FIREEYE™

CUSTOMER STORY

Utility District

When Federal Requirements Raise Security Stakes

FACTS AT A GLANCE

INDUSTRY

Government

SOLUTIONS

- FireEye Network Security
- FireEye Email Security
- FireEye Multi-Vector Virtual Execution

CUSTOMER PROFILE

A local water and sewer municipality serving 75,000 people spread across six cities. The utility has five major water reservoir sites, 10 sewer pumping stations and multiple connections to the regional water supply network, as well as many links with adjacent cities. It also serves a major regional hospitals.

A 1998 American Presidential directive set up a national program to identify critical infrastructure components that needed elevated protection from possible terrorist attacks. Critical infrastructures can include any element that supports emergency services, telecommunications, energy, financial, water, food, transportation sectors, and anything involved in ensuring continuity of government.

Given the year of its launch, the executive order was naturally biased towards the protection of physical components, but the exponential surge in cyber threats has widened thinking to include items such as digital assets and Internet-connected infrastructures.

The IT director for the utility district, observed, “Our security model was no longer comprehensive enough.” The utility had conventional firewalls and endpoint virus protection, which could not be relied on to be effective against sophisticated attacks, such as advanced persistent threats (APTs), custom malware and phishing attempts that were increasingly targeting it.

The utility also needed greater protection for its internal network, which included supervisory control and data acquisition (SCADA) systems, remote

> "In all 60 cases of multi-stage malware seen in the wild, the FireEye platform correctly identified and managed the attacks — a 100% success rate!"
>
> — **IT Director**, Utility District

sites such as water reservoirs, and mobile sites, including trucks and handheld devices, such as tablets and phones.

Not Another Newspaper Headline
At first, conventional layers of defense were deployed, consisting of hardware-based virtual private networks (VPNs) and intrusion protection systems (IPS) from the incumbent firewall vendor. Signature-based malware scanning was instituted for endpoints and a spam-filtering appliance was installed. The utility's web presence was segmented with a "demilitarized" zone (DMZ), intranet, and SCADA for remote telemetry of water and sewer sites.

Still, the IT director was uneasy because he knew it wasn't enough. For example, his endpoint antivirus defenses only reacted to malicious communication and code after a payload had been executed. Additionally, the reporting, logging and monitoring capabilities were not nearly comprehensive enough to battle increasingly sophisticated threats.

"I didn't feel we were ahead of the curve with security," said the IT director. "We were just holding our own and hoping we wouldn't be next." He already had insights into the experiences of a small nearby city that had been overrun by malware to the point that a botnet controlled all the PCs in the city administration, public works and police department! The city's IT department spent more than three months eradicating the intrusion. In addition, another city lost $400,000 in a cyber attack, and a nearby hospital was defrauded out of more than $1 million by hackers.

"I didn't want to be another headline in the newspaper," the IT director reflected. "We needed a modern, multi-layered and proactive defense."

Analysis Leads To FireEye
The IT director wanted to start by hardening the communication tunnels that the utility district deployed to its vehicles and tank sites. He also wanted to implement detailed reporting capabilities down to the endpoint level.

His own research and industry reports led him straight to FireEye and its market-leading incident response services from FireEye Mandiant Consulting.

The IT director liked that the FireEye Network Security platform offered behavioral analysis and real-time protection again custom malware, APTs and zero-day exploits.

A Smooth Implementation
The IT director configured FireEye Network Security for inline operation at the ingress and egress points of each subnet. "The platform was very easy to deploy," he recalled. The dual-port capability enables the utility to monitor its DMZ perimeter and intranet separately. In this configuration, the unit blocks web exploits, multi-protocol callbacks and multi-stage malware in real-time, as they occur.

"I was fascinated by the FireEye approach to analyzing new threats," says the IT director. "The FireEye Multi-Vector Virtual Execution (MVX) engine analyzes what the threat does in an isolated environment and reports on it, sharing the results to the cloud to warn other installations."

The utility also installed hardware firewalls at both ends of the network for its VPNs. FireEye Network Security was installed between the firewalls and the intranet switch, as the last line of defense. To fully leverage the utility's investments, all local and remote traffic is routed through the FireEye platforms deployed at the headquarters location: "We've architected the environment to ensure that there are no weak links and that everything has to go through the industrial-strength scrutiny of the FireEye solutions," commented the IT director.

A Shared Intelligence Community
The FireEye Network Security communicates information on real-time threats and attacks back to FireEye. The company uploads this information into its global database to alert all customers of the latest security challenges. The utility, in turn, gets the benefits of this near-real-time sharing of threat intelligence from FireEye deployments around the world. "Because of the immediacy, an exploit doesn't have much time to gain a foothold," described the IT director.

Deployed in inline mode, FireEye Network Security immediately identifies and proactively blocks anything

malicious that has passed through the firewall and reports it to the security team. "The very few false positives we initially received were minimized by minor adjustments of a few parameters," he recalled. The utility also subscribes to FireEye Managed Defense to provide an additional layer of protection for itself. "Managed Defense gives us access to broader set of capabilities without having to recruit additional headcount in an already overly competitive job market. Having this caliber of expertise and technology on call when we need it most really gives us the best of both worlds."

The IT director uses reports of blocked servers to contact his colleagues in other cities, districts and organizations to let them know they have an infected host. He also has implemented two-factor authentication and remote hardware-level encryption to minimize exposure.

The utility relies on FireEye Email Security to protect its email. "My decision to deploy this was heavily influenced by the positive results we had with FireEye Network Security," explained the IT director.

In the 12 months since deploying FireEye Network Security, the utility successfully resolved 12 signature-based alerts and 220 intrusion prevention system (IPS) events without incident. The IT director finds great value in FireEye Network Security because it shows him the exact types of attack attempts and probes that are occurring. He stated, "FireEye Network Security tells us where we need to enhance our defenses. FireEye keeps us informed: Everything starts with the data!" FireEye gives the utility insight into security issues that previously weren't known, helps harden its security stance and makes the utility better prepared for when a genuine alert sounds.

The IT director concluded, "We recently blocked several serious targeted attempts sourced from both email and websites—including ransomware and credential stealing—where FireEye more than proved its worth.

"It's critical to ensure there's a process to deal with the malware that's caught: No one wants to become the company that ignored a threat. With FireEye we are much more confident that we're prepared for whatever happens."

To learn more about FireEye, visit: **www.FireEye.com**

FireEye, Inc.
601 McCarthy Blvd. Milpitas, CA 95035
408.321.6300/877.FIREEYE (347.3393)
info@FireEye.com

©2019 FireEye, Inc. All rights reserved. FireEye is a registered trademark of FireEye, Inc. All other brands, products, or service names are or may be trademarks or service marks of their respective owners. CS-EXT-UD-US-EN-052019-01

About FireEye, Inc.
FireEye is the intelligence-led security company. Working as a seamless, scalable extension of customer security operations, FireEye offers a single platform that blends innovative security technologies, nation-state grade threat intelligence, and world-renowned Mandiant® consulting. With this approach, FireEye eliminates the complexity and burden of cyber security for organizations struggling to prepare for, prevent and respond to cyber attacks.

FIREEYE™