Power and Water Cybersecurity Suite

Overview

Emerson’s Power and Water Cybersecurity Suite helps customers operate their plants more securely, reliably, safely and efficiently. The suite is tightly integrated with industry-leading distributed control systems to:

- Protect assets
- Monitor and remediate threats
- Automate system cybersecurity management without disrupting controlled processes

For customers in the power industry, the suite assists in complying with the North American Electric Reliability Corporation (NERC) Critical Infrastructure Protection (CIP) standards.

These standards require power generators to identify and protect cyber assets that may impact the reliable operation of bulk electric systems.

Water and wastewater customers can implement the suite to help address internal cybersecurity initiatives as part of their overall efforts to safeguard public health and the environment.

Each customized solution includes integrated hardware and virtualized software modules, packaged within an enclosure that interfaces to the control system’s network.

The suite’s network is located outside of the control system’s security perimeter in a separate subnet and demilitarized zone (DMZ).

Features

- Provides enhanced control system protection for secure, reliable, safe and efficient plant operation without disruption
- Proactively monitors for threats and implements remedies
- Simplifies and automates security program management
- Increases security posture
- Tightly integrates with industry-leading distributed control systems
- Assists power generation customers with NERC CIP standards compliance for reliable operation of bulk electric systems
- Helps water and wastewater customers to implement cybersecurity initiatives that safeguard public health and the environment
Enhances Protection

The Power and Water Cybersecurity Suite keeps pace with and mitigates emerging cybersecurity risks. The suite includes modules focused on countering threats and protecting system network integrity. Real-time antivirus protection guards workstations and servers against viruses and malware. Application control effectively mitigates malware threats. Device control secures and centralizes management of storage devices associated with Windows-based workstations and servers. An agent-based solution determines patch needs within workstations and servers. Tools are provided for backup and recovery of important system data.

Proactively Monitors

Several modules within the Power and Water Cybersecurity Suite continuously monitor systems for emerging threats and implement remediation tactics to keep information secure. The network is continuously monitored for rogue or unmanaged devices that can be easily converted to managed clients by the user. Network intrusion detection monitors data traffic. All security incidents and events across the network are collected for further analysis.

Simplifies Management

The Power and Water Cybersecurity Suite manages system cybersecurity without disrupting controlled processes. The suite includes a dashboard and supporting modules that simplify security program management. The dashboard provides a high-level view of system security posture with enhanced query and reporting capabilities for data analysis and compliance requirements. The suite effectively maintains system configurations, proactively scans the systems for vulnerabilities and provides guidance for mitigating risks.

Communication

The Power and Water Cybersecurity Suite modules connect with control systems via a dedicated protective firewall, which simplifies operating system integration without the need for special setup or alteration.

Connectivity examples include:

- Multiple independent single network systems can be individually connected to the suite’s dedicated firewall from each respective system network switch
- A single multi-networked system can be individually connected to the suite’s firewall from a core switch or router
- A combination of the above two configurations

The suite’s firewall can connect to a plant LAN to deliver event notifications, alerts or reports generated from multiple security modules to plant or corporate locations outside the control room. Additionally, the suite can use this connection to receive module content and software updates such as new security patches, virus signatures and detection rules from other computers connected to the plant LAN.

User Interface

Power and Water Cybersecurity Suite modules are configured and maintained through a dedicated user interface located within the suite’s network. The user interface is a standalone Windows-based computer equipped with tools to:

- Access and manage the security modules
- Manage and view the dashboard
- View reports and alerts
- Deploy and manage the endpoints through a web interface

Service and Support

The Power and Water Cybersecurity Suite SureService™ support module¹ keeps the software, content, licenses and hardware elements of the suite promptly updated. The support module consists of:

- Power and Water Cybersecurity Suite module software updates
- Content updates including patches, definitions, rules or policies
- Component warranty and repair

¹ Requires the purchase of the SureService™ expert telephone support module.
## Power and Water Cybersecurity Suite Modules

<table>
<thead>
<tr>
<th>Module</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cybersecurity Dashboard</td>
<td>Provides a user-friendly interface to manage patch management, application control, device control, antivirus, rogue system detection and vulnerability assessment modules. The dashboard includes advanced reporting and query options.</td>
</tr>
<tr>
<td>Antivirus Protection</td>
<td>Provides real-time virus and malware protection for workstations and servers with Microsoft® Windows®-based operating systems.</td>
</tr>
<tr>
<td>Application Control</td>
<td>Enables users to effectively mitigate malware threats. Application control compensates for the shortcomings of blacklisting technology by “whitelisting” only those programs allowed to operate within workstations and servers.</td>
</tr>
<tr>
<td>Configuration Management</td>
<td>Effectively manages system configurations with a focus on Windows-based workstations and servers, network devices and Window’s Active Directory.</td>
</tr>
<tr>
<td>Device Control</td>
<td>Provides secure and centralized management of storage devices associated with Windows-based workstations and servers, such as embedded CD/DVD drives and serial/parallel ports, as well as various removable devices.</td>
</tr>
<tr>
<td>Network Intrusion Detection</td>
<td>Monitors data traffic through routers on the electronic security perimeter to provide deep-packet inspection and displays current system status on a dashboard.</td>
</tr>
<tr>
<td>Patch Management</td>
<td>Employs an agent-based solution to accurately inventory software and determine patch needs for each workstation and server.</td>
</tr>
<tr>
<td>Rogue System Detection</td>
<td>Real-time monitoring for detecting unprotected and unmanaged systems; converts rogue systems to a managed client.</td>
</tr>
<tr>
<td>Security Incident &amp; Event Management</td>
<td>Collects security events from various operating systems including Windows, Linux and Solaris; as well as switches, firewalls and routers. The module also gathers events from other data sources via the simple network management protocol (SNMP) or system log messages (Syslog).</td>
</tr>
<tr>
<td>Module</td>
<td>Description</td>
</tr>
<tr>
<td>--------------------------------</td>
<td>---------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>System Backup &amp; Recovery</td>
<td>Performs disk- or file-level data backup and recovery associated with each station’s hard disks. Consists of management server software embedded within the Power and Water Cybersecurity Suite and agents loaded on workstations and servers.</td>
</tr>
<tr>
<td>Vulnerability Assessment</td>
<td>Closes the gaps between vulnerabilities and risks by providing a reliable, flexible and proactive tool that scans the system’s environment for vulnerabilities and provides guidance for mitigating risks.</td>
</tr>
</tbody>
</table>