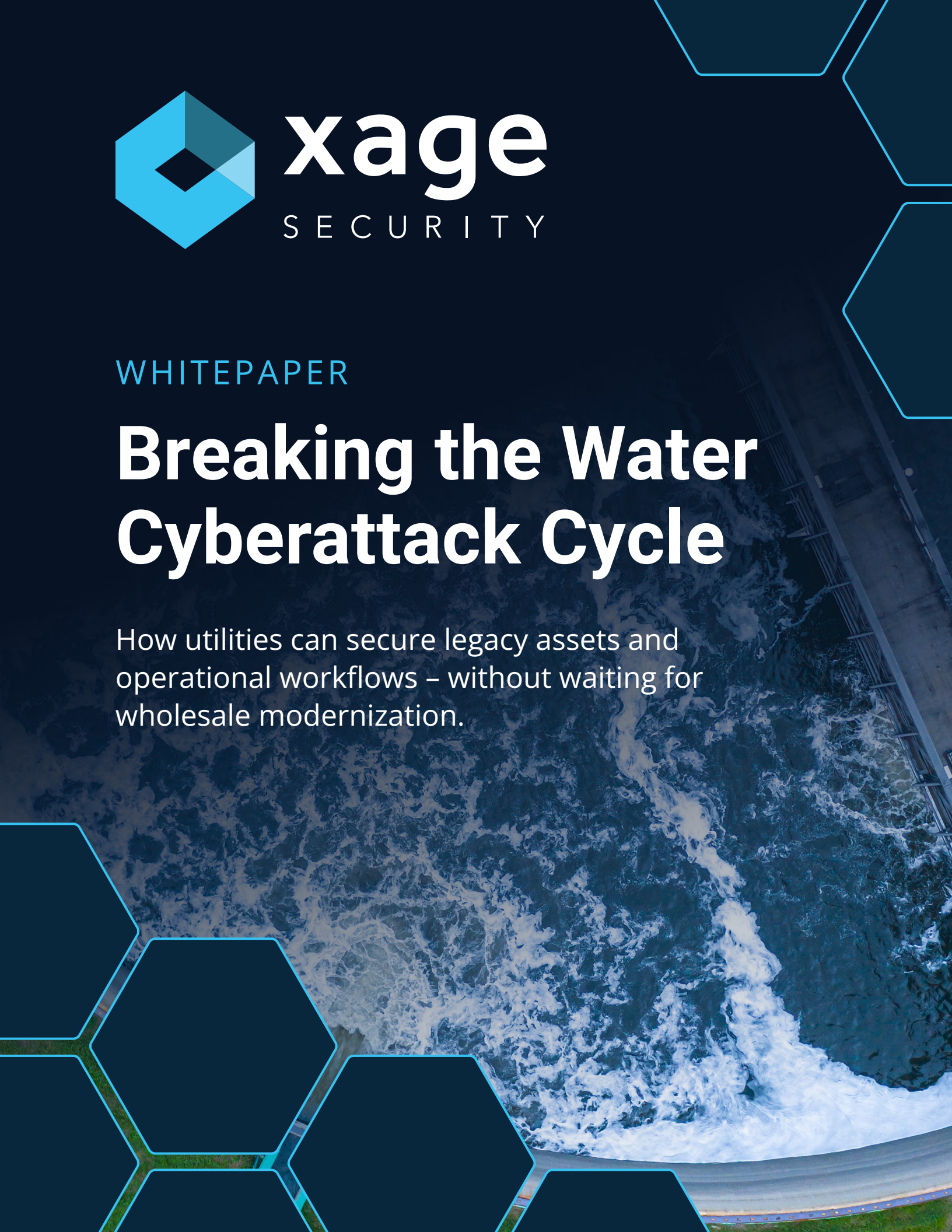
xage SECURITY

WHITEPAPER

Breaking the Water Cyberattack Cycle

How utilities can secure legacy assets and operational workflows – without waiting for wholesale modernization.



EXECUTIVE PERSPECTIVE

America does not have a shortage of warnings about water cybersecurity. It has a shortage of architectural change. Since 2019, U.S. water and wastewater utilities have faced insider misuse, ransomware in SCADA-related environments, manipulation of internet-facing controllers, persistent nation-state access and coordinated activity across multiple utilities.

The adversaries and motives differ, but the operational path is remarkably consistent: an asset that cannot defend itself becomes reachable through a connection that carries too much trust. Once a user, workstation or application is authenticated - or simply connected - the architecture often grants more control than the task requires.

The sector must modernize, but wholesale replacement will take years. The immediate strategic objective is to stop asking old control equipment to make security decisions it was never designed to make. Identity, MFA, least privilege, change governance and asset-level policy can be enforced before a connection reaches the operational equipment.

The device is often the least capable security control
Legacy PLCs and HMIs may lack individual identity, MFA, agents, encryption and meaningful logs.

Reachability repeatedly becomes control authority
Internet-facing OT, exposed remote tools and broad network access turn a connection into a path to physical operations.

The attacker changes; the trust failure repeats
Insiders, ransomware groups and nation-state actors repeatedly exploit reusable identities, excessive reach and weak change governance.

Utilities can reduce risk before wholesale replacement
Mediated access, MFA, just-in-time authorization, session oversight and asset-level segmentation can protect old assets now.

CENTRAL RECOMMENDATION: Protect what cannot yet be replaced. Make every human and machine connection earned, bounded, observable and revocable.

Scope and evidence

The paper examines selected publicly documented U.S. incidents from March 2019 through July 2026. It distinguishes targeting, confirmed compromise, operational disruption and public-health consequence; these outcomes are not interchangeable. Attribution is included only where federal authorities have made it public. The incident set is illustrative rather than exhaustive, and all claims are sourced in the endnotes.

01 | SECTOR REALITY

The PLCs are designed to run the process - not defend itself

Water systems are engineered for continuous, deterministic operation. A PLC at a well, pump station, treatment process or wastewater lift station may remain in service for 15, 20 or even 30 years. If it performs its control function reliably, replacement must compete with broken pipes, treatment upgrades, PFAS remediation, capacity projects and affordability pressures.

Many field devices were built before today's threat environment. Some lack individual user identities, role-based access, modern encryption, useful audit logs or any ability to support MFA. They may not be able to run an endpoint agent. Industrial protocols such as Modbus were not designed for untrusted networks and may provide no native authentication or encryption.

Even newer PLCs and HMIs can be deployed with default settings, directly exposed ports or remote-programming capability enabled for convenience. The controller may faithfully accept a command without knowing whether it came from an authorized operator, a compromised engineering workstation or an adversary using legitimate manufacturer software.

FOUNDATIONAL ASYMMETRY: The equipment with authority over the physical process often has the least ability to verify who - or what - is exercising that authority.

A distributed and resource-constrained operating model

The condition is not limited to the treatment plant. Wells, tanks, reservoirs, lift stations, pump stations and pressure-boosting facilities communicate over cellular, radio, leased or municipal networks. Remote access is part of the operating model; simply disconnecting everything is neither practical nor resilient.

The sector is also highly fragmented. The U.S. Government Accountability Office counts close to 170,000 drinking-water and wastewater systems with widely different capabilities and identifies workforce shortages, difficult-to-update technology and limited funding as persistent barriers. AWWA's 2025 survey identified cybersecurity as the leading human-caused concern, while about one-quarter of small systems reported limited ability to implement cyber controls.

≈170,000	15 - 30 years	>$2.1T
drinking-water and wastewater systems	typical service life for many field control assets	estimated 25-year U.S. drinking-water infrastructure need

Blaming operators or repeating "just patch it" does not solve these constraints. But accepting implicit trust because a device is old does not solve them either. An asset can remain old without remaining unprotected.

02 | INCIDENT RECORD

Seven years of incidents, one repeating architecture

The public record shows a progression from isolated access failures to scalable campaigns against operational technology. The incident names, actors and techniques change. The dominant trust failures repeat.

U.S. water cyber incidents: 2019–2026

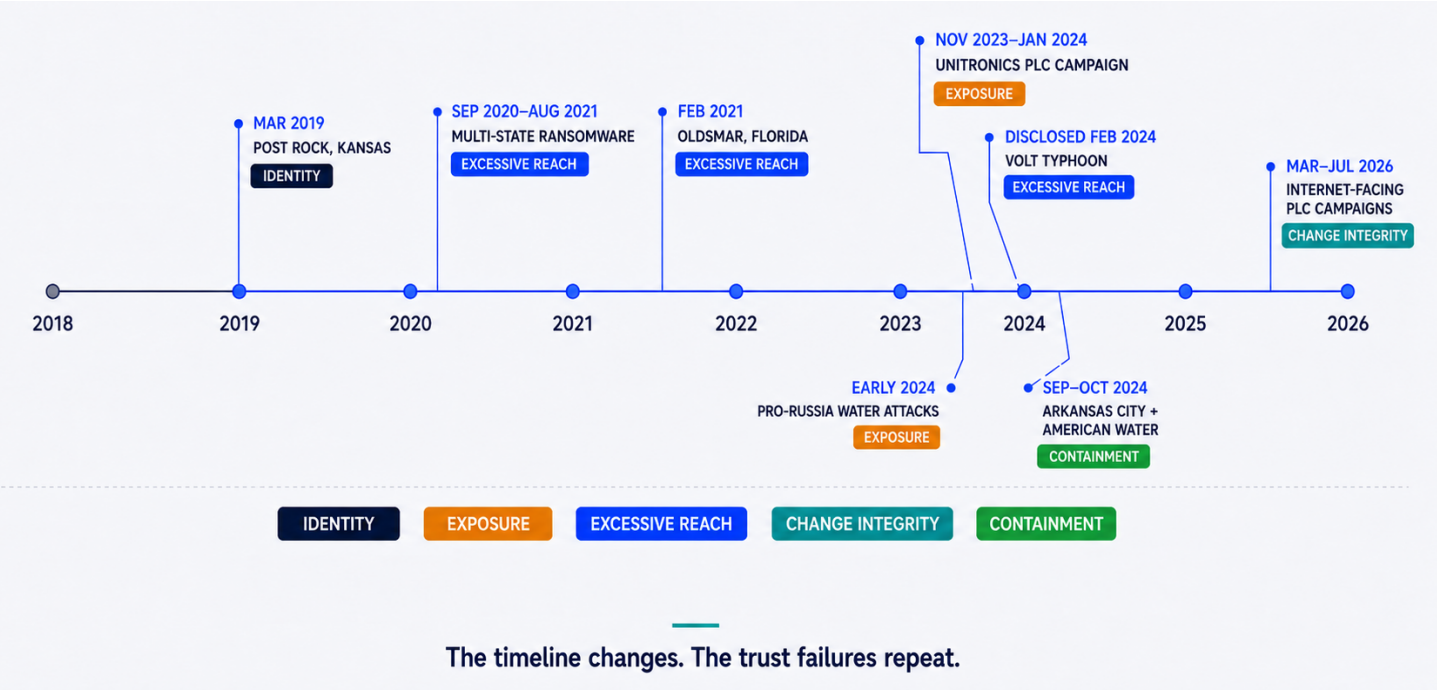


Figure 1- Major cyber incidents on U.S. water and waste water operations between 2019 - 2026

Date	Incident	Publicly reported effect	Dominant condition
Mar 2019	**Post Rock, Kansas**	A former employee used or retained remote access to shut down the plant and one filter.	**Identity**
Sep 2020–Aug 2021	**Multi-state ransomware**	Ransomware affected business and SCADA-related systems. Maine shifted to manual operations; Nevada reported SCADA and backup impacts; California malware persisted about a month.	**Excessive reach**
Feb 2021	**Oldsmar, Florida**	An operator observed and reversed a sodium-hydroxide setting change. Treatment was not affected; the FBI later could not confirm a targeted cyber intrusion.	**Excessive reach**

Nov 2023–Jan 2024	**Unitronics PLC campaign**	IRGC-affiliated actors compromised at least 75 Unitronics devices, including at least 34 in U.S. water and wastewater systems; logic and device settings were changed.	**Exposure**
Disclosed Feb 2024	**Volt Typhoon**	PRC state-sponsored actors maintained persistent access in critical-infrastructure IT, including water-sector entities, to position for possible disruption.	**Excessive reach**
Early 2024	**Pro-Russia water attacks**	Actors used exposed VNC access to change pump and blower settings, disable alarms and lock out operators. Some facilities experienced tank overflows.	**Exposure**
Sep–Oct 2024	**Arkansas City + American Water**	Arkansas City moved treatment to manual operation after suspected ransomware. American Water contained unauthorized corporate-network activity without operational impact.	**Containment**
Mar–Jul 2026	**Internet-facing PLC campaigns**	Federal reporting described password, IP and PLC project-file changes across exposed controllers. More than 30 Minnesota systems were targeted; the FBI cited incidents in at least seven states.	**Change integrity**

We do not need to speculate about attribution to learn from the architecture. The repeated conditions are already visible in how identities, network paths, control tools and recovery procedures were used.

03 | ROOT-CAUSE MODEL

The six conditions behind the repeating attack

The timeline is not merely a collection of weak passwords and old software. It reveals six conditions that repeatedly combine into a path from digital access to physical consequence.

1. **The asset cannot defend itself:** The PLC, RTU, HMI, variable-frequency drive or modem may lack native MFA, individual identity, encryption, logging or granular authorization. Unsupported assets may never receive another security patch. This is bigger than a vulnerability: it is a missing security function.
2. **The asset is reachable from somewhere it should not be:** Attackers repeatedly found internet-facing PLCs, HMIs, VNC services and cellular modems. Remote connectivity may be necessary; direct reachability is not. A user or vendor needs a controlled path to a specific resource, not network-level access to discover whatever responds.

3. **Identity lasts longer than the business need**: The 2019 insider case involved a former employee. EPA inspections have found default passwords, shared logins and access retained by former employees. The deeper failure is the absence of a reliable relationship between an individual identity, an approved task, a specific asset and a defined period.
4. **Authentication becomes broad authorization:** Traditional VPNs, jump servers and loosely segmented zones often answer only whether a user may enter the network. Once inside, the user - or an attacker using that identity - may discover unrelated devices and move toward OT. Logging in should not mean being trusted everywhere.
5. **Control changes are not independently governed:** Recent actors used legitimate engineering tools, not only custom malware. Federal investigators observed extracted project files, altered ladder logic, disabled alarms and changes that overrode safe operating instructions. Defenders must govern who uses the tool, which asset it reaches, what file moves and whether logic remains known-good.
6. **Manual operation contains the incident - but carries the burden:** Manual procedures, alert operators, stored water, physical interlocks and independent process checks repeatedly prevented worse outcomes. That is a resilience strength, but it requires people, travel, local expertise and sustained attention. It becomes harder across dozens of remote sites or during a coordinated campaign.

Six conditions keep rebuilding the attack path

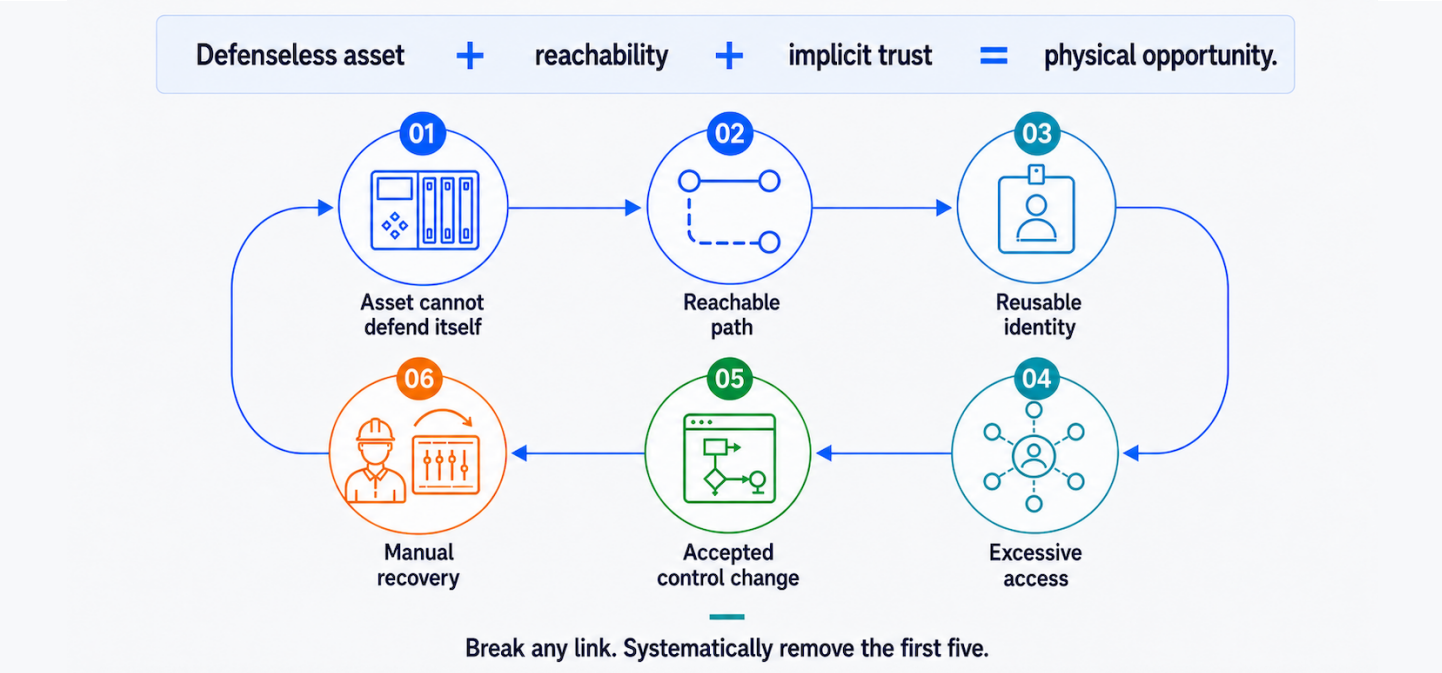


Figure 2. The repeating water cyberattack cycle. Break any link; systematically remove the first five.

DESIGN PRINCIPLE: No person, workstation, application or device should be able to exercise control solely because it can reach the controller.

04 | REMEDIATION STRATEGY

What is hard - and what can change now

Water leaders are right to resist strategies that assume unlimited funding, downtime or cybersecurity staffing. AWWA estimates drinking-water infrastructure needs of more than $2.1 trillion over the next 25 years. *The right response is a two-speed strategy: sustain a funded modernization program while immediately reducing the trust available to attackers.*

Long-cycle structural work	High-impact controls that can start now
Replace end-of-life PLCs, HMIs and operating systems	**Remove direct internet exposure from PLCs, HMIs and modems**
Redesign SCADA and wide-area communications	**Mediate every remote, local and third-party access path**
Create safe outage windows and test upgrades	**Require named identity and MFA before access reaches a legacy asset**
Recruit and retain OT cybersecurity expertise	**Replace standing vendor access with just-in-time, asset-specific access**
Modernize process safety and redundancy	**Record privileged sessions and govern engineering tools and files**
Build complete asset and dependency inventories	**Enforce user-to-asset and asset-to-asset segmentation**
Replace unsupported devices through capital plans	**Apply compensating controls and virtual patching around unpatchable assets**
Expand recovery capacity across remote sites	**Validate known-good logic, offline backups, safeguards and manual procedures**

This is not an argument against replacement. Unsupported equipment should be identified, isolated and retired through a funded plan. It is an argument against waiting for replacement before adding protection.

EPA reported helping 277 water systems eliminate 350 vulnerabilities in 2025, many through free or low-cost authentication and access-control changes. Cyber-informed engineering likewise starts with the physical consequence and works backward to the digital paths capable of causing it.

OPERATIONAL OBJECTIVE: Reduce reachability, reduce standing trust, govern every privileged interaction and contain every site - while capital modernization continues.

05 | ARCHITECTURAL RESPONSE

Give the legacy asset the security it never had

This is where Zero Trust becomes practical for water operations. Zero Trust should not be a corporate identity program that stops at the IT/OT boundary. It should govern the final interaction with the PLC, HMI, SCADA server, engineering workstation and remote field device.

For a legacy controller, the trust decision must be externalized. An enforcement layer in front of the asset can authenticate the user or machine, require MFA, evaluate policy and permit only the approved interaction. The PLC does not need to understand MFA; it must be unreachable except through a path where verification and authorization have already occurred.

Protect legacy assets and workflows with Xage

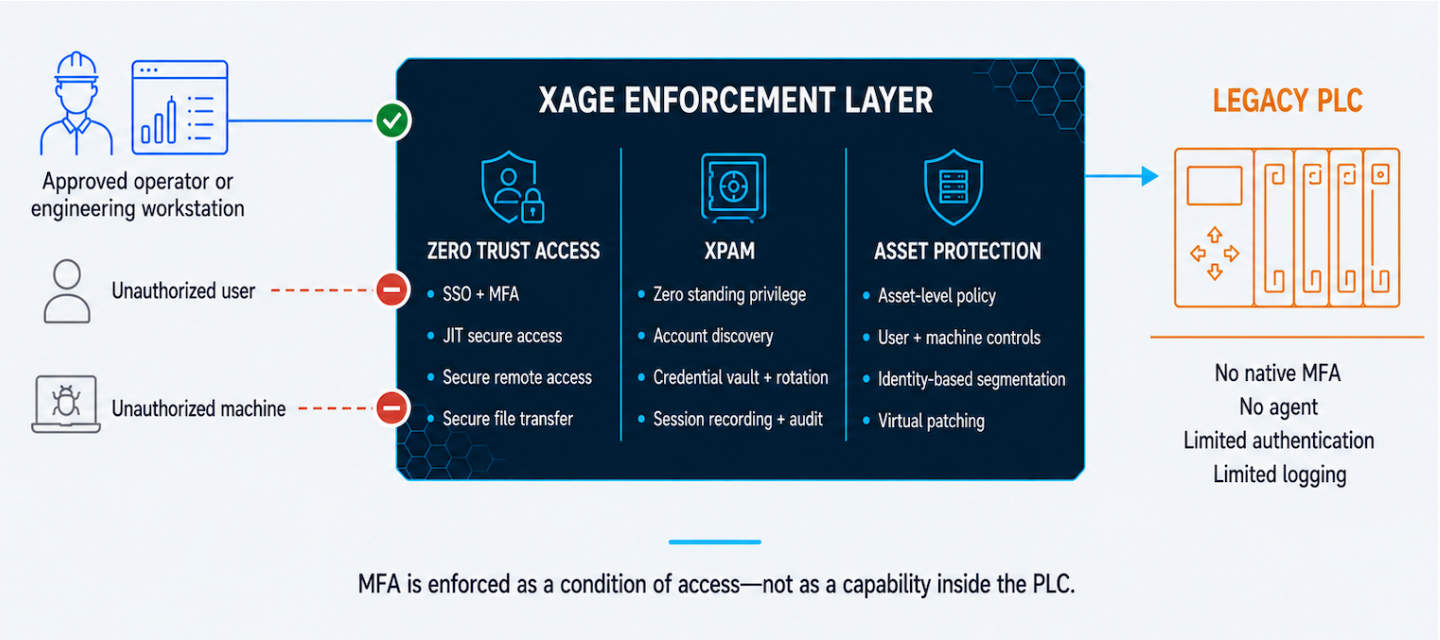


Figure 3. MFA and Zero Trust policy are enforced as conditions of access - not as capabilities inside the legacy PLC.

TECHNICAL DISTINCTION: Xage does not install MFA inside a 20-year-old PLC. Xage makes MFA and Zero Trust policy a condition of reaching it.

Xage Zero Trust Access protects the human path

Xage creates an identity-driven access layer in front of legacy and modern OT. It can apply modern trust decisions without requiring the target asset to run an agent or support native MFA.

- Require individual identity, SSO and MFA for remote and local access - even when the target device has no native authentication or MFA capability.
- Authorize a user or vendor to one specific PLC, HMI, application or engineering workstation instead of opening the OT network.
- Provide just-in-time access for an approved window and remove it automatically when the task ends.
- Support native engineering applications while controlling which asset and protocol the application may use.
- Record privileged sessions and create an audit trail tied to the actual person, target and time.
- Scan, encrypt and verify files moving into operational environments.

Xage Critical Asset Protection protects the machine path

Human access is only half the problem. A compromised workstation, application or neighboring device may also communicate with a controller. Xage Critical Asset Protection applies identity-based policy and segmentation to user-to-machine and machine-to-machine interactions, creating an asset-level security boundary around devices that cannot protect themselves.

- Prevent lateral movement within and between operational zones.
- Limit an engineering workstation to the controllers it is authorized to manage.
- Shield vulnerable or unpatchable devices with compensating controls and virtual patching.
- Convert observed legitimate communications into enforceable policy rather than relying only on static network assumptions.
- Contain compromise at one remote site so it does not become a repeatable path across the utility.

Distributed enforcement for distributed operations

Water infrastructure does not live in one data center, and security cannot depend on one either. The distributed Xage Fabric can enforce access and asset policies locally at treatment plants, wells, lift stations and other remote locations, including when WAN or cloud connectivity is denied or disrupted. It overlays the existing environment without requiring agents on protected PLCs or wholesale network replacement.

Repeated condition	Control objective	Xage architectural response
Asset cannot defend itself	Externalize identity, MFA and authorization; add compensating controls around the device.	**Zero Trust Access + Critical Asset Protection**
Reachable path	Remove direct exposure and make the approved brokered path the only route to the asset.	**Zero Trust Access**
Reusable identity	Use named users, SSO/MFA, time-bounded approvals and immediate revocation.	**Zero Trust Access / XPAM**
Excessive access	Authorize a specific person or application to a specific asset and method - not to the network.	**Zero Trust Access + segmentation**
Accepted control change	Record sessions, govern engineering tools and file movement, and restrict programming paths.	**Zero Trust Access + policy enforcement**
Manual recovery burden	Contain each site and asset, preserve local enforcement and validate recovery evidence.	**Distributed Critical Asset Protection**

Zero Trust does not replace inventory, patching, secure configuration, independent physical safeguards, engineering change control, incident response or manual recovery. It gives those programs a more defensible operating architecture and closes high-risk paths while modernization continues.

06 | EXECUTIVE ACTION

A practical 90-day agenda

The objective is not another compliance binder. It is measurable reduction in reachable assets, standing identities, access scope and uncontrolled changes - supported by evidence that each site can isolate and recover.

0–30 DAYS

Find and close direct control paths

- Inventory internet- and cellular-reachable PLCs, HMIs, modems, VNC/RDP services and vendor connections.
- Remove inbound exposure; change default/shared credentials; revoke stale access.
- Identify the digital actions with the highest physical consequence and confirm known-good logic and manual procedures.

31–60 DAYS

Make access individual, narrow and temporary

- Broker employee, integrator and vendor access and require MFA before any session reaches OT.
- Tie authorization to the person, approved asset, method and maintenance window.
- Record privileged sessions and govern engineering tools and file transfers.

61–90 DAYS

Contain the compromise you may not prevent

- Convert observed legitimate communications into asset-to-asset policy.
- Block unrelated paths and test isolation and recovery at representative remote sites.
- Measure time to determine who connected, what changed, what else was reachable and whether policy remained available during communications loss.

The executive test

At the end of 90 days, leadership should be able to answer four questions with evidence:

- Who can reach an asset capable of changing water pressure, chemical dosing, pumping or wastewater handling?
- What specific asset, protocol and time window is each person or application authorized to use?
- Can the utility determine what changed, who changed it and what other systems were reachable?
- Can policy, isolation and recovery procedures continue to operate when a remote site loses central connectivity?

OUTCOME: Fewer reachable assets. Fewer standing identities. Smaller access scope. Verifiable control changes. A materially smaller blast radius.

Break the cycle

The water sector does not need another strategy that ends with "patch, segment and train." Those practices matter, but seven years of incidents show that the underlying issue is deeper: devices that cannot verify identity remain connected through paths that assume trust after entry.

Utilities should stop asking the legacy asset to make a modern trust decision. Protect what cannot yet be replaced. Remove direct exposure. Make every human and machine interaction explicit. Put MFA, least privilege and policy in front of devices that never received them. Contain each site and each asset so one compromised path cannot become a campaign.

What leadership should measure

Indicator	Executive question
Direct OT exposure	How many PLCs, HMIs, modems and remote-control services are reachable from external networks? Target: zero.
Identity hygiene	How many shared, stale or standing privileged identities remain in operational access paths?
Brokered access coverage	What percentage of employee and vendor OT sessions use named identity, MFA and asset-specific, time-bounded authorization?
Asset policy coverage	What percentage of critical user-to-asset and asset-to-asset paths are governed by explicit enforceable policy?
Evidence and containment	How quickly can the utility identify who connected, what changed, what else was reachable and isolate the affected site?

CLOSING PRINCIPLE: The goal is not to make every water plant new overnight. It is to make every connection earned, bounded, observable and revocable - starting now.

xage SECURITY