Case Study

# Clean Energy Power Company Uses Gigamon to Securely Integrate Mission-Critical OT Assets into its Core Systems

Gigamon has been a very good tool for us—a great fit. It makes packet captures and troubleshooting a lot easier, as well application and traffic analysis.

**CYBERSECURITY NETWORK ARCHITECTURE TEAM LEAD**
Clean Energy Power Company

## Challenges

- Improving visibility of network traffic
- Enabling reliable traffic packet inspection in a critical, high-uptime OT environment
- Performing data deduplication and optimization

## Customer Benefits

- Reliable traffic inspection with deep observability into the packet
- Visibility into East-West traffic
- Integration with other software tools
- Easier troubleshooting

## Solution

- Gigamon G-TAP® A Series
- Gigamon NetFlow Generation
- GigaVUE Cloud Suite™ for VMware
- GigaVUE® HC Series
- GigaVUE-FM
- GigaVUE® TA Series
- GigaSMART®

## About the Customer

This leading clean U.S. energy provider, with $40 billion in assets and a footprint in 24 states, prides itself on being at the forefront of the clean energy industry. One of its parent companies owns and operates a large portfolio of renewable energy generation facilities across the country, providing a wide variety of utility, commercial, and industrial customers with specialized solutions. The publicly-traded organization also serves millions of households on the east coast through its subsidiaries, which provide natural gas and electricity distribution.

The organization's cybersecurity network architecture team is responsible for the physical security that houses many of the company's industrial control systems (ICS). A separate division from the IT organization, the team deals primarily with the "bread and butter" of the business: the OT assets that are part of the Open Smart Grid Protocol (OSGP) infrastructure. The OSG protocol is a new set of open interoperability standards put forth by the OSGP Alliance in 2016 after its "smart meter" pilots to "revolutionize energy demand side management" and enable a smart grid energy infrastructure that is secure, sustainable, and affordable. The standards are needed to guarantee adoption of new technologies and standards for a "future-proof modern smart grid."

## Business Challenge

With the goal of securing all OT assets according to the new standards, the main investment area for the cybersecurity network architecture team is asset discovery. It's a lengthy process. The integration of the OT assets into the core systems is being done manually, for the most part, with a great deal of custom code development.

Although the organization has been a Gigamon customer going on 10 years, the team lead still remembers the problems he and his staff faced prior to partnering with Gigamon. "Our biggest challenge was lack of discovery and visibility into the OT Assets," he recalls.

## Resolution

The lead of the cybersecurity network architecture team explains how Gigamon currently fits into the organization's network. "We aggregate traffic from our legacy endpoints, our OT assets, and our physical security assets to our data centers. Gigamon basically sits in line at each of these data centers, and our data centers are air-gapped," he says. Air-gapped networks are frequently utilized in critical infrastructure and high-uptime environments to prevent attackers from accessing a system through an external connection.

Before the traffic data goes into the core systems in the data centers, it gets pre-aggregated, inspected, and deduplicated with GigaSMART tools installed on GigaVUE TA Series, GigaVUE HC Series, GigaVUE-FM, and GigaVUE Cloud Suite for VMware. The team lead calls these security gateways "meet me" points. "We backhaul the traffic from our fiber networks through the 'meet me' points that bridge our OT assets with our state-of-the-art data centers," he says.

The team also utilizes NetFlow Generation to further monitor and optimize the flow of data traffic. As the team lead explains, "We're using NetFlow as an outbound tool port to our NTA tool, which builds an overview of packet flows. It's technically a source destination and gives us a nice little dashboard. Then each of these outbound tool ports that are stationed at the 'meet me' points are collected and centrally stored on our platform in our centralized data center," he explains.

## Benefit

Gigamon supports the power company's phased process of gaining deep observability and securing their OT assets in a mission-critical environment. The team lead maintains that they may require dedicated physical hardware for certain things, even as the architecture evolves, but at the same time, he is very much looking forward to getting into the virtualization phase of the project. "The virtualization side of our OT is going to be a very exciting next step," he declares.

The organization uses VMware software, along with GigaVUE Cloud Suite for VMware, in their private cloud data center infrastructure, with no plans to move to a public cloud anytime soon. The priority is cybersecurity and asset discovery, and the organization is exploring an integration with the asset visibility and security platform to further that goal. The team has already integrated Gigamon with other partner tools, including Trend Micro TippingPoint for network intrusion prevention, LogRhythm for SIEM, Dragos for ICS and OT security, IronNet for advanced real-time network threat defense, and SolarWinds NTA for NetFlow.

“Any equipment can see source and destination, but inside the packet is what matters. Now we’re able to get a lot more visibility into the packet. We also observe more East-West traffic,” says the team lead. Gigamon’s enhanced visibility has also benefited the team’s ability to troubleshoot problems. “Gigamon has been a very good tool for us—a great fit,” he asserts. “It makes packet captures and troubleshooting a lot easier, as well application and traffic analysis.”

## 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.

Gigamon®

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



03.24_02