aria | CYBERSECURITY

Zero Trust.
Zero Downtime. Defend Your Water Systems from the Next Wave of Cyber Threats.

aria | CYBERSECURITY

The Threat Is Real and Growing

- Nation-state hackers such as Volt Typhoon have already infiltrated U.S. water utilities - sometimes undetected for months - seeking to disrupt critical services and exfiltrate sensitive operational data.

- Recent attacks forced shutdowns at major water utilities, exposing chronic vulnerabilities in legacy OT systems and highlighting the urgent need for advanced protection.

- 70% of inspected water systems do not meet federal cybersecurity standards, leaving communities exposed to ransomware, data breaches, and potential service outages.

Why Water and Wastewater Are Prime Targets

- Water and wastewater systems are lifeline infrastructure - essential for public health, safety, and the environment.

- Legacy equipment, limited IT resources, and growing IT/OT convergence make these systems especially vulnerable to modern cyberattacks.

- Attackers exploit weak passwords, outdated software, and application access - often bypassing traditional antivirus or EDR solutions.

aria | CYBERSECURITY

Introducing ARIA AZT Protect—Purpose-Built for OT Security

AI-Driven, locks down critical applications from unapproved updates: Instantly stops attacks - known and unknown - at the endpoint, before they execute or spread.

No Cloud Dependency: Works autonomously, even in air-gapped or out of support application environments - no need for constant updates or internet connectivity.

No Cybersecurity Expertise Required: Deploys in minutes, requires no daily tuning, and protects even 20-year-old OS versions without disrupting operations.

Stops Nation-State and Ransomware Attacks: Neutralizes advanced threats - including those used by Volt Typhoon - by blocking exploits at both the application and OS level.

Cost-Effective and Scalable: Lightweight agent, full visibility, and optional 24/7 managed service - ideal for utilities of any size.

Real Results—Trusted by Water Sector Leaders

- Deployed by leading water treatment integrators to lock down critical OT assets and prevent both malware and sophisticated nation-state attacks.

- Proven to stop attacks that bypass traditional IT-centric security tools, protecting control systems and ensuring uninterrupted service delivery.

- Stops vulnerability risks, putting your systems into manual operation. AZT typically pays for itself in less than one week of security triggered manual operation per year.

Don't wait for the next attack to disrupt your operations. Discover how ARIA AZT Protect™ can secure your water and wastewater systems—today and for the future.

- Schedule a demo or security assessment with our experts.
- Learn how you can achieve full OT protection in minutes, not months.

Contact us now info@ariacybersecurity.com