

Securing Water Utility Operations with Cisco Cyber Vision

Protect source-to-tap operations by turning the industrial network into a defense system.



Benefits

- **Comprehensive visibility:**
See sanctioned and unsanctioned assets, communications, and remote-access paths across plants and remote sites.
- **Current, risk-informed inventory:**
Maintain asset profiles with identity, firmware, vulnerabilities, behavior, and prioritized risk context.
- **Network-native protection:**
Use compatible industrial switches and routers for OT sensing and enforcement without a separate visibility network.
- **Controlled remote access:**
Give employees, integrators, and vendors least-privileged, time-bound access to authorized OT assets.
- **Unified IT/OT operations:**
Share operational context with Cisco and Splunk workflows for correlation, investigation, and response.

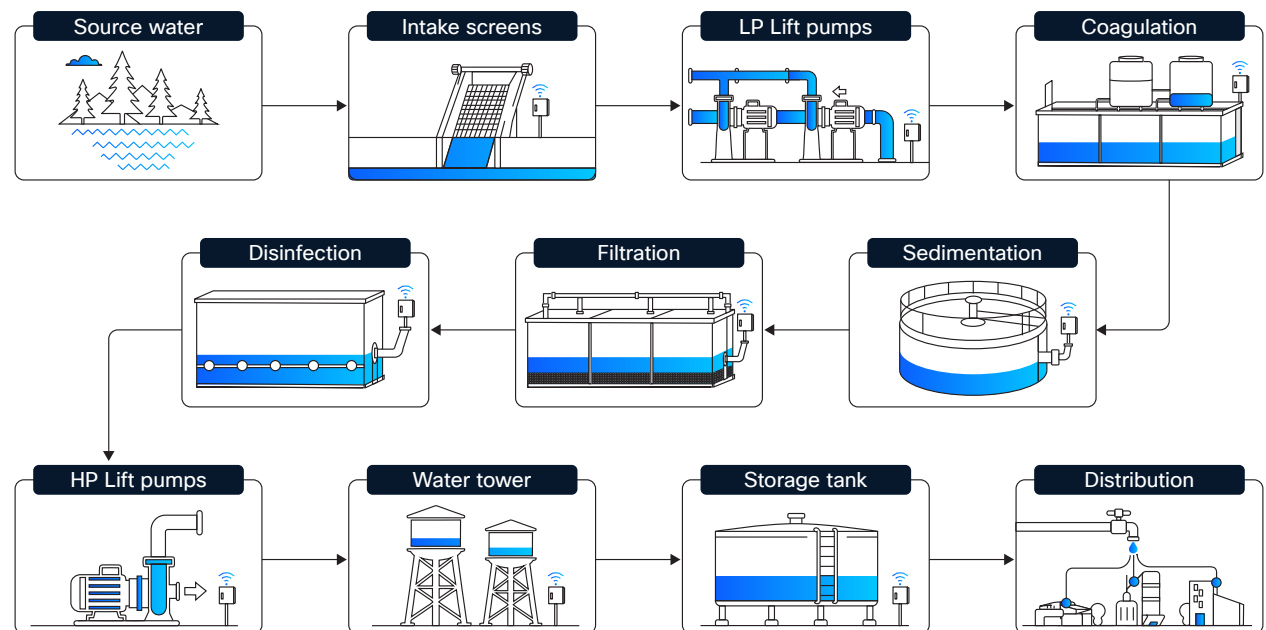
Water utilities depend on distributed operational technology across source–water intake, treatment and chemical dosing, pumping and storage, distribution and metering, wastewater operations, and physical security. Long asset lifecycles, remote sites, vendor access, and uneven visibility can make legitimate connectivity difficult to govern. Cybersecurity must reduce risk without interrupting safe, continuous service.

Cisco® industrial switches and routers, combined with Cisco Cyber Vision, provide a network-integrated foundation for securing water operations—continuously identifying OT assets, assessing risk, and turning process context into actionable security policy. Comprehensive asset visibility, AI-assisted segmentation, secure remote access, and integrations across Cisco and Splunk give operations, IT, and security teams a shared view from source water through wastewater.

How Cisco Cyber Vision helps secure water utility operations

Cisco Cyber Vision gives operations, IT, and cybersecurity teams a common understanding of OT inventory, risk, and communications. AI-assisted grouping and policy recommendations help design segmentation, while simulation shows potential impact before enforcement. Cisco Cyber Vision provides zero-trust remote access to specific OT assets when needed. Asset, vulnerability, activity, and security-event telemetry can be operationalized in Cisco Extended Detection and Response (Cisco XDR) and Splunk for dashboards, correlation, investigation, and response.

Connected Water Utility



Cisco Cyber Vision across water utility use cases

Water utility domain	Visibility	Segmentation	Secure remote access	Operational outcome
Source Water and Intake	- Identify intake controls, gates, pumps, analyzers, Remote Telemetry Units (RTUs), and communications - Map dependencies across reservoirs, raw-water stations, and telemetry	- Group assets by watershed, intake site, or process function - Preserve approved telemetry and control flows	- Limit staff and vendors to named intake and telemetry assets - Apply approved, time-limited sessions	- Protect raw-water availability and early-warning visibility - Reduce exposure across remote intake sites
Treatment and Dosing	- Inventory Programmable Logic Controllers (PLCs), Human Machine Interfaces (HMIs), analyzers, chemical-feed skids, and safety systems - Track setpoints, firmware, vulnerabilities, and process communications	- Create zones for filtration, disinfection, dosing, and laboratory systems - Simulate policies before enforcement	- Restrict integrators to assigned treatment assets - Monitor and audit maintenance sessions	- Reduce risk to treatment continuity and water quality - Contain issues to a process area
Pumping and Storage	- Map booster pumps, Variable Frequency Drives (VFDs), reservoirs, tanks, pressure sensors, and RTUs - See dependencies across Supervisory Control and Data Acquisition (SCADA) and field communications	- Separate stations and storage sites by pressure zone or fault domain - Permit only required supervisory traffic	- Grant access to specific stations and controllers - Use identity-, time-, and approval-based controls	- Keep pressure and flow stable - Limit multi-site propagation

Water utility domain	Visibility	Segmentation	Secure remote access	Operational outcome
Distribution and Metering	- Identify pressure and flow monitors, Pressure Reducing Valves (PRVs), Advanced Metering Infrastructure (AMI) gateways, and district meters - Map links to Geographic Information Systems (GIS), AMI, and operations platforms	- Separate AMI, field telemetry, and enterprise services - Restrict flows to approved protocols and destinations	- Limit field teams and vendors to assigned gateways and sites - Record high-risk sessions	- Preserve service visibility - Reduce lateral movement from edge and AMI systems
Wastewater Operations	- Inventory lift-station RTUs, pumps, process controls, and analyzers - Map remote-site behavior and alarm dependencies	- Zone collection, headworks, treatment, and discharge systems - Preserve required control and alarm flows	- Restrict access to named lift stations and process assets - Schedule and audit vendor sessions	- Reduce overflow and discharge risk - Contain incidents by site or process
Labs, Buildings and Security	- Identify lab interfaces, HVAC/ Building Management System (BMS), cameras, access control, and gateways - Map dependencies with OT and enterprise systems	- Separate support and security systems from control zones - Create distinct BMS, video, and access-control zones	- Limit contractors to named systems and devices - Provide approved, time-limited access	- Preserve site safety and security - Reduce third-party and lateral-movement risk

The operational impact

- **Greater resilience** across plants, pump stations and remote sites
- **Continuous visibility** into connected assets, communications, and risk
- **Smaller blast radius** through process-informed segmentation
- **Safer, auditable access** for operators, integrators, and equipment vendors
- **Faster, coordinated response** across operations, IT, and cybersecurity

Create a protected, resilient, and controlled foundation for water operations

Secure the OT infrastructure that supports safe, continuous water service.

Keep critical sites connected

Build resilient connectivity across plants, pump stations, storage facilities, and remote sites using ruggedized switching, redundant paths, and appropriate uplinks.

Know what is connected—and at risk

Identify OT assets from source water through wastewater, identify their vulnerabilities and risk, and map communications without disrupting the process.

Protect operations by restricting communications

Use observed communications and AI-assisted recommendations to create process-informed zones. Simulate proposed rules before enforcing boundaries.

Control remote access

Provision identity- and context-based access to named OT assets with MFA/SSO, schedules, approvals, and auditable sessions—without broad network reach.

Align operations, IT, and cybersecurity

Give stakeholders a shared understanding of OT assets, risk, and activity. Bring OT context into Cisco and Splunk workflows for detection, investigation, and response.



Start securing water operations with Cisco today

Talk to a [Cisco sales representative](#) or channel partner and visit cisco.com/go/OTsecurity to learn more.

The Cisco advantage

For more than 20 years, Cisco has been helping industrial organizations around the globe digitize their operations, working with manufacturers, power and water utilities, energy companies, mines, ports, railways, roadways, and more. Today, Cisco offers a market-leading portfolio of industrial networking equipment plus a comprehensive suite of cybersecurity products, integrated tightly together with a deep understanding of OT requirements. It's a rare combination.

By designing, developing, and testing products together, Cisco enables IT and OT teams to achieve advanced outcomes while reducing the complexity, time, and gaps incurred by the need to make point products work together. Our solutions come with comprehensive design and implementation guides that will help you reduce risk, accelerate implementation, and make the most of your technology stack.