Major Water Utility Applies Joint Solution to Achieve Pervasive Visibility and Monitoring Across IT and OT Networks

> With the four Gigamon appliances, we're able to really see or capture all the entry points that we were looking for."
>
> SECURITY ADMINISTRATOR
> Water Utility Company

CHALLENGES

+ Lack of visibility into the OT environment
+ Burden of manually monitoring ports
+ SPAN ports potentially dropping monitored traffic at busiest times

SOLUTION

+ GigaVUE H Series
+ GigaVUE TA Series

CUSTOMER BENEFITS

+ Visibility into the OT environment that does not affect sensitive devices
+ Ability to monitor up to eight ports at a time on one device
+ Noninvasive, improved collaboration between OT and IT environment
+ Vulnerability management for both networks, with the ability to correlate known vulnerabilities

ABOUT THE CUSTOMER

With a major presence in the Northeast, this water utility company provides residential, business, and municipal customers with safe, pure drinking water and other water utility services. The company has hundreds of employees and operates multiple water treatment facilities and multiple water reservoirs situated among 3,000 acres of woodlands.

CHALLENGE

The team that handles IT and OT for the utility consists of many individuals. About half of the IT team members are contracted support staff, providing help-desk functions and consulting on engineering details for network cloud infrastructure upgrades.

The in-house team is a core group of professionals with strong technical skill sets. Together they manage the various vendors, nearly 50 at last count, and projects that arise in collaboration with a contracted project manager who keeps everything on track. Considering the team's breadth and depth of responsibilities, they are highly leveraged.

The OT side focuses on the day-to-day operations of getting water delivered and wastewater removed, while the IT side handles the network security. The company's security administrator, explains, "Our IT and OT networks are separate and managed separately—and we want that separation of duties." Looking to be able to do more with the staff currently in place rather than adding team members, the utility wanted to add tools that would enhance the team's visibility into network traffic.

The IT team initially ran into an issue with capturing monitored traffic from switched port analyzer (SPAN) ports. SPANs work best for ad hoc monitoring of low volumes of data in locations where test access points (TAPS) have not been installed.

"If a switch ever gets hammered with traffic – which might occur when you're trying to see the traffic that would be causing it – that's when the more passive function of a SPAN port would potentially drop traffic in favor of the things needed to keep the switch up," says the security administrator. Additionally, the SPAN method has its limitations on some equipment, with some devices only capable of running two concurrent SPANs.

Although network TAPs are preferred over SPAN ports, they are still the first step in the process of achieving pervasive visibility across an entire network. The IT and OT teams really wanted passive visibility into the OT devices: monitoring without deploying any sort of probing that could potentially hurt the network or network devices on the OT side.

"We've found that any kind of touch into that network, even a very light touch, can sometimes affect devices," the security administrator points out.

SOLUTION

The team asked their current vendors for recommendations for internet of things (IoT) security vendors. Armis came highly recommended. The team compared reviews, looked at what was out there, and decided to jump right in and start with Armis. Shortly after, they added Gigamon appliances.

"Once we deployed Armis and saw the limitations of getting visibility into the network traffic, we turned to Gigamon," says the security administrator. At first, the team tried to monitor all the traffic with SPAN ports, but they ran into problems, since switching and routing equipment has limitations as to how many SPAN ports can run at a time from a particular device. They weren't able to get all the feeds that they needed to funnel into Armis.

"That's why we turned to Gigamon. Now, with the four Gigamon appliances, we're able to really see or capture all the entry points that we were looking for," says the security administrator.

BENEFIT

A top benefit achieved by the joint Gigamon and Armis solution is that visibility into the OT environment has fostered improved communication between the IT and OT departments and clarified the mutual goals of the network teams.

As the security administrator puts it, "Giving our teams visibility into what's going on in their network is definitely a huge value-add. We're able to create different panes of glass for the OT and IT side based on what they need to see." The expanded visibility is helping the OT and IT environments integrate with the security team in a non-invasive, non-threatening way.

With Gigamon, the security administrator notes that the biggest value-add is being able to monitor up to eight ports at a time on one of the copper devices, with no loss of monitored traffic. With Armis, he says, "The primary benefit is the visibility – being able to correlate things that we're already seeing in the network with the additional view that Armis provides."

He also highlights the added benefit of vulnerability management provided by Armis. He says Armis is valuable to be able to see devices on the IT and OT side that they didn't even know were there and then can correlate them with known vulnerabilities.

The manager of IT infrastructure adds that he really appreciates the partnership and account management that came with the vendor relationships, as it helps their highly leveraged team to fully utilize the two tools. He says, "The tools are sophisticated, and it takes some time and effort to make sure that they're working to maximum capacity. Throughout the entire engagement, Armis and Gigamon bent over backwards to provide support and advice. Working collaboratively with these two vendors has been an all-around positive experience for us."

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.

ABOUT ARMIS

Armis is the leading unified asset intelligence platform designed to address the new threat landscape that connected devices create. Fortune 1,000 companies trust our real-time and continuous protection to see with full context all managed, unmanaged assets across IT, Cloud, IoT devices, medical devices (IoMT), operational technology (OT), industrial control systems (ICS) and 5G. Armis provides passive and unparalleled cybersecurity asset management, risk management, and automated enforcement. Armis is a privately held company and headquartered in Palo Alto, California.

Gigamon®

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