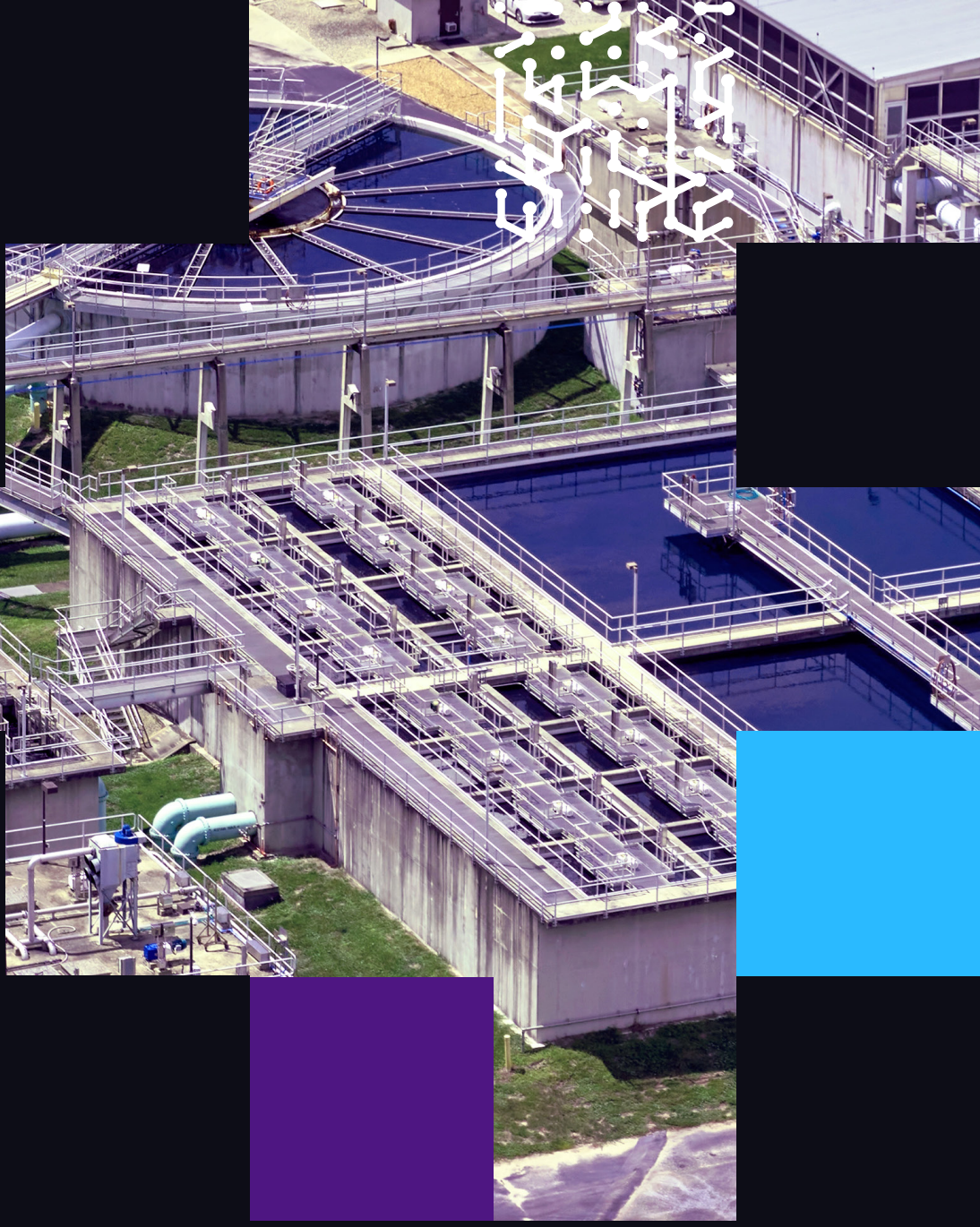
ARMIS®



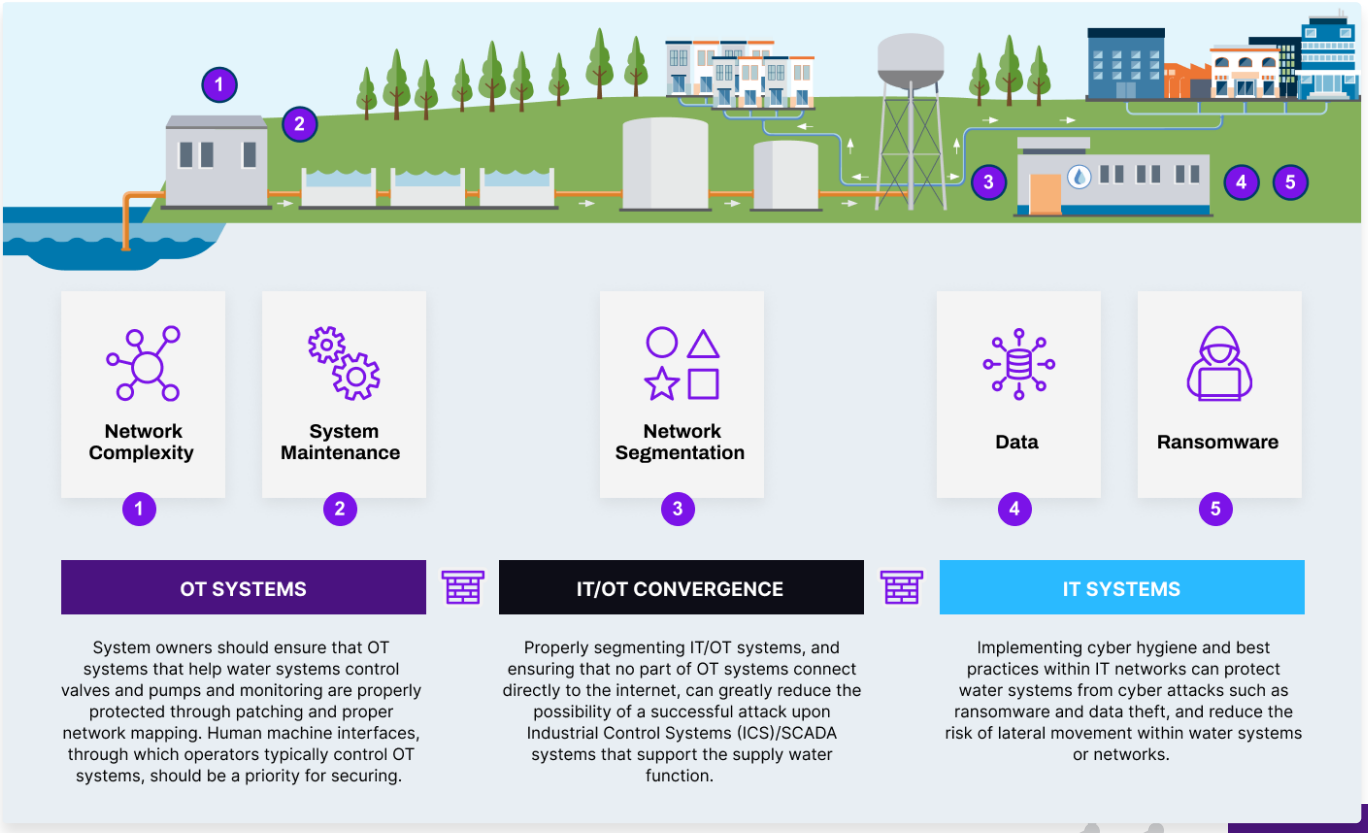
SOLUTION BRIEF

Armis Centrix™: Security for Water Treatment Facilities

Water treatment and purification facilities are completely essential to everyone. To put it simply, we all need safe water to live. Water contamination doesn't just lead to a public health crisis it also impacts economic stability and the environment and nature's fragile ecosystem. The increasing automation of drinking water and wastewater operations brings efficiency and reduces the risk of human error but also means we should take extra precaution to protect and monitor the assets at play. Water utilities in 2025 are unsurprisingly a huge target for nation state actors and face a growing wave of cyber threats that can threaten safety, damage infrastructure, and compromise public trust.

At Armis, we understand the operational sensitivities, aging infrastructure, and regulatory complexity that water utilities must navigate. Armis Centrix™, was built to provide the visibility, proactive asset intelligence, and control that CISOs and OT leaders need to defend their environments without impacting essential service delivery.

Water is our most Basic Requirement but Securing it is Complex



Source: CISA
https://www.cisa.gov/sites/default/files/2023-02/infographic-supply-water-national-critical-function-102021-508.pdf

Recent Attacks Highlight the Urgency

2025 (June)

Rural Kansas Water Cooperative Hit by Coordinated Ransomware Attack

An attack forced a multi-county water district to shut down supervisory control systems and switch to full manual operations for several days. Investigation revealed the use of compromised remote access credentials to deploy ransomware across OT workstations.

Impact: Temporary loss of telemetry, delayed water testing reports, and EPA notification due to potential regulatory exposure.

2025 (February)

Florida Municipal Water Authority Targeted by Nation-State Linked APT Group

A known advanced persistent threat group exploited a vulnerability in a remote access gateway used by operations staff. The attackers attempted to access programmable logic controllers (PLCs) linked to chlorine injection systems. Mitigation required segmented network reconfiguration and forensic review.

Impact: Chlorine level thresholds were not altered, but the breach raised public concern and led to a multi-week investigation involving state cybersecurity agencies.

2024 (December)

Southern California Wastewater Facility Breach Tied to Hacktivist Group

A politically motivated cyber group exploited misconfigured IoT leak detection sensors to gain internal access to WWTP control networks. While no damage was caused, reconnaissance and lateral movement were confirmed.

Impact: Facility was forced to isolate several systems for two weeks, delaying regular maintenance and audits.

2024 (March)

Muleshoe, Texas

A cyberattack disrupted water operations in Muleshoe. The attackers remotely triggered tank overflows that required immediate on-site response. The attack was later linked to a Russian-aligned hacktivist group.

Impact: Public water services were interrupted, and emergency protocols had to be initiated. Other nearby towns experienced similar disruptions.

Key Trends in Water Utilities

1 Centralized Control is Replacing Operational Silos

Utilities are shifting to unified platforms for better coordination and faster incident response.

2 Automation is Driving Critical Decisions

AI and control systems now make real-time choices, reducing human touchpoints but raising the stakes for visibility.

3 Smart Devices are Expanding the Attack Surface

Connected sensors and valves boost efficiency but introduce unmanaged, often unsecured endpoints.

4 OT-IT Convergence Demands Unified Security

Blended networks require full-spectrum visibility to catch threats moving between systems.

5 Cyber Resilience is Now a Core Priority

Utilities are prioritizing continuity, recovery speed, and regulatory readiness in every security strategy.

Real World Use Cases That Matter in Water Operations

As well as being a data and compliance issue, when things go wrong in water treatment environments they can cause a risk to public health and environmental safety. Below are real-world use cases that illustrate how Armis Centrix™ equips water utilities with the visibility, intelligence, and automation needed to detect, contain, and prevent operational disruptions.

Protecting Chlorination Systems from Remote Exploits

A chlorine injection unit used for water disinfection is accessible through an exposed internet-facing HMI. Armis Centrix™ detects suspicious commands coming from a foreign IP range. Through passive network monitoring, the system traces the attacker's lateral movement across the OT VLAN and identifies attempts to escalate privileges and alter dosing setpoints.

How Armis Helps:

- Flags abnormal control messages to the PLC
- Automatically correlates with threat intelligence and IOC data
- Sends real-time alerts to SOC teams and isolates the vulnerable HMI from the control network

Impact: Prevents a potentially dangerous over-chlorination event, safeguarding public health and avoiding regulatory violations under the Safe Drinking Water Act.

Detecting Insider Configuration Tampering in WWTP Logic

A disgruntled technician modifies ladder logic on a sludge return pump at a wastewater treatment plant (WWTP), altering pump cycles to create irregular flow rates and potential tank overflow. Armis Centrix™ detects configuration drift from the baseline logic, logs the change down to the tag level, and issues an alert before operations are disrupted.

How Armis Helps:

- Tracks every configuration change to PLCs and RTUs
- Compares updates to established good states and operating patterns
- Supports role-based access logs to attribute changes to specific users

Impact: Maintains control process integrity, enables quick root cause analysis, and supports compliance with EPA and NIST configuration control requirements.

Neutralizing Nation-State Reconnaissance Activity

A smart valve actuator installed in a regional DWTP begins beaconing to an IP address known to be associated with an APT group targeting critical infrastructure. Armis Centrix™ identifies the device, correlates the behavior with known command-and-control patterns, and alerts the SOC. Further investigation reveals a vulnerable third-party monitoring platform was compromised.

How Armis Helps:

- Detects subtle deviations in device communication behavior
- Tags devices for elevated monitoring and initiates automatic risk scoring
- Enables forensic review and segmentation policy enforcement in response

Impact: Disrupts threat actors early in the kill chain and prevents spread to more sensitive systems like SCADA servers or chemical dosing logic controllers.

Containing Ransomware in Distributed Pumping Stations

A ransomware variant infiltrates the IT network of a multi-site water district and begins scanning for exposed OT devices. Armis Centrix™ identifies the traffic pattern as malicious and automatically identifies at-risk PLCs, field sensors, and edge servers. Through policy enforcement integrations, the attack is contained before it can encrypt operational assets.

How Armis Helps:

- Detects abnormal SMB and RDP traffic traversing from IT to OT
- Tags known ransomware indicators and uses behavioral detection to spot zero-day variants
- Integrates with NAC and firewall solutions to quarantine devices automatically

Impact: Prevents loss of control over remote pumping assets and eliminates the need for prolonged manual fallback operations.

Uncovering Dormant Devices Reactivated After Months Offline

A valve actuator might only be used in an emergency overflow system suddenly comes online after months of inactivity. Armis Centrix™ detects the unexpected reactivation and flags it due to unpatched firmware and outdated authentication protocols. Investigation reveals the asset was unintentionally exposed through a new IoT gateway configuration.

How Armis Helps:

- Allows active querying in native protocols to see what dormant devices that aren't communicating on the network are doing.
- Cross-references firmware and patch levels with current vulnerability data provided in part by the Armis 6 billion strong database of assets.

Impact: Prevents the reintroduction of outdated or exploitable devices that could act as hidden entry points into the OT environment.

Why CISOs in the Water Treatment Industry Choose Armis Centrix™

Visibility Across the Entire Water Operation

Water treatment and distribution involve multiple industrial processes operating across geographically dispersed infrastructure. In drinking water treatment plants (DWTPs), this includes water source monitoring, intake pumping, chemical injection, filtration, disinfection, storage, and final distribution. In wastewater treatment plants (WWTPs), it covers the capture, filtration, aeration, sedimentation, and reuse of gray water. Blackwater systems involve advanced biological treatment and safe environmental discharge.

Each of these processes depends on a complex choreography of IT, OT, and increasingly, smart IoT systems. The move to IP-connected devices and convergence of IT/OT introduces new cyber risk, including lateral movement of threats across systems that were once siloed.

Armis Centrix™ provides security teams with:

- A unified view across IT, OT, and IoT environments
- Deep visibility into traffic flows, device relationships, and protocol behavior
- Early detection of anomalies or suspicious activity within and between process areas
- The ability to actively query in a safe way
- The capacity to segment at a network and asset level to protect mission critical devices
- A knowledgebase of 6 billion known good baseline behaviors to stack up against your network activity.

This holistic, 360-degree visibility enables CISOs to eliminate blind spots and spot threats before they cause service disruptions.

Real-Time Asset Inventory, Track Changes and Anomaly Detection

Water utilities operate over large areas, using diverse technologies from various vendors and generations. These networks include pump stations, chemical dosing systems, filtration units, SCADA workstations, and metering systems. Visibility into these assets is critical to operational resilience and cybersecurity readiness.

Armis Centrix™:

- Automatically discovers and classifies all connected assets across your DWTPs and WWTPs
- Tracks changes in device configurations, including dormant or intermittently connected systems
- Flags unexpected behaviors or unapproved devices connecting to the network
- Supports scalability for small municipal utilities and large, regional water authorities

By keeping your asset inventory live and accurate, Armis enables informed decisions, streamlined operations, and faster incident response.

Prioritized Vulnerabilty Management Based on Operational Impact

Water treatment is an always-on environment. Stopping operations to patch or reconfigure devices can introduce risk to public health and safety. Therefore, CISOs need to focus on vulnerabilities that have real-world consequences.

Armis Centrix™:

- Maps vulnerability intelligence to each device's role, network location, and business criticality
- Prioritizes threats to systems with public-facing exposure or direct control over water quality and flow
- Provides a triaged list of vulnerabilities, taking into account asset criticality, exploitability, and network exposure

This enables risk-based maintenance planning and ensures your teams focus on what matters most.

Designed for the Realities of Water Sector Operations

Support for Native Water Industry Protocols

Armis Centrix™ supports over 500 ICS protocols, including Modbus, DNP3, Profinet, BACnet, FINS, HART, and CIP. It passively monitors these protocols to understand device behavior without interfering with operations.

Behavioral Detection Without False Positives

Armis uses passive monitoring and advanced baselining to distinguish between routine activity and emerging threats. This gives you accurate alerts without overwhelming your SOC with noise.

Rapid Response and Recovery

Armis integrates with your firewalls, NAC, EDR, and SIEM tools to automate containment and recovery

Cybersecurity Is Now Foundational to Safe Water Delivery

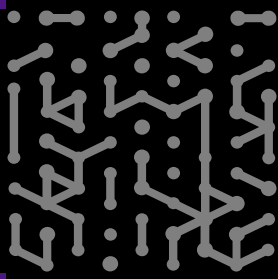
Regulatory frameworks such as the America's Water Infrastructure Act (AWIA) demand robust cybersecurity planning. But compliance alone is not enough. To secure the future of water, utilities need operational resilience and actionable intelligence.

Armis Centrix™ delivers:

- Unified visibility into IT, OT, and IoT assets
- Context-aware vulnerability management
- Threat detection tailored to industrial protocols
- Automated containment and configuration control
- Scalability for both small utilities and large regional systems

Summary

It doesn't get more essential than water. It is imperative to keep it safe, available, and resilient. Armis Centrix™ is trusted by some of the world's most critical infrastructure operators, and we are ready to partner with your utility to protect what matters most.



Armis, the cyber exposure management & security company, protects the entire attack surface and manages an organization's cyber risk exposure in real time.

In a rapidly evolving, perimeter-less world, Armis ensures that organizations continuously see, protect and manage all critical assets - from the ground to the cloud. Armis secures Fortune 100, 200 and 500 companies as well as national governments, state and local entities to help keep critical infrastructure, economies and society stay safe and secure 24/7.

Armis is a privately held company headquartered in California.

1.888.452.4011

Website
Platform
Industries
Solutions
Resources
Blog

Try Armis
Demo