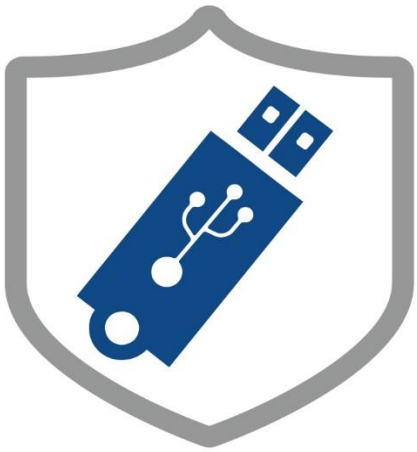
Power and Water Cybersecurity Suite – Device Control

Features



- Identifies storage devices connected to or embedded within machines
- Prevents malware infection or propagation
- Manages commonly used Microsoft® Windows-based devices
- Controls user access to devices
- Protects against potential data or program loss

Overview

Computer storage devices and their associated media (CDs, DVDs, or flash drives) are used to conveniently load or transfer information onto or from a control system.

Even though storage devices are valuable productivity tools, they can present a serious security threat to control systems when inadvertently or unknowingly used to transmit viruses or steal data. Evidence shows that many control systems have been infected with viruses due to the unmanaged use of private flash drives with operator workstations. Additionally, valuable application programs or confidential operating data could be transferred by an unauthorized user when copied to removable media.

Control system management best practices include policies that define the authorized use of storage devices. These policies must ensure system integrity by prohibiting the download of unknown or malicious software or unauthorized program changes as well as the improper use of workstations.

Solution

Device Control is a Power and Water Cybersecurity Suite application that enables secure and centralized management of storage devices associated with Windows-based workstations and servers, such as USB devices. The proper use of storage devices can be effectively administered by the policies defined within the Device Control application. Rules can be established for control system endpoints that completely block system access or provide different levels or permission for actions such as read/write, encrypt/decrypt, or import/export.

Permission for specific actions can be granted to authorized users. Policy enforcement can be set to occur always, on a predefined scheduled, or a temporary basis.

Loss of operating data or configuration information from workstations and servers threatens reliable system and plant operations. The Device Control application protects a system from the loss of information by guarding against unauthorized file transfers.

Event logs contain information regarding the use of storage devices within workstations and servers. Standard query and report templates are available for displaying configuration data.

Operation

The Power and Water Cybersecurity Suite Device Control application includes a dashboard powered by Trellix® ePolicy Orchestrator® with the following functions:

- **Discover:** Identifies all storage devices connected to or embedded within workstations and servers in an audit mode. The discover function also organizes the devices into collections for easier maintenance.
- **Define**: Creates rules or policies at both default and machine-specific levels for groups and individuals regarding device access by class, group, model, and/or specific ID. Assigns permissions to users, endpoints, and groups for access to allowed functions such as read, write, export to file, export to media, import, file filters, connections, drives, or encryptions.
- **Monitor**: Continuously observes device effectiveness and data usage policies in real time and identifies potential security threats.
- **Enforce**: Enforces file copy limitations, file type filtering, and forced encryption policies for data moved onto the storage devices.
- **Manage**: Uses dashboard widgets to create queries and reports on all devices, media, and data activity to identify gaps and track repeating offenders.

Compliance Summary

NERC Standard	Requirement	Emerson Response
CIP-010-R4	Documented plan(s) for transient cyber assets and removable media.	Preauthorize entity-approved removable media in the policy.