PACKETVIPER®

Closing the Water Sector's Attack Surface

A preemptive defense blueprint for America's water and wastewater utilities, in the wake of CISA's July 2026 advisory.

WHITE PAPER

What's inside

More than 100 U.S. water systems were targeted in a single month. What CISA's July 2026 advisory says to do about it, and how PacketViper's agentless, protocol-aware architecture maps to each recommendation — without a rip-and-replace project or a maintenance window.

Prepared September 8, 2026

Executive Summary

In July 2026, the Cybersecurity and Infrastructure Security Agency (CISA) confirmed that more than 100 internet-exposed U.S. water and wastewater systems, across at least a dozen states, were targeted in a single month of cyberattacks. Attackers, believed to be Iran-linked, went after programmable logic controllers (PLCs) connected directly to cellular modems — bypassing the layered defenses that a typical enterprise network takes for granted. Days later, the water-sector technology supplier Micro-Comm disclosed that nearly 850,000 files, including proprietary engineering documentation, had been stolen and were being used to build more targeted attack tooling.

CISA's response was direct: get operational technology off the public internet, route any necessary remote access through a secure, centrally managed gateway, enforce multi-factor authentication, and monitor continuously for anomalous activity. For most municipal water and wastewater utilities, that guidance is easy to agree with and hard to execute. The controllers involved were never designed to be secured this way, budgets are constrained, staff are stretched, and the systems cannot be taken offline to install new security software.

> **A note on how to read this**
>
> This paper reflects PacketViper's own positioning and stated architecture, read against a publicly reported incident. Capability claims below describe how the platform is designed to operate against this pattern of attack, not the results of an independent evaluation specific to any one utility's environment.

This paper walks through what happened, why the water sector's operational technology is uniquely exposed, and how PacketViper's preemptive, protocol-aware, agentless approach maps directly to what CISA is now asking every utility in the country to do — without touching a single PLC, RTU, or SCADA server, and without a maintenance window.

The Wake-Up Call: What CISA Confirmed in July 2026

According to reporting corroborated by CISA's own guidance, the July 2026 campaign specifically targeted PLCs that were reachable directly over cellular modems, rather than behind any managed remote-access layer. While attackers previously used blunt tactics — default-password changes, defacement messages left on HMI screens — security researchers now describe a marked escalation: threat actors exfiltrating PLC project files using vendors' own engineering software, and modifying add-on instructions to disable safety shutdowns while leaving operator displays looking normal.

Source: Over 100 US water utilities had cyberattacks in July, says CISA — SC Media

That trajectory accelerated with the Micro-Comm disclosure. Because Micro-Comm supports the engineering, configuration, and remote maintenance of control systems used across hundreds of utilities, the stolen files reportedly include product diagrams, system architecture documentation, and customer-specific configurations — the kind of detail that turns generic scanning into precision-guided targeting, and that industry analysts warn can now be handed to AI tools to generate working exploitation scripts with far less technical expertise than in years past.

Source: CISA: Over 100 Internet-Exposed Water Systems Targeted in July Cyberattacks — SecurityWeek

CISA's core finding is not that any one utility made a unique mistake. It is that internet-exposed OT, reachable without a managed gateway in between, is now a routine and repeatable target across the entire sector.

Why Water and Wastewater Utilities Are Uniquely Exposed

Operational technology that predates modern security

Modbus — the protocol underlying most water treatment and distribution control systems — was designed in 1979 for isolated serial links. It has no authentication, no authorization model, and no encryption. Any device that can reach a Modbus endpoint can command it: there is no built-in way to distinguish an engineer's legitimate setpoint change from an attacker's. Traditional firewalls can see that traffic is moving over TCP port 502, but they cannot see what command is inside the packet, which leaves operators with only two options — allow all Modbus traffic, or block it entirely. Neither is workable for a treatment plant that has to keep running.

Distributed, unmanned infrastructure

Water systems are not one control room; they are dozens or hundreds of pump stations, lift stations, and remote monitoring points, often unmanned, often with limited power and bandwidth, and often reachable only by a technician driving out to the site. That is precisely the profile CISA flagged: PLCs wired directly to a cellular modem because it was the fastest and cheapest way to get remote visibility, with no secure gateway in the path.

Constrained budgets and lean teams

Most municipal utilities do not have a 24/7 security operations center, and many cannot add IT-style security tooling that requires specialized training to operate. A solution that adds another interface OT staff don't understand, or that requires downtime to install, is a solution that will not get deployed — or will not get used once it is.

Why Conventional IT Security Falls Short Here

- Perimeter firewalls inspect ports and packets, not industrial commands — they cannot tell a routine sensor read from a malicious write to a chemical dosing register.
- Endpoint agents cannot be installed on PLCs, RTUs, or HMIs — many of these devices cannot run any third-party software at all.
- Active vulnerability scanning, a staple of IT security, can itself destabilize fragile legacy controllers not built to withstand it.
- Signature- and anomaly-based IT tools generate false positives that OT operators learn to ignore, which is functionally the same as having no monitoring at all.
- Rip-and-replace modernization is often the only "correct" fix on paper — and the least realistic one for a utility that cannot take a plant offline or fund a multi-year capital project.

These are not failures of effort; they are a mismatch between tools built for IT networks and the operational reality of a treatment plant. Closing the gap CISA identified requires security that is native to the control-system protocol itself, not layered awkwardly on top of it.

A Preemptive Defense Blueprint: Mapping CISA's Guidance to Action

PacketViper was built for exactly this environment: agentless, protocol-aware, inline enforcement that requires no software on legacy OT devices and no maintenance window to deploy. The table below maps CISA's July 2026 recommendations directly to how the platform addresses each one.

CISA Recommendation (July 2026 Advisory)	The Underlying Gap	How PacketViper Closes It
Identify all internet-exposed OT assets	Most utilities have no reliable, current inventory of what's reachable from the public internet.	Passive, agentless discovery across Modbus, DNP3, BACnet, S7COMM and other OT protocols — no active scanning that could disturb sensitive controllers.
Route remote access through a secure gateway instead of connecting directly to a PLC, HMI, or RTU	Direct PLC-to-cellular-modem connections — the exact pattern CISA says attackers exploited in July — remove any inspection point.	Inline enforcement appliances sit in front of every PLC/RTU/HMI, terminating and inspecting sessions before they ever reach the controller.
Change default credentials and enforce MFA for remote access	Credential hygiene alone doesn't stop an attacker who is already inside the session or spoofing a trusted source.	Geographic and time-based behavioral controls flag and block access outside approved windows and locations, layered on top of credential and MFA policy.
Patch and update systems where supported	A large share of water-sector OT runs on decades-old, unpatchable, or vendor-unsupported equipment.	Command-level Modbus protection acts as a compensating control — enforcing which commands and values are allowed — without ever touching the legacy device.
Continuously monitor for anomalous activity	Small utility teams cannot staff a 24/7 SOC, and generic IT tools generate alerts OT operators don't trust or understand.	Deceptive responders generate zero false positives — any interaction is by definition unauthorized — with alerts delivered in formats OT operators already recognize.

Table 1: CISA's water-sector guidance mapped to PacketViper capabilities.

Inside PacketViper's Approach for Water and Wastewater

Command-level Modbus protection

Rather than allowing or blocking Modbus traffic wholesale, PacketViper sits transparently in the traffic path as an agentless bridge and parses the Modbus Application Protocol header and payload to extract the unit ID, function code, register or coil address, and the specific value being written. That allows operators to build "surgical" policy — for example, permitting a historian to read tank levels while blocking any external source from writing to a chemical-dosing register — without disrupting legitimate control traffic. A simplified view of how function codes are classified for enforcement purposes:

Code	Function	Class	Risk if Unrestricted
1–4	Read Coils / Registers	Read	Low
5–6	Write Single Coil / Register	Write	State-changing — e.g., chemical dosing setpoints, valve position
15–16	Write Multiple Coils / Registers	Write	State-changing across multiple points simultaneously
8	Diagnostics	Control	Abuse risk — can force a controller into listen-only mode (a physical denial-of-

Code	Function	Class	Risk if Unrestricted
			service)
43	Read Device Identification	Recon	Fingerprinting — used to map targets before an attack

Table 2: A representative subset of Modbus function codes and how PacketViper's inspection engine classifies their risk.

Deployment follows a deliberately conservative philosophy — "start open, narrow in." The system first runs in observation mode, learning legitimate master/slave communication patterns with zero enforcement risk, before operators move to active policy and, finally, enforcement — dropping a single violating command while the rest of the session continues uninterrupted, or isolating a source entirely if it exceeds a write-rate threshold consistent with a flood or enumeration attack.

Automated Moving Target Defense and deception

PacketViper continuously reconfigures the network's visible attack surface — IP addresses, ports, and communication paths — so that reconnaissance, the first phase of nearly every attack described in CISA's advisory, yields outdated or misleading information. Deceptive responders that mimic real PLCs, RTUs, and SCADA endpoints add a second layer: because any interaction with a decoy is by definition unauthorized, alerts arrive with no false-positive tuning required, which matters enormously for lean utility teams who cannot staff a SOC to chase down noise.

Built for the field: unmanned, low-power, low-bandwidth sites

Water utilities' greatest exposure sits at the edge — unmanned pump stations and treatment points, often DC-powered with limited connectivity. PacketViper's remote enforcement appliances are DIN-rail mounted, low-power, and equipped with hardware bypass, so that if the device itself loses power or faults, physical operations continue uninterrupted rather than failing closed. Enforcement continues locally even without a live connection back to a network operations center, and results — a block, an isolation — propagate automatically once connectivity is restored.

Centralized policy at municipal scale

For a utility system with dozens or hundreds of remote sites, a policy authored once and pushed identically to every appliance in the network — regardless of which physical path traffic takes to get there — turns a fragmented, site-by-site security problem into a single, centrally managed one.

Regulatory Context: AWIA, EPA, and the State Patchwork

Under America's Water Infrastructure Act (AWIA) Section 2013, community water systems serving more than 3,300 people are required to complete a risk and resilience assessment that treats cyberattacks as a "malevolent act," develop an emergency response plan, and recertify both every five years. AWIA does not prescribe a specific control set, but EPA enforcement activity has repeatedly cited basic failures — default passwords, shared logins, and access left open for former employees — as evidence that an assessment was superficial. EPA's 2023 attempt to fold cybersecurity directly into state sanitary surveys was challenged in court and withdrawn, which has shifted meaningful enforcement to the state level: New Jersey, California, and others are already layering requirements on top of the federal floor.

The American Water Works Association (AWWA), partnering with EPA, CISA, and NIST, has published its own practical guidance built around the NIST Cybersecurity Framework: identify exposure, secure remote access, eliminate unnecessary internet-facing devices, and implement multi-factor authentication as immediate steps, followed by a documented risk management and incident response program. PacketViper's continuous monitoring, automated audit trail, and command-level enforcement generate the kind of evidence — of both control and monitoring — that these assessments and recertifications increasingly require, whether the recertification is being reviewed by EPA, a state regulator, or an internal governance board.

The Business Case: Security That Pays for Itself

Because PacketViper deploys inline at the boundary and at remote sites, its impact shows up in cost lines beyond the security budget alone. Deployments have typically reduced firewall traffic load by 30–70% within 90 days, restoring capacity on existing perimeter hardware and, in many cases, avoiding or delaying an expensive forklift firewall upgrade. That same traffic reduction — less noise, fewer events to triage — has driven reported reductions of more than 30% in the cost of volumetrically priced managed SIEM and SOC services for some clients.

For remote and unmanned facilities specifically, running detection and enforcement on ruggedized field appliances removes the need for a dedicated on-site industrial server and its associated acquisition, deployment, patching, and monitoring costs — a material line item multiplied across dozens or hundreds of remote pump stations and lift stations. And because the platform's deceptive elements and contextual filtering are false-positive free by design, utilities that have previously failed a penetration test with no cost-effective remediation path have used PacketViper as a documented compensating control, closing the finding without a capital project.

A compensating control, not a replacement for patching

None of this argues against patching where it's possible — it argues for not relying on patch cycles alone in an environment where a large share of controllers cannot be patched at all. Because PacketViper enforces behavior and protocol-level intent rather than a signature for a specific CVE, it does not need advance knowledge of a vulnerability to add a layer of defense-in-depth against the pattern it represents.

None of this requires an integration project: PacketViper is deployed inline, in front of existing infrastructure, and begins producing results from day one.

Case in Point: Oldsmar, Florida

In February 2021, an attacker gained access to a water treatment facility in Oldsmar, Florida, through remote access software that had been enabled during the shift to remote work and that lacked multi-factor authentication, geographic controls, or behavioral monitoring. The attacker increased the sodium hydroxide (lye) setpoint from 111 parts per million to 11,100 — a concentration dangerous to public health — and the change was caught and reversed by an operator who happened to notice the mouse moving on screen, roughly 30 seconds after the fact.

Oldsmar remains the clearest illustration of the exact gap CISA is now asking every water utility to close: a single point of unmanaged, unauthenticated remote access to a safety-critical control point, with detection resting entirely on a human happening to be watching at the right moment. Geographic and behavioral access controls, combined with command-level enforcement that would have flagged or blocked the out-of-range setpoint value itself, close that gap by design rather than by chance.

Conclusion: Turning Guidance Into a Roadmap

CISA's July 2026 advisory is not a warning about a single utility's mistake — it is a statement that the entire sector's pattern of internet-exposed OT is now a routine target. For municipal water and wastewater utilities, closing that gap does not require replacing control systems that have run reliably for decades, and it does not require a security operations center the utility cannot staff or afford.

It requires security that speaks the same protocol as the control system it protects, that enforces policy inline without an agent, and that keeps working at the edge even when connectivity does not. That is the specific problem PacketViper was built to solve for critical infrastructure, and it is available today — without a rip-and-replace project, and without a maintenance window.

To see how your utility's internet exposure compares to the pattern CISA described in July, or to walk through a no-cost assessment of your remote sites, contact PacketViper at www.packetviper.com.

Sources

- Over 100 US water utilities had cyberattacks in July, says CISA — SC Media
- CISA: Over 100 Internet-Exposed Water Systems Targeted in July Cyberattacks — SecurityWeek
- More than 100 water systems were hit in July cyberattacks — The Register
- EPA Water Cybersecurity Mandate: A Practical Guide — HydroKnowledge
- Cybersecurity Guidance — American Water Works Association (AWWA)
- PacketViper — Preemptive Network Security for IT & OT