Case Study

Gigamon Helps Government Agency Meet Cybersecurity Requirements

"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*

Customer 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

Gigamon Solution

- Gigamon Visibility Platform

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 cybercriminals, 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, 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 the Gigamon Visibility Platform. Gigamon provides pervasive visibility into CSIRC's networks without affecting the performance or stability of the production network. The solution replicates, filters and delivers the appropriate traffic to the organization's security, monitoring and management systems. Gigamon provides pervasive visibility into CSIRC's networks without affecting the performance or stability of the production network.

"The divisions each have their own security tools attached to their Gigamon solution, 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."

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

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.

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.

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.”

3006-04 06/17

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