CASE STUDY

How a California Water and Wastewater District Leveraged Fortinet Solutions to Protect Critical Water Treatment

Most residents of U.S. cities and towns are fortunate enough to take local water and wastewater service for granted. When we turn on a tap, we expect water to flow—likewise when we flush a toilet or run water down a drain. But for the agencies that provide these services, keeping water moving is a complex business. They rely on physical operational technology (OT) devices that require reliable Ethernet network connectivity to generate alerts for any process anomalies that might impact the cleanliness, safety, and availability of the water they supply.

"In an IT setting, if something goes wrong and systems shut down, users may get upset because they cannot access their email," says Web Jessup, CEO of JEGO Systems, a Roseville, California–based systems integrator that specializes in cybersecurity, networking, infrastructure, and related services for water and wastewater districts. "By contrast, the shutdown of an OT system may put customers' health, or even their lives, at risk," he continues.

One example widely reported in the media in 2021 was an incident in a Florida town in which an individual inexplicably changed the chlorine levels at a water treatment plant. While monitoring the process through the human-machine interface (HMI), the plant's operations team caught the problem in time to correct it before any damage was done. In the alternative scenario—had the devices not provided this level of visibility and had the staff not recognized the problem right away—hundreds of thousands of local residents could have been harmed.

Poor Security Controls Put OT Availability at Risk

Uninterrupted availability is absolutely crucial for OT devices. That is why one water and wastewater treatment district in Central California, which serves around 30,000 residents, turned to systems integrator JEGO Systems for help managing its OT infrastructure.

The district had previously engaged a different systems integrator to design and implement a supervisory control and data acquisition (SCADA) system and the underlying network and security infrastructure components. Unfortunately, the firm did not provide the district with access credentials or network and firewall configurations. Thus, the district's staff could not make even the most minor changes to their network, such as adding or deleting user credentials for network devices. Any time staff required a change, they had to request the update from the systems integrator, which would perform the task on its own timeline.

"Before, all the network components were a black box to the water and wastewater treatment district. With FortiGate firewalls and FortiSwitch with FortiLink, we have given them visibility to the network layer they never had before."

Web Jessup
CEO,
JEGO Systems

Details

Customer: Water and Wastewater Treatment District

Industry: Power and Utilities

Location: Central California

Business Impact

- Safer drinking water for area residents
- Significantly improved OT security through better visibility into the network and OT devices

Although the district's staff does not include any cybersecurity specialists, managers recognized the risks in their OT environment. For one thing, they were concerned that the systems integrator may have left backdoors in the network and security infrastructure through which its personnel could potentially access the district's OT devices. They also worried that, if a systems integrator disabled OT monitoring devices, there would be no way to track who had made the changes. Network security seemed to be an afterthought for the systems integrator even as the project was underway, and the district was not comfortable moving forward with the infrastructure the firm had developed.

The district engaged JEGO Systems to increase the security of its OT devices. As JEGO Systems helped guide the district through a needs assessment and solution selection, ease of use was a key consideration. Connecting to multiple devices via a command-line interface (CLI) would have been beyond the capabilities of the operations team, and the district did not have the time or budget to hire network and security experts. Instead, operations staff needed to be able to perform basic troubleshooting and make minor network and security adjustments through a graphical user interface (GUI). In addition, the water district wanted to receive timely notifications any time a potential security incident occurred.

Another criterion for new solutions was deep visibility into the current state of the district's OT network. Operations staff should be able to answer questions such as: Who is logged in to the network? In particular: Who is currently connected remotely via a virtual private network (VPN)? Communication with the programmable logic controller (PLC) is interrupted: What is happening with the switch? Decision-makers wanted to be able to provide systems integrators or other third parties with remote access so that they could support troubleshooting efforts that may require the assistance of a subject matter expert. Still, they wanted strict control and visibility around these remote sessions to mitigate the additional risk of external network access.

Finally, the district required multi-factor authentication (MFA). One of the reasons the management team worried about their legacy systems integrator was that the firm's staff used the same credentials (username/password) to log in to the district's systems, so there was no way to know who was doing what within the network. Although that firm would no longer be working on the district's systems, employing MFA would prevent the possibility of such sloppy security practices in the future.

Business Impact (cont.)

- Reduced risk of unplanned OT downtime, thanks to timely notifications about possible security issues
- Empowered operations team to troubleshoot issues, as well as add or delete user credentials

Solutions

- FortiGate Next-Generation Firewall
- FortiSwitch
- FortiToken Mobile
- FortiLink

"Visibility is great with Fortinet solutions. Fortinet is cost-competitive, and the products are highly reliable. Plus, the entire ecosystem is very handy."

Web Jessup
CEO,
JEGO Systems

Providing Visibility into the Networking "Black Box" for Nontechnical Staff

Based on these decision factors, JEGO Systems provided the district with a turnkey solution that involved Fortinet networking and security technologies. First, the firm rolled out a pair of FortiGate Next-Generation Firewalls (NGFWs), whose GUI management interface enables nontechnical operations staff to adjust users' access credentials and troubleshoot the environment.

Staff can also configure the FortiGate NGFWs to send notifications if they detect a security issue and to alert the operations team whenever an approved vendor logs in to the environment. These notifications are crucial in ensuring the district is aware of every incident and that the operations team dedicates the right resources to resolving it.

JEGO Systems also deployed FortiSwitch secure enterprise switches and enabled the FortiLink protocol, which turns the switches into a logical extension of the FortiGate. The result is tight integration between the FortiSwitch devices and the FortiGate NGFWs for single-pane-of-glass management of both security policies and network switch configuration. Now, operations staff at the district manage 100% of the district's VPN users.

"JEGO Systems will set up policies, rules, and destinations for users in a certain group so that members of that group can get to only the network resources they need," Jessup says. "Then, as the district's staff add new users, they add them to a specific group, which controls what the new users can access."

Thanks to the notifications they receive, the district's operations staff are also undertaking lightweight troubleshooting of network issues. Through FortiLink, JEGO Systems added tag names to the switch ports that the district's OT devices connect to—including its HMIs, PLCs, and variable frequency drives (VFDs)—and associated each device to a specific port on the FortiSwitch switches. This notification feature facilitates faster identification and troubleshooting of the affected devices, should a port experience a problem, because the district's operations staff find it easier to search for a device tag name rather than to remember its IP address.

"Before, all the network components were a black box to the district," Jessup says. "With FortiGate and FortiLink, we have given them visibility to the network layer they never had previously, from port status to cable testing, even to the trunks between ports. We chose Fortinet for this organization because once we installed the firewalls and switches and trained the district's staff on them, people who are not cybersecurity or network experts could use the system very effectively. Fortinet is very user-friendly, and it is enterprise-grade equipment."

> *"We chose Fortinet for this organization because once we installed the firewalls and switches and trained the district's staff, people who are not cybersecurity or network experts could use the system very effectively. Fortinet is very user-friendly, and it is enterprise-grade equipment."*
>
> **Web Jessup**
> CEO,
> JEGO Systems

When network or security issues require third-party support, JEGO Systems uses FortiCloud to manage the district's Fortinet devices remotely. "FortiCloud is unique in how it allows us to gain access to the FortiGate NGFWs," Jessup says. "For example, we had a situation where we enabled a setting by mistake, and users ended up locked out. Because of FortiCloud, we were able to get back in and change that. Tunneling from FortiCloud to the FortiGate is extremely helpful when performing remote services."

JEGO Systems also deployed FortiToken Mobile for the district. FortiToken Mobile provides two-factor authentication, acting like a hardware token but residing on the user's iOS or Android mobile phone.

Security Confidence Derived from the Fortinet Ecosystem

Ultimately, this initiative has made the district's OT devices much more secure, increasing the safety of area residents. In addition to alerts from OT systems, district staff also get network alerts now. "Sometimes it is as simple as an unplugged cable," Jessup says. "They can see where the problem is, and with the tag names in FortiLink, they can immediately know which device is connected to the port. This visibility is extremely handy when they need to troubleshoot a problem quickly."

Similarly, Jessup adds, the district now has the capability to set up alerts for certain security events. "They can set the FortiGate to notify them, for instance, anytime malware or viruses are detected, in the event of any network traffic violation, or when an approved third-party vendor logs in to the environment," he says. "Then, suppose there is something wrong with a certain lift station while a particular vendor is logged in. The district's operational team can recognize that correlation and check whether there is an issue."

The water and wastewater district is now far more confident in its security posture. And Jessup is confident in JEGO Systems' selection of Fortinet as a network and security partner. "Visibility is great with Fortinet solutions," he concludes. "Fortinet is cost-competitive, which is extremely helpful for getting solutions into customers' hands. And the products are highly reliable. Plus, the entire ecosystem is very handy."

May 10, 2023 12:00 AM

2145502-0-0-EN