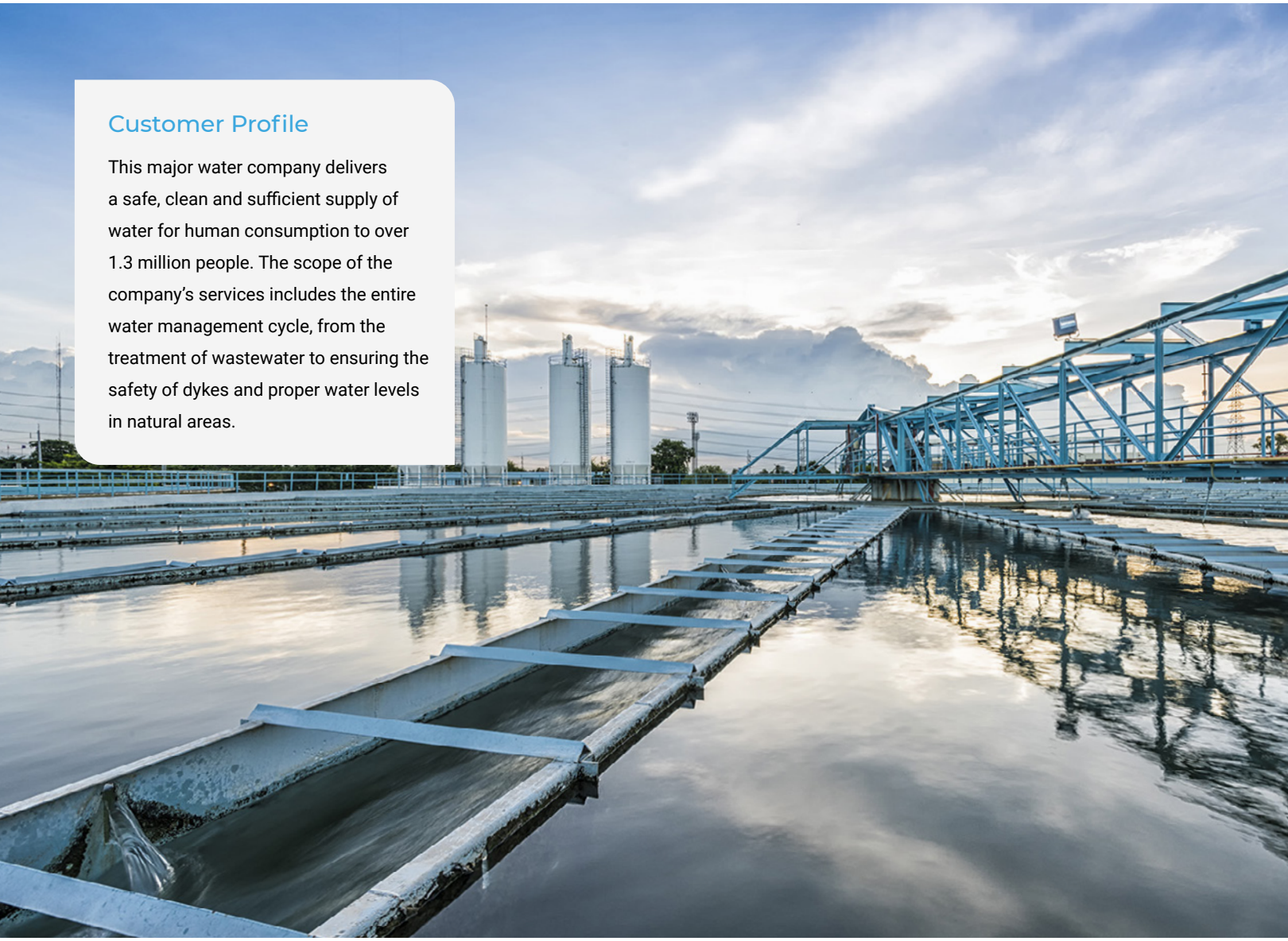
FORESCOUT

Case Study

# Water Management Company

A water management company deployed SilentDefense to improve their cybersecurity posture and keep up with evolving regulatory standards



## Customer Profile

This major water company delivers a safe, clean and sufficient supply of water for human consumption to over 1.3 million people. The scope of the company's services includes the entire water management cycle, from the treatment of wastewater to ensuring the safety of dykes and proper water levels in natural areas.

## The Challenge

Compliance is an ever-evolving and costly challenge. Within the utility world, more and more standards and regulatory frameworks now define all things cybersecurity and safety. For this customer, a national regulatory standard mandated the monitoring of all system assets. The company's objective was to proactively tackle compliance through periodical risk assessment and continuous industrial control system (ICS) network monitoring to be prepared for stricter safety and network security regulations. These requirements demanded more effective asset management, improved network segmentation and mature industrial cyber threat assessments and reporting capabilities across a complex IT-OT environment.

## The Project

A multi-year project was set up to assess and deploy network monitoring at the company. The initial scope of the project began with one pilot site. After a successful pilot, they began progressively deploying SilentDefense at all their sites.
The project represented an unprecedented improvement of the company's overall ICS network cyber resilience. Monitoring had been initially deployed only for regulatory compliance, but since its implementation, the company has utilized it for multiple objectives beyond just regulatory compliance, including:

- **Change Management & Commissioning:** Monitoring the flow of changes to the system and alignment with documentation.
- **Network Policy Monitoring:** Preventing unauthorized and/or dangerous behaviors like unscheduled maintenance.
- **Process Validation:** Checking the correct execution of complex or new processes on the ICS network.

The company has integration with ticketing/help desk systems for increased automation and is ready for further integration with the broader security ecosystem.

## The Results

The company can now automatically maintain a complete and continuously updated asset inventory and network communications map with details about hundreds of devices, including model, firmware and vulnerabilities. Additionally, they are now using SilentDefense for firewall-like monitoring of OPC communication. Some of the anomalies SilentDefense detected include:

- Unwanted communication links between the IT and OT network caused by firewall misconfiguration.
- Unwanted/unnecessary services and protocols enabled, including file transfer and device discovery.
- Maintenance operations not adhering to policies, including a supplier connecting their own laptop to network.
- Improved availability and cybersecurity posture.
- Identified manual/unscheduled PLC updates.
- Revealed unknown hosts, missing DNS records and prohibited communications.

## The Benefits

- Easier compliance with national regulations
- Reduced asset inventory costs
- Improved internal policy compliance
- Reduced workload
- Improvement of availability and overall security posture

FORESCOUT

Forescout Technologies, Inc.
190 W Tasman Dr.
San Jose, CA 95134 USA

Toll-Free (US) 1-866-377-8771
Tel (Intl) +1-408-213-3191
Support +1-708-237-6591

Learn more at Forescout.com