INDUSTRY BRIEF: GOVERNMENT

Network Security Solutions for Government Agencies

Overview

Cybercriminals, hackers, foreign government spies and viruses are all threats to cyber-based infrastructure systems and have driven government agencies to significantly increase their cybersecurity monitoring efforts.

To defend against today's advanced threats, government IT organizations require real-time visibility across their entire IT infrastructure — including physical, virtual and cloud environments.

Real-time visibility enables performance monitoring, but in today's world of breaches and hackers targeting data and information, it's also necessary to have advanced feature-rich solutions to secure all government data.

"Nation states, criminal syndicates, hacktivists and terrorists are all building capacity to infiltrate and undermine our networks. They are weaponizing the web."[1]

Key Cybersecurity Challenges for Government Agencies

Limited network visibility
Leads to a constant struggle to collect and analyze data across a disparate network and convert it to useable information for network and security operations teams.

Optimizing existing tools
Agency IT teams need help to leverage advanced technology that can scale the security tools analysts and operatives use to isolate threats.

Agility and availability
Security tool maintenance (moves and software or hardware upgrades) must be executed promptly with minimum network impact.

Increased network complexity and tool proliferation
Leads to higher infrastructure costs and difficulty managing and securing the network.

Gigamon the Essential Element of Your Infrastructure

The Gigamon Visibility Platform is stepping up to help tackle the key challenges for government agencies. Security tools connect directly to the Visibility Platform, which, as an intelligent data broker, selects, forwards and distributes the data as necessary to those tools. Visibility leading to agility, optimization and simplifying complexity are key objectives of the Visibility Platform.

Visibility
The Visibility Platform collects and aggregates traffic traversing your entire network (physical, virtual and cloud). Comprehensive visibility includes encrypted traffic from any TCP port or application, which will be decrypted and passed appropriately to each security and monitoring tool.

[1]Secretary of Homeland Security remarks, March 18, 2019,
https://www.dhs.gov/news/2019/03/18/secretary-nielsen-remarks-state-homeland-security-prepared-delivery

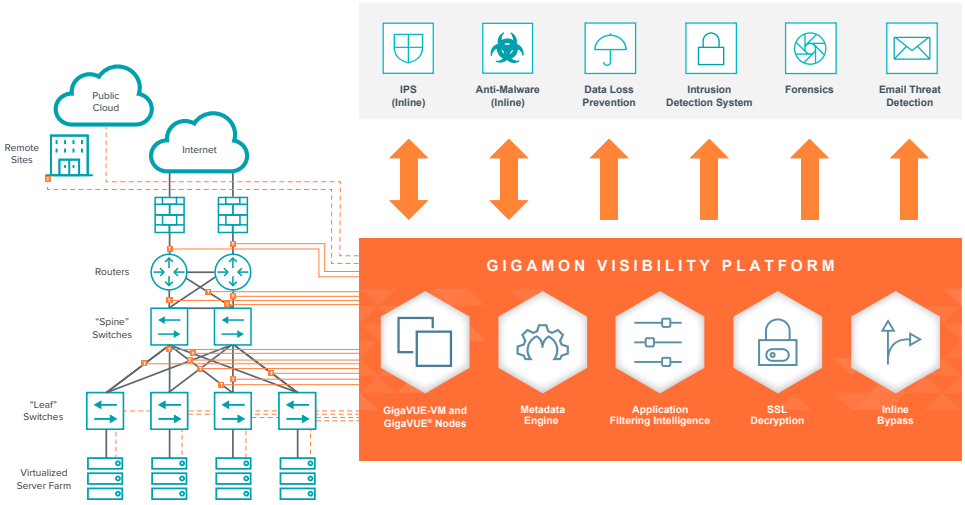

Figure 1: Aggregate traffic to the Gigamon Visibility Platform

Pervasive visibility is central to security capabilities that map to the National Institute of Standards and Technology (NIST) Cybersecurity Framework[2] – protect, detect, respond, and also to identify and recover.

The Identify function has been highlighted as "foundational" to the Cybersecurity Framework. Many Federal agencies have verified this via their experience with the Continuous Diagnostics and Mitigation (CDM) Program Phase 1 deployment, which includes the need to conduct physical and virtual device discovery to support a Hardware Asset Management (HWAM) solution.

Optimization

The Gigamon Visibility Platform offers Application intelligence. IT teams now have application awareness to improve the effectiveness of their entire ecosystem, make tools more efficient and reduce effort and costs.

With the massive growth of web traffic, a lot of low-risk and high-volume traffic can end up clogging security and monitoring tools; for example social media and video streams from YouTube, Netflix and Facebook.

With application intelligence built right into the core visibility infrastructure, administrators now have the flexibility to identify and isolate applications independently of IP addresses or TCP/UDP port numbers. They can, that is, extra relevant traffic automatically all the way up to Layer 7.

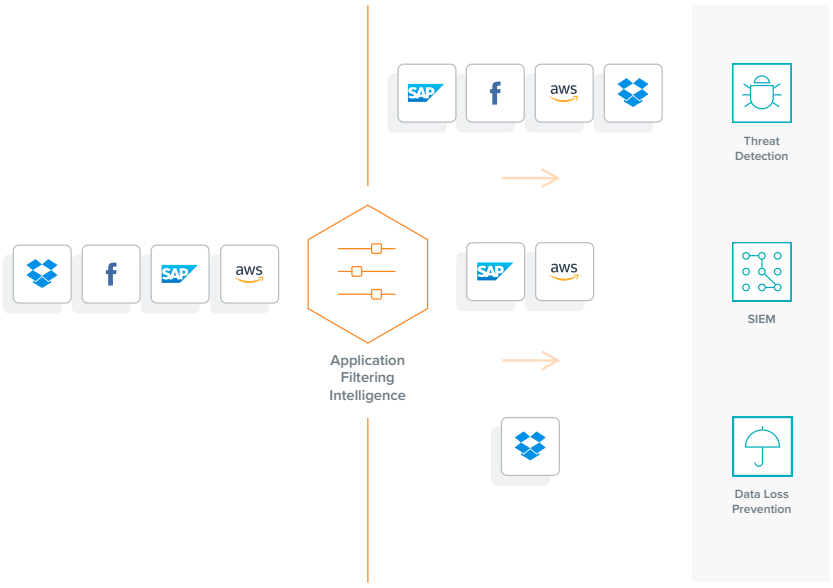

Figure 2: Optimizing tool analysis

[2]Framework for Improving Critical Infrastructure Cybersecurity

Now IT teams can leverage this information to route the right application to the right tool. This filtering dramatically reduces the load on tools, optimizing performance while preventing them from becoming bottlenecks that slow application performance. By filtering out low-risk and irrelevant communication, it also ensures tools can focus on high-risk traffic.

Agility

With Inline Bypass it's possible to prevent inline security tools from becoming single points of failure on the network.

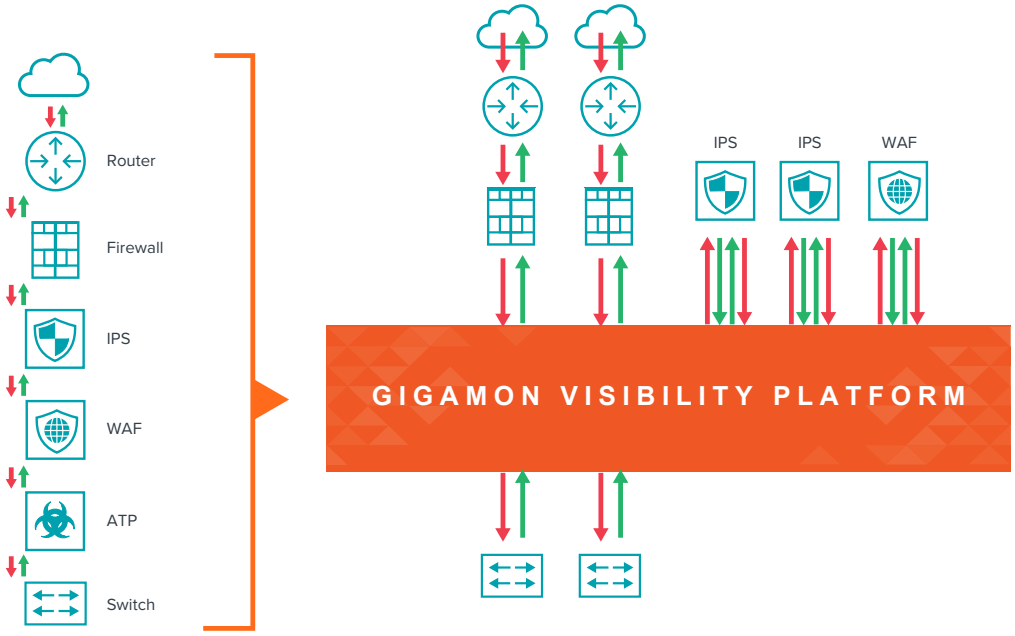

Figure 3: Scaling threat prevention tools with the Gigamon Visibility Platform

Inline bypass refers to a collection of features that increase the availability and performance of networks and tools, including load sharing, bypassing failed security tools, sensing when tools go offline or begin to malfunction, and toggling tools between inline and out-of-band modes.

Now security tool failures and upgrades can be easily managed without impacting network performance or interrupting access to applications. SecOps teams can apply fixes or updates rapidly without network interruption.

Continuing the agile theme, the Inline Bypass feature can easily switch devices from out of band to inline in seconds. It is, for example, possible to complete a full suite of tests on new tools with real network traffic before activating on to the network.

Simplifying Complexity

Organic growth can introduce uncontrolled network sprawl. In order to accommodate needs, security tools and links are added on an ad hoc basis, generally resulting in a difficult to manage and secure network, as illustrated in Figure 4.

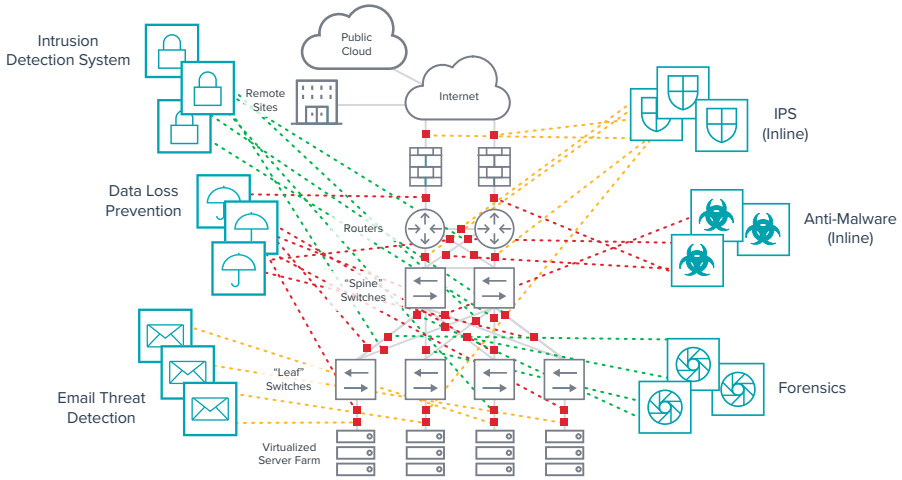

Figure 4: Tool sprawl and growth happens organically

Transforming a network architecture with the Gigamon Visibility Platform provides security solutions broad network visibility, access to metadata, application traffic and encrypted traffic, as well as fault tolerance and scale.

The result is an improved security posture that's easier to manage (see Figure 5).

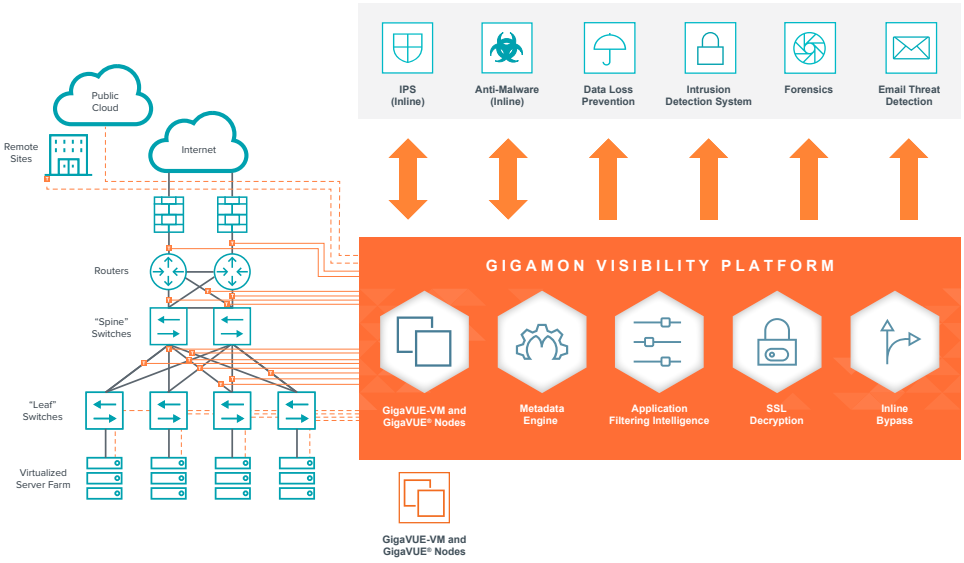

Figure 5: An effective and improved security posture

Summary: See, Secure and Empower Your Network and Security Operations

The Gigamon Visibility Platform is purpose built to help government agencies gain pervasive network visibility and maximize security tool efficiency — and meet demands for higher network performance. Key features of the solution include:

- **Full access to network traffic** across physical, virtual and cloud networks
- **Traffic intelligence** to optimize network traffic flows and filter out unnecessary traffic to each tool
- **Offloading of processor-intensive tasks** such as decryption and de-duplication
- **Load sharing** to spread traffic across multiple devices
- **NetFlow generation** from any selected traffic stream
- **Centralized orchestration** and integration with security workflows to enable dynamic response to infrastructure changes while reducing cost

The Proof is in the Numbers

Gigamon solutions have been deployed in many of the world's leading organizations, including those in the public sector, and have achieved the following industry milestones:

10 **Out of the top 10** U.S. federal agencies have deployed Gigamon solutions

153% **ROI improvement of** the security stack (Source: Forrester)[3]

50% **Decrease in costs associated** with security efforts (Source: Forrester)[3]

#1 Market leader in network monitoring equipment, with **37 percent** market share, twice the market share of the nearest competitor (Source: IHS Markit June 2018)[4]

61% Market share in the government sector, nearly **four times** its nearest competitor (Source: IHS Markit June 2018)[4]

[3]The Total Economic Impact™ of Gigamon, a commissioned study conducted by Forrester Consulting on behalf of Gigamon, April 2016
[4]Network Monitoring Equipment Annual Market Report: IHS Markit

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