BlastWave

SOLUTION BRIEF

AI-Resistant Cybersecurity Protection for Water

The Operational Technology Challenge for Water

Protecting a nation's critical infrastructure against an ever-growing arsenal of AI-powered cyber threats is crucial, particularly in the water and wastewater industry. With the rise of operational technology (OT) and the need for secure remote access, the risks and consequences of cyber attacks have grown significantly.

OT has made it possible to optimize the operation of water and wastewater facilities, but it has also created new risks that must be addressed. Water and wastewater companies are vulnerable to cyber-attacks that can disrupt operations, compromise public safety, and cause significant financial loss.

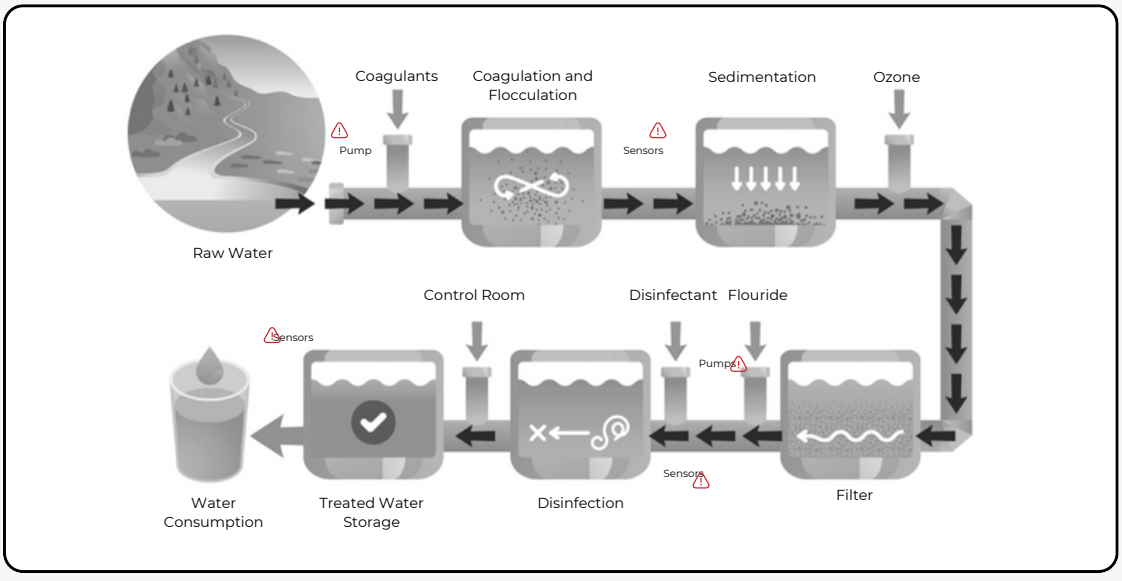
The water and wastewater industry has increasingly been the target of cybercriminals, bad actors, and hostile nation-states, and recent incidents highlight the importance of cybersecurity in this sector.

The US has about 150,000 public water systems and 16,000 publicly owned wastewater systems. Recently, bad actors have targeted this industry specifically. In recognition of this ongoing threat, CISA announced a free Cyber Vulnerability Scanning Service for Water Utilities. Hence, protecting your water facility is the first part of an in-depth defense strategy.

BlastShield Advantages:

- Reconnaissance-Proof Software Defined Perimeter to prevent device discovery and vulnerability exposure with Network Cloaking
- Phishing-Resistant Biometric Multifactor Authentication for Regulatory-Compliant Secure Remote Access
- Delivers Least Privilege Access Policies and prevents Lateral Movement with Network Microsegmentation

Figure 1: Vulnerable OT Systems in Water



BlastShield™: AI-Resistant OT Security For Water and Wastewater systems

BlastShield is an ideal solution to protect the water and wastewater industry. It is easily deployed as a simple migration without any changes to the existing IT or OT network architecture. Installing and administering the solution takes an order of magnitude less time and effort than comparable solutions. The user experience is comparable to Apple Pay, with simple biometric authentication granting access to only the devices the user needs.

BlastShield provides a PKI-authenticated secure gateway to the OT environment, where Industrial control systems, PLCs, IEDs, RTUs, turbine controllers, valves, and IoT devices remain in service for decades, long after vendors halt support. These systems often cannot be patched but require access to internal monitoring systems. BlastShield protects these systems from discovery by hackers by creating a virtual air gap with Network Cloaking, Only allowing biometric-authenticated Secure Remote Access to the devices and leveraging Network Segmentation to create microsegmentation of different device types to prevent lateral movement within an existing flat Layer 2 network.

Network Cloaking

Network Cloaking ensures that critical yet outdated legacy infrastructure such as PLCs, sensors, and pumps—becomes invisible to external threats. Rather than just obfuscating these systems, they do not appear in any scans or probes from a hacker. With BlastShield, water systems operators ensure security and compliance with industry standards and guidance like NIST 800-53, 800-207 (Zero Trust), and IEC 62443.

AI-enhanced reconnaissance tools cannot probe into the internal workings of a water facility because they have no path to reach the internal OT networks. Network cloaking provides a first line of AI-resistant security by preventing reconnaissance and breaking the cyber kill chain. It proactively secures systems, making them invisible to potential attackers by blocking all internet access for legacy OT systems. Network cloaking also creates a virtual air gap for OT systems that do not need access to the internet by only allowing them a hidden private

Secure Remote Access

BlastShield provides OT Secure Remote Access to critical OT water systems, ensuring operators can monitor and manage them without exposing them to cyber threats. BlastShield's phishing-resistant MFA biometric authentication protects against GenAI-powered phishing attacks and MFA hijacking. A full mesh of P2P encrypted tunnels is created to secure traffic from remote users to the water facility and any agent-enabled systems, protecting against Man-in-the-middle attacks. Policy changes take effect in real-time, facilitating dynamic and flexible policy enforcement during emergencies or administration changes.

Network Segmentation

BlastShield exceeds traditional segmentation by advancing the concept of microsegmentation as a superior security alternative. Unlike broad segmentation strategies, microsegmentation allows for incredibly detailed control, segmenting networks down to the level of individual devices, systems, protocols, or users. By isolating network segments, BlastShield effectively prevents the lateral movement of threats within the network, a critical defense mechanism against external and internal threats. Unlike many solutions that use ACLs and VLANs, microsegmentation scales effortlessly to large OT environments. BlastShield's microsegmentation solution is innovative and future-ready for network security.

About BlastWave

BlastWave prevents AI-powered cyber attacks on critical infrastructure with a unique combination of Zero Trust Cybersecurity capabilities and delivers industrial-grade security with consumer-grade ease-of-use. Visit www.blastwave.com to learn more