

Ovation™ Security Center

Features

- Provides enhanced control system protection for secure, reliable, safe and efficient plant operation
- Tightly integrated with the industry-leading Ovation control system
- Eases management of cybersecurity risks
- Assists power generation customers with NERC CIP standards compliance for reliable operation of bulk electric systems
- Helps water and wastewater industry customers tackle mounting pressure to implement cybersecurity initiatives that safeguard public health and the environment

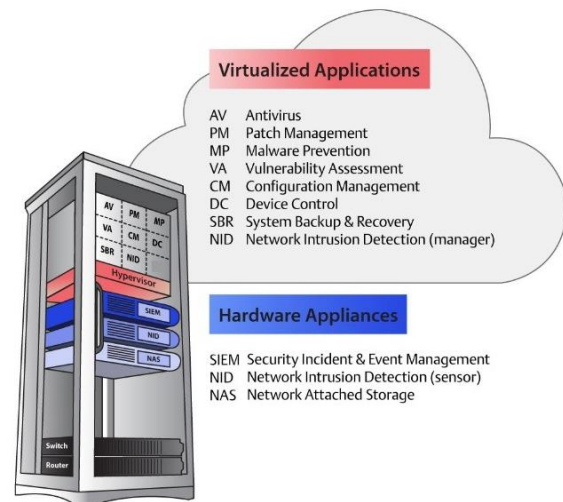
Overview

Emerson's Ovation™ Security Center helps customers operate their plants securely, reliably, safely and efficiently. Tightly integrated into the industry-leading Ovation control system, the Ovation Security Center makes it easier for Emerson's power generation, water and wastewater customers to automatically manage the execution of security control measures.

For customers in the power industry, the product assists in complying with the North American Electric Reliability Corporation (NERC) Critical Infrastructure Protection (CIP) standards. These standards require the power industry to identify and protect cyber assets that may impact the reliable operation of bulk electric systems.

Emerson's water and wastewater customers can implement the product to help deal with the mounting pressure to step up cybersecurity initiatives as part of their overall efforts to safeguard public health and the environment.

The Ovation Security Center consists of a suite of hardware-based and virtualized security applications



that have the ability to enhance and manage control system cybersecurity without disrupting the controlled process. These enhancements complement Ovation's native security functions, resulting in an integrated and robust solution.

The Ovation Security Center's integrated hardware and virtual software are packaged in an enclosure that includes an interface to the Ovation network. The cabinet is located outside of the control system's security perimeter in a separate subnet and demilitarized zone (DMZ). The Security Center applications use encryption to securely exchange information with Ovation network switches and routers as well as workstations and controllers.

Each Ovation Security Center application includes a dashboard with configuration tools and operating status displays. The applications also provide the capability to send alert notifications and generate security reports for operations management and regulatory compliance.

Periodic updates to patches, vulnerability databases and security signatures are downloaded through Emerson's SureService™ Ovation Security Center support program.

Ovation Security Center Virtualized Applications

Application Name	Description
Antivirus protection	Provides real-time virus and malware protection for workstations and servers with Microsoft® Windows®-based operating systems.
Configuration management	Effectively manages Ovation control system configurations with a focus on Windows-based workstations, network devices and Ovation's active directory.
Device control	Provides secure and centralized management of storage devices associated with Ovation Windows-based workstations, such as embedded CD/DVD drives and serial/parallel ports, as well as various removable devices.
Malware prevention	Enables Ovation users to effectively mitigate malware threats. Malware prevention compensates for the shortcomings of blacklisting technology by "whitelisting" only those programs allowed to operate within Ovation workstations.
Network intrusion detection	Protects against network attacks. Employs best practices by using routers to connect the Ovation control system to the enterprise LAN and field devices. This deployment provides both network isolation and access control.
Patch management	Employs an agent-based solution to accurately inventory software and determine patch needs in each Ovation workstation.
Security incident & event management	Collects security events from workstations running Microsoft Windows operating systems, as well as switches and routers. The application also gathers events from other data sources via the simple network management protocol (SNMP) or system log messages (Syslog).
System backup & recovery	Consists of management server software embedded within the Ovation Security Center and agents loaded on Ovation workstations that perform disk- or file-level data backup and recovery associated with each station's hard disks.
Vulnerability assessment	Closes the gaps between vulnerabilities and risks by providing a reliable, flexible and proactive tool that scans the Ovation system's environment for vulnerabilities and provides guidance for mitigating risks.

Connectivity & Communication

Communication with the Ovation Network

Ovation Security Center applications connect with the Ovation control system through a pair of network routers and switches inside the Security Center's cabinet. A dedicated DMZ for the Ovation Security Center simplifies integration with the operating Ovation control systems without the need for special setup or alteration. Examples of Ovation Security Center and control system connectivity include:

- Up to eight independent (non-multi-networked) Ovation systems can be individually connected to the Ovation Security Center switch from each respective Ovation control system network switch
- A single multi-networked Ovation system (with up to 16 connected Ovation subnets) can be singly connected to the Ovation Security Center switch from one of the core switches
- Combination of above two configurations

Communication with the Plant LAN

As an option, the Ovation Security Center router can connect to a plant LAN. The Security Center can provide event notifications, alerts or reports from multiple security applications to plant or corporate locations outside the control room. Additionally, the Security Center can use this connection to receive application content and software updates such as new security patches, virus signatures and detection rules from computers connected to the plant LANControl.

User Interface

Ovation Security Center applications are configured and maintained through a dedicated user interface provided on a standard non-Ovation Windows-based computer equipped with Remote Desktop and a browser. Emerson recommends connecting this workstation to the DMZ router for local management. The user interface can also connect to the plant LAN for remote management or further data analysis.

Service and Support

The Ovation Security Center SureService support module keeps the software, content, license and hardware elements of the Security Center promptly updated and renewed, as well as repaired in case of a mechanical failure. The use of this support module requires the purchase of the SureService expert telephone support module and it consists of:

- Application software updates
- Content updates including patches, definitions, rules or policies
- Component repair

Plant-wide Security Implementation

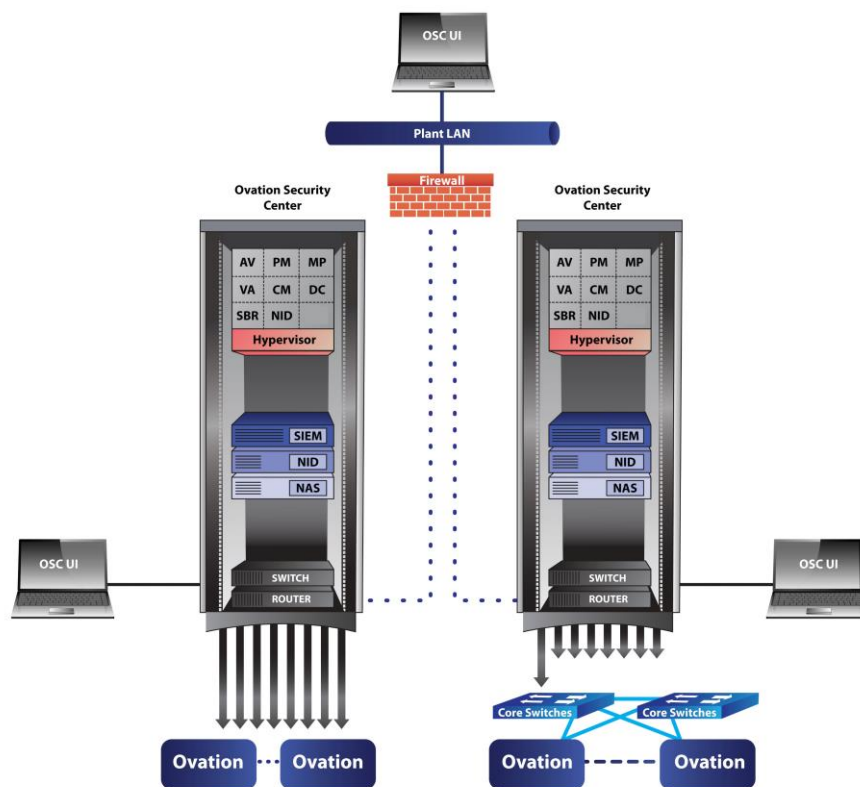
Ovation Security Center applications can be extended beyond Ovation to include other third-party control systems used within the plant. Network intrusion detection, security incident and event management, and vulnerability assessment can directly add other systems. The following applications require collaboration between the OEM and the asset owner for implementation:

- **Configuration management** – Standard functions are applicable to any Windows-based stations, however special applications may need to be developed by the OEM and asset owner for additional benefits.
- **Patch management** – Applicable security patches provided by the OEM can be distributed in the same manner as Ovation-based components.
- **Device control** – A device usage policy needs to be created for each station by the OEM and asset owner.
- **Malware prevention** – An application whitelisting policy needs to be created and thoroughly tested by the OEM and asset owner before being enforced.
- **System backup & recovery** - A backup plan is required that properly defines the OEM device data, scheme, access credentials and storage locations. A local database needs to be submitted for each third-party system.

Summary

The Ovation Security Center provides enhanced security management that assists Ovation control system customers with meeting regulatory compliance obligations.

The Security Center is a centrally located console that can be equipped with a host of applications to manage virus protection, control system configuration, device control, network intrusions, security incidents and events, patch retrieval and deployment, malware prevention, log storage and reporting, data recovery and vulnerability discovery.



Example of Ovation Security Center connections to the Ovation control system and plant LAN

©2017 Emerson. All rights reserved. The Emerson logo is a trademark and service mark of Emerson Electric Co. Ovation™ is a mark of one of the Emerson Automation Solutions family of business units. All other marks are the property of their respective owners. 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.