Automated Patch Management Service

- Establishes successful and proactive patch management strategy
- Helps to ensure the availability and business continuity of DeltaV DCS
- Reduces 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 security updates, Symantec anti-virus 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, anti-virus 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

Establishes 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 dd up to hundreds of hours per year. Automated Patch Management Service identifies the appropriate security patches, tests them on DeltaV DCS and advises the customer on which DeltaV DCS hardware needs updating with which particular software patches.

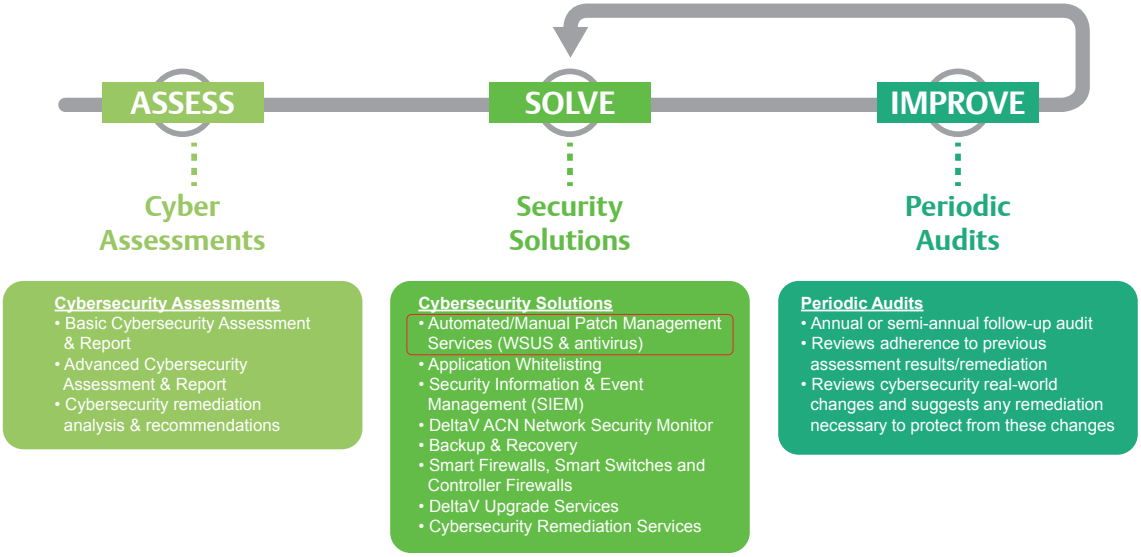
Helps to ensure the availability and business continuity of DeltaV DCS: Emerson tests and approves Microsoft Windows security updates and antivirus signature files on a regular basis. Experience has shown many of the disruptive events reported to the Emerson Global Service Center could have been avoided, had the relevant security update or hotfix been applied in a timely fashion.

EMERSON™
Process Management

Reduces manual system administrative activity and delays associated with software updates: 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.



Cybersecurity Management Solutions

Automated Patch Management is 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. 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 also cover:

- Disaster recovery
- Backup and recovery
- System health monitoring
- Smart firewalls
- On-site spare parts management
- Security consultation services

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™ anti-virus updates and DeltaV DCS hotfixes.

The software service enablers include:

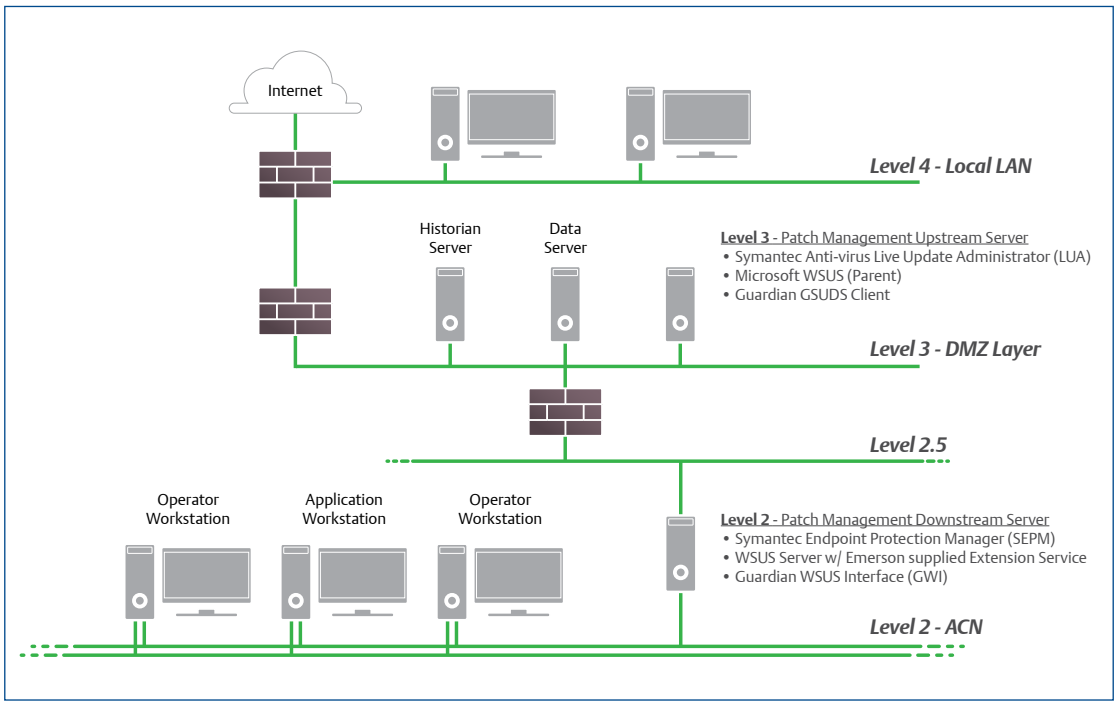
- Guardian Software Update Delivery Service (GSUDS) Client — an Emerson software application available for systems enrolled in Guardian Support service. It solicits system hot fixes and approval information for Microsoft security updates from Emerson via the Internet.
- Guardian WSUS Interface (GWI) — An Emerson software application that periodically checks with the GSUDS Client for new DeltaV DCS hot fixes 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 DCS control network, configured for a parent-child relationship. WSUS provides distribution, deployment and audit capabilities for Microsoft security updates and DeltaV DCS hot fixes.
- Symantec Live Update Administrator (LUA) —A software application that solicits anti-virus 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.

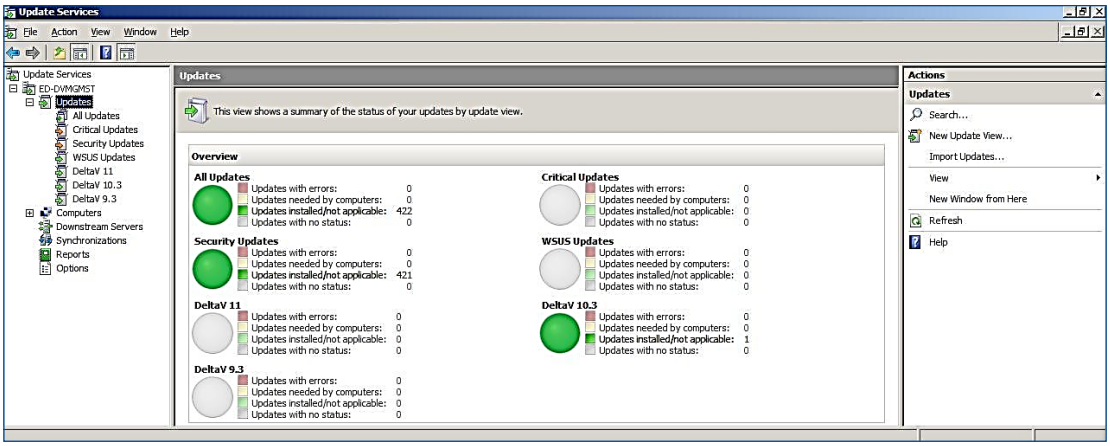
Service Prerequisites

Automated Patch Management Service prerequisites:

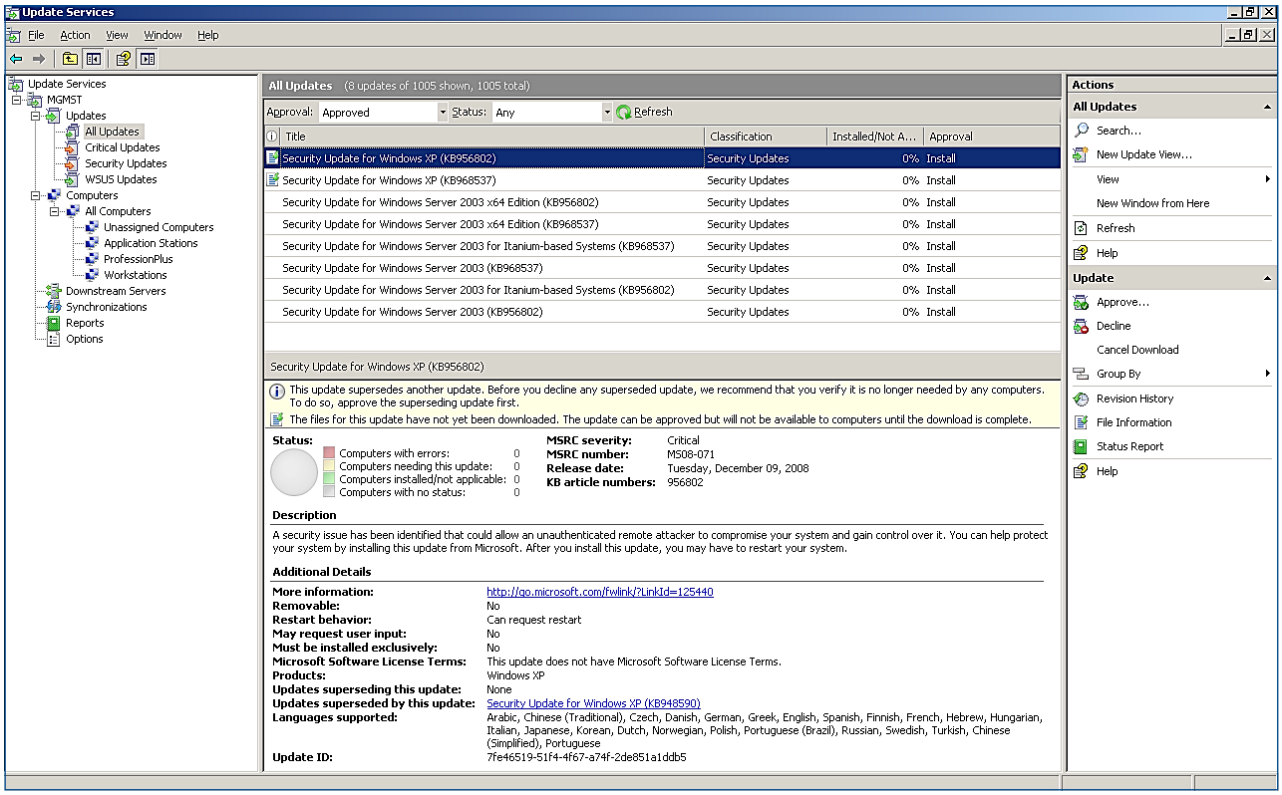
- DeltaV DCS set up as a domain, running DeltaV v9.3 software or higher.
- Enrollment in Guardian Support Service and annual purchase of the Automated Patch Management Subscription Service.
- A license to use Symantec Endpoint Protection Manager and clients (customer's responsibility).
- Support contracts from Symantec and Microsoft for WSUS and SEPM are recommended (customer's responsibility).
- 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 DCS control network.
- An Internet accessible server class computer licensed for Microsoft Server 2008, 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.



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.



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 DCS application station and workstation contacts the Downstream Server for new updates, and what action to take when a new update is available. These settings require careful consideration. In a typical service deployment; anti-virus updates are scheduled for automatic download and installation according to a schedule; Microsoft security updates are automatically downloaded according to a schedule with local computer notification that an update is ready to install; and DeltaV DCS 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 into their IT infrastructure through evaluation, design and implementation. 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. Upon completion, a implementation report will be provided to the customer.

Automated Patch Management Annual Subscription Service

Automated Patch Management Service requires a subscription based feed from Emerson that will provide the WSUS metadata feed through the prerequisite Guardian Software Update Delivery Service.

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

Automated Patch Management Project Support

Support for the Automated Patch Management infrastructure including WSUS and SEPM applications can be provided (if needed) through your local Emerson support representative or via a bank of consulting hours which are outside from standard Guardian Support contract. Furthermore, questions related to the day-to-day maintenance and administration of this solution will also be handled out of the bank of hours as the customer will be responsible for these activities.

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.

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 how comprehensive Cybersecurity Management Services address your cybersecurity needs, contact your local Emerson sales office or representative, or visit **www.emersonprocess.com/cybersecurity.**

Emerson Process Management
Asia Pacific: 65.6777.8211
Europe, Middle East: 41.41.768.6111
North America, Latin America:
T 1 (800) 833-8314 or
1 (512) 832-3774
www.emersonprocess.com/cybersecurity

EMERSON
Process Management