

THE ULTIMATE BUYER'S GUIDE FOR

WATER & WASTEWATER CYBERSECURITY PLATFORMS:

Protecting OT, IoT, and all other Cyber-Physical Systems

TABLE OF CONTENTS

Read this guide to learn more about:


Industrial cybersecurity landscape →


Criteria to consider when looking for a CPS security solution →


Key principles to achieving cyber and operational resilience →


Core Controls to Evaluate a CPS Security Vendor →

In state and local government operations, CPS encompasses the operational technology (OT) assets and connected devices that underpin essential community services—particularly public utilities such as water and wastewater systems. These systems are critical to the safe and efficient delivery of potable water, treatment and recycling of wastewater, reliable distribution processes, and regulatory compliance.

Key examples of CPS in water and wastewater operations include:

Traditional OT assets such as programmable logic controllers (PLCs) and remote terminal units (RTUs) that regulate water treatment plants, pumping stations, and distribution networks.

Internet of Things (IoT) and Industrial IoT (IIoT) devices like smart meters, connected flow sensors, pressure monitors, and water quality sensors, which enable real-time data exchange and predictive maintenance to optimize system efficiency and resilience.

Smart infrastructure and building management systems (BMS) within municipal water facilities, including HVAC, energy management, access control, and process automation systems, which ensure reliable, real-time operations in mission-critical environments.

By integrating these CPS technologies, water and wastewater utilities can improve operational visibility, enhance safety and reliability, and respond more effectively to both routine management needs and emergency situations.







STATE & LOCAL GOVERNMENT CYBERSECURITY LANDSCAPE

Digital Transformation & IT/OT Convergence

The "Smart Water" revolution has connected previously isolated OT environments with IT counterparts. While this convergence promises efficiencies in billing, analytics, and reporting, it has also given cyber-criminals new pathways into inherently insecure OT environments. An attack that once required physical access can now be launched from anywhere in the world, moving from the billing system directly to the PLCs that control water flow and chemical treatment.

Legacy Infrastructure

Many water utilities operate on equipment that is decades old, installed long before cybersecurity was a consideration. As digital transformation accelerates, these previously "air-gapped" devices, running legacy operating systems and unpatchable firmware, are now being connected to the network. The cost and operational disruption required to replace this equipment, such as shutting down a primary treatment basin, make full "rip and replace" projects impractical, leaving utilities with a permanently vulnerable foundation. This challenge is further compounded by the fact that most water systems in the U.S. are small, rural operations without the in-house technical expertise to manage these complex environments.

Modernized Workforce

The shift to remote and hybrid workforces has brought a wave of modernization to water and wastewater utilities, but it also introduces new challenges. Upgrading treatment plants, pumping stations, and distribution networks with connected sensors, automated controls, and integrated IT/OT systems can create complexity and expose previously isolated systems to potential vulnerabilities. Balancing the adoption of modern technologies with the continued reliance on legacy hardware and software requires careful planning, coordination, and ongoing oversight to maintain both operational continuity and security.

According to CISA 2025 report, Many OT systems are increasingly connected to business operations and applications that rely on process data and trends analysis for operations. If not assembled and integrated securely, these connections can introduce paths for cyber actors to move between networks.[1]

70%

According to Gartner, By 2027, **70% of OT security incidents** will originate from unmanaged IoT devices.[2]

68%

of organizations expect to face increased challenges in cybersecurity due to remote working.[3]

Remote Access

Water systems are inherently geographically dispersed, requiring utilities to rely on remote access for both internal staff and third-party vendors to support unstaffed sites such as pump stations, lift stations, and water towers. Without purpose-built controls, this remote access can bypass network segmentation, creating the primary entry point for attackers, including ransomware groups.

Mounting Regulatory Pressure

As a result of these growing risks, the EPA is taking a more proactive role, and regulatory requirements are tightening. The America's Water Infrastructure Act (AWIA), EPA enforcement alerts, and CISA advisories establish clear minimum standards for cybersecurity. Drinking water systems are now required to conduct risk assessments and develop emergency response plans that explicitly address cyber threats. To support compliance, the EPA offers direct technical assistance and resources such as the *Cybersecurity Procurement Evaluation Checklist*, helping utilities ask the right questions of their vendors.

Dutton explained that oftentimes, water and wastewater systems are using unsecured human machine interface (HMI) devices. By simply obtaining the device's IP address, he warned that "anybody with an internet connection could find it and turn off valves, turn on valves, change set points, change chemical levels".[4]

60%

New research from MeriTalk and Claroty reveals that **60% of federal & state OT leaders** say their agency lacks sufficient in-house expertise for OT/cyber-physical systems.[5]

WATER & WASTEWATER EDITION

CRITERIA TO CONSIDER AT THE COMPANY LEVEL

Water Sector Expertise

Many CPS systems in water and wastewater utilities rely on proprietary industrial protocols and legacy devices that traditional IT security tools cannot adequately protect. It is critical to evaluate vendors that are OT-centric and demonstrate deep expertise in the water sector. Key criteria include native recognition of the specific protocols used in W/WW environments, such as Modbus, DNP3, and EtherNet/IP, and a proven track record of deployments with similar utilities. Vendors with real-world experience in water and wastewater operations are better equipped to secure treatment plants, pumping stations, distribution networks, and other mission-critical assets.

Portfolio Breadth and Depth

A CPS security vendor should provide a unified platform that addresses all stages of the cybersecurity journey from asset discovery to threat detection, monitoring, and secure operational workflows. Robust and scalable options for both on-premise and SaaS deployments ensure flexibility across diverse network architectures, utility sizes, and regulatory frameworks such as AWIA, NIST CSF, and CISA CPGs. The platform should empower utilities to maintain visibility and control across all CPS assets while meeting operational and compliance needs without adding unnecessary complexity.

Industry Contributions and Research

A vendor's commitment to advancing cybersecurity is reflected in its research capabilities. Look for providers with in-house teams actively discovering and responsibly disclosing vulnerabilities in ICS and OT devices common in the water sector, including PLCs, RTUs, network switches, and other automation hardware. This demonstrates the ability to protect against both known and emerging threats, ensuring water and wastewater operations remain resilient in the face of evolving risks.

Service and Integrator Support

Given the ongoing cybersecurity skills gap in the water sector, utilities often rely on third-party integrators and Managed Security Service Providers (MSPs) for OT security. Research from MeriTalk and Claroty shows that 60 percent of federal OT leaders report insufficient in-house expertise for managing OT and CPS systems. Vendors should therefore offer a strong ecosystem of trained integrator partners and robust support services. The platform should enhance the capabilities of your existing team or a trusted MSSP rather than requiring utilities to hire a separate group of cybersecurity specialists.





KEY PRINCIPLES FOR ACHIEVING CYBER AND OPERATIONAL RESILIENCE

Gain CPS Visibility

Complete, granular visibility into your OT/ICS environment is the cornerstone of any CPS security strategy. This directly addresses the top gap identified by the EPA: a "general lack of asset awareness." Utilities cannot protect what they cannot see, and as the EPA found, many were unaware that critical devices were exposed to the internet.

Achieving this visibility in water and wastewater environments is especially challenging. Many assets rely on proprietary protocols and legacy systems that are fragile, meaning traditional IT network scans could crash a PLC or disrupt operations. For this reason, it is crucial to choose a CPS solution that offers multiple, flexible discovery methods to safely deliver full visibility across your CPS landscape. This approach ensures all assets are accurately identified and mapped without compromising operational continuity or regulatory compliance.

Integrate Your Existing IT Tools & Workflows with OT

State and local agencies often operate critical infrastructure that depends on legacy systems and proprietary protocols. While these assets may not be compatible with traditional IT security tools, they remain essential to operations and cannot simply be replaced. Rather than adding more complexity to an already extensive technology environment, agencies should evaluate CPS security solutions that integrate seamlessly with existing OT and IT systems.

By extending current tools and workflows from IT into the OT environment, such as your NGFW, SIEM, SOAR, or CMDB, utilities can safely uncover previously hidden risks without disrupting mission-critical operations. This approach enables organizations to centralize visibility and risk management across departments that have historically operated in silos. Integration also maximizes the value of existing technology investments, reduces operational risk, and establishes a unified strategy for securing both legacy and modern infrastructure.

Extend Your IT Security Controls & Governance to Your XIoT Environment

Water systems rely on legacy OT/ICS systems designed for operational reliability and safety rather than cybersecurity. As these systems increasingly connect to IT networks, visibility and governance gaps emerge, leaving utilities vulnerable to operational and cyber risks.

When evaluating CPS security solutions, water systems should prioritize platforms that enable centralized governance and robust reporting across all CPS assets. Key features include automated compliance reporting, audit trails for operational changes, policy enforcement across both IT and OT environments, and dashboards that provide actionable insights for executive and operational teams. Solutions should integrate with existing IT tools such as NGFWs, SIEMs, SOAR platforms, and CMDBs to resist or contain threats, unify visibility, risk management, and decision-making. By strengthening governance and reporting, utilities can ensure accountability, meet regulatory requirements, and maintain operational resilience across mission-critical water systems.





EVALUATE CPS SECURITY VENDORS BY THESE CORE CONTROLS

EVALUATE CPS SECURITY VENDORS BY THESE CORE CONTROLS

CORE CONTROLS	EVALUATION CRITERIA
Asset Management Most water systems lack a complete and up-to-date asset inventory, creating critical security and operational gaps. Legacy OT systems often use proprietary protocols that standard tools cannot track, leaving treatment plants, pumping stations, and distribution networks exposed. Manual inventories cannot keep pace with emerging vulnerabilities, outdated firmware, or regulatory and operational reporting requirements, putting mission-critical water and wastewater systems at risk.	• Supports proprietary industrial protocols (Modbus, DNP3, etc.) and provides multiple, safe collection methods (especially passive). • Continuously monitors and automatically inventories all assets, including vendor, model, firmware version, and backplane configuration. • Optimizes workflows by integrating with your CMDB to align enterprise and industrial environments.
Exposure Management Finding a vulnerability alone is not enough. In water and wastewater OT environments, standard IT vulnerability scanners cannot be used because they are disruptive and potentially dangerous. Additionally, patching is rarely permitted due to 24/7 operational requirements, regardless of a vulnerability's severity. Agencies must therefore assess each asset's context and potential operational impact to prioritize and remediate risks effectively while maintaining safe, continuous operations.	• Accurately matches exact assets with known exploitable vulnerabilities (KEVs) based on vendor, model, and firmware version, all without disruptive active scanning. • Evaluates and scores vulnerabilities based on the unique risk they pose to your specific water process, allowing for efficient prioritization. • Provides recommended compensating controls (e.g., segmentation policies, rule-tuning) to mitigate risk when patching is not an option.
Network Protection Many networks across water systems remain flat, greatly expanding the blast radius and enabling attackers to move easily from less-critical assets to core PLCs that control critical treatment processes. Manually defining and enforcing network segmentation is time-consuming, complex, and prone to errors, leaving critical systems exposed.	• Provides recommended segmentation policies, based on observed traffic, that can be easily enforced via your existing infrastructure (firewalls, switches). • Enables continuous monitoring to understand normal asset communication, allowing for automatic alerts on any policy violations.

EVALUATE CPS SECURITY VENDORS BY THESE CORE CONTROLS

CORE CONTROLS	EVALUATION CRITERIA
Secure Access Traditional remote access tools (VPNs, RDP) are designed for IT, not OT. They grant broad, “all-or-nothing” network access, are cumbersome for third-party vendors, and lack the monitoring needed to stop risky user actions. This is how unsecured HMIs become internet-exposed, creating a direct path for attackers to critical processes.	• Provides a purpose-built solution for secure remote access to OT environments. • Defines and enforces granular, time-bound , role-and-policy-based access controls • Supports Zero Trust and least-privilege principles. • Includes real-time session monitoring with the ability to supervise and terminate sessions.
Threat Detection Proprietary protocols in OT environments are invisible to traditional threat detection tools. IT-based solutions cannot differentiate between legitimate engineering commands and malicious actions aimed at disrupting critical processes, such as altering chemical dosing.	• Utilizes multiple detection engines including behavioral, signature-based, and policy-driven methods to automatically profile all assets, communications, and processes. • Possesses deep knowledge of water and wastewater protocols and device behaviors, enabling the detection of anomalies and malicious commands within legitimate traffic. • Offers a comprehensive portfolio of threat detection capabilities that integrates seamlessly with existing SIEM and SOAR tools, helping bridge the IT-OT expertise gap.
Incident Response When an alert fires, the security team or MSSP often lacks the operational context needed to respond effectively. Questions such as what a particular PLC controls or how taking it offline would affect water quality can cause critical delays, wasting valuable time during an incident.	• Provides rich, contextual data for every alert, integrating with response playbooks in your SOAR. • Offers asset and communication details that help personnel (both on-site and remote) quickly troubleshoot operational issues or respond to security incidents. • Provides comprehensive reporting to support recovery efforts and demonstrate compliance for AWIA audits.

The pressure to reinforce the cybersecurity of our nation's water infrastructure has never been higher. As cybercriminals become more sophisticated, partnering with the right CPS security vendor is a critical step in protecting your operations and ensuring public safety.

The vendor selection process is not easy. By using this guide and evaluating vendors against these core capabilities, your utility can select a true partner that directly addresses the visibility and asset awareness gaps identified by the EPA. The right solution should not be just another tool but a unified platform that provides comprehensive visibility, context-aware risk management, and robust controls to protect your entire CPS ecosystem, ensuring the safety, reliability, and availability of our most critical resource.



[1] https://www.cisa.gov/sites/default/files/2025-08/joint-guide-foundations-for-OT-cybersecurity-asset-inventory-guidance_508c.pdf?
[2] https://www.gartner.com/en/conferences/apac/security-risk-management-australia/featured-topics/operational-technology-iot-security?
[3] https://blog.gitnux.com/remote-work-cybersecurity-statistics/#:~:text=63%25%20of%20businesses%20have%20experienced,it%20comes%20to%20remote%20work.
[4] https://www.cisa.gov/resources-tools/resources/internet-exposed-hmis-pose-cybersecurity-risks-water-and-wastewater-systems
[5] https://www.meritalk.com/articles/epa-finds-major-cyber-gaps-in-water-sector-pushes-for-greater-visibility/

Configuration Management Database (CMDB	Configuration management database (CMDB) is a database that contains all relevant information about the hardware and software components used in an organization's IT services and the relationships between those components.
Cyber-Physical Systems (CPS)	Cyber-physical systems are defined by Gartner as engineered systems that orchestrate sensing, computation, control, networking and analytics to interact with the physical world — resulting in improved operations, resilient, reliable systems, and a deeper understanding of the physical things they control.
Known-Exploited Vulnerabilities (KEV)	A CISA-maintained database of vulnerabilities that have been exploited in the wild.
Configuration Management Database (CMDB	Configuration management database (CMDB) is a database that contains all relevant information about the hardware and software components used in an organization's IT services and the relationships between those components.
Security Information & Event Management (SIEM)	A security information and event management (SIEM) platform ingests network, application, and system-level log data in real-time to provide synthesis of insights and threat intelligence for security operations teams.
Security Orchestration Automation & Response (SOAR)	A security orchestration, automation & response (SOAR) platform is a trigger-based solution performing actions on systems and infrastructure for the purpose of containing threats and streamlining incident response, provided quality real-time event data.



About Claroty

Claroty has redefined cyber-physical systems (CPS) protection with an unrivaled industry-centric platform built to secure mission-critical infrastructure. The Claroty Platform provides the deepest asset visibility and the broadest, built-for-CPS solution set in the market comprising exposure management, network protection, secure access, and threat detection – whether in the cloud with Claroty xDome or on-premise with Claroty Continuous Threat Detection (CTD). Backed by award-winning threat research and a breadth of technology alliances, The Claroty Platform enables organizations to effectively reduce CPS risk, with the fastest time-to-value and lower total cost of ownership. Claroty is deployed by hundreds of organizations at thousands of sites globally. The company is headquartered in New York City and has a presence in Europe, Asia-Pacific, and Latin America.

For more information, visit claroty.com or email contact@claroty.com.

©Copyright Claroty Ltd. All rights reserved.