Features

- Scans for vulnerabilities
- Discovers assets
- Deploys security patches transparently
- Allows only white-listed applications to run in workstations
- Provides virus protection for Ovation Windows® workstations
- Aggregates, normalizes and correlates events for security incident identification
- Stores logs for forensic analysis with integrity check
- Inspects data packets across the Ovation perimeter
- Implements image backup and recovery of the Ovation system
- Sustains cybersecurity of multiple Ovation control systems

Introduction

The Ovation™ Security Center (OSC) consists of a suite of security functions which have the ability to enhance and regulate the cybersecurity of Ovation’s distributed control system without disrupting the controlled process.

These security products were specifically selected for their capability to advance system security while simultaneously reducing the cost of complying with North American Electric Reliability Corporation’s (NERCs) Critical Infrastructure Protection (CIP) standards.

The products’ ability to automate procedures that are now manually executed as well as their capacity to integrate with real-time control systems, gives Ovation customers advantageous benefits with system security.

While targeted to address NERC CIP standards, the OSC’s functions enhance plant reliability and availability through a well-managed security operation of control systems. The OSC is comprised of the crucial security functions for normal plant operations and are deployed based on the customer’s security priorities.

The OSC’s integrated hardware/software solution is packaged with a network interface to Ovation control systems. All security functions are managed from outside the security perimeter, which provides a separate DMZ for maximum integrity, flexibility, and security.

The OSC executes all administrative, monitoring and reporting functions, and provides local and/or remote display capabilities through standard web browsers.
Emerson institutes the support infrastructure necessary for the OSC application functions. The support includes regular functional testing of software and content updates for compatibility with multiple Ovation releases. The infrastructure support includes maintaining the user support website for transmitting updates.

**Ovation Security Center Components**

**Vulnerability Assessment**

The Vulnerability Assessment function addresses CIP-010-1 Configuration Change Management and Vulnerability Assessments, section R3: Vulnerability Assessment Requirements.

The Vulnerability Assessment function provides centralized asset identification and vulnerability assessment functions for Ovation systems. It is a network-based and agent-less scanning solution that performs comprehensive examinations of all devices on the Ovation network, including servers, workstations, routers, printers and switches. The scan also identifies devices on the network and determines their vulnerabilities (e.g., missing patches), then remediates them prior to exploitation.

The Vulnerability Assessment is also capable of running detailed configuration checks that enumerate ports, users, shares, groups, agents and services. Notification of scan-related events and remediation can be sent via Simple Network Management Protocol (SNMP) or email.

The manager of the Vulnerability Assessment function operates in a virtualized environment and utilizes encrypted communication within the client browser.

**Vulnerability Assessment Benefits:**

- Automates discovery of all network devices, operating systems and infrastructure
- Performs precise scans, targeting single or multiple machines
- Identifies vulnerabilities, impact to the organization and fixable solutions
- Ability to allocate schedule scans

**Patch Management**


The Patch Management function provides a centralized security patch distribution mechanism for Microsoft® and Windows®-based Ovation workstations.

This function compiles a comprehensive, centralized view of the patch status of the Ovation system through agent-based scans of each managed endpoint. A graphical “dashboard” consisting of more than 20 standard reports document the current patch status, history of patch deployments, trends, client inventory and more – at the individual machine or aggregated levels. This information is integrated into the Security Incident & Event Management functions to support compliance reporting requirements.

The Patch Management function is capable of deploying security patches for the underlying systems.
operating systems and selected integrated third-party applications. Patch deployment is automated and based on user-configurable distribution policies. Patch update downloads are initiated from the OSC and retrieved through Emerson’s SureService™ Ovation Security Center Support Module.

Patch deployment can run automatically, but typically requires a workstation reboot for maximum effectiveness.

The manager of the Patch Management function operates in a virtualized environment, utilizing an agent that is installed on each managed workstation to permit the remote installation of software updates.

Patch Management Benefits:
- Allows processing of patches, auto scanning, inventory and scan access
- Enables multiple machine/patch deployment in schedulable jobs
- Capabilities to patch multiple operating system types
- Option to reboot each station automatically or manually after patch deployment

Malware Prevention

This function provides centralized configuration and control of the Malware Prevention agent that resides on each Ovation host workstation. If an executable file name does not reside on the whitelist, the security software restricts that executable from running, thus rendering it “quarantined.”

Malware Prevention software logs any applications that have been blocked, and then forwards the logs to Security Incidents Event Management for collection and aggregation.

The Malware Prevention function provides a unique approach for protecting Ovation workstations against viruses, worms and Trojans. Rather than regular updates to a blacklist and assuming all intrusions will be caught, this appliance uses application whitelisting at the kernel level in each endpoint workstation, effectively blocking any unauthorized executable from running. If the executable is not on the list, it does not run. This appliance defends against security breaches on four fronts:

1. Directly defeats malware and other exploits by preventing them from executing
2. Limits user privileges
3. Prevents end users from altering the approved and validated system configuration
4. Intercepts any inappropriate behavior (e.g. memory exploits/DLL injections) and examines other mechanisms that malware attempts to exploit

The manager of the Malware Prevention function operates in a virtualized environment utilizing an agent that integrates into the kernel space of each protected workstation. This allows the workstation to incorporate protection from memory exploits (even if they’re using approved applications) and provides integrity checks including file digest, location and size.

Malware Prevention events are reported to the Ovation Security Center Security’s Incident & Event Management function as a security event. Standard reports are available for operations, management and regulatory compliance.
Malware Prevention Benefits:
- No malware, grayware or other unauthorized executables running that compromise security, performance or availability
- Tamper protection guards against unauthorized access and attacks
- Enforces regulatory policy compliance
- Provides preventative protection against targeted attacks

Antivirus Protection
The OSC’s antivirus function addresses CIP-007-5 – System Security Management, section R3: Malicious Code Prevention. This function provides real-time virus protection based on known signatures of malicious software. Signatures are tested weekly and released by Emerson. The targets of protection are Windows workstations which are more susceptible to virus attacks.

The protection is more effective when devices of the stations, such as disk drives, USB ports, or CD/DVD drives, are closely controlled and tightly restricted. The virus-laden files cannot be transferred from removable media to the station when access is blocked. It also further protects against potential, illegal information leaks through unauthorized file transfers.

The manager of the antivirus function operates in a virtualized environment, utilizing an agent that is installed on each managed workstation to permit the remote installation of software updates.

Antivirus Benefits:
- Mature technology
- Easy deployment
- Affordable pricing
- Device control for addressing root issues

Security Incident & Event Management
The OSC’s Security Incident & Event Management function provides centralized collection and correlation mechanisms that expedite analysis and reporting of Ovation system’s security posture.

The function aggregates and normalizes all events and logs reported by the variety of firewalls, intrusion detection software, anti-malware products, vulnerability scanners, network devices, workstations and active directories that exist within the system. These actions address CIP-007-5 Systems Security Management, specifically section R4: Security Event Monitoring.

Additionally, the function simplifies large amounts of disparate types of data to provide indicators that a security incident may be happening. The Event Management function analyzes the data in detail and provides depth of context. Distinct reports can be generated specifically for NERC CIP compliance.
Security Incident & Event Management

Benefits:
- Smart protection, confidence and regulatory compliance
- Expansive security events collection and monitoring for multi-vendor secure environments
- Real-time event correlation to detect both known and unknown threats
- Comprehensive interactive reporting for fast and intuitive security analysis
- Simple setup, dashboard, report and alert customization

Log Management

As part of the Security Incident & Event Management function, the Log Management function provides abilities to retain and preserve the original log files for extended time periods. The storage of the multiple raw logs requires an external Network Attached Storage device. This feature is required per CIP-008-5: Incident Reporting & Response planning, in the event that a real cybersecurity occurrence has been identified and evidence needs to be retained.

Log file integrity checking is provided with the calculated message digest with an MD5 algorithm. Changing a single bit in the data causes a completely different message digest to be generated. The original digested messages are protected with encryption.

Log Management Benefits:
- Compliant log retention requirements
- Adaptable storage and retention for each log source
- Ability to analyze and conveniently search
- Stores logs in a managed NAS

Network Intrusion Detection

OSCs Network Intrusion Detection function addresses the growing concerns and possibilities of cyber-attacks from the plant network rather than from compromised control workstations or end points. It is connected online or to a span port monitoring traffic at Ovation’s perimeter access points.

The data traffic across these access points will be extensively inspected against the protocol headers and payloads. Potential network-based attacks, including worms, Denial-of-Service (DoS) and other forms of malware are detectable.

This detection mechanism can be signature or anomaly-based, so that either known or unknown attack patterns can be effectively detected. At this time, this function is intended for Ovation perimeter protection or between Ovation systems within an Ovation multi-network architecture.

---

1 Log Management and Network Intrusion Detection is available with the Ovation Security Center 2.1 and 3.0 releases
The manager of the Network Intrusion Detection function operates in a virtualized environment, interfacing with external hardware appliance(s) to monitor network traffic. The intrusion events can be optionally forwarded to the Security Incident & Event Management module of the OSC for further correlation or analysis.

Network Intrusion Detection Benefits:
- Discovery of cyber-attacks from adjacent networks
- Extensive inspection of protocols and payloads
- Integration of detection information with the Security Incident & Event Management

Network Attached Storage
Network Attached Storage provides an easy-to-use, high-performance storage solution to share and protect critical data. Installed in the Ovation Security Center cabinet, it serves the following purposes for the Ovation Security Center's functional modules and Ovation control systems:

- Bulk storage of Log Management archived data
- Diverse storage for proxy images of the Ovation Security Center appliances
- Ovation backup images from the new System Backup & Recovery
- Remote replication to another storage device to support offsite archiving

System Backup & Recovery
The disaster recovery goal of System Backup & Recovery is to expedite full retrieval if the Ovation system experiences a partial or full loss of its software assets.

Based on image technology, the System Backup & Recovery function can perform disk- or file-level backups that include the host's operating system, application software, configuration and data. A backup plan can be created for full, differential, incremental or a combination of any or all backup types.

The plan can be executed by schedule, event-triggered or manually. The backup files may be sent to multiple locations, although the Network Attached Storage is the preferred selection.

Software restoration can be performed for the entire Ovation system, an individual workstation, folders or files.

System Backup & Recovery Benefits:
- Leverage the established OSC infrastructure for supporting multiple Ovation systems
- Fast recovery available from disk images in case of disaster recovery
- Scripted plan for recovering full Ovation when real-time database and controller synchronization needs to be considered

Ovation Security Center Configuration
The OSC is designed to be safely added to an Ovation system while the controlled process is in operation. As such, the OSC consists of the necessary network equipment to establish its own DMZ and does not require modification to any existing DMZ or field LAN communications equipment, nor is there any special setup or alteration of the existing Ovation system. The only requirement is TCP/IP connectivity. All of the appliances are interconnected in a private DMZ, which is router-isolated from Ovation and the customer’s plant network. Figure 1 on the following page illustrates an overview of standard OSC communications.

---

2 Network Attached Storage is available with the Ovation Security Center 2.1 and 3.0 releases
3 System Backup & Recovery is available with the Ovation Security Center 3.0 release
OSC Communications to Ovation

The standard OSC network package is designed with the inherent flexibility for connecting to the most common Ovation plant configurations.

Possible communication configurations:

- Directly connect to one and up to eight independent (non-multi-networked) Ovation DCS networks. The connection point on each Ovation network is a port on one of the Ovation switches in each DCS LAN.
- Directly connect to a single multi-networked Ovation system (with up to 16 connected Ovation subnets). The connection point on the multi-network system is a port on one of the Ovation core switches.
- Directly connect to a port on any one of the multi-networked DCS LANs if the multi-network Ovation system is not using the Emerson collapsed backbone architecture. The multi-network configuration must be reviewed in order to verify that all appliances can be implemented.

Intra-appliance Communications

The standard OSC network package provides a dedicated DMZ that allows communication between the functions. This feature enables the Security Incident & Event Management function to collect and consolidate the security information from the other security functions.

An Emerson-provided router with integral firewall capability is used to secure the DMZ and control all traffic between OSC and Ovation control system. This router also controls any traffic to or from the plant LAN. The router is configured to log security events to the Security Incident and Event Management functions.

Figure 1 Connection of up to eight independent Ovation DCS networks and connections to a single multi-networked Ovation system (up to 16 Ovation subnets)
Ovation Security Center Communications from the Plant LAN

The standard OSC network package provides a single access point for secure communications from a corporate plant LAN to the OSC. This connection is used for report generation, event analysis, updating patches, vulnerability definitions and maintenance.

To ensure security, this connection exists via a VPN tunnel from the user’s workstation to the OSC router. The tunnel is configured to authenticate the user with either the corporate or the Ovation Domain Controller. Additionally, the same VPN tunnel approach is used if the customer requires/permits SureService support for the OSC.

If desired, an optional firewall appliance may be used in series with the Emerson-provided router.

Ovation Security Center User Interface

Users can manage and monitor the OSC functions using the OSC User Interface (OSC UI). The OSC UI is a standard Windows machine with Remote Desktop and a browser. The machine itself does not have any Ovation functionality. Emerson recommends that this workstation is connected to the DMZ router for local management. The OSC UI also can connect to the plant LAN for remote management or further data analysis.

Ovation Security Center Support

The Ovation Security Center SureService Support Module requires the purchase of the SureService Expert Telephone Support Module.

Ovation Software Support

The OSC levels 2.0 and 2.1 will support Ovation 2.4 through 3.3.1 level systems for Microsoft Windows and Ovation 1.7.2 through 1.9.2 level systems for Sun Solaris. The OSC level 3.0 and 3.1 will support Ovation 3.0 and above level systems for Microsoft Windows, except for the System Backup & Recovery function. The System Backup and Recovery function supports Ovation 3.5 and above level systems.

Keeping Your Ovation Security Center Up-to-Date

The Ovation Security Center SureService Support Module is designed to keep both the software and hardware elements of the Ovation Security Center performing at their highest levels. The support module consists of:

Software Updates and Security Patches

Emerson validates important patches supplied by third-party vendors applicable to the Ovation system including:

- Microsoft® Windows® 7 Operating System
- Microsoft® Windows® Server 2008 and Server 2003 Operating System
- Microsoft® Internet Explorer
- Adobe® Reader®

It is important to keep the OSC current with software updates and security patches. Packages consisting of tested patches, vulnerability definitions and any appliance updates are delivered through a dedicated support web site on a monthly basis.

A customer-provided PC with an Internet browser is used to download the posted file(s). These files are then transferred to the OSC via the OSC UI using removable media (e.g. flash drive). Additionally, a cumulative DVD of all patches is delivered once per year.

Component Repair

Repairs to any of the OSC components will be made during the term of a valid SureService contract that includes the Ovation Security Center SureService Support Module.

Annual License Renewal

Also provided is the annual renewal fee for each of the three licensed components.

The support module will need to be purchased on a yearly basis. However, the first year of the Ovation Security Center SureService Support Module is included with the purchase of the OSC.
Non-Ovation Applications

Many functions of the OSC can easily be extended to other control systems in the same plant. Implementation of those functions may require collaboration between the control system OEM and the asset owner.

Every device that is to be covered must be network-accessible to the OSC. Routers and firewalls within the plant’s network infrastructure may have to be modified to support the OSC’s communication requirements.

Vulnerability Assessment

- Nonintrusive vulnerability scans are administrable from network-accessible devices to the OSC. The scanner determines a device’s operating system (and other attributes) once administrative credentials have been provided

Patch Management

- A host agent will be installed on each supported workstation. After the host agent is incorporated, the workstation’s OEM or asset owner can verify the correct operation of the workstation
- The monthly tested operating system patches are generally available from each workstation’s OEM. The list of the approved patches can be compared with the approved patch list from Emerson
- Any unnecessary patches can be removed from the deployment list
- Any additionally required patches can be packaged separately and deployed to the OEM’s workstations by the asset owner

Malware Prevention

- Agents are created for each workstation’s protection
- Each agent is developed between the OEMs of the workstation and the Malware Prevention appliance and supported by the asset owner

Security Incident & Event Management

- Security Incident & Event Management can accept information sourced by other devices

- Standard parsers included with the Security Incident & Event Management receive, normalize and correlate events from many devices
- A special parser may need developed if the device generates logs in a non-standard format

Network Intrusion Detection

- Network Intrusion Detection is usable with other customer supplied network devices
- List of the supported network devices is available for compatibility verification

System Backup & Recovery

- A backup plan needs to be created so that the data, scheme, access credentials, and storage locations can be properly defined
- Local database needs to be attended particularly with the assistance from the OEM

Summary

The OSC provides enhanced security management that enables Ovation control system customers to meet NERC CIP standards for regulatory compliance. It also provides a centrally located management console equipped with appliances that manage security events, patch retrieval and deployment, malware prevention, log storage and reporting, intrusion prevention, data recovery and vulnerability discovery.

The OSC also lends itself to non-Ovation control systems via collaboration with other control system OEMs. The OSC could supply vulnerability assessments, patch management, malware prevention, security incident and event management, network intrusion detection, and system backup and recovery functions for non-Ovation based plants.