CASE STUDY

Gigamon®

Major US Retailer Leverages Pervasive Visibility to Solve Both Security and Operational Challenges

AT A GLANCE

Customer Benefits

- Provides greater visibility into the network than legacy solutions
- Offers use cases for operational tasks like decommissioning servers or diagnosing switch misconfigurations
- Focus on high quality detections helps prevent false positives

Gigamon Solution

- Gigamon ThreatINSIGHT

Challenges

Running a heterogeneous infrastructure at a campus HQ can be a complex undertaking. That's what a large clothing retailer was facing on its main campus: a large network sprawling across multiple buildings. They had different kinds of network detection tooling in several locations, but they needed better visibility across the entire enterprise.

The Director of Information Security knew that he needed a tool to give him visibility into the network—but not one that overburdened his team with a huge volume of security alerts. "I don't have a lot of people working in the department, so we don't have a lot of time to deal with false positives," he said. "I have an operational background and I have a pretty firm stance that too many false positives create noise and eventually everyone starts ignoring the alerts."

In addition to network visibility and detections, the team had a need to operationalize their new-found network visibility to also handle operational tasks, in addition to security. For example, in order to be compliant with the Payment Card Industry ("PCI") Data Security Standard, the team has to ensure all external traffic is using version 1.1 or higher of the TLS protocol.

Solution

This large US retailer chose Gigamon ThreatINSIGHT, a cloud-native, high-velocity network detection and response solution, to meet these challenges. ThreatINSIGHT consolidates intrusion detection, investigations and incident response in a single solution that rapidly scales to meet customer needs.

"If we want to investigate or detect something on the network, then we go to INSIGHT for it. Since detections are easy to build out in ThreatINSIGHT, we don't need to try and build out a lot of network detections in our SIEM."

Gigamon ThreatINSIGHT offers the ability to customize detections using rich, structured INSIGHT Query Language ("IQL"), to ensure that false positives don't waste their time. "ThreatINSIGHT detections are actionable — even the ones I design myself — and with the flexibility of the INSIGHT Query Language, I can filter out noise effectively," said the Director of Information Security.

The rollout process was smooth, thanks to the world-class customer team from Gigamon. "I love working with the INSIGHT team. I can shoot something over to them and will frequently get an answer back the same day," he said.

> "Gigamon ThreatINSIGHT is our go-to tool for detections. If it's something that's been detected on the network, then we go to ThreatINSIGHT for it."

Results

With sensors reporting back to the INSIGHT Cloud Data Warehouse, the team now can see its network from a more holistic perspective than it ever could before. Gigamon ThreatINSIGHT provides holistic network visibility to enable both security and operational moves. For instance, ThreatINSIGHT can provide:

- A quick event list showing what clients accessed a particular server over the previous 30 days, which can help the team decide whether or not that server can be decommissioned. Operational controls such as reporting if a session has TLS 1.1 or higher, an important component of their PCI compliance
- Troubleshooting operations: "A few weeks ago some end users started reporting lost connectivity. Investigation showed that the workstations were getting IP's from the wrong DHCP server. Because Insight can parse DHCP messages we were able to quickly isolate the day and time the problem started, and matched that up with a scheduled configuration change. Someone had misconfigured a switch, which caused a DHCP server on one VLAN to get bridged to another network. After we resolved the configuration problem, we built a detection in ThreatINSIGHT that will alert us if something similar ever happens again."

The large US Retailer Director of Information Security states, "Without ThreatINSIGHT, it would have been tricky to track back to the proper switch. We saved at least a week of multiple people's troubleshooting time. With ThreatINSIGHT, it took only an hour and a half to get to the root cause."

Overall, the IT team has found that Gigamon ThreatINSIGHT is a comprehensive tool for figuring out what's happening on the network. "Whenever a network problem comes up, we solve it using ThreatINSIGHT."

"ThreatINSIGHT detections are actionable — even the ones I design myself — and with the flexibility of the INSIGHT Query Language, I can filter out noise effectively."

About Gigamon

Gigamon is the first company to deliver unified network visibility and analytics on all data-in-transit, from raw packets to apps, across physical, virtual and cloud infrastructure. We aggregate, transform and analyze network traffic to solve for critical performance and security needs, including rapid threat detection and response, freeing your organization to drive digital innovation. In short, we enable you to run fast, stay secure and innovate. Gigamon has been awarded over 75 technology patents and enjoys industry-leading customer satisfaction with more than 3,000 organizations, including 80 percent of the Fortune 100. Headquartered in Silicon Valley, Gigamon operates globally. For the full story on how Gigamon can help you, please visit www.gigamon.com.

Gigamon®

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