Case Study

Riverside County Adopts Zero Trust Model, Delivering Secure Services to Millions

> By eliminating the noise from irrelevant data, our tools can now pinpoint critical information with greater accuracy. This leads to more reliable results and better decision-making. Today, we enjoy the peace of mind that the continuous uptime and reliability Gigamon delivers with a 100 percent ROI in less than 18 months.

ANTHONY H. CHOGYOJI
Chief Information Security Officer, Riverside County

Challenges

- Needed reliable access to and full visibility into network traffic to secure government data and resources
- Lacked integration with security tools stack to detect and respond quickly to attacks
- Wanted to maintain uptime while safely bypassing inline tools

Customer Benefits

- Improved network visibility and progressed toward a Zero Trust architecture
- Reduced mean time to remediation (MTTR) and increased efficiency
- Gained the ability to reconfigure systems without downtime using inline bypass
- Achieved ROI in less than 12 months

Solution

- GigaVUE-FM fabric manager
- GigaVUE® HC Series

About Customer

Riverside County, California is the fourth largest local government agency in the state and the tenth largest in the nation, sprawling from the suburbs of Los Angeles all the way to the border of Arizona. The county is serious about its role of serving its nearly 2.5 million residents and upholds its mission to improve their quality of life. With 25,000 employees and 500 facilities, the county provides many vital services to its residents, ranging from public safety to operating a fully-modernized, 439-bed medical center.

Anthony H. Chogyoji is the county's CISO. He and his lean team of six analysts manage the county's cyber security operations center (SOC), while overseeing the county's information security, privacy, governance, risk management, and compliance programs for the 44 departments and agencies that serve the county.

Chogyoji joined the County in 2008 and became the CISO in 2018. He was instrumental in building a highly advanced SOC for the county. He equipped the SOC with best-of-breed security tools, including an intrusion detection and prevention system, network and endpoint detection and response solutions, and a breach and attack simulation system.

Since then, the IT environment has evolved with the adoption of cloud services, including Amazon Web Services (AWS) and Oracle Cloud Infrastructure (OCI) and container technologies for application development. Chogyoji is incorporating cloud telemetry and network inspection and monitoring capabilities into his operations, which are foundational for observability in cloud infrastructures, as they provide deeper insights into performance, reliability, security, and bandwidth consumption.

ANTHONY H. CHOGYOJI
Chief Information Security Officer, Riverside County

Business Challenge

Despite having a vendor risk management solution in place, Chogyoji had serious concerns about the security postures of the county's hundreds of third-party vendors. He had witnessed neighboring counties fall victim to ransomware attacks that affected their critical infrastructure and observed that some suppliers had insufficient security preparedness. For this reason, he identified Zero Trust as a top initiative for the county.

"Our move to Zero Trust has more to do with our business partners, vendors, and outsiders than anything else," he explained. "Deploying a Zero Trust architecture is our number one goal."

Chogyoji is well aware that implementing a Zero Trust security framework requires a new way of thinking about network design. The focus must shift from looking at what's coming into the network, such as malware, to what's leaving the network, such as data, and ultimately creating a safe data lake that the 44 departments and agencies across the county can access and share. For example, whole health score intake forms are shared across all departments. With public safety and data safety always top of mind, Chogyoji wanted to ensure that county workers have secure access to a single source of protected data. To achieve this requires complete network visibility, but Chogyoji was only seeing about 20 percent of the lateral East-West traffic prior to deploying Gigamon.

Another challenge Chogyoji pointed out was the need for faster detection and response so that security breaches can be quickly identified and remediated. Though the county had a full stack of security tools for this purpose, the tools were only as good as the data flowing into them. With some cities a six-hour round-trip drive from the department headquarters, the county needed a solution that could be upgraded or reconfigured without physical recabling.

Resolution

The county deployed the GigaVUE-FM fabric manager to meet its visibility needs. The platform is used for inspection of out-of-band tools for lateral East-West traffic and inline tools for North-South traffic.

The county's network has two internet gateways at a primary and secondary site. There is a pair of GigaVUE-HC2 appliances deployed at the primary site, and a pair of GigaVUE-HC1 appliances at the secondary site. The secondary site handles mostly VPN traffic, and the GigaVUE-FM fabric manager provides visibility into logs from that traffic.

As Chogyoji continues to build out the county's Zero Trust security framework, he is also taking a deeper look into Gigamon Precryption™ technology, which will further extend visibility into cloud traffic, regardless of the form of encryption used. Precryption will help eliminate blind spots to threaten activity in the cloud by providing security tools with plaintext visibility, without the need for decryption. Gigamon Precryption generates network-derived application metadata that continuously verifies all network activity, following the Zero Trust principle of "never trust, always verify."

Benefit

Chogyoji calls Gigamon the county's "bullet-proof vest," protecting the organization from ransomware, data security and privacy breaches, and other cyberattacks that target local governments and the third-party entities they depend on.

"I honestly can't imagine how we would have been able to measure and realize the maximum effectiveness of our entire security tool stack had we not invested in our GigaVUE appliances," Chogyoji remarked. "It would have been a lot more complicated architecturally speaking—it may not even have been technically possible." The tools can also work more efficiently now because only the important traffic is shared to the tools and not all the noise."

The GigaVUE-FM fabric manager has proven to be the crucial element in Riverside County's vastly improved security posture. Chogyoji shared that his team was "obsessed" with the fabric manager's Inline Bypass feature. During upgrades, he said, "We'll place one of our IPSs into bypass mode temporarily just to ensure we are still seeing traffic flow. I can honestly that say we have not had a single interruption to our network, thanks to the Gigamon bypass module."

GigaVUE-FM has also saved precious staff time and resources. "It's been a huge timesaver to cable everything in advance," Chogyoji noted. "We route traffic when we need to move things around, then go into GigaVUE-FM and reconfigure everything on the fly with zero downtime."

As the county deepens its security measures and develops its Zero Trust security framework, Chogyoji and his team know that there are capabilities built into GigaVUE-FM that will take them there, including de-duplication and decryption. "Two of my staff attended Gigamon training, and it was an eye-opening experience for them," he says. "They reported back on how much they learned about the capabilities of Gigamon appliances, which inspired us to more fully leverage them today and in the future."

Perhaps more than any individual feature, the greatest benefit Riverside County has enjoyed is peace of mind and continuous uptime. "Just about every one of our tools flows through Gigamon at some point, even our cloud-based tools. It's the core for our internet. And it's one of those trusted products that does such a great job that you don't really think much about it. It's extremely reliable and does exactly what it's advertised to do. It's a rock-solid solution."

He adds that the county has also "… saved substantial amounts of money by deploying Gigamon. Fiscal responsibility and security are core values at the county. We don't want to just throw money at our tools—we need them to be effective—and Gigamon has met our criteria and then some. In fact, we achieved a return on our investment in less than 12 months."

About Gigamon

Gigamon offers a deep observability pipeline that efficiently delivers network-derived intelligence to your cloud, security, and observability tools, helping organizations eliminate security blind spots, reduce tool costs, and better secure and manage your hybrid cloud infrastructure. Gigamon goes beyond security and observability log-based approaches by extracting real-time network intelligence derived from packets, flows, and application metadata to deliver defense-in-depth and complete performance management. 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 worldwide. To learn more, please visit gigamon.com.

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