Summary

Protection and safety are the primary objectives of every water treatment facility. Invensys has the knowledge, expertise and resources to help protect water and wastewater facilities by identifying and addressing critical gaps.

Business Value

Compromises to critical water treatment plant infrastructure assets from cyber attacks can have a significant detrimental impact. Water Treatment Cyber Security Solutions offer a holistic approach and address three tenets of a comprehensive security program:

- Information security – integrity, availability and confidentiality
- Physical security
- Business continuity

Water Treatment Cyber Security Solutions

Invensys' Critical Infrastructure and Security Practice (CISP) offers solutions that provide a cyber-secure network infrastructure, securing critical systems with two key areas of focus:

- A lifecycle approach as opposed to a point solution within the control automation area, and
- Optimization through network management and secure data acquisition

Water Treatment Cyber Security Solutions are designed specifically to protect industrial control systems (ICS) since increasing connectivity, proliferating access points, escalating system complexity and widening use of common operating systems and platforms have all contributed to heightened security risks. In addition, many of the ICS currently operating across the Water & Wastewater Industry are being used in ways that were never intended. Many ICS were designed decades ago with little or no consideration of cyber security. Today's reliance on ICS makes the industry potentially vulnerable to targeted cyber attacks as well as accidental cyber events. Security is no longer simply about blocking hackers or updating anti-virus software. Today, a security breach can directly impact water & wastewater operations, potentially affecting the safety, reliability and affordability of the water supply and associated services – key corporate concerns tied directly to public health and the environment.

WATER TREATMENT CYBER SECURITY SOLUTIONS

Component	Functionality	Benefits
Network Security Scanning and Patch Management	Vulnerability Assessment	Automates discovery of all network devices, operating systems and infrastructure; performs ad hoc scans targeting one or many machines
	Patch Management	Allows processing of patches, auto scanning and inventory; enables multiple machine/patch deployment in schedulable jobs
	Network and Software Auditing	Detailed analysis of what is happening on the network; visibility of applications installed, the hardware on your network and the state of security applications
	Assets Inventory	Creates an inventory of every device on your network
	Change Management	Provides a complete history of network changes and change notifications
	Risk Analysis and Compliance	Security issues are rated by their severity level; provides numerous executive, technical and statistical reports
Management Server	Network Performance Monitoring & Alarming	Quickly detect, diagnose and resolve network performance problems; real-time dashboards enable at-a-glance network performance tracking and network topology maps
	Security Management Software, Anti-Virus, Backup Storage and Testing	Integrate, manage and monitor security programs such as anti-virus and firewall software via an interactive console; centralized backup file storage
Event Logging and Reporting	Security Information and Event Management	Provides centralized event monitoring services collecting data from various systems, archiving events and providing notification capabilities with a central repository of data logs; supports network-wide control and management of Windows event logs, W3C logs, SYSLOG, and SNMP TRAPS
Remote Relay Access Server	Remote Access	Administrative function; diagnostics and configuration; non-operator observation
Cyber Security Workshops	Security Perimeter Workshop	Identify and classify plant's critical digital assets and define appropriate corresponding Electronic Security Perimeters that are easier to manage and maintain compliance
	Network Design and Road Mapping; Active Directory Workshop	Design and road map secondary network required to host security programs, technologies and solutions required for compliance
Managed Secure Services	Designs and implements specifically for process control networks; 24/7/365 monitoring of security devices with timely identification and remediation of security vulnerabilities	Eliminates need for expensive full-time security expertise; maximizes reliability and uptime; continues data analysis to identify existing and predict future security challenges; enforces policy management and change control; reduces staff workload; lower and more predictable cost of ownership
Supporting Services	Gap analysis; assessments; incident response; documentation policy and procedure creation, updates and assessments; network management	Customizable services that complement and extend Water Treatment Cyber Security Solutions; services can be leveraged individually to identify and fill any gaps in client's compliance program or against their internal security posture

To learn more about Invensys' Critical Infrastructure and Security Practice solutions, contact your sales representative or visit: http://iom.invensys.com/CyberSecurity.

Invensys • 5601 Granite Parkway III, #1000, Plano, TX 75024 • Tel: (469) 365-6400 • Fax: (469) 365-6401 • iom.invensys.com

Rev. 02/15 PN IN-0216