

# Local Patch Management Update Service

- Establishes successful and proactive patch management strategy
- Tailored patch management service
- Defined scheduling helps ensure the availability and business continuity of DeltaV DCS



*The Emerson Local Patch Management Update Service is a combination of people, technology and security best practices designed to ensure the availability of DeltaV™ DCS, maintain business continuity and reduce your system administrative activities.*

## Introduction

Every month there are new Microsoft™ security updates, Symantec anti-virus updates and DeltaV™ distributed control system (DCS) system hotfixes that need to be acted upon. Emerson's Local Patch Management Update Service provides an effective delivery 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.

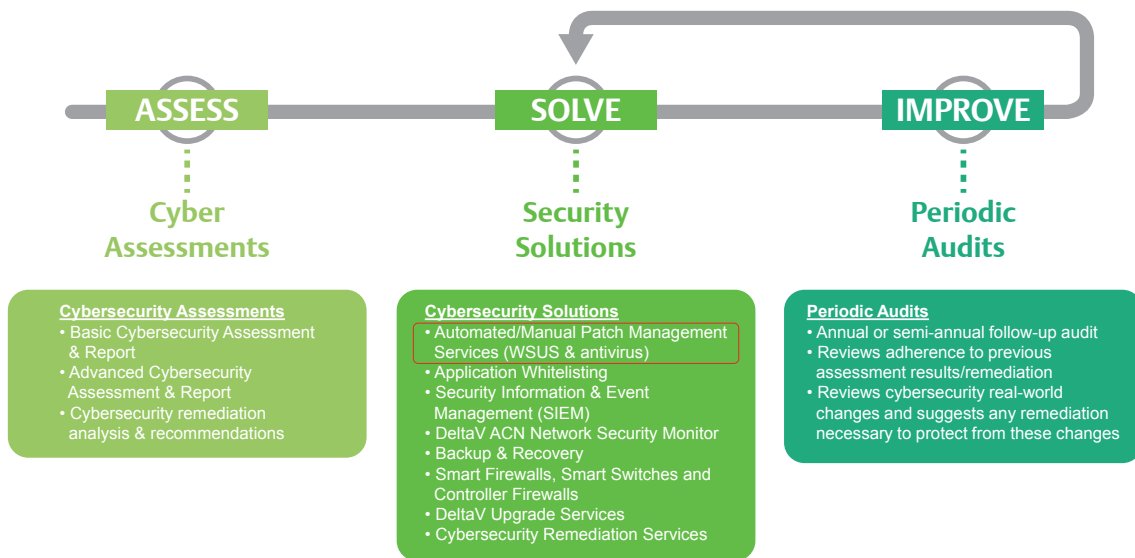
It is very common for the most critical security, anti-virus and application hotfix updates to go uninstalled for extended periods of time, or not be installed at all. Often the reasons are due to limited skilled resources and day-to-day judgment calls about what is more important; to either address 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:** Emerson's Patch Management Update Service delivers the routine aspects of software update deployment for timely dependable implementation, while freeing plant staff to devote more time to your own priorities. For large systems, this time savings can add up to hundreds of hours per year. The Local Patch Management Update Service identifies the appropriate security patches required for DeltaV DCS and schedules updates to the DeltaV DCS hardware in a routine fashion common to your plant's policies and procedures for security patching.

**Tailored patch management service:** Security patch management and hotfixes are essential to your system’s security and availability. this service can be tailored to your site’s work practices and resource-load to ensure these critical updates are deployed consistently.

**Defined scheduling helps 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.



## Local Patch Management Update Tiered Services Suite

Emerson offers a multi-tiered approach to the application of Microsoft™ security patching, Symantec antivirus signature screen updates and DeltaV DCS hotfix installations.

- **Full Manual Service:** Utilizing Emerson certified local service resources, this service provides a scheduled monthly (or quarterly) visit to your site in order to manually deploy the required security patches and antivirus signature screen updates on each DeltaV DCS node requiring these updates. Our service will determine what Emerson-approved patches are required for which network nodes, deploy those patches, install and commission them as appropriate. A Guardian™ Support service contract is not needed for this service.
- **Assisted Manual Service:** Also utilizing Emerson certified local service resources, this service level provides a scheduled monthly (or quarterly) visit to your site in order to deploy the required security patches and antivirus signature screen

updates on each DeltaV DCS node requiring these updates. We will determine what Emerson-approved patches are required for which network nodes, deploy those patches, install and commission them as appropriate. A Guardian Support service contract is not needed for this service.

This service can also include the installation of local server(s) for the automatic downloading of the Microsoft (WSUS) monthly patches and/or the downloading of the Symantec Live Update Administrator (LUA) and monthly upkeep of these server(s). If hardware is required, this can be added at the time on initial service and will be quoted as at additional cost.

This service also includes the manual transfer and downloading of the Emerson-approved Symantec signature screen onto each appropriate network node. Retrieval of the approved Symantec signature screen would come from the on-site Symantec server running the LUA platform. The customer is responsible for the purchase of appropriate licenses from Symantec; however, the Emerson service personnel will deploy these Symantec signature screens.

### ■ **Assisted Manual Service for Guardian Support Customers:**

Also utilizing Emerson certified local service resources, this service level provides a scheduled monthly (or quarterly) visit to your site in order to deploy the required security patches and antivirus signature screen updates on each DeltaV DCS node requiring these updates. We will determine what Emerson-approved patches are required for which network nodes, deploy those patches, install and commission them as appropriate. A Guardian Support service contract is needed for this service. This service deliverable is two-fold: a review of the system's Guardian Dashboard and deployment of necessary OS Security, Symantec antivirus patches and/or DeltaV DCS hotfixes.

This service also includes the manual transfer and downloading of the Emerson-approved Symantec signature screen onto each appropriate network node. Retrieval of the approved Symantec signature screen would come from the on-site Symantec server running the LUA platform. The customer is responsible for the purchase of appropriate licenses from Symantec; however, the Emerson service personnel will deploy these signature screens.

This service can also include the installation of local server(s) for the automatic downloading of the Microsoft (WSUS) monthly patches and/or the downloading of the Symantec Live Update Administrator (LUA) and monthly upkeep of these server(s).

## Local Patch Management Update Services Description

**Full Manual Service:** This Patch Management Update Service is a scheduled site-based service, delivered by your local Emerson service representative and includes the following services:

- Deployment of Appropriate Microsoft Security Updates:
  - Determination of the required "Emerson-approved" Microsoft security patches needed for each device type.
  - Scheduled deployment, installation and commissioning of each identified patch for each node.
  - Emerson will supply required Microsoft patches.
- Deployment of Appropriate Symantec Antivirus Signature Screen Updates:
  - Determination of the Emerson-approved Symantec antivirus signature screen needed for each device type.

- Scheduled deployment of the selected Symantec antivirus signature screens for each device.
- File must be locatable on the customer Symantec server.

**Assisted Manual Service:** This Local Patch Management Update Service is a scheduled site-based service, delivered by your local Emerson service representative and includes the following services:

- Includes services necessary to set-up communications between the Microsoft WSUS website and the Symantec antivirus website.
  - Separate quotation for required server is also available
- Deployment of Appropriate Microsoft Security Updates:
  - Determination of the required "Emerson-approved" Microsoft security patches needed for each device type.
  - Scheduled deployment, installation and commissioning of each identified patch for each node.
  - Emerson will supply required Microsoft patches.
- Deployment of Appropriate Symantec Antivirus Signature Screen Updates:
  - Determination of the Emerson-approved Symantec antivirus signature screen needed for each device type.
  - Scheduled deployment of the selected Symantec antivirus signature screens for each device.
  - File must be locatable on the customer Symantec server.

### **Assisted Manual Service for Guardian Support Customers:**

This Local Patch Management Update Service is a scheduled site-based service, delivered by your local Emerson service representative. Generally, the service is two-fold: a review of the system's Guardian Dashboard status and deployment of necessary OS Security, Symantec antivirus patches and/or DeltaV DCS hotfixes installation.

- The Guardian Support Dashboard Review focuses on several key tiles:
  - **System Profile** - Provides system content information relative to your DeltaV DCS including last update information.
  - **Knowledge Based Articles (KBA's)** – Provides important insight into the update status and requirements of KBAs associated with your DeltaV DCS.

- **Microsoft Update Compatibility** – Provides important MS security update compatibility information about your DeltaV system including last update information.
- **Lifecycle Status** - Provides important lifecycle information by node name and Emerson model number for all DeltaV DCS devices.
- Deployment of Appropriate Security Updates:
  - Determination of the required “Emerson-approved” Microsoft security patches needed for each device type.
  - Scheduled deployment, installation and commissioning of each identified patch.
  - Determination of the required Symantec antivirus signature screens needed for each device type.
  - Scheduled deployment of the “Emerson-approved” Symantec antivirus signature screens for each device.
  - File must be locatable on the customer Symantec server
- Deployment of Appropriate DeltaV DCS Hotfixes:
  - Determination of the uninstalled DeltaV DCS hotfixes needed.
  - Scheduled deployment, installation and commissioning of each identified hotfix.

## Service Prerequisites

**Full Manual** Local Patch Management Update Service prerequisites:

- A license to use Symantec Endpoint Protection Manager and clients (customer’s responsibility) and installed and operational Symantec LUA connection to the Symantec website.
- An Internet accessible server class computer licensed for Microsoft Server 2008 (Upstream Server) to host Symantec application.

**Assisted Manual** Local Patch Management Update Service prerequisites:

- Installed and operational Microsoft WSUS connection to the Microsoft website.

- A license to use Symantec Endpoint Protection Manager and clients (customer’s responsibility) and installed and operational Symantec LUA connection to the Symantec website.
- An Internet accessible server class computer licensed for Microsoft Server 2008 (Upstream Server) to host applications that require Internet access.

### Assisted Manual for Guardian Support Customers

Local Patch Management Update Service prerequisites:

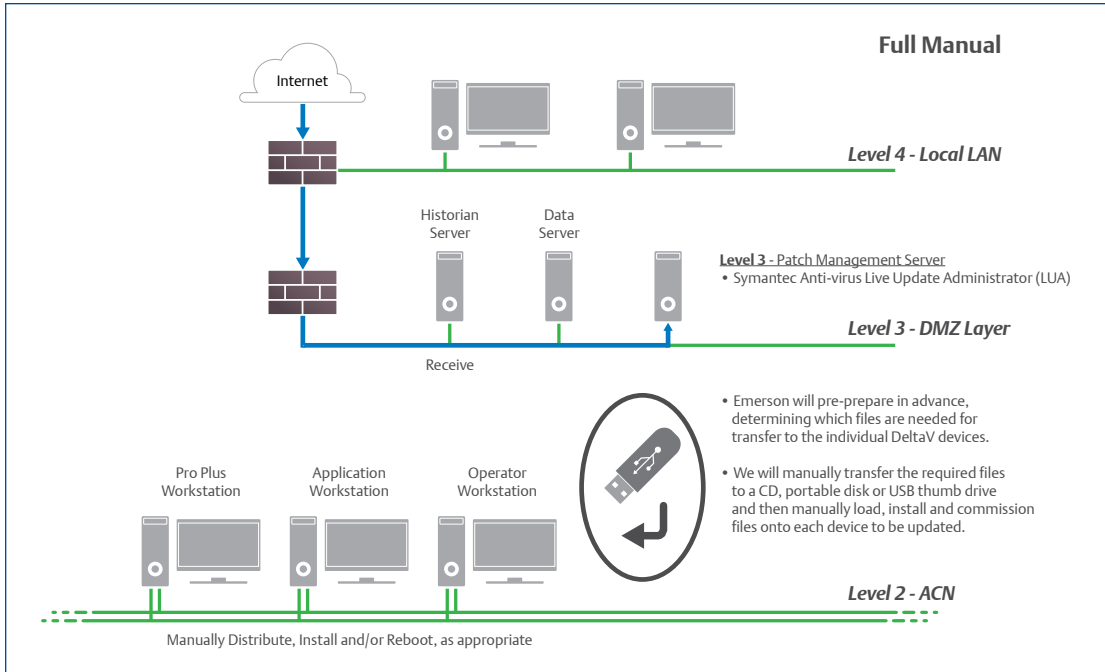
- Installed and operational Microsoft WSUS connection to the Microsoft website.
- Each system ID must be enrolled in Guardian Support Service contract
- A license to use Symantec Endpoint Protection Manager and clients (customer’s responsibility) and installed and operational Symantec LUA connection to the Symantec website.
- An Internet accessible server class computer licensed for Microsoft Server 2008 (Upstream Server) to host applications that require Internet access.

## Local Patch Management Update Service Architecture

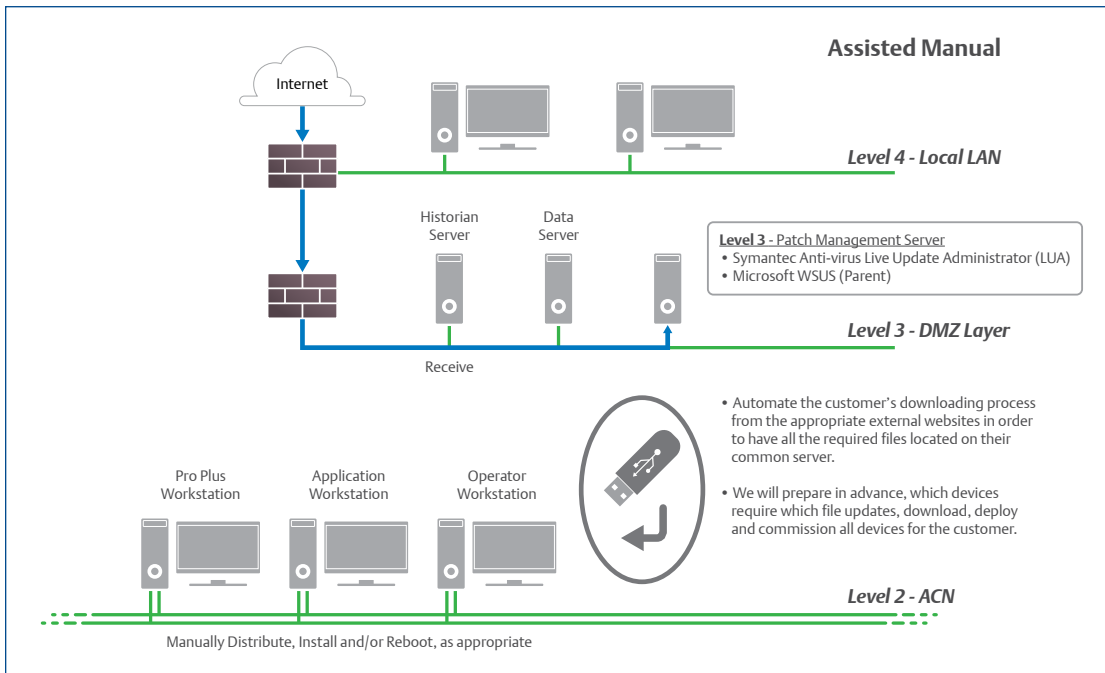
- Software service enablers are combined with Emerson’s expert consultation and optional on-site deployment capability for Microsoft security updates, Symantec anti-virus updates and DeltaV DCS hotfixes.

### The software service enablers may include:

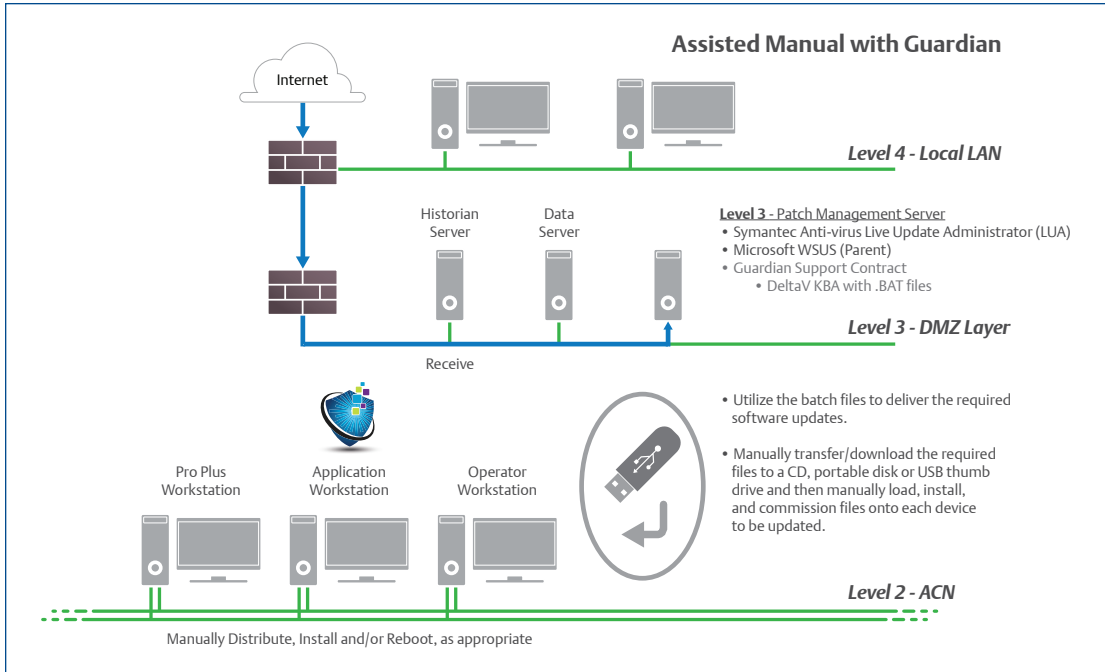
- Microsoft Windows Server Update Service (WSUS) version 3 or higher. — A no-cost add-on to the Microsoft server operating system installed on a customer supplied upstream server.
- Symantec Live Update Administrator (LUA) —a software application that solicits anti-virus updates from Symantec via the Internet, typically located on a customer supplied server.
- 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. (Required only for the Assisted Manual for Guardian Support Customers option.)



Typical Full Manual Local Patch Management Update Service Deployment Architecture.



Typical Assisted Manual Local Patch Management Update Service Deployment Architecture.



Typical Assisted Manual for Guardian Support Local Patch Management Update Service Deployment Architecture.

## Ordering Information

This service requires a current DeltaV DCS Guardian Support Contract covering the System IDs at a given plant site be in place.

Description	Model Number
Local Patch Management Update Service – <b>Full Manual Support</b>	Please Contact Your Local Emerson Sales Office
Local Patch Management Update Service – <b>Assisted Manual Support</b>	Please Contact Your Local Emerson Sales Office
Local Patch Management Update Service – <b>Assisted Manual Support for Guardian Support Customers</b>	Please Contact Your Local Emerson Sales Office

*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](http://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](http://www.emersonprocess.com/cybersecurity)

©2016, Emerson Process Management. All rights reserved.

The Emerson logo is a trademark and service mark of Emerson Electric Company. The DeltaV logo is a mark of one of the Emerson Process Management family of companies. All other marks are the property of their respective owners.

The contents of this publication are presented for informational purposes only, and while every 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 design or specification of such products at any time without notice.

