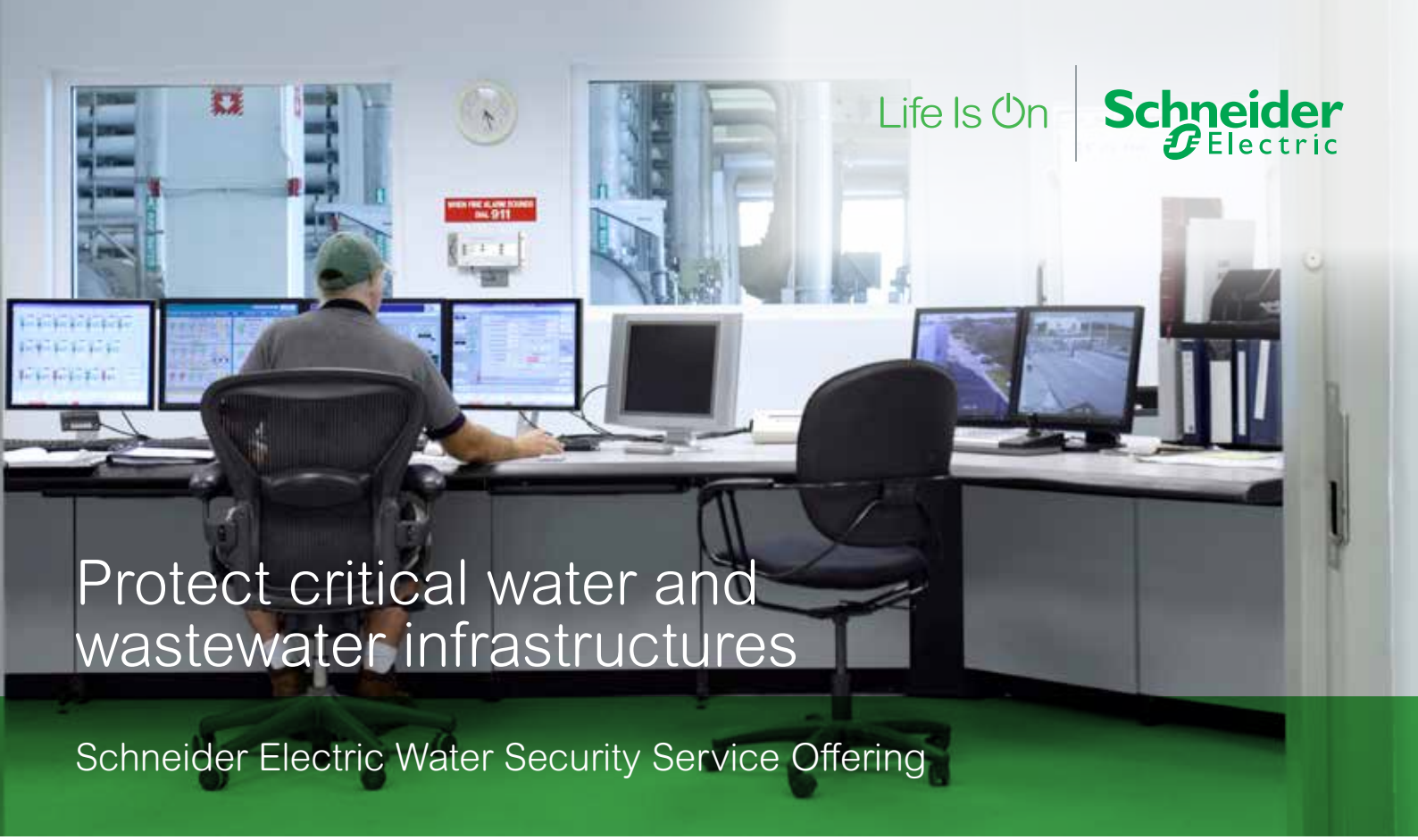


Life Is On | Schneider Electric

# Protect critical water and wastewater infrastructures

## Schneider Electric Water Security Service Offering

### Service at a glance

The Schneider Electric™ Water Security Service Offering (WSSO) is an independent set of service offerings and components designed specifically to protect the infrastructure and critical systems required to run and manage water and wastewater related infrastructure.

### Water security

As industrial control systems (ICSs) have become more affordable, easier to use and evolved from proprietary to more open systems, most utilities have adopted them for process monitoring and/or control. This reliance on ICSs has left the water sector and other dependent critical infrastructures potentially vulnerable to targeted cyber attacks or accidental cyber events. ICS security is no longer simply about blocking hackers or updating antivirus software. A new underground digital economy now provides a multi-billion dollar incentive for potential adversaries to exploit ICS vulnerabilities.

Increasing connectivity, the proliferation of access points, escalating system complexity, and wider use of common operating systems and platforms have all contributed to heightened security risks.

# Protect critical water and wastewater infrastructures

## Schneider Electric Water Security Service Offering

Also, many of the ICSs that operate our current water and wastewater sector infrastructure are being used in ways that were never intended. Many ICSs were designed decades ago with little or no consideration of cybersecurity.

A security breach can have consequences that directly impact water and wastewater operations' ability to provide reliable, affordable, high-quality water and services, the key goals that allow utilities to look after public health and the environment.

## Breach/impact matrix

| Unauthorized tampering with operations, settings, and alarms that cause: | Result in: |
|---|---|
| • Service disruptions<br>• Incorrect doses of chemicals<br>• Deliberate release of chemicals<br>• Deliberate release of raw sewage<br>• Damage to environment<br>• Safety hazards | **Public health risks** |
| • Deletion or alteration of data<br>• Non-compliant water quality | **Regulatory violations*** |
| • Damage to infrastructure<br>• Service disruptions | **Economic/ financial impact** |
| • Damage to property<br>• Damage to people<br>• Damage to environment | **Liabilities** |
| • Events caused by security breaches | **Negative PR and loss of public confidence** |

*Potential fines and permit issues.

Leaders from the water and wastewater industry and the government have recognized the need to plan, coordinate, and focus ongoing efforts to improve ICS and overall security. These leaders concur that an actionable path forward is required to address critical needs and gaps and to prepare the sector for a secure future.

Schneider Electric Water Security Service Offering (WSSO) is an independent set of service offerings and components designed specifically to protect the infrastructure and critical systems required to run and manage water- and wastewater-related infrastructure. The offering spans across facilities networks, control rooms, field sites, and any interconnections including corporate and business networks.

While our solutions regularly complement control systems provided by Schneider Electric, we bring the same expertise and benefits to any industrial control system, SCADA system, network, and plant or business.

WSSO is designed using a holistic approach to cybersecurity and takes into consideration the following three tenets of a comprehensive security program:

1. Information security (Integrity, Availability and Confidentiality)
2. Physical security
3. Business continuity

Schneider Electric's cybersecurity consulting practice applies the three tenets of a security program across all domains:

- Operations
- Network and IT
- Business

# Protect critical water and wastewater infrastructures

## Schneider Electric Water Security Service Offering

As a control system vendor, Schneider Electric has been engaged by various customers across multiple industries, with varying levels of security requirements. These span from nuclear power plants with the strictest regulatory compliance programs to chemical plants, refineries, and the water and wastewater sector.

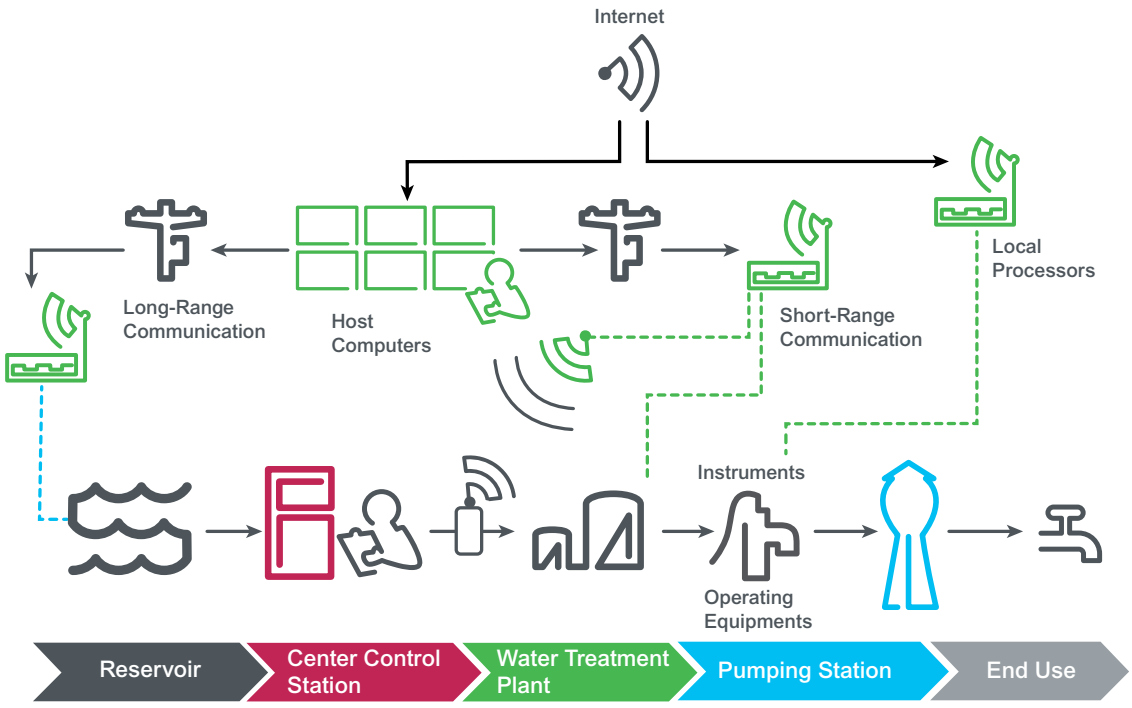
Through these efforts, Schneider Electric has gained a high level of understanding for security requirements and has developed the WSSO.

We firmly believe in designing and implementing a defense-in-depth strategy and a segmentation approach to cybersecurity. WSSO components and services address remote field site units, control centers and up to the corporate IT layer, facilitating a secure integration between operations, and IT networks. This includes protecting cyber assets and the interconnecting communications network in:

- Reservoirs
- Central control stations
- Water treatment plants
- Wastewater treatment plants
- Pumping stations

The specific assets addressed in the areas above include:

- Site field devices such as remote telemetry units, programmable logic controllers, intelligent embedded field devices
- Control centers, which include ICS and SCADA control servers, HMI and operator workstations, database/logging systems, historians, network devices, printers, and other application systems and devices



# Protect critical water and wastewater infrastructures

## Schneider Electric Water Security Service Offering

Achieving an effective security program for the water and wastewater sector is a series of steps and is not achieved with a single product. WSSO is a set of components that can be implemented as a packaged solution or as independent components that implement security best practices, services and security technologies, depending on the progression of customer's overall security posture and program.

These security products have been specifically selected to assist Schneider Electric customers in reducing the cost of implementing and automating current manual procedures and for their ability to be integrated with the real-time control system. The WSSO consists of software, hardware and services dedicated to specific functions required for a comprehensive security program. WSSO can be deployed as a comprehensive solution or as independent components. The software and services implements the multiple functions outlined in the following next sections.

## Features

- Investigate and report vulnerabilities in operating systems and configurations
- System scanning and hardening; identifying and securing open ports, USB interfaces, patch levels, running services, system bios; bios passwords; boot sequences; wireless network interfaces, modems, CD-ROM
- Manage antivirus definition files ensuring they are up to date with manufacturing approved patch levels for all systems
- Provide ICS backup processes, file storage, restoration, and testing procedures
- Provide a Web-based console for managing security programs and customizable dashboards for reports
- Auto discover assets such as network devices, including servers, workstations, laptops, switches, and routers
- Monitor and analyze real-time, in-depth, network performance statistics for routers, switches, wireless access points, servers, and any other SNMP-enabled devices
- Provide powerful workflow capabilities that increase ICS administrators' effectiveness allowing them to quickly define and deploy security as well as respond to security events and issues
- Centralized management of:
  - Network performance monitoring and alarming
  - Network security scanning and patch management
  - Event logging and reporting
  - DCS backup and storage
- Solution/services that are platform agnostic and support all operating platforms
- Supports cybersecurity of multiple control systems
- Managed security services

## WSSO components

1. Network security scanning and patch management
2. Management server (MGT Server)
3. Event logging and reporting
4. Remote access — relay server
5. Cybersecurity workshops
6. Supporting services
7. Managed security services

# Protect critical water and wastewater infrastructures

## Schneider Electric Water Security Service Offering

### 1. Network security scanning and patch management

The WSSO network security scanning and patch management component provides a complete network security overview with minimal administrative effort, while also providing remedial action through patch management features. This component provides a centralized vulnerability assessment and identification function for control systems. It is a network-based scanning solution that performs a comprehensive external examination of all devices on the control network including servers, workstations, routers, printers, and switches.

The scan's purpose is to identify vulnerabilities including missing patches and out-of-date antivirus signatures so that they are remediated before they are exploited.

The network security scanning and patch management component provides you with a complete picture of your network set-up, provides risk analysis and helps you to maintain a secure and compliant network state faster and more effectively. It provides functionality in these key areas:

- Patch management
- Vulnerability assessment
- Network and software auditing
- Assets inventory
- Change management
- Risk analysis and compliance

**Patch management**

Patch management is a feature of utmost importance as missing security patches are one of the main reasons for network security breaches. WSSO eliminates this risk by providing on-demand or fully automated detection, downloading and deployment of missing patches. WSSO helps you fix vulnerabilities before they are exploited and reduces the time required to patch machines on your network.

WSSO enables administrators to manage industrial control systems and Microsoft® patches and service packs for all languages supported by Microsoft. It also provides features like patch rollback and uses an existing WSUS patch repository.

**Vulnerability assessment**

The vulnerability assessment feature performs over 45,000 checks on your systems and allows you to analyze the state of your network security, what the risks are, how exposed your network is, and how to take action before it is compromised.

**Network and software auditing**

Network and software auditing gives you a detailed analysis of what is happening on your network — which applications or default configurations are posing a security risk. You get a complete picture of what applications are installed, the hardware on your network, the state of security applications (AV, antispam, firewalls, etc.), what ports are open, any existing shares, and services running on your machines.

**Assets inventory**

Assets inventory allows you to create an asset inventory of every device on your network; be they servers and workstations, virtual machines or IP-based hardware such as routers, printers, switches and so on. Asset inventories help you identify devices attached to your network that you were unaware of or had forgotten and these, unless properly patched and secure, could become entry points for hackers and malware.

# Protect critical water and wastewater infrastructures

## Schneider Electric Water Security Service Offering

**Change management**
The best way to maintain a secure network over time is to know exactly what's happening on your network. Changes to configurations that could have security implications, new applications that are installed, services that are started/stopped and so on, are all events that an administrator needs to know about. WSSO gives you a complete history of network changes that are relevant to the security of your network and sends notifications when these occur.

**Risk analysis and compliance**
Risk analysis and compliance makes it easier for the administrator to know what needs to be fixed with urgency. Security issues are rated by their severity level and each computer is given a risk and vulnerability rating so that you know where the main problems exist on your network. WSSO provides numerous executive, technical and statistical reports that help you to understand what is happening on the network, to prioritize remediation operations efficiently and to prove, if required, that the network is secure.

**Benefits**
Network security Scanning and Patch Management reduces the total cost of ownership by centralizing vulnerability scanning, patch management and network auditing.

## 2. Management server

Management server is a single multi-function server that can provide multiple services across your network infrastructure. These services range from DCS backup storage, network performance monitoring and alarming to access control and security software management applications.

**Network performance monitoring and alarming**
Network performance monitoring and alarming component provides a network availability and performance monitoring solution that delivers the critical information you need to stay on top of your evolving network. Enabling you to quickly detect, diagnose, and resolve network performance problems and outages. It provides the ability to monitor and analyze real-time, in-depth, network performance statistics for routers, switches, wireless access points, servers, and any other SNMP-enabled devices.

Monitoring your network environment provides a crucial function in the overall security infrastructure and strategy. Each device distributes its own unique set of data to be analyzed by the network or security team. Having a monitoring system in place to receive that data for analysis, and receive alarms and alerts from anomalies is crucial.

In addition to the security related data, performance data must be monitored as well. Information such as throughput, utilization, and error rates must be gathered so that the devices can transmit and analyze the traffic effectively and efficiently. You can also configure to monitor disk space on servers or infor mation pertaining to historical CPU, disk and memory utilization.

This WSSO component is a Web-accessible tool that collects and maintains statistics, which it stores in an SQL database. The platform has the capability to monitor any device that utilizes simple network monitoring protocol (SNMP). The platform can pull data from a device to report conditions and can be a recipient of data generated by a device exception (trap).

The dashboard displays device names and statistics in traffic light style, green dot for normal operating condition, yellow for degraded and red for problems. Detailed metrics like availability, bandwidth utilization, and interface traffic for routers, switches, servers, and any other SNMP-enabled devices are served up and displayed. Every network element is "hot," allowing you to immediately view

# Protect critical water and wastewater infrastructures

## Schneider Electric Water Security Service Offering

alerts and to drill-down into detailed metrics to see exactly what's happening with each and every system on the global network and get the data you need to quickly isolate, diagnose, and repair problems.

**Security management software**
Access control and security software management is an integrated security software component designed to integrate, manage and monitor the numerous security programs used by companies via an interactive single Web-based console. It is a security management technology that improves protection and the reduction of the threats corporations face.

It is important to protect your computer from viruses, hackers, and other issues. This requires effective network architecture as well as installing and managing various different programs to meet each of these needs, including firewalls and anti-virus software. This WSSO component provides a single console that interfaces with each software program at a single point of contact, making it easier to configure, monitor and publish reports about threats, attacks and protection status. You can create, deploy and manage policies for controlling USB drives, host firewall policies, rogue system detection setup, and configure server to pull AV DAT updates from a centralized proxy server if available.

Because the component is Web-based the dashboard opens in a browser, reports are created and accessed easily and users can customize the dashboard according to need. Managing systems is easier improving the usability of directories through synchronization. Automate and create actionable reports as well as export to the required formats for distribution and ease of access. Updating security policies and staying in touch with the ongoing security changes is made easier.

**Backup file storage**
The backup file storage component is comprised of a customized set of procedures and software for backup, recovery and test efforts of control systems. File storage is managed on MGT Server. The WSSO component includes backup software and services to provide:

- Recovery plan
- Backup and restore plan
- Testing of backup media

The three delivered plans are created to meet the following specifications:

Recovery plan — This may comprise one or more documents depending on the size of the procedures.

- Defines roles and responsibilities of responders
- Specifies the required actions in response to events or conditions of varying duration and severity that would activate the recovery plan
- Annual review of recovery plan
- At least annual exercise of the recovery plan which can range from a paper drill, to a full operational exercise, or recovery from an actual event
- Plan is updated to reflect any changes or lessons learned as a result of an exercise or recovery from an actual incident
- Updates to recovery plan are communicated to personnel responsible for the activation and implementation of the recovery plan, within thirty calendar days of the change being completed

# Protect critical water and wastewater infrastructures

## Schneider Electric Water Security Service Offering

Backup and restore plan — This may reference and/or be part of the actual recovery plan documentation.

- Documented processes and procedures for the backup and storage of information required to successfully restore cyber assets
- Backups may include spare electronic components or equipment, written documentation of configuration settings, tape or alternate media backups, etc.

Testing of backup media — This may reference and/or be part of the actual recovery plan documentation.

- Information essential to recovery that is stored on backup media is tested at least annually to ensure that the information is available

**Benefits**

Management Server provides centralized management of network performance monitoring, end point management of security programs and backup file storage and restoration.

## 3. Event logging and reporting

The event logging and reporting component provides security information and event management (SIEM) capabilities. Control system assets such as cyber assets (workstations and switches) can forward security events to a central monitoring server. The server collects data from the various systems, provides notification on selected events, and acts as a repository to allow the data to be analyzed at a later date. System logging supports SYSLOG, SNMP TRAPS and Windows Events.

As a network administrator, you have experienced the cryptic and voluminous logs that make log analysis daunting. This solution provides network-wide control and management of Windows event logs, W3C logs, SQL Server audit logs and Syslog events generated by your network sources. The component supports SNMP for devices such as routers, sensors, firewalls, etc. Through SNMP, users can monitor a whole range of hardware devices on their infrastructure and gain the ability to report on the health and operational status of each device.

The component dashboard includes a number of filtering-enabled charts to provide administrators with fast and easy access to the data they need as they go about their day. These include the top critical and high importance rules triggered within a certain period of time, the top 10 users who fail to log on or who log on during and outside working hours, service status across network, how many events are stored in the database per log type and a comprehensive graph based on Windows events that shows network connections at application and user level. The dashboard is highly customizable and can be zoomed individually in separate windows that can be automatically arranged on the desktop to show real-time data about the most important events.

**Benefits**

The WSSO event logging and reporting component:

- Is easy to install, configure and run
- Provides a quick view dashboard of important events
- Supports reporting and logging for SYSLOG, SNMP and Windows events
- Features real-time alert capabilities for both SNMP and Windows events
- Is agentless, there is no software to be installed on monitored servers

# Protect critical water and wastewater infrastructures

## Schneider Electric Water Security Service Offering

- Contains pre-configured rules that include events processing rules for hundreds of types of events, automatically categorizing them in typical groups
- Offers event browsing and filtering quickly view all critical-level events with just one click of the mouse; use the filtering option to narrow down list of events to browse
- Features fast scanning that optimizes network traffic with local cache mechanisms used to avoid retrieving redundant information; it can store up to six million events per hour
- Provides events archiving

## 4. Remote access relay server

The purpose of this WSSO component is to secure remote access associated with maintenance of Industrial LAN and PCN applicable to critical facilities. For business reasons, it is necessary to provide a means for users to remotely access Industrial LAN and PCN resources.

Remote access may be required to perform items such as:

- Administration functions
- Diagnostics
- Configuration
- Non-operator observation and non-routine or infrequent control.
- Applications such as:
  - Telnet, SSH, and remote desktop software

Access to the industrial LAN is normally achieved through some type of connection between the industrial LAN and the business network. While this allows legitimate users access to needed data, it often creates security holes allowing unauthorized access to industrial LAN and PCN cyber assets.

The solution for protecting the industrial LAN and PCN from exposure to the business network is to deploy an intermediate access platform as a relay server, which is also known as a jump server. Deploying a remote access relay server removes direct access to the industrial LAN.

The jump server solution requires a firewall with the capability for creating separate secure zones for the business network, industrial LAN and jump server. The resulting implementation of secure zones will segment the industrial LAN from outside (off network) access providing no direct connections to the Industrial LAN from the business network.

**Benefits**

The remote access relay server protects the industrial LAN and process control network from exposure to the business network by converting untrusted inbound remote connections from the business network into trusted outbound connections from virtual workstations with separate IP addresses into the industrial LAN and process control network cyber assets.

## 5. Available workshops

**Electronic Security Perimeter (ESP) and Physical Security Perimeter (PSP) Workshops**

The objective of these workshops is to help clients identify their critical cyber assets, protected cyber assets, and non-protected cyber assets and to help define and limit the size of clients' ESPs per plan.

- Help identify cyber assets and critical cyber assets (CCAs)
- Help identify and define electronic security perimeters (ESPs)
- Bring stakeholders from various groups together

# Protect critical water and wastewater infrastructures

## Schneider Electric Water Security Service Offering

**Secondary Network Design and Road-Mapping**
This workshop helps the client develop a roadmap for the secure network support of current and future business and industrial control system requirements. A secondary network is essential in proving an infrastructure to host the security solutions detailed in this document.

**Design and roadmap** a secondary network in support of cybersecurity management requirements for centralized management of:

- Backups
- Antivirus management
- Patch management
- Event management
- Network performance monitoring
- Historical data reporting
- Security event historical data and reporting
- Active Directory access controls
- Secure remote access relay server

**Active Directory Workshop**
This workshop helps the client integrate and design the Microsoft Active Directory services and domain controllers that provide user access control of cyber assets.

- Help identify customer requirements for Active Directory including user and security group requirements
- Identify and document external network connectivity requirements
- Identify and document any corporate security requirements
- Identify and document future ICS requirements or feature additions
- Create an Active Directory functional design specification and audit plan
- Help educate customer on features and options for Active Directory
- Bring stakeholders from various groups together

## 6. Support services

The following is a list of supporting services to augment a client's security program and network infrastructure.

- **GAP Analysis —** We work with customers to identify shortfalls or starting points for their security programs, and then we make an assessment of client's environment and map it against their internal security program. Shortcomings in client's program are identified and a remediation plan is created with prioritized tasks.
- **Vulnerability Assessments —** We identify attack vectors and the risk associated with cyber attacks. Provides a unique approach of reviewing particular site and system specific vulnerabilities. The results are provided in a conclusive report that highlights the critical assets, vulnerabilities and risks.
- **Policy and Procedure Creation, Updates and Assessments —** Policies and procedures are written to meet control network requirements.
- **Access Controls —** Access controls include firewalls, intrusion detection systems, secure zones configuration, design, and documentation. It also includes the installation, configuration, and documentation of security and network devices, cybersecurity technologies, and WSSO components as required.
- **Network and Security Infrastructure Design and Implementation —** Design focus for network and security infrastructure is based on segmentation and takes a layered security approach when possible and appropriate.

# Protect critical water and wastewater infrastructures

## Schneider Electric Water Security Service Offering

### 7. Managed security services

Many companies approach cybersecurity with a strong technology focus, installing firewalls and advanced IDS/IPS systems to secure their networks. This approach may solve the problem for the short term. But new threats are always surfacing, technology is continually evolving, and system health can deteriorate rapidly. Dedicated resources enforcing strict policies and procedures are necessary to ensure that these and other problems are anticipated and resolved before an actual security attack occurs. This is the only way to keep the process control network secure.

However, most companies are challenged to find and fund such resources. Any crack in the armor of resources, policies or expertise will open up their network to the risk of an actual attack even though the company has installed security equipment.

Schneider Electric has teamed with an industry leader in managed security services (MSS), to offer a comprehensive MSS package. The offering is part of Schneider Electric's cybersecurity portfolio and WSSO, coupling the company's deep process control and IT knowledge with Integralis' security practitioners and technologies and providing a solution specific to the process industries.

The offering is extremely effective in preventing security breaches while keeping the overall cost of ownership low.

The service includes:

- **24x7 monitoring and alerting —** Monitors vital health signs and operating conditions on the platform and analyzes data continuously so that problems or issues are escalated to the designated customer security contacts quickly and efficiently
- **System health monitoring —** Proactively monitors all cyber security system hardware to ensure optimum performance and to reduce or prevent outages
- **System availability checks —** Facilitates system availability checks which are a fundamental component of the fully managed service; these checks prove that the device is accessible and can be reached from the Internet
- **Alert management —** Ensure complete and timely communication of various levels of security issues, from performance warnings to the escalation of major breakouts or vulnerabilities
- **Platform management —** Maintains and manages the day-to-day operations of the security system, performing software updates, configuration changes and configuration backups to keep the system running reliably and securely
- **Policy management —** Allows a customer to call on experienced operations staff at any time to make configuration changes to security policies; extensive network security expertise is applied to validate, design and implement changes to a company's security policy
- **Remote system management and rebuild —** Assures that a catastrophic failure need not mean that communications are impacted for long; once the hardware replacement has been installed, a remote system rebuild can commence, using the most recent configuration within a matter of hours
- **Reporting (via a secure Web portal) —** Provides a wealth of reporting options via the secure Web portal; these reports include information and details about alerts, system availability statistics and graphs, system resource usage and policy modification events; reporting parameters are flexible and data can be downloaded in CSV format to allow tailored reporting

# Protect critical water and wastewater infrastructures

## Schneider Electric Water Security Service Offering

The key to effective delivery of these services is the implementation of a comprehensive security infrastructure including:

**Security service appliance (SSA) —** This proven device is placed at clients' sites alongside the security products under management, the SSA is a vital link in the secure monitoring and management of security systems providing full real-time log file analysis and alert creation. The SSA also provides the platform for secure remote access. An out-of-band connection ensures that the SSA is reachable, even when the primary Internet connection is unavailable. Correlation of events starts at the SSA level ensuring that your bandwidth is not taken up with excess data being sent back to the security management centers for analysis.

**ISMS —** The information security management system, ISMS, has a wealth of standard reporting capability as well as fully configurable business rules for alerting. This allows e-mail and SMS text messages to be sent alerting the user of rule changes and logins and other interesting events based on time of day and type of activity. ISMS offers advanced reporting and event correlation on a wide range of event types, making sure the user is fully aware of any threat to the network at all times.

**Security management centers —** Security management centers (SMCs) are located in multiple countries around the world, making them resilient to any single point of failure and providing the experts where clients need them.

**Benefits of managed security services**

- Design and implementation specifically for process control networks
- 24 x 7 x 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
- Continuous analysis of data to identify existing and predict future security challenges
- Enforces policy management and change control
- Skilled security practitioners worldwide
- Reduces workload for the internal staff
- Lower and more predictable cost of ownership

## Summary

All of the supporting services and workshops can be customized to meet the individual requirements of our customers realizing their unique situation with regard to specific internal compliance programs. This ranges from customers who need a starting point to begin creating their compliance plans to customers who may already have a detailed plan in place but require assistance with specific areas of compliance or are installing or upgrading to new systems. Customers can also leverage these services as a complete, comprehensive solutions offering or as individual components.

# Protect critical water and wastewater infrastructures

## Schneider Electric Water Security Service Offering

## Service matrix

The following table is a service matrix mapping the WSSO solution components.

| Schneider Electric Water Security Service Offering | | |
|---|---|---|
| **WSSO Component** | **Functionality** | **Benefits** |
| 1. Network security scanning and patch management | • Vulnerability assessment<br>• Patch management<br>• Network and software auditing<br>• Assets inventory<br>• Change management<br>• Risk analysis and compliance | **Vulnerability Scan**<br>• Automates discovery of all network devices, operating systems, and infrastructure<br>• Performs ad hoc scans targeting one or many machines<br>• Over 45,000 vulnerability assessments carried out across your network, including virtual environment<br>• Provides details of identified vulnerabilities, impact to the organization, and options to fix<br>• Offers ability to schedule scans<br>**Patch Management**<br>• Allows processing of patches, auto scanning, inventory and SCAN access<br>• Enables multiple machine/patch deployment in schedulable jobs<br>• Ability to patch multiple operating system types<br>• Option to reboot each station automatically or manually after patches are deployed<br>• Deployment of custom software and scripts<br>• Agent-less or agent-based auditing<br>**Network and Software Auditing**<br>• Detailed analysis of what is happening on the network providing a complete picture of what applications are installed, the hardware on your network, the state of security applications (AV, anti-spam, firewalls, etc.), what ports are open, any existing shares and services running on your machines<br>**Assets Inventory**<br>• Creates an assets inventory of every device on your network<br>**Change Management**<br>• Provides a complete history of network changes that are relevant to the security of your network and sends notifications when these occur.<br>• Includes changes to configurations that could have security implications, new applications that are installed, services that are started/stopped and so on — are all events that an administrator needs to know about<br>**Risk analysis and compliance**<br>• Security issues are rated by their severity level and each computer is given a risk and vulnerability rating so that you know where the main problems on your network are<br>• Provides numerous executive, technical and statistical reports that help you to understand what is happening on the network, to prioritize remediation operations efficiently and to prove, if required, that the network is secure |

# Protect critical water and wastewater infrastructures

## Schneider Electric Water Security Service Offering

| Schneider Electric Water Security Service Offering | | |
|---|---|---|
| **WSSO Component** | **Functionality** | **Benefits** |
| 2. Management server (MGT Server) | • Network performance monitoring and alarming<br>• Security management software<br>• Antivirus<br>• Backup storage and testing | **Network Performance Monitoring & Alarming**<br>• Quickly detect, diagnose, and resolve network performance problems and outages<br>• Real-time views and dashboards that enable you to visually track network performance at a glance with hot links to any SNMP enabled device on your network<br>• Provides dynamic network topology maps and automated network discovery features<br>• Monitors performance data such as throughput, utilization, disk space and error rates.<br>**Security Management Software**<br>• Integrate, manage and monitor security programs such as antivirus and firewall software via an interactive web-based console<br>• Centralized backup file storage |
| 3. 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<br>• Provides a central repository of data logs and events<br>• Supports network-wide control and management of Windows event logs, W3C logs, SYSLOG and SNMP TRAPS<br>• Provides alert capabilities for SNMP and Windows events |
| 4. Remote access — relay server | • Remote access | Provides secure remote access to Industrial LAN and Process Control Network for required items such as:<br>• Administrative functions<br>• Diagnostics<br>• Configuration<br>• Non operator observation<br>• Applications such as:<br>– Telnet, SSH, and remote desktop software |
| 5. Cybersecurity workshops | • ESP and PSP workshop<br>• Secondary network design and road mapping<br>• Active Directory workshop | • Identify and classify plant's critical cyber assets and define appropriate corresponding electronic security perimeters that are easier to manage and maintain compliance<br>• Design and road map secondary network required to host security programs, technologies and solutions required for meeting NERC CIP compliance<br>• Quickly identify plant requirements for Active Directory including user and security group access requirements. Design domain controllers to manage assess to one or more control systems |

# Protect critical water and wastewater infrastructures

## Schneider Electric Water Security Service Offering

| Schneider Electric Water Security Service Offering | | |
|---|---|---|
| **WSSO Component** | **Functionality** | **Benefits** |
| 6. Supporting services | • Gap analysis<br>• Vulnerability assessments<br>• Documentation<br>• Policy and procedure creation, updates, and assessments<br>• Access controls<br>• Network and security infrastructure design and Implementation | • Customizable services that compliment and extend the WSSO<br>• These services can be leveraged individually as required to identify and fill any gaps in clients compliance program or against their internal security posture |
| 7. Managed security services | • Designs and implements specifically for process control networks<br>• 24 x 7 x 365 monitoring of security devices with timely identification and remediation of security vulnerabilities | • Eliminates need for expensive full-time security expertise<br>• Maximizes reliability and uptime<br>• Continuous analysis of data to identify existing and predict future security challenges<br>• Enforces policy management and change control<br>• Skilled security practitioners worldwide<br>• Reduces workload for the internal staff<br>• Lower and more predictable cost of ownership |

Schneider Electric

70 Mechanic Street
Foxborough, MA 02035 USA
+1 877 342 5173

schneider-electric.com/processautomation

Life Is On Schneider Electric