Power and Water Cybersecurity Suite Antivirus Protection

Features

- Provides virus protection for Microsoft® Windows®-based workstations and servers
- Centrally monitors and manages antivirus status and activity through Trellix® ePolicy Orchestrator®
- Delivers validated weekly antivirus signature updates
- Notifies or reports detected infections by date and antivirus signature version status

Introduction

Attacks targeted at power generation, water, and wastewater plants usually originate from outside sources. External attacks in the form of viruses, worms, or other tools used by malicious hackers can impair control system operation in the form of:

- Loss of control that can upset operating processes or cause equipment damage.
- Performance degradation from increased data traffic.
- Increased risk from stolen or changed data without proper authorization.
- Weakened system integrity due to unauthorized access.

There are two main approaches to virus and malware protection: signature- and behavior-based methods. Signature-based methods use known virus signatures to identify infections and must be frequently updated for effective protection. Behavior-based methods examine files for malware-like behavior to identify potential infections that are not well known or yet identified.

Solution

Antivirus Protection is a Power and Water Cybersecurity Suite application that provides real-time virus and malware protection for workstations and servers with Microsoft Windows operating systems. This comprehensive application employs the signature-based method for effective virus detection. Antivirus Protection automatically identifies and repairs or quarantines spyware, adware, viruses, and other malicious intruders.

Regularly implemented virus signature updates maintain reliable operation of the control system. Emerson validates new virus signatures for currently supported Ovation™ releases on a weekly basis. You can download these software updates through Product Support.

The Antivirus Protection application consists of two major pieces: a server and an agent. The application is installed on a dedicated antivirus server, a dedicated Power and Water Cybersecurity Suite Lite server, or in a virtual host of the Power and Water Cybersecurity Suite Full server, all operating with a Windows-based operating system. The antivirus server loads an agent on to each workstation. For smaller deployments, you can install the Antivirus Protection application in self-managed mode. Self-managed mode requires no server, but it does require management on each endpoint individually.

Antivirus Protection performs the following functions:

- Installs agent software.
- Configures and manages the Windows agents.
- Distributes antivirus signatures.
- Generates antivirus status reports.

You can group endpoint stations for wave deployments of virus signatures or scan engine software. Group membership for these deployments is based on the endpoint station's criticality to the control system's operation.

Operation

You can access the Antivirus Protection application through the Power and Water Cybersecurity Suite's user interface browser. With the Antivirus Protection application, you can perform the following functions:

Scan Endpoints

The system performs virus scans automatically per a pre-determined schedule or manually on-demand. Actions taken upon malware detection include:

- Attempt to disinfect
- Attempt to delete or quarantine
- Notify

Information Management

The system generates events during virus scanning or operation. You can display these on the antivirus server, send them to Windows event logs, or email them to the appropriate personnel.

Reports generated by the antivirus server include important information such as antivirus signature file version number, identification of the infected endpoint over a specified time period, or a list of events that occurred during operation.

Signature Database and Scan Engine Update

You can access an update file that contains signature updates and/or engine upgrades from a secure Emerson website on a weekly basis.

Compliance Summary

NERC Standard	Requirement	Emerson Response
CIP-007-6 R3 Part 3.1	Deploy method(s) to deter, detect, or prevent malicious code	Antivirus is the first step to detect and prevent malicious code
CIP-007-6 R3 Part 3.2	Mitigate the threat of detected malicious code	Act immediately on detected virus infection
CIP-007-6 R3 Part 3.3	Have a process for the update of the signatures or patterns. The process must address testing	Virus signature updates are available weekly after being successfully tested on multiple Ovation levels in labs
CIP-007-6 R4 Part 4.1	Log events at the BES cyber system level for identification of and after-the-fact investigation of cyber security incidents	Detected malicious code is logged