BAYSHORE NETWORKS
INDUSTRIAL NETWORK SECURITY

Field Application
Case Study: Water

Large Metro Water Utility and Treatment Plants
Capital City in Southern State, USA

BACKGROUND

"Southern State, USA's" capital city is the largest in the state. Its water utility serves nearly 500,000 households and businesses. It also uses two separate water treatment facilities to provide a combined capacity of nearly 160 million gallons processed per day. Primary water sources are drawn from two natural lakes that feed into a large nearby reservoir.

The utility began a slow but comprehensive upgrade to its SCADA system, revising operations and processes at 20+ remote storage tanks and 20+ booster pumping stations, all managed from a centralized control room. They had a heterogenous OT environment with a mix of vendor equipment and software from Rockwell, Schneider Electric and others, plus Check Point firewalls at perimeters.

CHALLENGES

Like many others in the water industry, the plant's network architecture was largely flat, allowing anyone who gained access to connect to any asset in the production environment. This was seen as essential to keep things running when fast problem-solving was needed. Budget and staffing constraints made large-scale changes unfeasible, because they would result in a rate change approval request, which was always politically difficult.

Management had previously focused most on physical security, but rising incidence of successful malware and other types of cybersecurity threats had caused concern. They were less concerned about nation states and malicious attackers. The majority of their disruptions occurred from unavoidable security gaps in operations which allowed honest errors and (mis)use by employees, third parties, vendors, and others. However, they also knew those same weaknesses could be leveraged to cause them to become disrupted and potentially victims.

The customer agreed that their perimeter firewalls were important but wouldn't be enough given how connected they and their vendors were becoming. They used third parties for point-to-point wireless connections to some remote sites, and their IT team had an increasing interest in monitoring operations. They had a short checklist of requirements to begin the search for a technology partner to help shore up obvious weaknesses:

- **The solution had to install alongside (not replace) existing SCADA systems**
- **Would not require downtime**
- **Would not introduce complex or time-consuming changes to their existing networks and processes**
- **Not difficult to install and manage by operations staff, without the need for IT**
- **Able to protect assets against malware**
- **Was cost-effective**
- **Provides a solid answer when asked by leaders in the business community, "What have you done to secure the city's water?"**

SOLUTION AND DEPLOYMENT

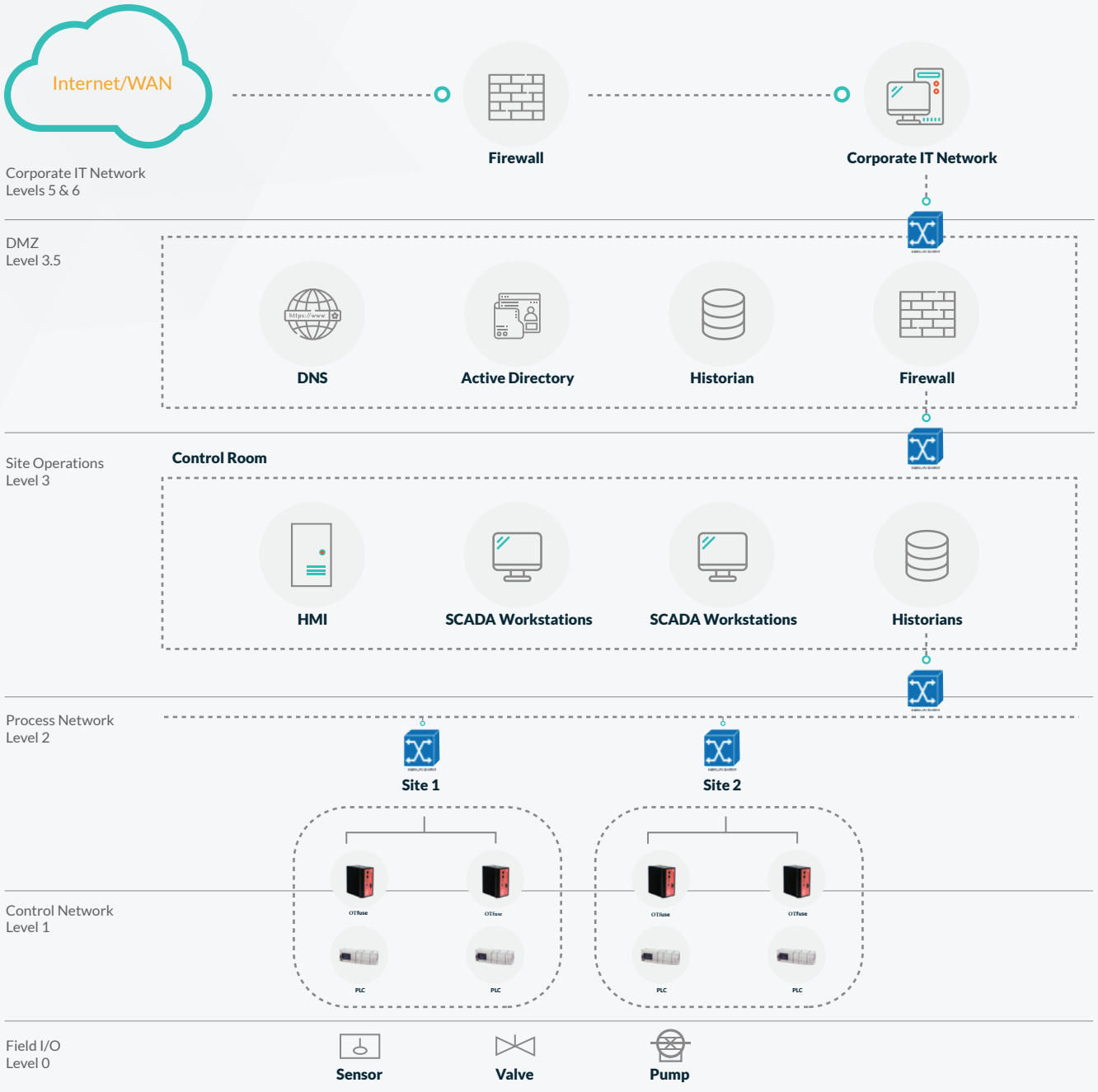
In mid-2019, the plants began the installation of Bayshore security appliances, starting with the OTfuse® Industrial Security Appliance. Although IT maintained the plants' perimeter firewalls and the DMZ, the operations team liked the purpose-built industrial DIN-rail format, allowing them to place the solution closer to the critical assets such as at remote pump stations.

Reference Deployment Architecture

(simplified Purdue Model)

In the early stages of deployment, the plant engineering team were surprised that the entire implementation took place in less than an hour, with no network downtime. Then, after operating in a "learning mode" for 48 hours, they were able to examine traffic they were not expecting, including native OT protocol activity they didn't know was on the network.

Now, OTfuses are also protecting critical systems with direct connections into the central control room. They report status via the SCADA HMI management consoles, displayed in real time alongside other critical plant operating factors.



BENEFITS & EXPANSION PLANS

This water utility was quickly able to deploy strong security and enforce policies for their PLCs and other essential equipment without having to change processes or network architecture.

Cost Savings

Clearly, the solution went in without requiring network changes. There were obvious cost savings to the immediate benefit of increased cybersecurity without requiring a significant project, cross-functional coordination, IT time, OT time and potential downtime for production.

"Stronger mandated cyber-security requirements are coming, and this puts us ahead of the curve. It also gives our community some confidence that we're aware of the threat climate and are taking action."

Operations Management, Regional Water/Wastewater Utility

Further, given what was now being seen in advance of major incidents, the engineering team recognized benefits such as:

- **Maintaining safety and availability of production systems by enforcing consistent behaviors related to PLC access, functionality, update schedules, etc.**
- **Removing the need for human troubleshooting and potential clean-up costs when something unexpected occurs. At machine speed,** OT**fuse can enforce automated protection, and while there still may be troubleshooting to occur as to root cause, etc at least the processes will continue unaltered and investigations will have traffic, alert and log information from** OT**fuse.**
- **This organization had scarce human resources and minimal cybersecurity skills. They relied on outside organizations and the time-to-resolve could take hours in some instances when an incident occurred. The control room could now centrally see and manage plant resources for ICS safety and security. Processes to support the smooth, safe, and cybersecure operation of the water utility could be developed without being in the middle of a crisis.**
- **When security incidents such as fast-moving malware occur, there is a cascade of collateral costs that can be avoided such as risks to human safety, water supply and distribution, negative public opinion, communications regarding the crisis, etc.** OT**fuse automatically inspect traffic for malware and can respond to protect the assets from infection.**

Deployment Speed

This water utility was quickly able to deploy strong security and enforce policies for their PLCs and other essential equipment without having to change their processes or network architecture. Even in scenarios where they might have discovered an unintended operating condition, it relied on one of their SCADA tools generating a useful alert in the control room, and an operator seeing that quickly enough to undo the condition and restore normal operations. If that takes five minutes on a main feed line, potentially a half million gallons could have moved through under unsafe conditions.

Public Safety

With OTfuse's ability to provide instant protection from unintended instructions, the erroneous instruction which might have tainted half a million gallons and caused a public health advisory would instead have been blocked before it took any action on the relevant part of the plant.

Process Improvement

The customer also experienced process improvement because not only is there no public notice required, but they have the opportunity to understand where that bad instruction came from and take steps to address and avoid that risk in the future, without the crushing pressure of emergency response timelines.

Future Expansion Plans

Having achieved success during the initial trial deployment, the water utility/treatment plant has budgeted significant funds for the next five years to scale up the deployment of Bayshore security solutions. These will include not only added OTfuse, but also NetWall™, to enable further connectivity to protected domains for their SCADA system data via replication techniques.

For more information and a discussion about your site needs,
Email **info@bayshorenetworks.com.**

BAYSHORE

© 2020 Bayshore Networks Inc.