Power and Water Cybersecurity Suite Dashboard

Features

- Provides a unified view of Power and Water Cybersecurity Suite applications from a single user interface
- Centralizes security management
- Increases visibility of all security management activities
- Streamlines and automates compliance processes
- Integrates with Trellix Security Incident & Event Management tools
- Allows customizations for specific operational needs
- Provides advanced query and reporting options

Introduction

Emerson's Power and Water Cybersecurity Suite dashboard is an enterprise-class collection of functions that unifies security management across endpoints, networks, data, and compliance solutions.

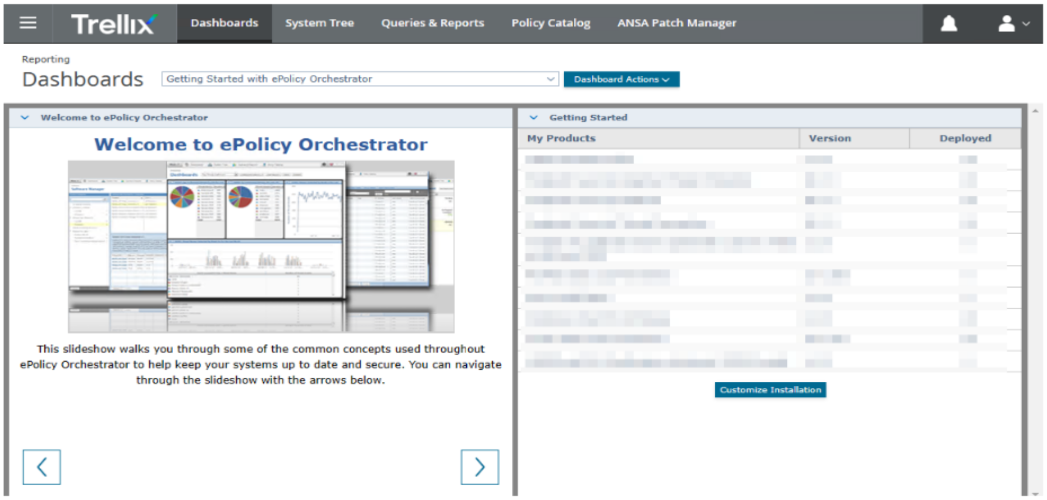
The dashboard automates security maintenance tasks and simplifies what can be a time-consuming and complex compliance process.

Powered by Trellix® ePolicy Orchestrator®, the dashboard streamlines and centralizes management of Power and Water Cybersecurity Suite applications. This intuitive user interface provides comprehensive views of all security activities, providing insights that help proactively detect and address potential security issues. Embedded tools help to identify unknown, rogue assets and simplifies the process of incorporating them into the management process.

The dashboard enables detailed analysis with extensive reporting capabilities for a stronger security posture. It also has provisions for developing automated workflows between the security infrastructure and the operational technology systems.

Dashboard Overview

The Power and Water Cybersecurity Suite dashboard is provided with the purchase of patch management, application control, device control, and/or antivirus protection applications.



Welcome to ePolicy Orchestrator

This slideshow walks you through some of the common concepts used throughout ePolicy Orchestrator to help keep your systems up to date and secure. You can navigate through the slideshow with the arrows below.

Initial implementation includes a standard dashboard interface for configuring, monitoring, and managing purchased suite applications. Drag-and-drop functions can be used to customize the dashboard's contents to meet specific operational needs.

A single agent is deployed to each Microsoft® Windows-based workstation and server that resides on the system network to manage the operating security applications. Additionally, the agent monitors for unprotected and unmanaged systems through a rogue system detection application. Reports are created using the built-in query system wizard that displays informative, user-configured charts and tables.

Dashboard workflow functions streamline the deployment process by automatically running queries and tasks to continuously monitor system health. The workflows distribute the most current content to client systems on a periodic basis.

Display

The initial dashboard view provides an overview of the system security including blocked events, blocked devices, quarantined viruses, offline endpoints, and discovered unmanaged endpoints. The collection of windows provides a concise view of system security in easily understood charts and graphs. The individual windows are customizable and include drill-down functions that provide in-depth details about an event by user, endpoint, or device. A report based on the drill-down information can be generated to capture important event data for later analysis. Report generation can be automated for continuous review of repeat or new offenders.

System Tree

An efficient and well-organized system tree provides a graphical representation of how the security system is organized. The tree simplifies maintenance and assists with generating an efficient workflow. Additionally, the system tree manages assigned endpoint policies, configurations, and agent deployments for patch management, application control, device control, and antivirus protection.
The system tree is a separate window accessed from the dashboard that provides a high-level view of endpoints that can assist with managing endpoint policies.

The tree can be organized to show:

- Automatic synchronization with Active Directory.
- Criteria-based sorting, using criteria applied to systems manually or automatically.
- Manual organization from the console (drag-and-drop).

Groups and subgroups can be used to organize how information appears within the system tree. Groups represent a collection of systems with similar characteristics such as machine type, location, or any other criteria that supports operational needs.

Queries and Reports

The dashboard includes a query and report builder for creating queries and reports for displaying data charts and tables.

Query results can be exported to various formats, which can be downloaded or sent as an attachment to an email message. Custom queries and reports can be created to define how data is retrieved and displayed. Most queries can be used as near real-time dashboard monitors.

Report examples include:

- Antivirus reports that identify infected endpoints over a specified time or provide a list of events that occurred during operation.
- Device Control reports can show attempts to plug in an unauthorized removable storage device such as a Universal Serial Bus (USB) stick.
- Patch Management reports confirm that patches were deployed to a specific endpoint.

Policy Catalog

A policy is a collection of settings that ensures the managed security software products are configured and perform accordingly. The dashboard provides the ability to configure policy settings for all products and systems from a central location.

Policies are assigned to endpoints to generate the security posture. A policy includes configurations such as permitted devices for device control, trusted applications for application control, and endpoint signature deployment waves for antivirus protection. The policy catalog includes custom policies that are deployed to agents so an endpoint can operate as desired.

Summary

The Power and Water Cybersecurity Suite's dashboard, powered by Trellix ePolicy Orchestrator, provides a centralized and unified view of security activities.

The dashboard simplifies the compliance process by automating security management tasks. The user-friendly interface is customizable to meet specific operational needs.

Advanced query and reporting options are available for detailed event analysis. Automated workflows can be created to bridge the gaps between the security infrastructure and the operational technology systems.

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.