



# Zero Trust for Water Operations

© 2026 Zscaler, Inc. All rights reserved.

**Solution Brief**

## The Issue at Hand

Water infrastructure is distributed: central treatment plants, remote booster stations, reservoir monitoring sites, and field-deployed IoT sensors. Most OT and SCADA networks were designed for isolation and physical reliability, not for today's converged IT/OT threat or digital operating tempo.

Traditional water utility architectures typically combine legacy radio telemetry, leased lines, localized industrial firewalls, vendor VPNs, and hub-and-spoke backhaul into central control rooms and data historians. As threat actors increasingly attack these vulnerable and critical systems, this legacy approach exposes five persistent problems:

- **Expanded Blast Radius:** Flat OT networks and routed site-to-site connectivity unintentionally make lateral movement easier once any remote pump station, cellular RTU, or IT workstation is compromised—turning a localized incident into a facility-wide operational crisis.
- **Fragmented Security Operations:** Location-based security policies (per-site industrial firewalls and ACLs) are managed separately from user and device posture, creating a divide between IT and OT, multiple “panes of glass,” inconsistent controls, and delayed threat response.
- **High Cost and Rigid Deployment:** Private lines and specialized cellular APNs for remote monitoring are expensive and slow to provision; bringing new remote telemetry or modernized pump stations online frequently means weeks or months of network buildout, complex firewall changes, and troubleshooting.
- **Unsecured Third-Party Vendor Access:** Specialized water treatment equipment (centrifuges, UV systems, automated dosing pumps) requires continuous remote maintenance and troubleshooting by outside OEMs and contractors. Relying on shared VPNs or jump servers gives these external vendors broad, unmonitored network access, introducing immense risk to the OT environment and violating the principle of least privilege.
- **Unpatchable Legacy Vulnerabilities:** Water treatment infrastructure relies on PLCs, RTUs, and HMIs with lifecycles spanning 15 to 30 years. These legacy devices cannot run modern endpoint protection, don't support modern identity solutions and often cannot be patched without unacceptable downtime. When traditional network layers are bridged to enable remote monitoring, these highly vulnerable, critical systems are instantly exposed to lateral threats they have no ability to defend against.

And because water treatment is operationally “real,” not theoretical—continuous chemical dosing, real-time flow monitoring, and third-party vendor maintenance happen 24/7—network complexity becomes a public health and compliance issue, not just an IT issue. A common example is remote vendor troubleshooting and SCADA telemetry polling, where legacy protocols (like Modbus or DNP3), fragile VPN dependencies, and complex jump servers create operational blind spots, delayed maintenance, and wide-open backdoors into the plant's most critical control systems.

## How this Impacts Water Utilities

### Complexity

Site-based industrial firewalls are slow to change, and routing overlays share routes across the entire utility network

### Risk

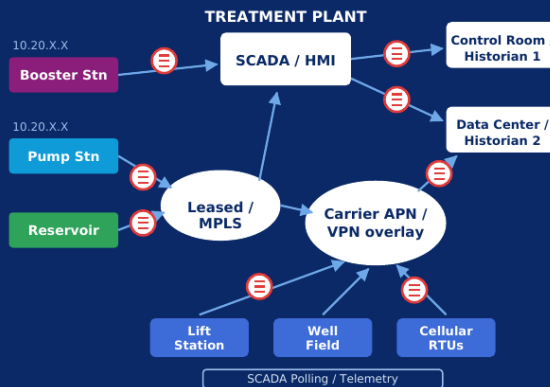
A breach at any remote site can directly spread to critical SCADA and data historian assets

### Cost

Reliance on expensive leased lines, private APNs, and hardware firewalls drives endless refreshes

### Slow Provisioning

Onboarding new pump stations, resolving overlapping IPs, and adding telemetry takes weeks or months



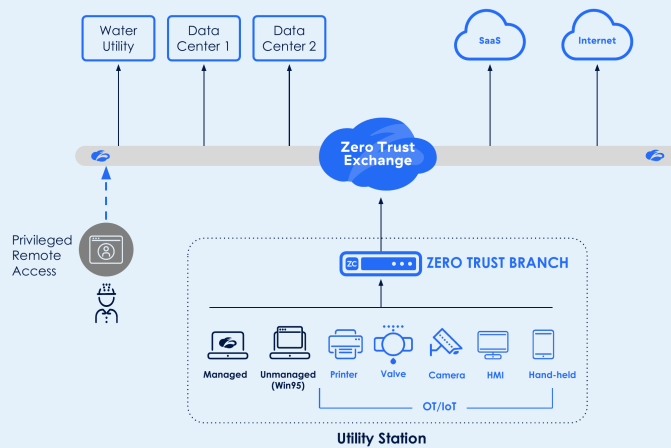
**Legacy security architectures are the water infrastructure modernization bottleneck**

## What Can You Do

A water infrastructure security strategy that actually scales should aim to:

- Stop lateral movement by default between remote pump stations, and from corporate IT/office LANs to critical SCADA control networks and data historians.
- Reduce the remote site security footprint eliminating industrial firewall and VPN sprawl and simplifying operations with a repeatable “pump station and treatment plant blueprint,” leveraging Zscaler Cellular to securely connect remote telemetry without the need for complex edge routing or vulnerable carrier-managed APNs.
- Segment and protect OT and IoT devices (like PLCs, RTUs, and chemical dosing sensors) that can’t run modern EDR agents and are severely constrained by unpatchable, legacy operating systems.
- Enable safe third-party access for OEMs, system integrators, and maintenance contractors without exposing inbound ports or granting broad network access through risky jump servers or shared VPNs.
- Accelerate the deployment of new infrastructure (such as cellular telemetry and smart water sensors) without requiring weeks of complex network buildouts or routing changes.
- Apply policy consistently across dozens or hundreds of remote facilities and connected endpoints without manual, per-site firewall rule engineering.
- Enhance monitoring and threat detection across all OT, IoT, and IT traffic, providing deep visibility to identify anomalous behaviors, alert on potential ICS malware, and rapidly contain cyber events before they impact physical water operations.

## Zero Trust Water Operations: Secure OT and IoT



**Zero Trust SD-WAN:** Replace complex hub-and-spoke networks and complex routing overlays while eliminating lateral threat movement and attack surface

**Device Segmentation:** Automatically discover, visualize and isolate every device, OT, IoT, cellular, managed, and unmanaged systems - without agents

**Privileged Remote Access:** Give third-party vendors controlled access only to specific devices and systems

### What Gets Eliminated

✗ MPLS

✗ VPN

✗ Firewalls

✗ Complex Routing

## Zero Trust for Water Operations

Zero Trust for Water Operations is an OT-focused approach built on Zscaler Zero Trust Branch (ZTB) and Zscaler Cellular capabilities: modern connectivity plus integrated, policy-driven controls for plant operators, legacy devices, and critical control applications—without ever relying on implicit trust in the underlying network.

### Zero Trust Water Infrastructure Architecture Overview

At each treatment plant or remote pump station, the Zscaler platform becomes the standard model for secure operations. It:

- **Delivers Clientless Security via Zero Trust Branch (ZTB)**, enabling device-level microsegmentation for legacy OT and IoT endpoints (like PLCs, sensors, and HMIs) inside the plant LAN. This blocks lateral movement without requiring complex VLANs or impossible-to-install endpoint agents.
- **Secures Remote Telemetry with Zscaler Cellular**, extending private access to “headless” devices like cellular RTUs and reservoir monitors, ensuring they securely transmit data to central SCADA systems via a protected APN, never touching the public internet.
- **Controls Third-Party Maintenance via Privileged Remote Access (PRA)**, replacing risky vendor VPNs with agentless, browser-based access to specific equipment (like chemical dosing controls or centrifuges). This guarantees zero inbound firewall exposure and provides full session recording for audits.

- **Supports Inside-Out Connectivity Models** across the entire water district, ensuring that whether a connection originates from an office laptop, a plant sensor, or a remote vendor, it is strictly brokered based on identity and policy.

The result is a water facility design where connectivity and security are policy-driven and identity/context-aware, rather than dependent on physical isolation, flat OT networks, and sprawling industrial firewall rules.

## Three Core Capabilities

### 1. Modernize Water Facility Connectivity with Zero Trust

Legacy hub-and-spoke designs and routed overlays make connectivity and security tightly coupled to routing, NAT, and per-site industrial firewall configuration. Zscaler modernizes water infrastructure connectivity with a simpler, more scalable model that leverages Zero Trust Branch and Zscaler Cellular:

- Reduce reliance on expensive leased lines, hub backhaul, and fragile VPN overlays.
- Use direct, policy-governed paths for plant-to-SCADA and sensor-to-historian communication.
- Shrink the attack surface created by broad site-to-site connectivity and eliminate the firewall sprawl typically required to connect remote pump stations.

### 2. Support Agentless Device Segmentation for OT, IoT, and Unmanaged Endpoints

Water treatment plants and pump stations are full of legacy devices that cannot support agents—PLCs, chemical dosing controllers, flow meters, legacy Windows HMIs, and embedded platforms. Device segmentation must work without EDR dependencies. Zero Trust for Water Operations applies an agentless segmentation model via Zero Trust Branch that can:

- Discover and profile ICS devices in-line using passive signals (e.g., DHCP fingerprinting, protocol observation, and other network-visible telemetry).
- Enforce “network-of-one” isolation (e.g., /32-style segmentation) so highly sensitive PLCs are treated as distinct security entities—not as members of a broadly trusted plant subnet.
- Control east-west traffic inside the treatment facility by forcing device communications through the enforcement point—so being on the “same VLAN” does not mean “implicitly trusted.”
- Apply policy based on device identity and context (e.g., device type, role, observed behavior), not just IP address.

This clientless approach is designed to contain ransomware-style lateral movement and reduce the probability that a compromised IT workstation or cellular remote terminal unit (RTU) can pivot into critical control systems.

### 3. Privileged Remote Access for Vendors and Third Parties

OEMs, system integrators, and third-party contractors routinely need remote access to specialized water treatment equipment for maintenance and troubleshooting. Traditional methods (shared vendor VPNs, jump boxes, exposed inbound firewall ports) expand the attack surface and significantly increase the likelihood of lateral movement and credential abuse. Zscaler Privileged Remote Access (PRA) supports zero trust access patterns for vendors that:

- Provides inside-out connectivity, meaning there is zero inbound exposure to the internet and firewalls can be closed.
- Enable clientless, browser-based access to specific targets using common protocols (e.g., RDP, SSH, VNC, HTTP) without ever granting the vendor broad network reachability.
- Support granular, auditable access policies aligned to least privilege, complete with full session recording to satisfy compliance mandates (like EPA/AWIA cybersecurity guidelines).

### Water Operations Spotlight: Remote Telemetry & SCADA Polling

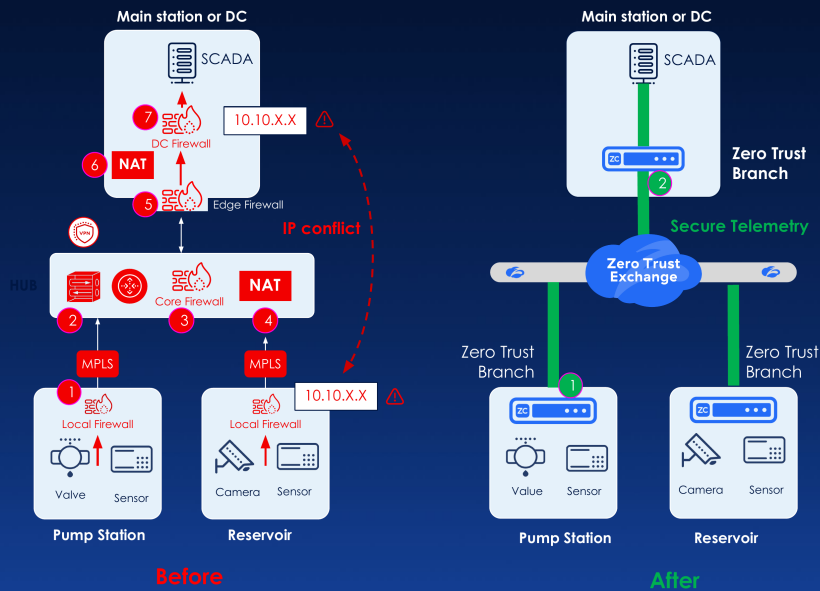
Remote telemetry collection is a high-friction example of how legacy OT networking shows up in day-to-day water operations. Commonly:

- Sensors (flow, pressure, chemical dosing) are located at highly remote pump stations, lift stations, or reservoirs.
- SCADA polling engines and Data Historians are centralized in a municipal data center or cloud.
- Telemetry traffic traverses carrier cellular networks, complex IPsec VPN tunnels, NAT domains, and multiple industrial firewalls—often becoming brittle, highly latent, and hard to troubleshoot.

Zero Trust for Water Operations simplifies this workflow by utilizing remote cellular-attached sensors secured via Zscaler Cellular. This provides direct, policy-brokered, and agentless connectivity for “headless” OT devices straight to the centralized application. It makes it easier to scale sensor deployments across vast geographies, eliminates the need for carrier-managed private APNs and complex firewall rules, and completely removes IP overlap as a blocker—especially when deploying new infrastructure or merging municipal water districts.

When your environment relies on centralized historians, bridging cellular sensor networks into the core OT environment is often one of the first “felt” problems that reveals whether your operational security architecture will actually scale.

# Secure Telemetry from remote stations



Isolate SCADA and historians from remote sites

Accelerate sensor rollout and integration

Make overlapping IPs and carrier APNs irrelevant for instant telemetry access

©2026 Zscaler, Inc. All rights reserved

## Key Water Infrastructure Use Cases

- **Rapid onboarding of new remote facilities** (pump stations, lift stations, wells) and municipal M&A integration even with overlapping IP ranges, using policy-brokered access patterns rather than network adjacency.
- **OT and IoT segmentation and containment** for industrial devices that cannot run agents (PLCs, RTUs, smart meters, chemical sensors), including those with legacy operating systems and embedded ICS platforms.
- **Remote site-to-data center blast-radius reduction** by removing implicit trust and enforcing least-privilege communications to central SCADA and data historians.
- **Third-party OEM and system integrator remote access** without VPN sprawl or inbound firewall exposure.
- **Secure internal and external communications** (plant operators and headless cellular sensors accessing approved private OT applications and external telemetry dashboards).

## Benefits

### Reduced Cyber Risk

Reduce ransomware and ICS malware propagation pathways by limiting east-west movement inside treatment plants and blocking remote-site-to-core lateral pivots by default.

### Faster Operations with a Repeatable Infrastructure Blueprint

Define policy once and apply consistently across hundreds of dispersed sites (template-driven), rather than engineering and maintaining complex, site-specific industrial firewall rules.

### Lower Cost and Footprint

Retire or reduce dependency on expensive leased lines and carrier-managed private APNs, reduce industrial firewall/VPN sprawl at remote sites, and avoid perpetual hardware refresh cycles for stacks that don't scale.

### Better Operational Reliability

Remove avoidable network friction from SCADA-dependent workflows and cellular telemetry collection, improving operational uptime and reducing troubleshooting time for field engineers and control room operators.

## Deployment and Operational Model

- Physical or virtual form factors to fit treatment plant and remote site constraints (including hypervisor-based edge deployments when available).
- High availability options (e.g., active/standby) for facilities that require additional resiliency.
- In-line enforcement + passive discovery so device identification and segmentation are practical at scale, even when agents are not possible.
- East-west control inside the facility using enforcement-point policy rather than assuming VLAN = trust boundary.



### About Zscaler

Zscaler enables organizations to move faster and be more secure by replacing network-based security with a true Zero Trust architecture. The Zscaler Zero Trust platform secures users, workloads, and devices by connecting them directly to approved applications and services based on identity, context, and policy—reducing attack surface and limiting lateral movement.

© 2026 Zscaler, Inc. All rights reserved. Zscaler™, Zero Trust Exchange™, Zscaler Internet Access™, ZIA™, Zscaler Private Access™, ZPA™ and other trademarks listed at [zscaler.com/legal/trademarks](https://zscaler.com/legal/trademarks) are either (i) registered trademarks or service marks or (ii) trademarks or service marks of Zscaler, Inc. in the United States and/or other countries. Any other trademarks are the properties of their respective owners.