Case Study

State Government Amplifies Network Power and Data Fidelity Using Deep Observability

> Gigamon is best of breed. It's helping us close the gap between what's observable and what's not on our network.

NETWORK ARCHITECT
State Government IT Office

Challenge

- Acquiring traffic data from multiple sources at high speed
- Automatically exporting traffic data to monitoring tools
- Gaining packet-level visibility into cloud traffic
- Complying with government cybersecurity and data protection regulations

Solution

- Network Taps
- NetFlow
- GigaVUE-FM
- GigaVUE HC Series

Customer Benefits

- Increased threat visibility across network
- Automated record generation and data exports
- Reaped operational savings from traffic optimization
- Decreased time to identify risk

This State Government's Office of Information Technology (IT) ensures secure and reliable access to internet and IT services for more than 11,000 state employees, state agencies, and its citizens, numbering more than 1.3 million. The IT team manage's network, voice, security, and infrastructure programs. Due to increasing internet service bandwidth and investment in infrastructure, one of their priorities is to build high-speed access to the major cloud providers and homogenize the cloud environments. As part of this effort, they are working to uplevel the security and visibility tools for cloud services so they meet or exceed current on-premises standards.

The state's network architect has been with the office for nine years and is responsible for the design of all network and cloud environments. With significant cloud-based developments on the horizon, his hope is that deep observability will provide access to all the traffic across their cloud infrastructure and the ability to inspect packets, flows, and application metadata. From there, the goal is to pass the relevant network-derived intelligence on to the cloud, security, and observability tools to amplify their power and fidelity.

Business Challenge

The state's IT office entered the world of network traffic monitoring through a switched port analyzer (SPAN). However, as their network matured and traffic increased, the value they received from the SPAN ports decreased. Visibility was low, and packets were being dropped. It became apparent that SPAN technology wasn't designed to monitor large-scale network traffic. SPAN ports were intended for troubleshooting traffic, not sustained and deep network monitoring.

Unchecked traffic was making it onto the state's network, inflating traffic cost and negatively impacting network speed, but the IT office wasn't aware of the scale of the problem at first.

"Our biggest challenge was gaining visibility into traffic at high speeds. We were overly reliant on SPAN ports and blind to threats," said the network architect.

This gap in visibility was putting the network at risk and jeopardizing the security standards they uphold in accordance with cybersecurity policies and regulations set by the state. The IT office required packet-level visibility in real time at high speeds. Beyond that, they needed to bring that data into security and performance monitoring tools to fully protect the network from malicious activity.

Resolution

Delivering reliable, cost-effective, and secure IT services to its citizens is the state IT office's mission. The network team works hard to reach that goal, and they need their technology to work even harder. Once the network architect realized that using SPAN ports to monitor traffic was ineffective and inefficient, he sought out a tool that could meet their visibility and monitoring needs.

Instead of relying on SPAN sessions, the network architect and his team investigated network taps to monitor network traffic continuously and efficiently. They discovered that taps offer visibility that SPANs could not into bi-directional network traffic at full line rate. Passive taps are always on, and all traffic is passed through them. The network architect knew this was the way to go, but he also needed a tool that would integrate well with the existing cybersecurity stack. Surprised by the simplicity of Gigamon implementation, he and his team launched Gigamon Network Taps as part of the Gigamon Deep Observability Pipeline to ensure consistent visibility to all network traffic across the entire infrastructure.

With all traffic data accounted for, the next step was to bring that data into the state's monitoring tools. The team chose NetFlow to set up automatic exports and bring records directly into monitoring tools. The state IT office also relies on the GigaVUE HC Series appliances to aggregate, filter, and forward traffic to existing security and monitoring tools. And to consolidate and simplify management, the team implemented the GigaVUE-FM fabric manager. The intuitive, customizable dashboard makes integration easy and automates policy creation and deployment.

"Gigamon is best of breed. It's helping us close the gap between what's observable and what's not on our network," the network architect said.

Benefit

As soon as the IT office implemented Gigamon, they immediately saw benefits. They had been experiencing continuous firewall issues, but, once they could fully see all traffic, they were able to pinpoint ongoing domain name system (DNS) attacks that were threatening the network. Additionally, they are now able to optimize traffic by eliminating duplications and by filtering application traffic, saving them time and money.

The network architect put it best when he said, “With the deep observability that Gigamon provides, we’re gaining access to all traffic across our infrastructure and amplifying the power and fidelity of our networks.”

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