Case Study

Major National Museum Standardizes on Deep Observability as a Foundation for Its Data Integrity and Security

> Gigamon has been a godsend for us, and it’s the foundation for every security solution we have.

MICHAEL TROFI
Trofi Security

Challenges

- Lack of deep observability into the hybrid cloud environment
- Constant attacks from malicious and state-sponsored threat actors
- High volume of noise, false positives in event logs, and duplicated traffic

Solution

- GigaVUE Cloud Suite for AWS
- GigaVUE HC Series
- GigaVUE-FM

Customer Benefits

- Improved East-West traffic observability
- Reduced the volume of traffic flowing into network detection and response (NDR) systems in AWS
- Streamlined and cleaned data
- Integrated easily with existing tools, using the same data set, to increase integrity and predictability

About the Customer

Tasked with guarding more than 1.7 petabytes of single-source sensitive historical artifacts from genocide atrocities around the world, the United States Holocaust Memorial Museum plays a critically important role. It serves as a living memorial to the Holocaust, inspiring citizens and leaders worldwide to confront hatred, prevent genocide, and promote human dignity. Federal support guarantees the museum's permanent place at the National Mall in Washington, D.C., and its far-reaching educational programs and global impact are made possible by generous donors.

Michael Trofi has served as the museum's CISO for almost a decade and is responsible for protecting its valuable archives. His firm, Trofi Security, offers virtual CISO and security operations center (SOC) services from its headquarters in Lafayette, Colorado. Trofi has over 40 years of experience in the information technology and cybersecurity space, spanning a variety of industries. With staffing an ongoing challenge, he has been an early adopter of artificial intelligence (AI) and machine learning (ML) technologies to be more proactive in preventing attacks, automate everyday cybersecurity tasks, and better leverage his team.

Business Challenge

In addition to guarding sensitive historical data, the museum also reports on current atrocities, such as the treatment of the Uyghurs in China, to the U.S. State Department. For this reason, the museum is often the target of hostile attacks from multiple sources around the world. At the same time, the museum has a mission to make its data widely available and is in the process of accelerating its transformation into the public cloud, which presents a whole host of security challenges. By leveraging the cloud and replicating data at points of presence, the museum can improve access to its educational services worldwide. Trofi expects the museum's data to be almost fully in the hybrid cloud within about five years, with a minimal onsite data center footprint.

Historically, Trofi and his team have used firewalls and point-to-point VPNs to secure their client's data, but Trofi felt something was missing. With the new hybrid workforce model, VPN is no longer an optimal solution for remote connectivity, and a move to a SASE (secure access service edge) solution is a must to extend your security perimeter. More importantly, Trofi also points out that metrics, events, system logs, and traces are "not the answer" because each application has its own data set — and they don't always agree. Slogging through all the noise and duplicated traffic took a lot of staff time, and there were often false positives. The lack of data integrity was affecting the team's ability to effectively feed security products into Amazon Web Services (AWS).

What was missing? It was deep observability. Trofi wanted better observability into North-South and East-West traffic to answer questions like: Where is your data going? Who is the recipient? Are they legitimate? Another issue he pointed to is the limitations inherent in AWS security, which looks only at events and not traffic flow.

"Expanding into traffic flow is a big benefit," he remarks. "Packets, packets, packets. The packets don't lie. Logs, though important, don't tell the entire story, so we needed to go down to the packet level." That's where Gigamon came in, with its ability to quickly surface anomalies in traffic that may point to threat activity.

Resolution

GigaVUE® Cloud Suite™ for AWS was deployed and provided Trofi and his team far greater observability into the museum's AWS environments. The De-duplication and Flow Mapping™ features of Gigamon dramatically reduced the volume and improved the quality of traffic flowing to the museum's NDR systems.

The streamlined, cleaned-up data set made it possible for the team to effectively integrate their security tools. "It was really noisy before. Cleaning the traffic so we can actually see it and clearing out the noise was a big deal," comments Trofi.

Thanks to the exceptional ability of Gigamon to tap, aggregate, and de-duplicate traffic, the museum is now using it as the foundation for all its security solutions, including Fortinet, Check Point, Armis, and Forescout Technologies. Trofi asserts that the data integrity Gigamon provides the museum is the biggest benefit: “Gigamon serves as the single source of truth that feeds all our systems.”

The improved data integrity gave the team the ability to automate routine tasks, which couldn’t be done before with competing data sets. “Gigamon’s observability provides us with the ability to take advantage of AI and machine learning,” says Trofi.

With AI tools, he points out, a lot of mundane tasks can be automated so the truly skilled individuals can “go after real problems.” For example, one of the team’s current big projects is to eliminate all unencrypted traffic. With the old way of using logs, that would have taken years, Trofi points out. “Gigamon has been a godsend for us, and it’s the foundation for every security solution we have,” he says.

Benefit

In addition to improving the museum’s security posture, Gigamon also improved network performance. By making the traffic flows observable, Gigamon has enabled the network operations team to eliminate rogue traffic that shouldn’t be there.

“That creates a whole new world for us. We can actually ‘traffic shape’ our network through observability, which was really hard to do 20 years ago. Observability is making this easier,” Trofi asserts. “By analyzing through observability how our applications are accessed, we can optimize our paths through our firewalls. So not only are we addressing security issues through observability but also performance issues through observability. And that’s a big benefit for us moving forward.”

Now that his team knows what a valid path is, they don’t have to treat everything as hostile and can provide a better experience for the user. Trofi points out that improved observability has the added benefit of bringing the various IT functions to work together collaboratively, which he sees as a step forward for the entire industry.

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