Automated Patch Management Service

- Establish successful and proactive patch management strategy
- Ensure the availability and business continuity of your DeltaV™ process control system
- Reduce manual system administrative activity and delays associated with software updates

The Emerson Automated Patch Management Service is a combination of people, technology and best practices designed to automate the routine aspects of manual security software update deployment.

Introduction

Every month there are new Microsoft® Windows® OS security updates, McAfee® Endpoint Security for DeltaV Systems antivirus updates, Symantec™ Endpoint Protection antivirus updates and DeltaV DCS hotfixes that need to be acted upon. Emerson's Automated Patch Management Service provides an effective solution that address the five deployment steps — identification of required Emerson-approved updates, acquisition of update executables, distribution to appropriate DeltaV DCS nodes, installation and compliance auditing.

It is very common for the most critical security, antivirus and application hotfix updates to go uninstalled for extended periods of time, or not be installed at all. Often the reasons are due to limited skilled resources and day-to-day judgment calls about what is more important; to either address an immediate need with a measurable business benefit or deploy the current batch of system software updates with their unknown and often un-quantified effect on system vulnerability.

Benefits

Establish successful and proactive patch management strategy : Automated Patch Management Service automates routine aspects of software update deployment for timely dependable implementation, while freeing staff to devote more time to your own business. For large systems, the savings can add up to hundreds of hours per year. Automated Patch Management Service identifies the appropriate Microsoft Windows security patches, tests them on DeltaV DCS and advises the customer on which DeltaV DCS hardware needs updating with which particular software patches on an individual system-by-system basis.

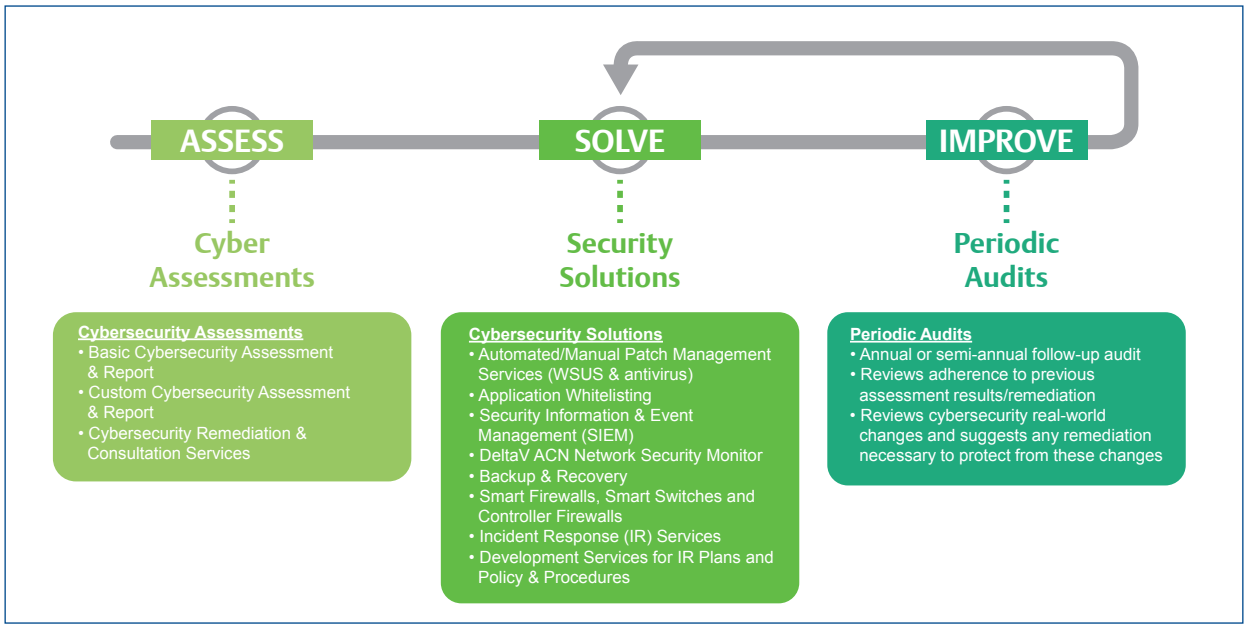
Ensure the availability and business continuity of your DeltaV system: Emerson provides approved Microsoft Windows security updates as well as antivirus signature file updates on a regular basis. Experience has shown many of the disruptive events reported to the Emerson Global Service Center could have been avoided, had the relevant security update or hotfix been applied in a timely fashion.

EMERSON

Reduce manual system administrative activity and delays associated with software updates: Maintaining security patch management and hotfixes are essential to your system's security and availability.

This automated service ensures that critical updates are deployed consistently.

By delegating patching to Emerson's Automated Patch Management Service, site resources can focus on delivering quality product and bottom-line results; spending less time evaluating and deploying patches, and more time focusing on process management and operations.



Emerson's Cybersecurity Management Solutions Process and Services Portfolio.

Cybersecurity Management Solutions

Automated Patch Management Service is an integral part of Emerson's Cybersecurity Management Solutions portfolio. A comprehensive cybersecurity solution consists of many different components; each one specific to reducing risks associated with various process control system entities. Emerson's Cybersecurity Management is an integrated approach to finding the best cyber solutions to fit your current process control system and existing plant security policies and procedures.

Cybersecurity Management solutions cover:

- Automated/Manual Patch Management Services (WSUS & antivirus patching)
- Disaster recovery
- Backup and recovery
- System Health Monitoring
- Applications Whitelisting
- Network Security Monitor
- Security Information & Event Management (SIEM)
- System Health Monitoring
- Smart firewalls, Smart Switches and Controller Firewalls
- On-site spare parts management
- Security consultation services
- Incident Response Services
- Development Services for IR Plan and Site Policies & Procedures Review

Reduction of risks associated with the use of these solution components reduces the time spent on controllable issues and allows focus on other important day-to-day issues.

Automated Patch Management Service Architecture

Software service enablers are combined with Emerson's expert consultation and optional on-site commissioning to implement automated deployment capability for Microsoft® Windows® security updates, Symantec™ antivirus updates and DeltaV DCS hotfixes.

The software service enablers include:

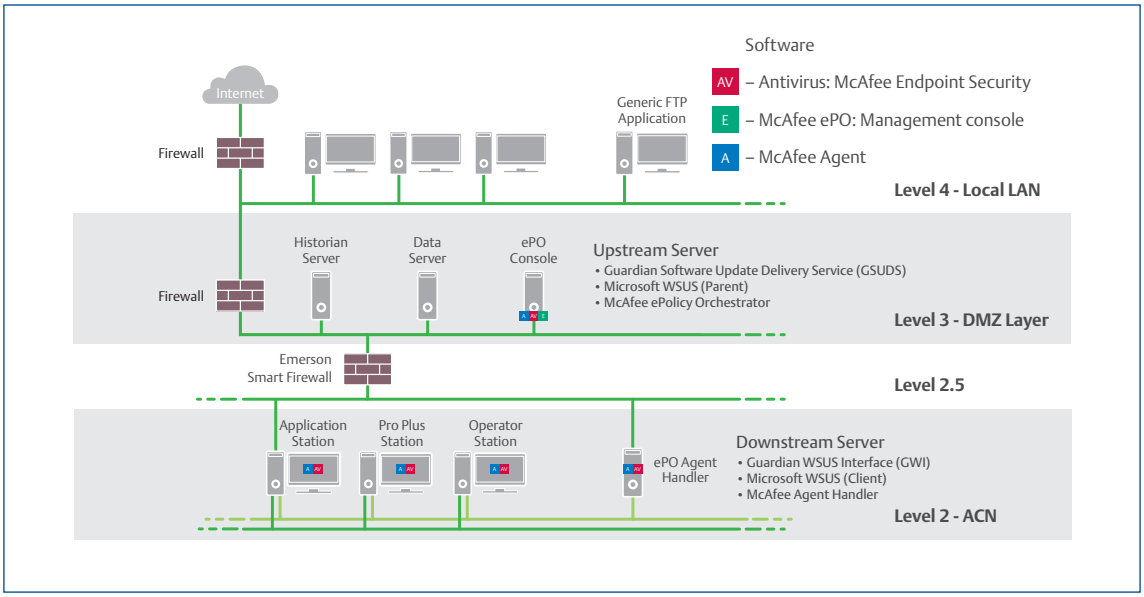
- **Guardian Software Update Delivery Service (GSUDS) Client:** an Emerson software application available for systems enrolled in Guardian Support service. It solicits system hot fixes and approval information for Microsoft security updates from Emerson via the Internet. It is typically located on a web facing Upstream Server.
- **Guardian WSUS Interface (GWI):** An Emerson software application that periodically loads new DeltaV hotfixes and the latest approval information for Microsoft security updates, and programmatically injects them into WSUS. It is typically located on the Downstream Server.
- **Microsoft Windows Server Update Service (WSUS) version 3 or higher:** A no-cost add-on to the Microsoft server operating system. Two instances of the WSUS application are required; one on an internet facing server (Upstream Server) to solicit security updates from Microsoft and a second located on a non-DeltaV DCS server (Downstream Server) on the DeltaV side of the firewall, synchronized to move data to and from on another. WSUS provides distribution, deployment and audit capabilities for Microsoft security updates and DeltaV hot fixes.
- **For McAfee Endpoint Security for DeltaV Systems:**
  - McAfee ePolicy Orchestrator® Console (McAfee ePO™) — A software application that solicits antivirus updates from either Emerson or via the Internet, typically located on a server located on the L2.5 or L3 network.
  - McAfee Super Agent/Agent Handler - An application platform that deploys the antivirus updates obtained by the ePO console to the agents located on the DeltaV ACN nodes.
- **For Symantec Endpoint Protection Solutions:**
  - Symantec Live Update Administrator (LUA) —A software application that solicits antivirus updates from Symantec via the Internet, typically located on the Upstream Server.
  - Symantec Endpoint Protection Manager (SEPM) — A software application that deploys antivirus updates obtained by the LUA, located on the Downstream Server.

Service Prerequisites

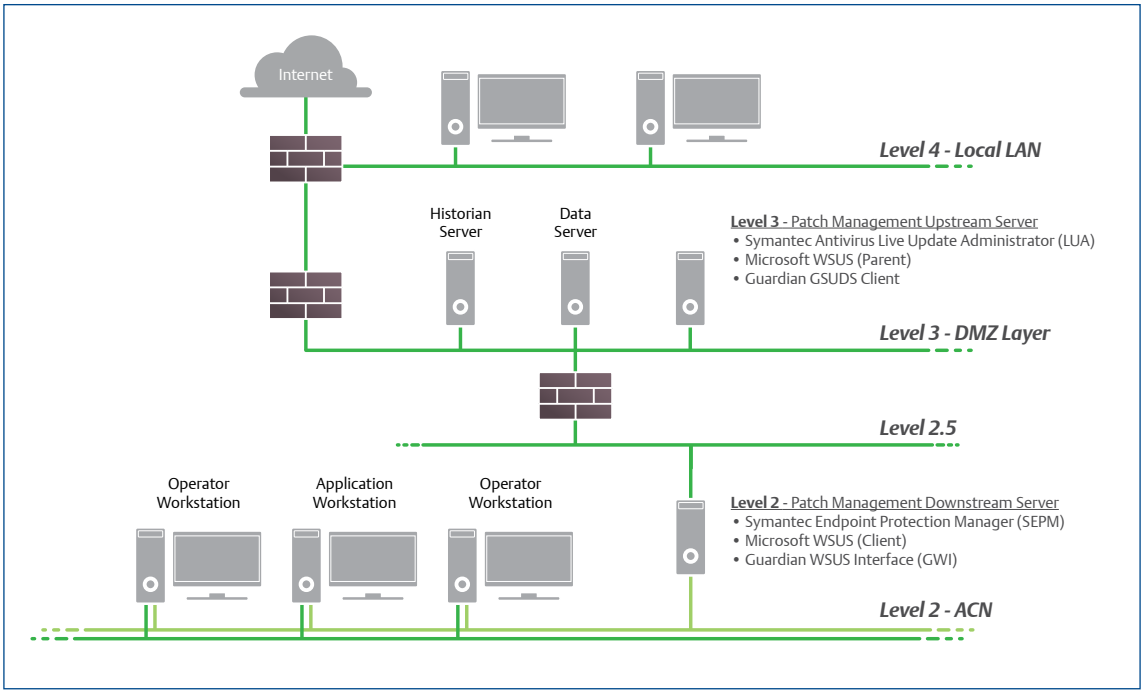
Automated Patch Management Service prerequisites:

- DeltaV installed in a domain environment, running DeltaV v11.3.1 software or later.
- System(s) enrollment in Guardian Support Service.
- Annual purchase of the Automated Patch Management Subscription Service for each system ID.
- For McAfee Endpoint Security for DeltaV Systems:
  - Licenses to use McAfee ePO, Super Agent/Agent Handler and agent clients (all supplied by Emerson).
- For Symantec Endpoint Protection:
  - License to use Symantec Live Update Administrator (LUA) (customer's responsibility to procure).
  - License to use Symantec Endpoint Protection Manager (SEPM) and clients (customer's responsibility to procure).
  - Support service contract from Symantec is recommended (customer's responsibility to procure).
- Support contract from Microsoft for WSUS is recommended (customer's responsibility to procure).
- Hardware required for McAfee Endpoint Security for DeltaV Systems:
  - McAfee ePO Server - A server class computer licensed for Microsoft Windows Server 2008 R2, Windows Server 2008 SP2 (x64only) or later, Windows Server 2012 and Windows Server 2012 R2.
  - An Internet accessible server class computer licensed for Microsoft Windows Server 2008 R2, Windows Server 2008 SP2 (x64only) or later, Windows Server 2012 and Windows Server 2012 to host applications that require Internet access.
  - Customer-managed network infrastructure that allows the ePO Super Agent/Agent Handler to securely access the McAfee ePO console.
- Hardware required for Symantec Endpoint Protection Solution:
  - A server class computer licensed for Microsoft Server 2008, Windows Server 2008 R2, Windows Server 2012 and Windows Server 2012 R2 to be installed as a non-DeltaV DCS node (Downstream Server) on the DeltaV control network.

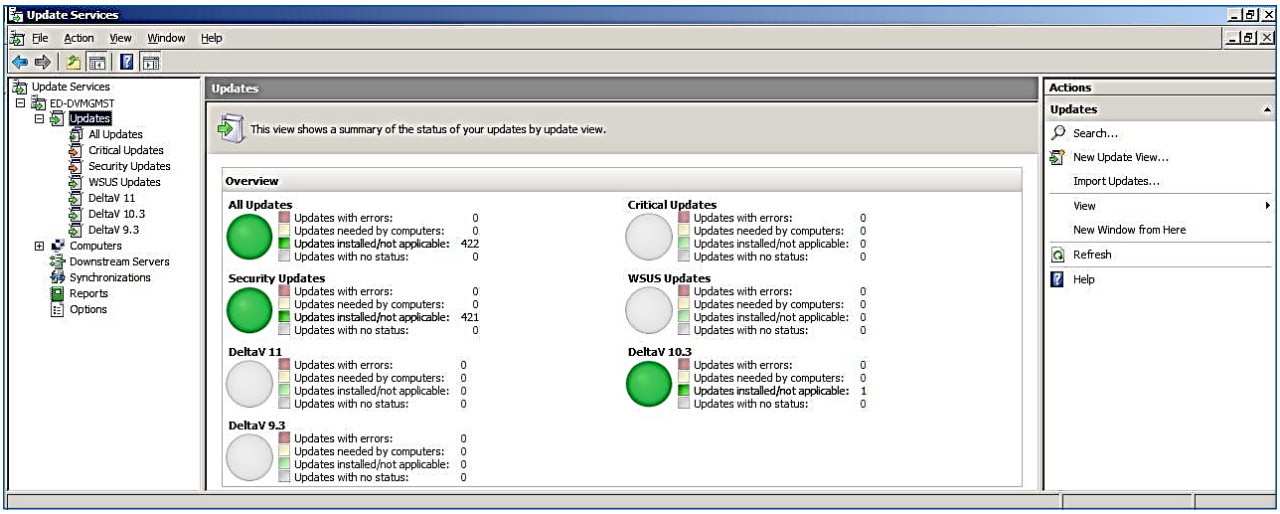
- An Internet accessible server class computer licensed for Microsoft Server 2008 SP2, Windows Server 2008 R2, Windows Server 2012 and Windows Server 2012 R2 (Upstream Server) to host applications that require Internet access.
- Customer-managed network infrastructure that allows the Downstream Server to securely access the Upstream Server.



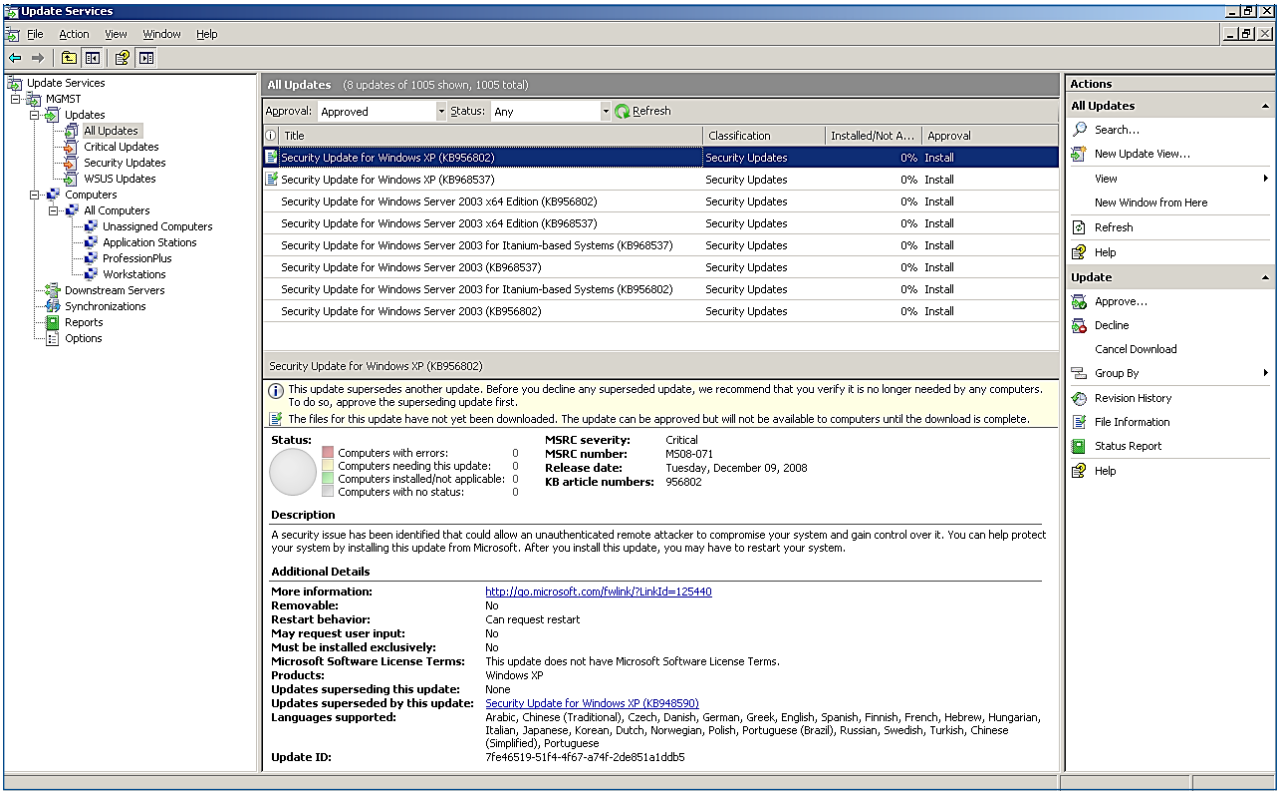
Reference Architecture for Emerson Automated Patch Management Service utilizing McAfee Endpoint Security for DeltaV Systems software.



Reference Architecture for Emerson Automated Patch Management Service utilizing Symantec Endpoint Protectrion for DeltaV Systems software.



Sample WSUS Control Panel for deployment and audit of security updates.



Sample WSUS Control Panel for deployment and audit of security updates.

Operational Characteristics

Group policy or individual computer settings dictate how often each DeltaV application station and workstation contacts the Downstream Server for new Microsoft Security updates, and what action to take when a new update is available. These settings require careful consideration. In a typical service deployment; antivirus updates are scheduled for automatic download and installation according to a schedule, however these updates do not require reboots; Microsoft security updates are automatically downloaded according to a schedule with local computer notification that an update is ready to install; and DeltaV hotfixes are only downloaded and installed upon request.

Automated Patch Management Services

While some customers prefer to design, install and start-up their own solutions and simply use the Automated Patch Management subscription service to provide the downloaded metadata, Emerson also offers services to help our customers integrate Automated Patch Management Service into their network infrastructure through evaluation, design and implementation services. These services include:

- **Automated Patch Management Evaluation:** Emerson will work with the customer to evaluate their request for services. The evaluation will: Define the scope of work to be performed.
  - Analyze the system architecture desired and any high level technical considerations requested.
  - Define any testing that may be required to future validate the overall system architecture and configuration desired.
  - Provide an Evaluation Report outline the customer request, considerations, and Emerson's recommendations.

- **Automated Patch Management Detailed Design**: Based on the findings from the Patch Management Evaluation, this optional service will develop a proposed architecture, detailed configuration, and policies to test and verify proper functioning of the proposed Patch Management system. The detailed design phase may include:
  - System staging based on the customers desired system architecture and configuration. This pre-work will determine the best configuration and installation processes to be used on site. Equipment to be used in the plant can be provided by the customer for system staging.
  - Detailed consultation regarding the newest features and enhancements contained in the new versions of Guardian Update Delivery Service, Windows System Update Service, Symantec Endpoint Protection, and the Guardian WSUS Interface.
  - An outline of the testing procedure to be performed
  - Complete test reports outlining notable system behavior and installation and configuration issued found.
  - A detailed roadmap indicating any site installation and configuration prerequisites required.
  - Testing of any desired system modification identified during the Evaluation phase.

- **Automated Patch Management Implementation**: Based on the findings of the evaluation and detail design, Emerson will work with the customer to install, configure and implement Patch Management Service. Upon completion, a implementation report will be provided to the customer.

Please contact your Emerson Service Representative for a quote if these services are required at your site.

Automated Patch Management Annual Subscription Service

Automated Patch Management Service requires an add-on subscription service to Guardian. This subscription service enables Guardian to produce metadata specific to the customers covered DeltaV systems. The metadata, along with the Guardian WSUS Interface software (GWI) will approve Microsoft Security Updates and import DeltaV Hotfixes required by the DeltaV System ID's configured.

Customers deploying Automated Patch Management Service without the use of Emerson services can purchase Consultation hours if assistance is required.

Automated Patch Management Project Support

Automated Patch Management Service is a solution composed of a combination of standard Emerson products and an engineered environment that delivers patches through a customer network to individual machines. Standard Guardian Support provides initial support for any issues or questions regarding the Automated Patch Management solution (including but not limited to WSUS and Symantec SEPM) through Emerson's Global Support Center (GSC). Relatively simple and straightforward questions and issues that are non-site/system specific will be fully covered by Guardian Support. Issues and questions that are more complex and are more site/system specific will most likely require and additional service contract either through your local Emerson Service Representative and/or Emerson's Performance Service group. In systems where an Emerson-supplied McAfee antivirus solution (Endpoint Security for DeltaV Systems) is part of the Automated Patch Management solution, Emerson Guardian Support extends to McAfee support issues as well.

Ordering Information

This subscription service requires a current DeltaV DCS Guardian Support Contract covering the System IDs at a given plant site be in place. The model number selection is independent of whether an Emerson Endpoint Security for DeltaV Systems or the Symantec Endpoint Protection solutions are utilized. Components of these solutions are not included with this subscription service offering.

Description	Model Number
Automated Patch Management Subscription Service: 1-Year Cybersecurity, Automated Patch Management; for Small Systems less than 5,000 DSTs	VE9117SM
Automated Patch Management Subscription Service: 1-Year Cybersecurity, Automated Patch Management; for Medium Systems from 5,000 DSTs to 19,999 DSTs	VE9117ME
Automated Patch Management Subscription Service: 1-Year Cybersecurity, Automated Patch Management; for Large Systems 20,000 DSTs or greater	VE9117LG
Automated Patch Management Subscription Service: 1-Year Renewal for Cybersecurity, Automated Patch Management; for Small Systems less than 5,000 STs	VE9117SM-RENEW
Automated Patch Management Subscription Service: 1-Year Renewal for Cybersecurity, Automated Patch Management; for Medium Systems from 5,000 DSTs to 19,999 DSTs	VE9117ME-RENEW
Automated Patch Management Subscription Service: 1-Year Renewal for Cybersecurity, Automated Patch Management; for Large Systems 20,000 DSTs or greater	VE9117LG-RENEW

This product and/or service is expected to provide an additional layer of protection to your DeltaV system to help avoid certain types of undesired actions. This product and/or service represents only one portion of an overall DeltaV system security solution. Emerson does not warrant that the product and/or service or the use of the product and/or service protects the DeltaV system from cyber-attacks, intrusion attempts, unauthorized access, or other malicious activity ("Cyber Attacks"). Emerson shall not be liable for damages, non-performance, or delay caused by Cyber Attack. Users are solely and completely responsible for their control system security, practices and processes, and for the proper configuration and use of the security products.

To learn more, contact your local Emerson sales office or representative, or visit **www.emerson.com/cybersecurity.**

Emerson
North America, Latin America:
+1 800 833 8314 or
+1 512 832 3774

Asia Pacific:
+65 6777 8211

Europe, Middle East:
+41 41 768 6111

www.emerson.com/cybersecurity

EMERSON