Zero Trust OT Cybersecurity Protection for the Water and Wastewater Industry

The Zero Trust Challenge for Water OT Networks

Water and wastewater utilities are increasingly targeted by cyberattacks, posing significant risks to public health and safety. BlastWave builds an easy-to-use Zero Trust secure infrastructure designed to protect from evolving threats, ensuring the reliable and safe delivery of essential water services. BlastWave delivers the following benefits for Water Utilities:

Secure Remote Monitoring and Maintenance: Enables secure remote access for monitoring and maintenance, crucial for geographically dispersed infrastructure, without compromising security.

Protection of Legacy Systems: Provides a "virtual air gap" for legacy OT devices that cannot be patched, protecting them from modern cyber threats.

Prevention of Chemical Injection System Attacks: Protects chemical injection systems from unauthorized manipulation, preventing potentially hazardous imbalances.

Reduced Attack Surface: Hides critical assets from hackers and granular segmentation limits the damage of a breach or any malware resulting from physical compromise.

Zero Trust Protection: Ensures all users and devices are verified before access is granted.

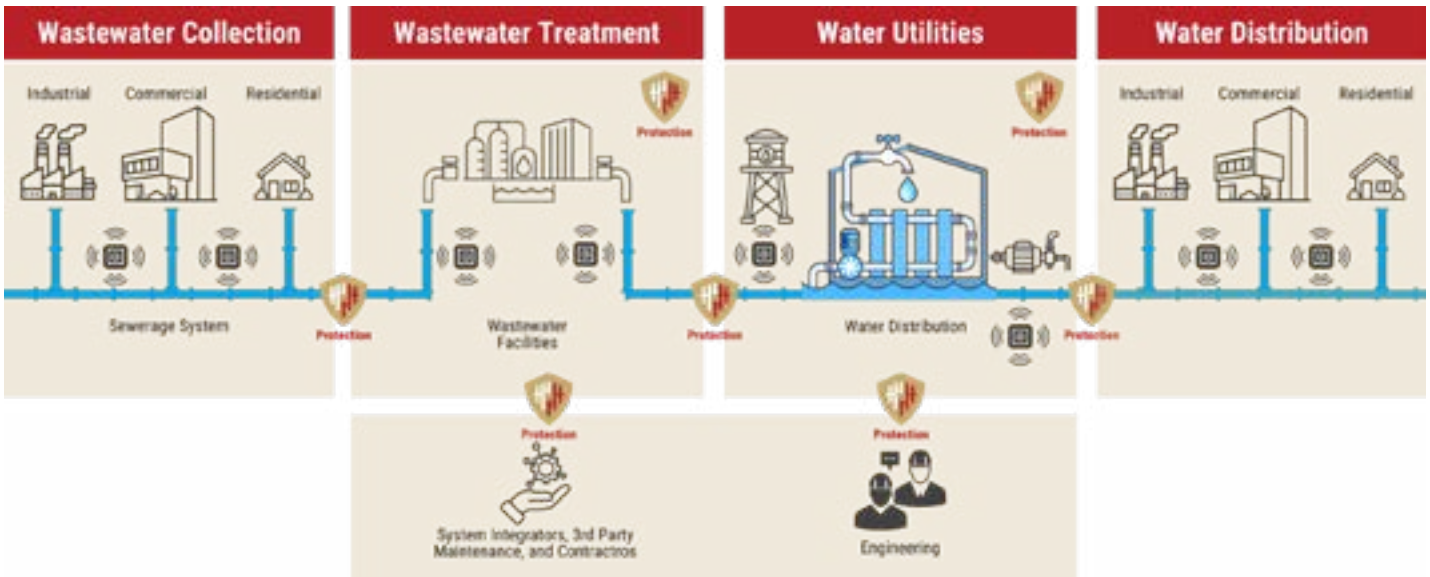
BlastShield™

Protection of Critical SCADA Systems: BlastWave safeguards SCADA systems, preventing unauthorized control that could lead to service disruptions or contamination..

Secure Third-Party Vendor Access: It enables secure access for contractors and vendors, limiting their access to only necessary systems and data.

Protection Against AI-Powered Threats with network cloaking and passwordless MFA

Figure 1 Shielding Water and Wastewater Industry Operations



©2025 BlastWave Inc.

BlastShield™: Zero Trust OT Protection for Water and Wastewater Systems

BlastShield is an ideal solution to protect the water and wastewater industry. The solution is low-cost and scales perfectly for water deployments, unlike many complex and costly firewalls. Our solution is designed to be easy to deploy and manage, minimizing disruption to existing operations.

BlastWave implements a true Zero Trust architecture, assuming no user or device is inherently trustworthy. We verify every connection, enforce least privilege access, and continuously monitor network activity to detect and respond to threats in real-time. By implementing BlastWave, water and wastewater utilities significantly strengthen their cybersecurity posture, protect their critical infrastructure, and ensure the reliable and safe delivery of essential services to their communities. BlastWave delivers a number of key use cases for Water and Wastewater:

Securing SCADA Systems:

BlastWave protects the critical SCADA systems used for monitoring and controlling water treatment, distribution, and storage. The secure infrastructure prevents unauthorized control that could lead to water contamination or service disruptions. This is a critical function as water utilities have been a favored target for bad actors over the past several years, and a number of high profile hacks have occurred.

Secure Remote Access for Maintenance and Monitoring:

Water systems frequently need to grant secure remote access for maintenance crews and engineers to diagnose and repair equipment problems. Providing secure access for remote monitoring of water system operations for remote users and maintenance personnel with phishing-resistant secure remote access eliminates a major initial attack vector used by hackers in many successful cyberattacks.

Protecting Remote Pump Stations and Reservoirs:

Securing remote pump stations and reservoirs from unauthorized access and manipulation is one of the main goals of any water cybersecurity deployment,.BlastShield's software-defined perimeter (SDP) creates a secure boundary for the waster utility, regardless of the geographical separation or number of devices at remote sites, enabling secure remote monitoring and control of these geographically dispersed assets.

Securing Telemetry Units (RTUs):

In water treatment, protecting RTUs used for data collection and transmission is critical, as any manipulation of this data or compromise of these systems can result in a compromised water system and cost lives. Blastshield's protection and encryption of data-in-flight ensures prevents manipulation of sensor data and control signals.

Protecting Chemical Injection Systems:

Similar to RTUs, access and control of chemical injection systems used for water treatment must be protected from unauthorized access. Bad actors gaining control of these systems could create hazardous chemical imbalances and affect the health of entire communities.

Securing Filtration and Purification Systems:

Likewise, protecting control systems for filtration and purification processes is also important. Shielding these systems from discovery, vulnerability exploit, and eliminating zero day breaches prevent disruptions to water quality.

Securing Distribution Networks:

Protecting the control systems used to manage water distribution pipelines and valves ensures the continuous flow of water to the communities water systems serve. Preventing unauthorized control of water flow helps prevent malicious disasters that can cause havoc in a local community.

Software-Defined Segmentation and Microsegmentation:

Water utilities leverage network segmentation and microsegmentation to limit the blast radius of a cyber attack and control access to legacy devices that cannot be patched.

Zero Trust Architecture:

BlastWave's Secure By Design architecture shields the OT network against AI powered reconnaissance and GenAI generated phishing. Deploying a Zero Trust architecture ensures that your network is hard to hack, yet easy to use, delivering the strongest possible security architecture without impacting your business process.

v20260330

Prevent industrial cyberattacks, and ensure the world's critical infrastructure stays protected, productive, and profitable. Together we can build a resilient future for OT networks. Join the movement at **www.blastwave.com**

©2025 BlastWave Inc. | 1045 Hutchinson Ave., Palo Alto, CA 94301 USA | T: +1 650 206 8499

BlastWave
PREVENT
INDUSTRIAL
CYBERATTACKS