Case Study

Department of Defense Subcontractor Tackles Cybersecurity Threats in Global Conflict Zones with Gigamon

It was clear that Gigamon products' modular capabilities mean they can perform a wide range of tasks previously covered by multiple tools. This enables us to remove unneeded equipment from the fly-away kit, freeing up valuable space. This is so important when you travel the type of miles our team does, and the cost savings are nice, too. Given that the previous vendor's model was meter-based, this will result in cost savings of hundreds of thousands of dollars per year.

SUBCONTRACTOR
Department of Defense

Challenges

This Department of Defense (DoD) subcontracting firm needed a solution that would meet the needs of its teams in active conflict zones to route network data to security tools for analysis.

Customer Benefits

- Reliable data delivery to security tools
- Improved visibility without impacting performance
- Consistent generation of NetFlow and other metadata

Solution

- Gigamon Deep Observability Pipeline
- GigaSMART®

As a Department of Defense (DoD) subcontracting firm, this federal Gigamon customer offers network incident response, computer forensics network design and configuration services to its customer at military hot spots around the globe.

Not only does its team need products that are accurate and certified, but anything they use must also be light—literally. Lightweight, that is.

This is because the DoD subcontractor researches, builds and travels with a tactical kit, also known as a "fly-away kit." This kit includes all of the hardware and software the firm needs in the field to quickly tap into its customer's network and run the tests and processes required to spot and mediate vulnerabilities in real time. Given the nature and remote locations of the firm's projects, the lighter and smaller the kit is, the better—because every ounce and inch counts, both in transit and on the ground.

Additionally, all of the computer equipment and software that the subcontractor connects to DOD networks must first pass the necessary federal government testing and accreditation. This includes compliance with the National Institute of Standards and Technology (NIST) Risk Management Framework, FIPS 140-2 and DoD Security Technical Implementation Guide (STIG). In essence, any solution included in the kit would need to meet the federal government's requirements.

Selecting a Lightweight Solution

Ultimately, the DoD subcontractor decided to add the Deep Observability Pipeline with GigaSMART modules, including NetFlow Generation and other network metadata generation for advanced traffic intelligence, to its kit.

And with Gigamon already on the federal government's approved product list, the accreditation and compliance process was greatly simplified. "Each accreditation requires 200 to 300 pages of documentation, so any time you can select a product that has already been approved, it's a huge win and time savings," said the firm's president.

Benefits

"When we realized that the Deep Observability Pipeline could generate NetFlow data that we can then send on to other tools for analysis, we were thrilled," he said.

This allows security tools to operate on relevant security information to quickly pinpoint the location of a possible network compromise without causing performance issues, versus flooding tools with raw packet streams. When used in tandem with some of the new, big data–based analytics tools, the metadata generated by Gigamon also allows for a more focused, in-depth security scan as a second phase of investigation.

"It was clear that Gigamon products' modular capabilities mean they can perform a wide range of tasks previously covered by multiple tools. This enables us to remove unneeded equipment from the fly-away kit, freeing up valuable space. This is so important when you travel the type of miles our team does, and the cost savings are nice, too," the firm's president added. "Given that the previous vendor's model was meter-based, this will result in cost savings of hundreds of thousands of dollars per year.

"Think of it as our doctor kit. We gather the equipment and medicine required to diagnose and heal our patients, put it in our doctor bag and go to work," he said.

About Gigamon

Gigamon offers a deep observability pipeline that harnesses actionable network-level intelligence to amplify the power of observability tools. This powerful combination enables IT organisations 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 10 largest mobile network providers, and hundreds of governments and educational organisations 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

03.24_02