

Case Study

Department of Defense Subcontractor Leverages Solutions from Gigamon to Tackle Cybersecurity Threats While in Conflict Zones Around the Globe

“When we realized that the GigaSECURE Security Delivery Platform is able to generate NetFlow data that we can then send on to other tools for analysis, we were thrilled. Given the previous vendor’s model was meter-based, this will result in cost savings of hundreds of thousands of dollars per year.”

–Department of Defense subcontracting firm’s president

Customer Benefits

- Significant cost savings.
- Reduced number of security tools required.
- Easier compliance with federal regulations.

Gigamon Solutions

GigaSECURE® Security Delivery Platform with:

- GigaVUE® visibility nodes.
- GigaSMART® traffic intelligence including NetFlow / Metadata Generation and Application Session Filtering.
- Inline bypass.

Challenges

An intriguing Gigamon customer in the federal space is a Department of Defense (DoD) subcontracting firm that provides its customers with network incident response, computer forensics network design and configuration services. As part of this role, the firm is always on the hunt for the most powerful, trustworthy security and analytics tools on the market. Not only do the products need to be accurate and certified, they must also be light – literally.

Yes, lightweight. The DoD subcontractor researches, builds and travels with a tactical kit, also known as a “fly away kit.” The kit includes all of the hardware and software the firm needs to provide on-the-ground support to its customer in military hot spots around the globe. The firm’s team uses this equipment to quickly tap into its customer’s network and run the tests and processes needed to spot and mediate vulnerabilities in real time. Given the nature of the remote locations where these projects are done, the lighter and smaller the kit is, the better. Every ounce and inch counts both in transit and on the ground.

“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,” said the firm’s president.

Solution

Specifically, the DoD subcontractor leverages the GigaSECURE Security Delivery Platform and GigaSMART for advanced traffic intelligence, including NetFlow and other network metadata generation. This allows the security tools to operate on relevant security information versus flooding them with raw packet streams to quickly pinpoint the location of a possible network compromise without causing performance issues. When used in tandem with some of the new big data-based analytics tools, metadata also allows for a more focused, in-depth security scan as a second phase of the investigation.

“As we make these crucial selections, 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 types of miles our team does, and the cost savings are nice too,” said the firm’s president.

Results

“When we realized that the GigaSECURE Security Delivery Platform is able to generate NetFlow data that we can then send on to other tools for analysis, we were thrilled. Given the previous vendor’s model was meter-based, this will result in cost savings of hundreds of thousands of dollars per year,” said the firm’s president.

A final benefit is accreditation. All of the computer equipment and software that the subcontractor connects to the Department of Defense networks must first pass the necessary federal government testing and accreditation, including compliance with the National Institute of Standards and Technology (NIST) Risk Management Framework, FIPS 140-2 and DoD Security Technical Implementation Guide (STIG). Gigamon already has a number of federal accreditations in place and has guides and expertise to help customers get through these processes.

“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. “By working with companies like Gigamon who are on the federal government’s approved products list, it simplifies the compliance process.”

About Gigamon

Gigamon (NYSE: GIMO) provides active visibility into physical and virtual network traffic, enabling stronger security and superior performance. The Gigamon Visibility Platform and GigaSECURE®, the industry’s first Security Delivery Platform, deliver advanced intelligence so that security, network and application performance management solutions in enterprise, government and service provider networks operate more efficiently and effectively. Learn more at www.gigamon.com and the [Gigamon Blog](#) or follow Gigamon on [Twitter](#), [LinkedIn](#) or [Facebook](#). See What Matters.™