

Customer Success

Leading U.S. telecommunications provider enhances security posture while reducing tool costs by 75 percent with the Gigamon Deep Observability Pipeline



For us, the Gigamon solution was an absolute necessity in securing our infrastructure and containing costs..

NETWORK PLANNER

Leading Telecommunications Provider

Challenge

- Improve tool efficiency
- Lack of network visibility
- NetFlow generation support and traffic intelligence

Solution

Gigamon Deep Observability Pipeline with:

- GigaVUE® HC Series Series visibility nodes with Inline Bypass
- GigaVUE TA Series edge traffic aggregation nodes
- GigaSMART® Traffic Intelligence with NetFlow Generation and Application Filtering Intelligence modules

Customer Benefits

- Decreased tool costs by 75 percent
- Simplified infrastructure by reducing 24 DDoS tools to six
- Gained the ability to deploy multiple security tools inline
- Customized negative heartbeat to determine proper tool performance

Challenges

When a leading U.S. telecommunications provider began to redesign its network infrastructure from the ground up, its first thought was security.

“Security should never be an afterthought,” said one of the company’s network planners, who is responsible for network tapping and security tool optimization.

“For us, good security starts with having complete visibility into our network traffic and so, we knew we needed a solution that would allow us to see all traffic across the network.”

The company’s top priority was finding a solution that could support NetFlow Generation, especially to help the security operations (SecOps) team with triage in the event of an attack. Additionally, the network operations (NetOps) team wanted a solution that offered advanced filtering capabilities to help future-proof the infrastructure for subsequent requirements or tool additions.

Solution

“We’re like family, NetOps and SecOps; and we work collectively to determine the optimal solutions for the best overall architecture,” said the network planner.

“You could say I learned about Gigamon through osmosis. The security team I used to belong to has a trusted relationship with Gigamon and had successfully rolled out Gigamon solutions to help with intrusion detection in our video hub offices. By all accounts, Gigamon seemed like a perfect match for our network upgrade.”

While the company looked at several vendors, it found that only Gigamon could support the requisite NetFlow Generation capabilities. Moreover, the Gigamon Deep Observability Pipeline offers additional traffic intelligence features like Application Filtering Intelligence – to improve tool efficiency and limit performance degradation, and Inline Bypass – to maximize network and security resiliency by detecting failure of an active tool and redirecting traffic to a standby tool. “My team was excited about the concept of a customized negative heartbeat, and Gigamon was

the only vendor to help us create this for our distributed denial of services (DDoS) devices,” said the network planner. “In conjunction with the regular heartbeat, we are now able to send our DDoS tools a negative heartbeat packet that they should drop. If this packet is returned – or in fact, if the tools respond to that physical-layer heartbeat at all – we know the tools are not functioning properly or consuming the necessary traffic, allowing us to troubleshoot quickly to mitigate security risks.”

Results

“If you’re in the process of building or upgrading a network, you need to ensure visibility into network traffic to help prevent attacks and ensure proper network operations. So, before you do anything else, get Gigamon – and get the access to and control of data you need,” said the network planner. “For us, the Gigamon solution was an absolute necessity in securing our infrastructure and containing costs.”

Today, the GigaVUE HC series sits inline between the provider networks and the underlying compute and storage architecture. All traffic passes through the GigaVUE HC series’ visibility node, where it can be redirected to the company’s DDoS tool. After scrubbing malicious packets, the DDoS tool then sends sanitized traffic to an open source cloud platform. Thus far, the company has been able to decrease the number of DDoS security appliances and reduce costs by 75 percent.

“While our most immediate requirement was to support SecOps – and feed the right traffic to the right security monitoring tools – we realized that with GigaVUE-HC2 sitting on the network, we could also provide other service assurance and operations teams with visibility into network traffic,” said the network planner. “In the future, we hope to see even greater efficiency gains thanks to the Gigamon solution.”

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.

**Worldwide Headquarters**

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

© 2022-2023 Gigamon. All rights reserved. Gigamon and Gigamon logos are trademarks of Gigamon in the United States and/or other countries. Gigamon trademarks can be found at gigamon.com/legal-trademarks. All other trademarks are the trademarks of their respective owners. Gigamon reserves the right to change, modify, transfer, or otherwise revise this publication without notice.