Case Study

Leading Global Semiconductor Manufacturer Enhances Visibility, Strengthens Cloud Security, and Lowers Costs by Partnering with Gigamon

We have embraced Gigamon as a partner to help us align with our enterprise strategy roadmap. Gigamon helped us plug all the visibility gaps in our environment and improve our efficiency around security operations.

NITIN
Director, Network and Security Services

Challenges

- Closing gaps in network visibility and gaining deep observability
- Integrating and consolidating data from various sources into its network detection and response ecosystem
- Aligning the environment with the overall enterprise strategy roadmap

Customer Benefits

- Streamlined and optimized data feeds
- Reduced data volume entering appliances by 40 to 50 percent
- Improved network visibility and closed security gaps
- Shortened time to response and time to resolve for security incidents

Solution

- GigaVUE® HC Series
- GigaVUE Cloud Suite™
- GigaVUE-FM Fabric Manager

About Customer

In business for over 45 years, this leading global semiconductor manufacturer and one of the top three semiconductor manufacturers in the U.S. With headquarters in Boise, Idaho, the company develops and makes memory and data storage solutions that are used in automobiles, consumer electronics (USB and Flash drives), communications products, servers, and computers. The publicly traded company recently pledged to make a major investment in new manufacturing facilities in the U.S.

Business Challenge

Nitin is the Director, Network and Security Services. He is responsible for the company's worldwide corporate information security for hybrid infrastructures, security platforms and services, security engineering, and operations.

Nitin's top challenge was achieving visibility across the network due to the many different sources of security data from multiple vendors and products. The company has a significant presence in all three major cloud security providers—Microsoft Azure, Amazon Web Services (AWS), and Google Cloud Platform (GCP)—as well as several on-premises private clouds and container services. An immense amount of data flows into the organization's complex hybrid cloud environment from such diverse sources as IoT devices, IT infrastructure, and manufacturing applications.

Nitin was also concerned about potential blind spots, inefficiencies, and security gaps as well as the need for continuous monitoring in public cloud environments.

Another concern of Nitin's was the ability to scale security to accommodate more security data and insights. He explains: "We wanted to define a simpler ecosystem of security partners that would help us provide more robust security in our hybrid environment and establish more predictable costs."

Resolution

Nitin shares they chose Gigamon as a key strategic supplier to support its hybrid cloud journey. Nitin installed GigaVUE® HC Series appliances at the organization's on-premises data centers, and GigaVUE Cloud Suite™ to manage the company's public and private cloud presence. He also chose GigaVUE-FM fabric manager to manage all the deployments.

"We embraced Gigamon as a partner to help us align with our enterprise strategy roadmap," Nitin remarks.

Benefit

Since deploying Gigamon, the company has seen huge cost savings by leveraging its Gigamon's data deduplication, packet slicing, and application profiling capabilities. "Now I can choose the data that is really supposed to feed into our network detection and response (NDR) platform," he notes. He went on to remark that Gigamon has helped reduce the volume of data going into appliances by 40 to 50 percent.

In addition to cost savings, the optimized data feeds have improved the organization's security posture by bridging visibility gaps in the data that enters the NDR platform, asset management and asset inventory platforms, and the intrusion prevention system. "Gigamon helped us plug all the visibility gaps in our environment and improve our efficiency around security operations. Time-to-response and time-to-resolve have dramatically improved," asserts Nitin.

Since deploying Gigamon, another benefit Nitin observed is how deep observability enables relevant business data to tag along with packet flow and application metadata. This provides a tighter, more coordinated cybersecurity ecosystem across every aspect of the business—products, technologies, and suppliers. For example, now that manufacturing data is feeding into the system, the company can move further along on its Zero Trust digital transformation path.

The customer is one of the first companies to embrace the Gigamon Precryption™ Technology, which enables security teams to inspect cloud traffic in clear text without decryption overhead, proxies, key management hassles, or intrusive embedded agents. The plaintext traffic is forwarded to the Gigamon deep observability pipeline and then forwarded on to tools for inspection and analytics. This helps security teams see where threat payloads might be hidden in encrypted lateral traffic.

"We are very excited about Gigamon Precryption™ technology ," says Nitin. "It helps us identify the weaknesses in the business workloads, in the containers, and in Kubernetes, and those types of serverless infrastructure. And that's really critical for us." He also points out how Gigamon Precryption™ technology is helping the company cut costs by reducing the compute pressure across the appliance infrastructure.

Looking to the future, Nitin contends that Generative AI will be driving even more data into organizations and creating additional challenges for cybersecurity leaders. They will have to manage enormous amounts of data as well as defend against more sophisticated and complex AI-based threats.

He states that businesses that want to stay ahead of the curve should strive to understand how to take advantage of AI-driven data. He stresses, "AI brings with it a great deal of complexity, and that's why you need to bring more automation, orchestration, and augmentation of network into your ecosystem."

He points out that a business should understand where the baseline level of traffic is at in the environment so that it can see anomalies and develop high-confidence indicators for focus areas. "Email and web are the most notorious channels for any kind of threat vectors, so we should focus on areas where we see anomalies and take advantage of high-confidence indicators to define the right profile sets and encryption strategies," Nitin asserts.

About Gigamon

Gigamon® offers a deep observability pipeline that efficiently delivers network-derived telemetry to cloud, security, and observability tools. This helps eliminate security blind spots and reduce tool costs, enabling you to better secure and manage your hybrid cloud infrastructure. Gigamon has served more than 4,000 customers worldwide, including over 80 percent of Fortune 100 enterprises, 9 of the 10 largest mobile network providers, and hundreds of governments and educational organizations. To learn more, please visit gigamon.com.

Gigamon®

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

09.25_01