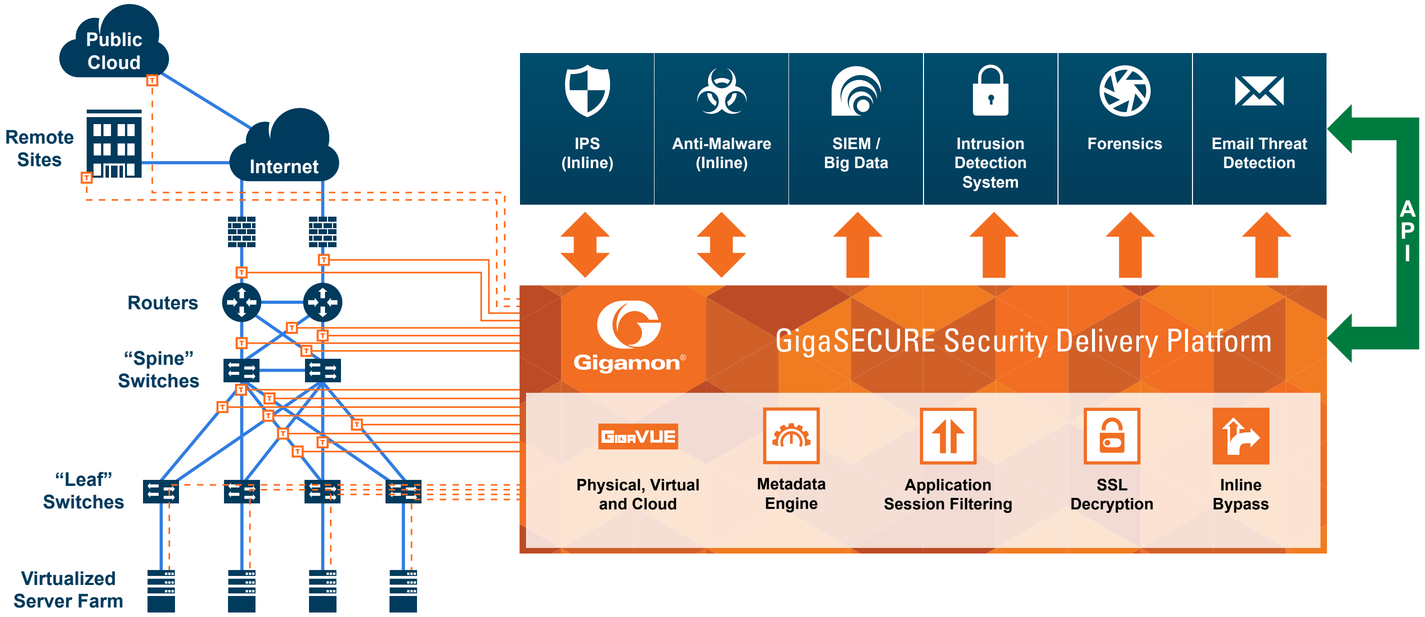

Figure 1: An Architectural Approach to Security

represent potential points of failure in the network and often operate at speeds significantly slower than that of the network. Whether due to a hardware failure, software malfunction or processing bottleneck, failing or slow inline tools can disrupt the very applications and services they are meant to protect. The logical and physical inline bypass mechanism of a security delivery platform solves this problem.

By centralizing security tools, security can be applied across physical, virtual and cloud environments by acquiring traffic from devices and applications present in the data center across physical and virtual, remote sites as well as private clouds and public clouds. This approach provides a view of the entire infrastructure to any operational tools that require network traffic or flow records derived from network traffic, eliminates blind spots and furnishes quick access to the whole network.

"Further, by its very nature, the security delivery platform provides an important foundation for improving cybersecurity. For example, it allows SecOps to integrate multiple disparate security solutions—including inline and out-of-band tools—into a single, integrated platform that simplifies deployment, operation and management across these products. The security delivery platform also acts as a "clearinghouse" for traffic to ensure that the appropriate traffic is directed to the right security tool. This not only optimizes the performance of these devices or software, but it also helps reduce the number of unnecessary instances of these products, which can be quite costly."[3]

The Enterprise Strategy Group (ESG) recently wrote about the architectural approach of consolidating tools. "As clearly evidenced by ESG's research data, most organizations can improve their network visibility and reduce their security vulnerabilities. However, they must make smart investments. Adding more point tools to an already fragmented security and monitoring environment may make security outcomes worse, not better. Rather, it is more likely that the typical organization can achieve better security outcomes by investing in staff (who are likely spread too thin today) or consolidating tools through a platform-based approach to visibility in which data, analytics and reports from multiple tools can be aggregated and consumed in one control panel. This architectural methodology is a particularly intriguing solution because it allows organizations to preserve investments in existing tools, making them work better, while also empowering the personnel. Improving the utilization of existing IT and human resources within the organization is a prudent way to meet these challenges."[4]

Introducing The GigaSECURE Security Delivery Platform

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.

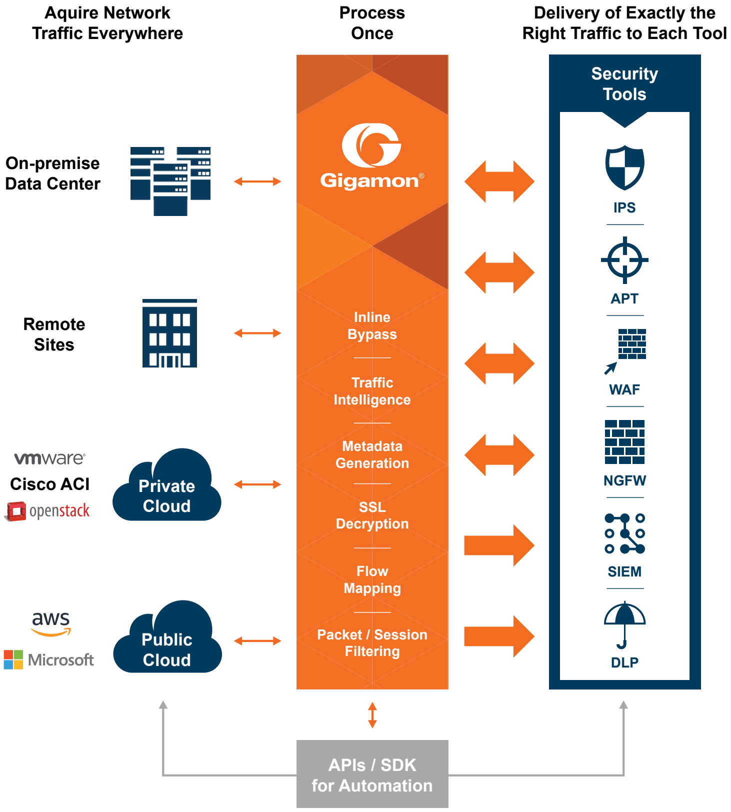

Figure 2: The Gigamon GigaSECURE® Security Delivery Platform

[3] IDG Tech Dossier, "A Security Delivery Platform Benefits the Entire Organization." https://www.gigamon.com/content/dam/gated/wp-security-delivery-platform-benefits-entire-organization.pdf

[4] Dan Conde, "Understanding the State of Network Security Today," The Enterprise Strategy Group, Inc., January 2017. https://www.gigamon.com/content/dam/gated/wp-esg-research-insights-gigamon-state-of-network-security.pdf

Benefits of the GigaSECURE Security Delivery Platform

While there are many benefits of the GigaSECURE Security Delivery Platform, let's focus on three main ones as they relate to the challenges of more data on faster networks.

1. Improve Security Posture

The GigaSECURE Security Delivery Platform is a fast, economical way to improve the effectiveness of existing security tools. It fits neatly into existing IT environments and eliminates the need to have every new security tool integrate with multiple networking devices.

The GigaSECURE Security Delivery Platform helps existing security tools realize their potential by:

- Giving them pervasive visibility into network traffic throughout the enterprise, eliminating blind spots caused by complex, segmented networks, East-West traffic and virtual environments.
- Giving them visibility into encrypted traffic, even at 100Gb.
- Making every security tool more efficient by offloading processor-intensive tasks such as SSL decryption and metadata generation.
- Reducing the number of security devices required and simplifying the security infrastructure by using techniques such as traffic intelligence and de-duplication.

With these benefits, IT organizations can optimize the performance of their existing security tools regardless of network speeds – improving security posture without tool sprawl or added costs.

2. Reduce Costs

A 2016 Total Economic Impact™ commissioned study conducted by Forrester Consulting on behalf of Gigamon estimated that by adopting the GigaSECURE® 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.[5] Additional benefits included:

- 153 percent return on investment through hardware and software savings.
- Seven-month payback in investment.
- More than 50 percent reduction in security costs.
- Reduced downtime due to fewer maintenance windows when security and monitoring tool maintenance or operational changes were required.

Simon Gibson, former Bloomberg CISO and Gigamon Fellow and CISO, further explains how companies reduce costs with the GigaSECURE Security Delivery Platform:

> "The GigaSECURE Security Delivery Platform can significantly cut the cost of security without making the organization less secure. Without the GigaSECURE Security Delivery Platform, security teams buy expensive, high-performance security tools to deploy at every critical point in the network. For example, if there were six points of entry, the organization would likely procure a dozen next-generation firewalls (two at each location for redundancy). Once it is in place, traffic from each point can be aggregated to a single point. So instead of buying 12, they would only need to purchase a pair. Also, you can send only the traffic to the security tool that it actually needs, significantly cutting down on the performance requirements. The norm is to overspend on security tools, but the GigaSECURE Security Delivery Platform allows businesses to buy exactly what they need, plus it has session load balancing, so that extra security tool capacity can be added when needed rather than the traditional rip-and-replace approach."[6]

3. Eliminate Compromise

With GigaSECURE Security Delivery Platform, there is no need to compromise in securing higher traffic volumes on faster networks because there are no trade-offs between security, performance and cost. The GigaSECURE Security Delivery Platform provides pervasive and intelligent visibility across the entire infrastructure, thereby enabling security teams to obtain broad and consistent network visibility. In addition to network traffic, the GigaSECURE Security Delivery Platform can be customized to extract specific application sessions, metadata and decrypted traffic. In this architecture, prevention tools can operate at peak performance without compromising network resiliency or slowing the network. The result is a more effective network security infrastructure with a vastly improved return on investment (ROI).

[5] Shaheen Parks, "The Total Economic Impact™ of Gigamon Cost Savings and Business Benefits Enabled by Gigamon," Forrester Research, Inc., April 2016. https://insight.gigamon.com/forrester-tei-report.html

[6] Zeus Kerravala, "How CIOs can relieve the tension between security and network operations," CIO, November 30, 2017. https://www.cio.com/article/3239167/leadership-management/how-cios-can-relieve-the-tension-between-security-and-network-operations.html

Summary

As data in motion across on-premises and cloud environments continues to grow, world-class organizations who want to compete must respond by upgrading to higher-speed networks running at 40Gb and 100Gb. But this creates worrisome security gaps, escalating costs and painful compromises that need to be addressed in order to fully realize the benefits of upgrading to higher speed networks. To solve these critical challenges, forward-looking companies are smart to benefit from the architectural approach of a security delivery platform that enables the deployment of a diverse set of security solutions as a centralized security tool farm – significantly reducing associated overhead, complexity and costs. The security delivery platform of choice for companies looking to future-proof their security operations is GigaSECURE Security Delivery Platform, which integrates with a wide variety of network security solutions, such as detection, prevention, security analytics, forensics and other tools. GigaSECURE Security Delivery Platform enables information security teams to respond to new threats in a timely manner while eliminating security tool sprawl, improving security and reducing costs. The result is a far more effective network security infrastructure with a vastly improved return on investment.

Next Steps

- Stop the sprawl. Build an efficient network security architecture that increases the return on investment of security tools while reducing complexity, cost and tool overload across physical, virtual or cloud infrastructure with the **GigaSECURE Security Delivery Platform**.
- Find out why Gigamon is the best choice for your organization: **Speak to a Gigamon expert**, **ask for a demonstration** or **sign up for a free trial today**!

About Gigamon

Gigamon provides active visibility into physical, virtual and cloud network traffic, enabling stronger security and superior performance. The Gigamon Visibility Platform and GigaSECURE – the industry's first Security Delivery Platform, deliver advanced intelligence so that security, network and application performance management solutions in enterprise, government and service provider networks operate more efficiently and effectively. See more at **www.gigamon.com**, the **Gigamon Blog**, or follow Gigamon on **Twitter**, **LinkedIn**, or **Facebook**. See What Matters™.