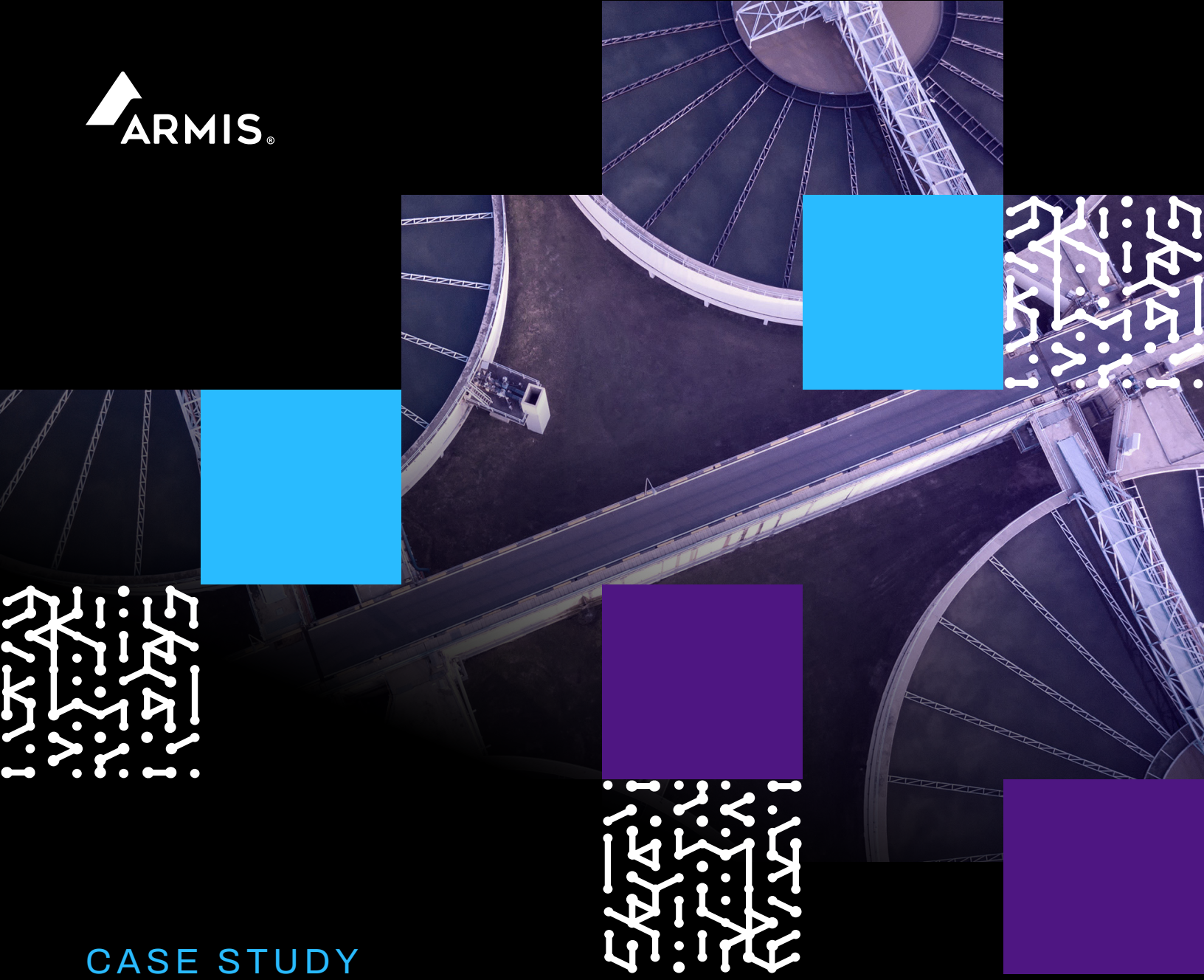

CASE STUDY

Water Utility Gains Passive Visibility into OT Assets Without Affecting Sensitive Devices

Enhanced visibility into OT network helps secure and protect drinking water for millions of people

Industry

Water Utility Services

IT environment

Over 1,000 IT and OT assets, including water pumps and valves

Introduction

This major U.S. water utility needed a nonintrusive way of seeing devices in its sensitive OT network while ensuring service continuity. The OT network is managed separately from the IT network, yet both are under the same security umbrella. By deploying Armis in combination with Gigamon's deep observability into network traffic, the security team achieved full visibility into the utility's OT assets, along with deeper visibility into the traffic traversing the IT and OT networks.

With hundreds of employees operating multiple water treatment facilities and reservoirs, this regional water utility serves millions of residential, business, and municipal customers with clean, safe drinking water. A small in-house team of skilled professionals manage IT and OT for the utility. Due to its small size, the IT/security team heavily utilizes contracted and vendor support to efficiently manage its responsibilities.

The utility's security administrator, in particular, has played a leading role in maturing the organization's security program. When he started with the utility company seven years ago, there was a strong need to bring in professionals, software, and hardware to establish a foundation for the utility's security.

"We've been evolving from doing the basic things such as getting a good firewall, spam filters, and web filters to then looking at advanced solutions like Armis and next-generation endpoint protection. We're continually trying to evolve and keep up with the industry, and that's what led us to Armis about two years ago," remarked the security administrator, who is solely responsible for purchase decisions of new security products and tools.

The need for passive visibility into OT assets was the key driver for Armis deployment

The majority of the utility's OT assets are related to cleaning, moving, and storing water. "If there is a major vendor that is a provider of equipment for that, it is probably in our environment," the security administrator explained. With the IT and OT environments being managed separately, there was a need, from a security perspective, for visibility into the OT environment. Yet, for a while, the team avoided scanning the OT network because of the sensitive nature of the OT devices.

Even performing simple scans to create an inventory of OT devices would cause issues. He pointed out that any company that lacks visibility into an OT environment likely has hardware or software that is sensitive to scanning. "But there is definitely the need to see what was going on in there and have some sort of reporting," he said. "Where that is the case, Armis can provide an immediate value-add." Armis provides 100% passive traffic monitoring that won't disrupt sensitive environments.

Close collaboration with Armis made for a smooth deployment

The team started out with a proof-of-value (PoV), working closely with an Armis engineer to deploy and configure the solution. "The PoV showed us what life would be like going with Armis," said the security administrator. He noted that working with Armis has been markedly different from his experience with other companies, which essentially left his team on their own after the purchase was made.

"We've definitely found that's not the case with Armis," he commented.

Challenges

- Gaining visibility into OT assets
- Enabling passive visibility so as not to impact sensitive devices
- Decreasing overall risk to the organization
- Prioritizing vulnerabilities

With the help of Armis experts, the security team fine-tuned the rules to filter out unnecessary alerts for guest and personal devices. Even after filtering out the excess noise, the team discovered over a thousand devices on the network that they did not have visibility into previously.

Up until three months ago, the security team was having regular weekly calls with Armis, but they are now having bi-weekly calls. "It's been a good experience in terms of the interaction with Armis on the product side," he added.

The Armis-Gigamon integration provides traffic inspection and improves OT security posture

After the initial deployment, the team realized there were some limitations in terms of getting all the feeds that they needed into Armis. The issue had to do with capturing monitored traffic from switched port analyzer (SPAN) ports, which work best for monitoring low volumes of data and can potentially drop traffic if the switch gets overloaded. By swapping the SPAN ports for Gigamon network test access points (TAPS), the team was able to capture and see all the traffic in a noninvasive way. "Once we added that, we saw thousands of devices pretty immediately. The network TAPS just see everything," noted the security administrator, adding, "That was probably what gave us the biggest visibility from a traffic standpoint."

The Armis-Gigamon integration enabled the team to see traffic that they could not inspect prior to this implementation. The security administrator shared an eyebrow-raising story from when they first deployed Armis: "We had internet access pretty tight, down to ports that are necessary for various types of devices to talk to each other. Keep in mind that, for someone to access the internet, they would need to have rules on both firewalls to allow that to begin with. We don't allow all traffic between the OT networks. That said, when we first deployed Armis, we saw devices doing DNS lookups to Russian and Chinese domains." Fortunately, there were always firewalls and tight firewall rules in place between the IT and OT environment. Prior to the Armis deployment, there was no way to inspect the traffic and detect DNS requests.

"We'll get notifications from industry partners on new exploits found in the wild. We can then go into Armis and, at the same time, it will have the up-to-date vulnerability information and already have the devices listed that might be affected. We can sort by the highest vulnerabilities in our environment."

Security Administrator
Water Utility

Additional integrations advance vulnerability management capabilities

Aside from Gigamon, Armis is integrated with the utility's internet firewalls, VPN firewalls, a multi-factor authentication tool, a virtualization platform, an identity management service, and an endpoint protection solution. On the hardware side, Armis is integrated with wireless controllers. The security administrator leveraged the prebuilt integration templates from Armis, which made the job easier and worked seamlessly.

A secondary use case for Armis is vulnerability management. The security administrator appreciates the fact that Armis is device-agnostic, unlike other vulnerability management consoles that only show vulnerabilities for specified devices. "With Armis, if you have a web vulnerability, it will show you every type of device that falls into that category," said the security administrator, adding that he finds it helpful to see vulnerability information in addition to threat activity.

Another Armis capability the team plans to leverage is the quarantine feature. The security administrator tested this with one of the devices in IT and verified that, within seconds, the potentially malicious or infected device was automatically disconnected from the network by Armis. "It's definitely good to know we have that capability if we ever need it," he said.

The security administrator also appreciates how Armis provides prioritized lists of devices that may be affected by a newly discovered vulnerability, saving his team a great deal of time and effort. "We'll get notifications from industry partners on new exploits found in the wild. We can then go into Armis and, at the same time, it will have the up-to-date vulnerability information and already have the devices listed that might be affected. We can sort by the highest vulnerabilities in our environment." With a small and highly leveraged team, time-saving features like these have made a big difference, allowing the team to focus on other priorities rather than spend time on threat-hunting.

Armis Results

- Provided full visibility into OT assets
- Enhanced security posture
- Prioritized vulnerabilities for the highly leveraged security team

Armis, the asset intelligence cybersecurity company, protects the entire attack surface and manages the organization's cyber risk exposure in real time.

In a rapidly evolving, perimeter-less world Armis ensures that organizations continuously see, secure, protect and manage all critical assets.

Armis secures Fortune 100, 200 and 500 companies as well as national governments, state and local entities to help keep critical infrastructure, economies and society safe and secure 24/7.

Armis is a privately held company headquartered in California.

1.888.452.4011

Website

Platform
Industries
Solutions
Resources
Blog

Try Armis

Demo
Free Trial