Gigamon Helps Government Agency Meet Cybersecurity Requirements

// Case Study

"Gigamon helps us with visibility for the Trusted Internet Connections Initiative, replicating all of our traffic so we're able to clearly see everything that's going across the network."

*// **Travis Richardson,** NETWORK SECURITY MANAGER, HHS CSIRC*

The Department of Health and Human Services (HHS) Computer Security Incident Response Center (CSIRC) is the primary entity responsible for not only maintaining department-wide operational Information Technology (IT) cybersecurity, but also determining the overall operational IT security risk posture of the HHS infrastructure. The CSIRC complies with reporting guidelines from the National Institute of Standards and Technology (NIST) Computer Security Incident Handling Guide and the United States Computer Emergency Readiness Team (US-CERT).

Securing Confidential and Private Information

Whether it is cyber criminals, hackers, foreign government spies, viruses, or other malicious activity, threats to cyber-based infrastructure systems have driven government agencies to increase their cybersecurity monitoring efforts significantly. A combination of highly skilled experts and a rapid response system can help to monitor and respond to the potential impact on resources, the possible loss or destruction of healthcare-related and privacy information, in addition to the potential loss of productivity and reputation damage.

The Department of Homeland Security (DHS) developed the Trusted Internet Connections (TIC) Initiative to optimize and standardize the continuous monitoring of cybersecurity for external network connections in use by federal agencies in order to improve security posture and incident response capabilities, as well as provide enhanced monitoring of external network connections. With these demanding objectives for the HHS and all of its operating division (OPDIV) networks, including the Centers for Disease Control (CDC), Federal Drug Administration, (FDA), National Institute of Health (NIH), and Centers for Medicare and Medicaid (CMS), CSIRC was looking for a powerful and strategic solution.

According to Steve Swansbrough, Security Hardware and Software Engineering Team Lead with HHS CSIRC, "We needed something that would allow us to connect multiple tools to perform various monitoring and security functions. We had to do malware analysis, network packet capturing analysis,

Challenge

When the Department of Health and Human Services (HHS) Computer Security Incident Response Center (CSIRC) needed to meet rigid requirements to ensure security, the organization set out to find a solution that would enable continuous cybersecurity and situational awareness monitoring, as well as provide a scalable framework to meet its future growth.

Solution

A Gigamon® Visibility Fabric™ solution built on modular GigaVUE® fabric nodes with patented Flow Mapping® to provide intelligent aggregation, filtering and replication of traffic flows

Benefits

- Pervasive visibility of network traffic across geographically dispersed locations so issues can be addressed quickly and Department of Homeland Security requirements can be met
- Traffic is directed through security devices so it is safe from viruses and malware before entering the network
- CSIRC's 1Gb and 10Gb sensors, probes and collection devices are provided with the critical voice, video and data necessary to fully realize their potential

Intrusion Detection (IDS) and Intrusion Prevention Systems (IPS) monitoring, application monitoring, and more. We also needed an out-of band solution that could handle the traffic of our multiple 10Gb networks, because we sit outside of each division and monitor from here. So we had very specific requirements."

Layers of Security

The organization carefully evaluated solutions from leading traffic visibility vendors and finally selected Gigamon. With the help of Annapolis, Maryland-based BAI Federal, CSIRC deployed eight GigaVUE-420 Traffic Visibility Fabric Nodes across each HHS OPDIV. Those systems are the first layer of visibility for the OPDIV traffic, enhancing the functionality of deployed packet analysis, IDS, IPS, application and performance monitoring tools. Additionally, a mixed stack of two GigaVUE-2404 fabric nodes and one GigaVUE-420 with bypass TAP modules are deployed at all TIC locations to provide direct visibility of all traffic coming in and out of the HHS enterprise. Lastly two GigaVUE-2404 fabric nodes are installed at the central CSIRC location for consolidated oversight of all divisional and enterprise traffic by additional analysis and monitoring tools. Gigamon provides pervasive visibility into CSIRC's networks without affecting the performance or stability of the production network. The Fabric replicates, filters and delivers the appropriate traffic to the organization's security, monitoring and management systems.

"The divisions each have their own security tools attached to their GigaVUE, and they monitor their own networks," said Swansbrough. "We're outside of each division, a layer above, so you could say we're watching the watchers. The Gigamon solution ensures that the tools we have deployed receive the information they need so we can accurately monitor the networks and ensure all security objectives are met."

> ***"We appreciate the port density and Gigamon's ability to replicate traffic and stream it across multiple tools like probes and sensors."***
>
> *// **Travis Richardson,** Network Security Manager, HHS CSIRC*

Richardson is contracted through Merlin International, a technology solutions provider for federal government agencies and organizations focused on activities such as civilian services,

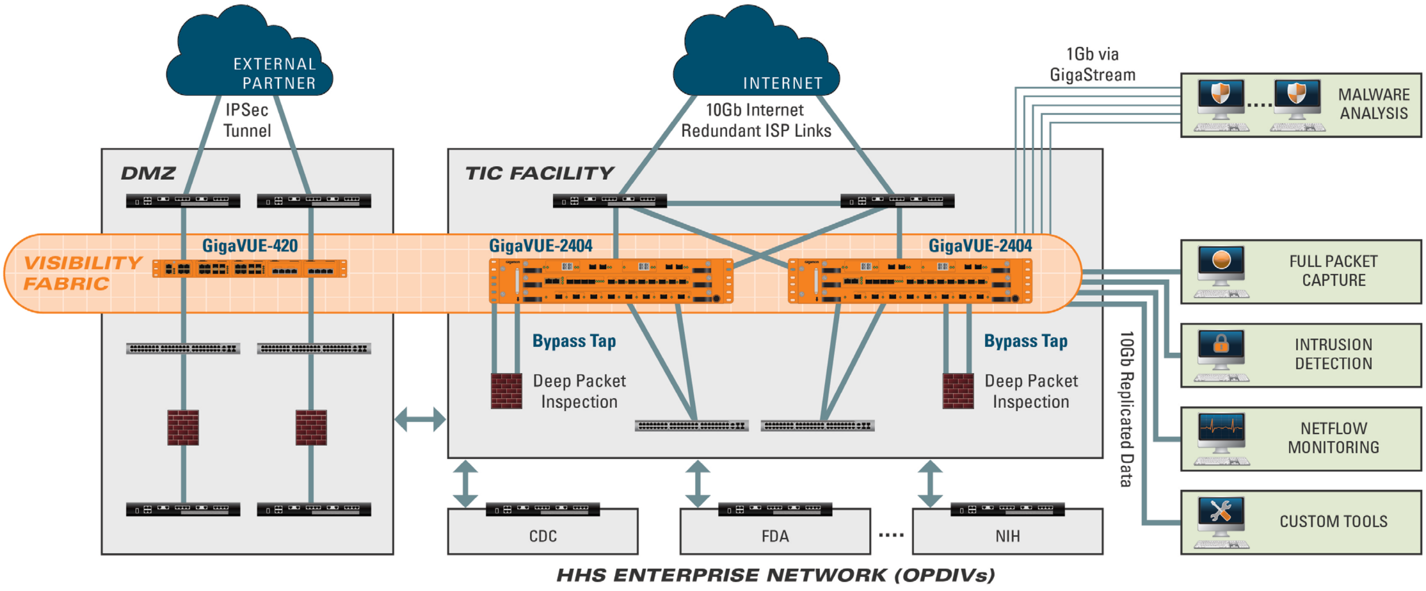

Figure 1: Four HHS TIC sites across the U.S. service all HHS OPDIVs

defense, intelligence, and healthcare. "We also have a 10Gb network so it's essential that the Gigamon Visibility Fabric solution performs at wire speed with no degradation. Gigamon helps us with visibility for the TIC Initiative, replicating all of our traffic and data flows so we're able to clearly see everything that's going across the network," adds Richardson.

Gigamon recognizes the importance of traffic visibility when it comes to a comprehensive security strategy. Having completed the National Information Assurance Partnership (NIAP) Common Criteria Evaluation and Validation Scheme (CCEVS) for its Traffic Visibility Fabric Nodes, this investment helps to assure customers and serves as a proof point of Gigamon's ongoing commitment to meeting the security needs of government organizations.

Optimal Performance and Failover Protection

The Gigamon GigaVUE-2404 using patented Flow Mapping technology filters traffic across CSIRC's tools at full line-rate performance. In addition its modular design allows the organization to deploy the number of ports needed according to its current requirements, enabling true flexibility. The GigaVUE-420 Traffic Visibility Fabric Node supports 10/100/1000 and 10Gb Ethernet, and other tools may be added without affecting the network at any hour, without configuration management review.

"The Gigamon solution makes our security tools far more valuable than they are without it."

*// **Steve Swansbrough,** Security Hardware and Software Team Lead, HHS CSIRC*

Gigamon allows CSIRC to extend the use of its 1Gb tools on its 10Gb network. "We've got 1Gb interface analysis and monitoring tools on a 10Gb network. Gigamon allows us to leverage our 1Gb tool investments in a 10Gb environment. We'd have been in trouble if we didn't have the modularity and the choice of interfaces Gigamon provides. That kind of modularity is a huge benefit," add Swansbrough.

Gigamon GigaStream™ optimizes tool performance and security with dynamic load balancing ensuring complete traffic flows while maintaining persistent and session-based integrity of data—from the pervasive to the elusive. Keeping all related packets together, GigaStream delivers the information necessary to CSIRC's tools for maximum security and performance monitoring.

Furthermore, Gigamon GigaBPS, a 10Gb fiber optic tap module for the GigaVUE-2404, supports two bypass switches for the integration of CSIRC's in-band (or inline) IPS tools, offering active and passive protection against possible network downtime due to failure of these tools. A heartbeat feature allows for proactive monitoring of in-band tools confirming that the IPS is functioning and if not, is able to respond or react and flow traffic to alternative devices as appropriate. Traffic entering and leaving the in-band tools can also be replicated, aggregated and filtered to out-of-band monitoring tools thereby enabling out-of-band monitoring.

Simplified Reporting and Management

The GigaVUE stackable architecture provides additional scalability and simplified management with the ability to manage the stack centrally. Connecting GigaVUE systems in a cross-box stack means that data arriving at a network port on one GigaVUE can be forwarded to a tool port on another GigaVUE, providing a full network view as well as management simplicity for the entire CSIRC team.

"The Gigamon solution lets us create trending logs so we're able to look for and clearly identify security-related issues," said Richardson. "We use the Visibility Fabric to replicate traffic across the entire department to do more in-depth research when we see an anomaly, or if someone at an operating division asks us to do a more thorough check. All of the traffic the division security teams review is regenerated to our monitoring or IDS/IPS tools so we can look more closely and make sure HHS is meeting its security goals."

Prepared for the Future

CSIRC appreciates the expertise of both Gigamon and certified reseller BAI, complimenting both organizations for their dedication to ensuring a smooth implementation. "Gigamon representatives were extremely knowledgeable when they presented the solution to us, making sure they thoroughly knew our requirements and priorities," said Richardson. "BAI was and continues to be instrumental in meeting our needs. We've established true partnerships with both organizations and appreciate their responsiveness and commitment to our organization."

Swansbrough expects HHS to move to parallel 10Gb networks as everything transitions to the cloud and traffic increases. Currently there are few cloud-based tools for control reasons, but that is the anticipated direction. "Whatever cloud services we implement, from a trusted network point of view, the TIC Initiative will still be in place," said Swansbrough. "With Gigamon, we're able to keep historical data and track trends, such as network areas and times of the year where certain things happen so we're able to plan for the future. The bottom line is Gigamon extends the capabilities of our tooling infrastructure, allows CSIRC to add more tools without impacting the network, and enables us to centralize management."

About Gigamon

Gigamon provides an intelligent Traffic Visibility Fabric for enterprises, data centers and service providers around the globe. Our technology empowers infrastructure architects, managers and operators with pervasive visibility and control of traffic across both physical and virtual environments without affecting the performance or stability of the production network. Through patented technologies and centralized management, the Gigamon GigaVUE portfolio of high availability and high density products intelligently delivers the appropriate network traffic to security, monitoring or management systems. With over eight years' experience designing and building traffic visibility products in the US, Gigamon solutions are deployed globally across vertical markets including over half of the Fortune 100 and many government and federal agencies.

For more information about our Gigamon products visit:
www.gigamon.com