Power and Water Cybersecurity Suite – Application Control

Features

- Protects against zero-day exploits
- Defends against memory injection attacks
- Eliminates weekly virus signature updates
- Provides four trust mechanisms for regular operation and maintenance
- Logs allowed or denied application events

Introduction

Emerson uses malware as an abbreviated term used to describe a malicious software program with varying characteristics such as:

- **Virus**: reproduces itself by attaching to other programs or making copies of itself
- **Worm**: runs itself by replicating on networks without a host program
- **Logic Bomb**: lies dormant until activation of a specific piece of program logic
- **Trojan Horse**: facilitates unauthorized access in a desirable program
- **Rootkit**: maintains command and control over a computer system without the computer system user knowing about it

Traditionally, antivirus software includes signatures of known malware that are stored in a file referred to as a Blocked list. Blocked list files are regularly updated to protect users from access to infected files.

New malware continues to emerge at an alarming rate. An independent information technology security institute registers almost 400,000 malicious programs every day. Detecting the large volume of new malware daily makes it difficult for antivirus product vendors to create timely signatures. Managing blocked list files from update server to endpoints can quickly become burdensome to users.

Solution

Application Control is a Power and Water Cybersecurity Suite application that enables users to effectively mitigate malware threats. Application Control compensates for the shortcomings of blocked listing technology by “Allow listing” only those programs permitted to operate within servers and workstations. Instead of trying to encompass the ever-increasing malware list, application-allow listing technology protects the permissible applications.

This mode of protection is especially relevant to control systems with static programs where new applications are rarely added during normal operations.

The control system has a fixed set of programs that perform real-time, mission-critical process control. The control system's static nature in terms of its resident application software creates an ideal environment for a policy-based software lockdown.

Even though the control system is static in nature, some online software changes are still necessary. Examples include frequent virus signature updates upon implementation of an antivirus product, monthly security patches for operating systems and key application software, or necessary administrative actions.

Trusted change mechanisms provide mandatory updates that maintain a well-protected control system. A trusted updater, trusted publisher with a digital certificate, or trusted path in a specified file system or local authorization can initiate changes.

Memory injection presents a new threat when external or malicious codes are executed within an authorized process. The code could originate on the local file system such as the dynamic link library (DLL) or outside the local file system such as reflective memory injection (RMI).

The Power and Water Cybersecurity Suite's Application Control application extends the Allow listing model from files and applications to a workstation's memory. Application Control monitors the memory address space and associated processes and detects distinct exploitations.

Operation

The Application Control application includes a dashboard powered by Trellix® ePolicy Orchestrator® with the following functions:

- **Discover:** applies auditing functions to selected endpoints with logging enabled. This builds an Allow list of existing application files without blocking new applications or updates to existing ones. The system adds these files to the application library and organizes them into application groups.
- **Define:** creates and applies trusted change policies (trusted publisher, trusted updater, or trusted path). Usage logs record authorized changes.
- **Monitor:** reviews application control logs daily to determine blocked applications when enforcement was enabled. Adjust trust policies and use local authorization if needed in the transition to lockdown.
- **Enforce**: applies lockdown policies in selected endpoints.
- **Manage:** provides continuous monitoring of the network and maintains trusted changes.

Compliance Summary

NERC Standard	Requirement	Emerson Response
CIP-007-6 R3 Part 3.1	Deploy method(s) to deter, detect, or prevent malicious code	Application Allow listing monitors all process execution and prevents the execution of non-authorized applications
CIP-007-6 R3 Part 3.2	Mitigate the threat of detected malicious code	Application Allow listing prevents the execution of non-authorized applications
CIP-007-6 R4	Log events at the BES cyber system level for identification of and after-the-fact investigation of cybersecurity incidents.	Logs blocked applications for review

The contents of this publication are presented for information purposes only, and while effort has been made to ensure their accuracy, they are not to be construed as warranties or guarantees, express or implied, regarding the products or services described herein or their use or applicability. All sales are governed by our terms and conditions, which are available on request. We reserve the right to modify or improve the designs or specifications of our products at any time without notice.

Emerson strives to deliver products, services, and documentation that reflect our commitment to diversity and inclusion. Some publications, including software and related materials, may reference non-inclusive industry terms. As diversity and inclusive language continue to evolve, Emerson will periodically re-assess the usage of such terms and make appropriate changes.