CASE STUDY

Flowing into the Future

Major water treatment plants around the world have been connected to the internet since the 1990s. Today, administrators routinely check tank levels via laptop; tomorrow, as the internet of things evolves, "smart" tanks may self-monitor in real-time, enabling engineers to predict issues before they occur. But the tools that improve water reliability are also the source of growing anxiety. Were these controls to fall into the wrong hands, these water systems could potentially harm the very lives they were built to sustain.

Trustwave®

Client Spotlight

Created in 1989 when a Western European country privatized its water industry, this company provides water to roughly 2.5 million people across four municipal areas. The company has upgraded water systems while improving environmental quality at 55 sites throughout the area.

The Challenge

A water company in Western Europe still relied on the antiquated Forcepoint (formerly known as Websense) URL filtering system it implemented in 1997. But as web usage skyrocketed and threats proliferated, the filter was no longer effective against modern threats. The company needed a proactive content-scanning system that would catch both current and future threats. Many security providers claimed to offer a strong scanning and analysis program, but they failed to explain their capability with enough specificity to satisfy the administrators.

> *"Trustwave's content scanning engine has proven to be excellent. It enables our staff to work efficiently, and because it doesn't cause any headaches or excessive management, we are now free to concentrate on other critical responsibilities."*
>
> – Information security analyst, regional water authority

The Solution

The water system selected Trustwave Secure Web Gateway, which eliminated the hundreds of pieces of malware that previously snuck into the system each year. Its real-time detection technology prevents malware, helps ensure business continuity, and even helps protect against emerging mobile and social media threats. As a result, plant operators and regular citizens can sleep a bit easier now—and well into the future.

Industry Threat

Stories about municipal utility hackers, while uncommon, show the potential environmental and human health risks posed by unsecured systems. The most successful attack, so far, involves a disgruntled former employee who hacked into a municipal waste management system in 2000 and spewed millions gallons of raw sewage into local parks, rivers, and canals.

More recently, hackers managed to infiltrate an unidentified water treatment plant in 2016 through its web payment system, changing the level of chemicals used to treat the water four times. Though system operators noticed unusual movements in the system's valves and were able to reverse the chemical changes before they affected customers' health, the attack underscores the vulnerability of aging and under-resourced infrastructure systems. To wit: The security company that uncovered the problem said the water plant was using a decade-old operating system.

> *"With Websense, we had 250 virus detections in one year. In the year since implementing the Trustwave SWG, we have not seen one."*
>
> – Information security analyst, regional water authority

Trustwave®