Cybersecurity in the Water Treatment Sector:

Challenges & Solutions

Water treatment facilities are **critical infrastructure**, ensuring clean and safe water for millions. Yet, they are increasingly targeted by cyber threats such as ransomware, insider attacks, and supply chain vulnerabilities.
The **NIS2 Directive** expands cybersecurity regulations in the EU, affecting thousands of water service providers and reinforcing strict security measures.
With the rise of IT/OT convergence, cloud adoption, and remote access, water systems must implement stronger cybersecurity frameworks to prevent service disruptions and protect public health.

Did You Know?

- 90% of EU critical infrastructure entities expect an increase in cyberattacks.
- NIS2 regulations now apply to 300,000 organizations, including water utilities.
- Cyber incidents in the water sector have doubled in the past three years.

The water treatment & NIS2 Compliance

The NIS2 Directive mandates that water utilities implement robust cybersecurity measures to protect critical infrastructure.

A key requirement is the segmentation of regulated and non-regulated components within their operations. This involves creating clear distinctions between systems that fall under regulatory oversight and those that do not, ensuring that sensitive areas receive appropriate protection.

To enhance security, water utilities must also employ network segmentation across multiple tenants. This practice involves dividing the network into isolated segments, each serving different departments or external partners. Such segmentation limits access to critical systems.

Cybersecurity Guide for Water Utilities

1

Device & Endpoint Security
- Managed Devices: Protect SCADA workstations, industrial control systems (ICS), and monitoring stations from unauthorized access.
- Unmanaged Third-Party Devices: Contractors and service providers access water infrastructure using personal devices.

2

Cloud & SaaS Security in Water Operations
- SCADA and remote monitoring increasingly rely on cloud services.
- Web-based control systems for pumps, treatment plants, and distribution networks must be protected against unauthorized access.
- Avoid additional infrastructure risks: Eliminating jump servers reduces attack surfaces while ensuring secure cloud access for operational technology (OT) teams.

3

Secure Remote Access for Field Operators
- Water utility engineers and field technicians often use tablets to monitor and adjust water treatment processes in real time.
- Clientless browser-based access allows secure login without exposing critical systems to VPN vulnerabilities.

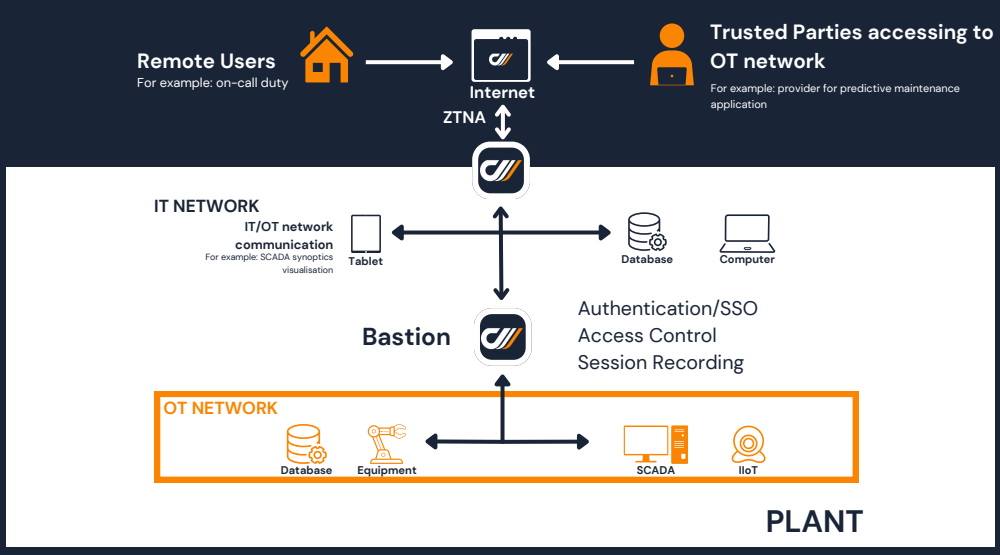
4

End-to-End Traceability & Access Control
- Every change to water treatment settings must be traceable. Implement access logging for compliance and operational security.
- Identity & Access Management (IAM) ensures only authorized personnel can modify pump flow rates, chemical dosing, or distribution controls.

5

IT/OT Convergence:
- OT systems were traditionally isolated, but increased connectivity with IT systems exposes them to cyber threats. Separate IT & OT environments using a Zero Trust solution

Zero Trust IAM: cyberelements for the Water Treatment sector



Multi-Factor Authentication (MFA): Secure remote access to SCADA, industrial control systems, and operational dashboards, preventing unauthorized logins.

Least Privilege Access: Ensure that water treatment operators, engineers, and technicians only access the systems and data necessary for their roles, reducing the risk of human error or insider threats.

Continuous Monitoring & Threat Detection: Identify and respond to unauthorized access attempts or suspicious activity in water treatment processes before they escalate into operational disruptions.

Identity Management: Centralized identity governance ensures that only authorized personnel can access pumps, chemical dosing systems, filtration units, and water distribution networks, with full audit trails for regulatory compliance.

Privileged Access Management (PAM): Restrict and monitor access to critical control systems, ensuring that administrative actions on SCADA, telemetry, and process automation tools are logged and protected against misuse.

Are You Ready for NIS2 Compliance?

cyberelements provides cybersecurity solutions tailored for water utilities, ensuring compliance with NIS2 regulations while protecting critical infrastructure.

Contact us now to discuss your challenges with our experts