Case Study

University Health Network Identifies Ransomware Attacks with Gigamon

A couple of incidents that we had within the last six months we were able to catch quite quickly—within about an hour or so of the time the attacker took ownership of a server. We were able to catch them just in time before any real damage was done. And the reason is we have security tools in place, and Gigamon is feeding all the data into those security tools.

KAJEEVAN RAJANAYAGAM

Director of Cybersecurity, University Health Network

Challenges

- Gaining East-West visibility into the network
- Feeding traffic data to security tools
- Working within a resource-constrained public sector environment

Solutions

- GigaVUE® HC Series
- GigaVUE TA Series

Customer Benefits

- Provides improved visibility of traffic and East-West traffic
- Makes it easy to pilot new security tools requiring a network connection
- Feeds data to security tools without effecting performance of the switches
- De-duplicates traffic and decreases bandwidth requirements which extends life of legacy hardware

About the Customer

Canada's University Health Network (UHN) is a public healthcare organization funded primarily by the Ontario Ministry of Health. It operates four hospitals in Toronto that are affiliated with the University of Toronto. The organization is the largest hospital-based research program in Canada and conducts leading-edge research in cardiology, transplantation, neurosciences, oncology, surgical innovation, infectious diseases, genomic medicine, and rehabilitation.

Kajeevan Rajanayagam is the Director of Cybersecurity for UHN. He oversees a team of eight. Three of his team members work on compliance, and the other five are responsible for the technical implementation and management of security tools. While another team is responsible for the network, his team is responsible for three key areas of security: vulnerability management, network perimeter, and endpoint. For every product in the UHN security stack, Rajanayagam ensures that at least two of his team members—a primary and a backup resource—know exactly how it is configured and how to troubleshoot it if there is an issue.

Business Challenge

Like many healthcare organizations, UHN is primarily an on-premises environment, with 98 percent of its assets in virtual machines (VMs) and 2 percent in the public cloud. Rajanayagam points out that most of the information stored in the cloud is public information.

The initial reason UHN acquired Gigamon over four years ago was to address the need for visibility, including visibility into East-West traffic, in the network. "Visibility is the most important thing for any security team," asserts Rajanayagam. "The sooner we can catch something, the sooner we can isolate the incident and prevent it from causing damage."

Ransomware is a particularly pressing concern for Rajanayagam and for the healthcare sector in general. "Every time I read that another hospital is dealing with ransomware, I know that we could be the next target," he shares.

To improve visibility into the network, the team tapped into a span port to monitor traffic and network access using ForeScout. However, because it is not an inline appliance, it requires traffic to be duplicated. The team had also brought in other security tools that were not configured to be inline. They needed a solution that could provide visibility without impacting the performance of the switches.

Resolution

Gigamon was brought in to feed data to various security tools, such as Armis and Forescout. In the first phase, GigaVUE-HC1 appliances were added to the legacy environments. These copy the traffic, feed it to the tools, and de-duplicate the traffic. In the next phase of implementation, GigaVUE-HC3s and GigaVUE-TA200s will be installed to support higher bandwidth requirements of 40, 60, and 100GBs.

The set up was remarkably easy. Rajanayagam explains that it took one day onsite to stack and rack the appliances and connect them, and another two to three hours to configure them and get everything set up and running. "It was almost out of the box. Everything was done. We didn't have to touch our existing security tools or upgrade them. All the work was done within Gigamon," he asserts.

Benefit

Rajanayagam appreciates how easy Gigamon makes it to pilot new security tools. Though there are always two or three tools connected to Gigamon, there are still spare ports used to copy traffic for new tools that require a network connection.

Another benefit he points out is that Gigamon has significantly extended the life of existing products. "We don't necessarily have to worry about upgrading our existing hardware appliances, even though we are upgrading our core network," he asserts. That is because Gigamon is able to remove the duplicates and decrease the bandwidth so that the legacy appliances are still capable of handling the same volume of data.

Visibility is the most important thing for any security team. The sooner we can catch something, the sooner we can isolate the incident and prevent it from causing damage.

KAJEEVAN RAJANAYAGAM

Director of Cybersecurity, University Health Network

In the next phase, Rajanayagam will be exploring how to use the SSL decryption feature of Gigamon. "That is one of the priorities I want to focus on in 2024," he says. He foresees this feature providing value in multiple ways. It will provide savings on their processing costs and reduce the time it takes to decrypt. Also, it will increase the value of all of the security tools at UNH because currently they are blind to 60 to 70 percent of the traffic.

In the last six months, Gigamon has helped identify a couple of potentially costly ransomware attacks. In one incident, the attacker took ownership of a server, but the team was alerted to the threat. With the data feeds from Gigamon, Armis, and Forescout each caught an incident before any real damage was done.

Rajanayagam says that it is hard to put a value or a number on the potential cost of such an attack, because the attack was thwarted. But given that the incident matched the pattern of particular ransomware actors, he is confident that it would have been a ransomware attack. Fortunately, "We were able to catch it quite quickly—within about an hour," he shares.

About ISA Cybersecurity

ISA Cybersecurity is an IDC recognized full-service cybersecurity firm with over 30 years of delivering cyber services and solutions across 5 key practices including; Governance, Risk, Compliance Strategy, Architecture & Engineering, Assurance and Offensive Cybersecurity Services, Managed and Hosted Services plus, Digital Forensics & Incident Response Management. We partner with leading technology solutions to enable our customers to securely and safely support their clients, staff, and the general public at large. Learn more at isacybersecurity.com.

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 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 10 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