Case Study

The Department of Health and Human Services Meets Cybersecurity Initiative Requirements with Help from Gigamon

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.

STEVE SWANSBROUGH
Security HW and SW Engineering Team Lead
Department of Health & Human Services

Challenges

The Department of Health & Human Services (HHS) needed reliable data access for its many monitoring and security tools to comply with the requirements of the Trusted Internet Connection (TIC) initiative.

Solution

Gigamon Deep Observability Pipeline

Customer Benefits

- Accelerated compliance with TIC
- Reliable data access for security tools
- Visibility into geographically dispersed locations
- Extended lifecycle of existing security stack

To comply with the Trusted Internet Connections (TIC) initiative, many federal agencies, including the Department of Health & Human Services (HHS), needed to optimize and standardize monitoring for external network connections. For many, this meant significantly increasing the scope of current monitoring technology and ensuring resiliency.

At HHS, the task fell to the Computer Security Incident Response Center (CSIRC), which oversees the operational IT security risk posture of the department.

"We needed something that would allow us to connect multiple tools to perform various monitoring and security functions," explained Steve Swansbrough, Security Hardware and Software Engineering Team Lead with HHS CSIRC.

"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," Swansbrough added.

Facing these demanding objectives for 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 knew it needed a strategic solution.

Reliable Data Access For Tools and Teams

The department carefully evaluated solutions from leading next-generation network packet brokers and ultimately selected Gigamon. The technology vendor had completed the National Information Assurance Partnership (NIAP) Common Criteria Evaluation and Validation Scheme (CCEVS), which reaffirmed its commitment to meeting the needs of government organizations such as the HSS. The Gigamon Deep Observability Pipeline replicates, filters and delivers the appropriate traffic to an organization's security, monitoring and management tools. With the help of certified reseller Blackwood Associates, CSIRC deployed Gigamon, gaining pervasive visibility without affecting the performance or stability of its production networks. This approach gave CSIRC the visibility required by the TIC initiative as all traffic and dataflows are now replicated and routed to the correct tools for analysis.

"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."

Failover Protection

With Gigamon, a core feature allows for the proactive monitoring of in-band tools, confirming that the IPS is functioning and, if not, it responds by delivering traffic to alternative devices as appropriate. Now, if a security tool fails due to a power outage, software malfunction or processing bottleneck, the applications and services it protects will continue to function. This approach enables HHS to optimize network uptime without sacrificing security.

Additionally, 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.

Future-Proof Visibility

Gigamon also allowed CSIRC to extend the use of its 1Gb tools on its 10Gb network and thus avoid unnecessary tool upgrades.

The ability to accommodate existing tools optimized for lower rates and the newly gained visibility will continue to benefit the department when it comes to future network upgrades, such as cloud services. Since the HHS expects to move to parallel 10Gb networks as everything transitions to the cloud with inevitable traffic increases, Swansbrough says, "Whatever cloud services we implement, from a trusted network point

of view, the TIC Initiative will still be in place." Another benefit is historical trends with related data. "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," Says Swansbrough.

CSIRC appreciated the expertise of both Gigamon and Blackwood Associates, and it complimented both organizations for their dedication in 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."

About Gigamon

Gigamon offers a deep observability pipeline that harnesses actionable network-derived intelligence to amplify the power of observability tools. This powerful combination helps IT organizations to assure security and compliance governance, speed root-cause analysis of performance bottlenecks, and lower operational overhead associated with managing hybrid and multi-cloud IT infrastructures. The result: Modern enterprises realize the full transformational promise of the cloud. Gigamon serves more than 4,000 customers worldwide, including over 80 percent of Fortune 100 enterprises, nine of the ten largest mobile network providers, and hundreds of governments and educational organizations worldwide. To learn more, please visit gigamon.com.

Gigamon®

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

06.23_02