Blue Coat™ Industrial Control System Protection (ICSP) Support for DeltaV™ Systems

This document describes the use cases and tested environment for using Blue Coat Industrial Control Systems Protection on DeltaV Workstations for secure removable media use.

Table of Contents

Introduction

Misuse of removable media represents an important cyber-threat and this is also true for Industrial Control Systems (ICS). Most of the cybersecurity issues are still initiated from 'inside', and removable media is a component that contributes a lot with this statistic.

The Blue Coat ICSP is a third party solution that has been tested with the DeltaV system and is available from the solution provider at https://bto.bluecoat.com/ or through their sales channels at insidesales@bluecoat.com.

The Blue Coat ICSP solution is compatible with DeltaV systems version 13.3.1 and higher.

Emerson recommends that USB ports and CD/DVD drives are disabled, which still remains the best practice for the hardening of DeltaV workstations and servers. However, if you require to use removable media, then the Blue Coat Industrial Control System Protection (ICSP) is an available secure option to use removable media without completely exposing the endpoints to malware within the DeltaV Area Control Network (ACN).

The Blue Coat ICSP solution was tested for compatibility with DeltaV systems as an alternative for users who need to use removable media while enforcing media usage requirements.

Blue Coat ICS Protection Solution Overview

The Blue Coat ICSP is comprised of three basic components:

- **Blue Coat Scanner Station** is a physical appliance used to scan the removable media prior to be used on workstations running the Blue Coat ICSP Agent.
- **Blue Coat ICSP Agent** is a software application that validates if the removable media was pre-scanned (and deemed clean) by the Blue Coat Scanner Station.
- **Blue Coat Malware Cleaner** is used as a resource to clean malware found on removable media scanned by the Blue Coat Scanner Station (optional).

Figure 1 — *Blue Coat ICSP components.*

The Scanner Station is required to be frequently updated to make sure the latest anti-malware signatures are installed, and this activity can be done offline (updates are loaded via USB) or online (when the station is connected to a network with internet access). The Scanner Station is also responsible for the Agent installation files creation which is loaded into a removable media to then be installed in each DeltaV workstation/server where the Blue Coat ICS Protection will be running. There is also an option to create a malware extraction tool to help scanning and cleaning files if needed – Emerson recommends the use of supported antivirus software on DeltaV workstations and servers such as: Endpoint Security for DeltaV Systems (powered by Intel McAfee) or Symantec Endpoint Protection.

Once the Agent installation files are loaded into the removable media, they can be installed manually in each workstation, and once installed only scanned removable media without malware will be allowed to run on those workstations where the Blue Coat ICSP Agent was installed. In order to uninstall the Agent, the installer executable will need to be available on the removable media and executed again (uninstall option) – the Agent is not listed within Microsoft Windows Program and Features list for security reasons.

The Blue Coat Scanner Station can be remotely accessed to provide additional settings on how the removable media will be protected by the Blue Coat ICSP. The settings can be accessed via a web interface served by the Scanner Station itself. The Scanner Station should not be connected directly to the DeltaV ACN, but instead it should be connected beyond the DeltaV system perimeter protection, if the online option is chosen. Figure 2 illustrates the Blue Coat Scanner Station connected to the DMZ network as an example.

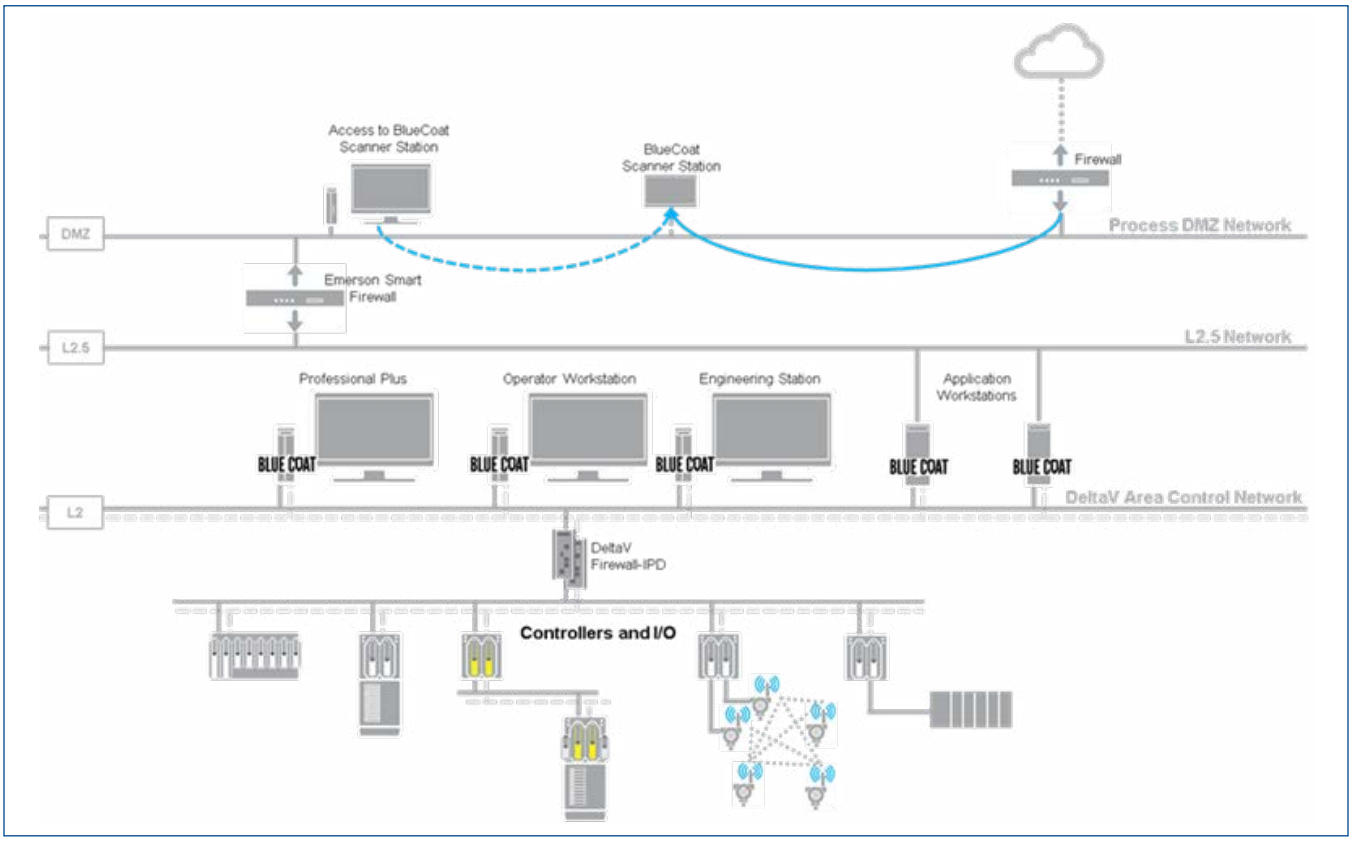

Figure 2 — *Reference Architecture showing the Blue Coat ICSP within DeltaV systems.*

Blue Coat ICS Protection and Supported DeltaV Scenarios

Once deployed Blue Coat will protect each DeltaV workstation by only allowing removable media to be accessed if previously verified by the Scanner Station. With that in mind, the following use cases can be considered as a way to further explain how the protection is implemented as part of the Blue Coat ICSP deployment:

a. The removable media is first checked by the Scanner Station and no malware is identified. In this case the removable media can be fully accessed by the DeltaV Workstation once it is connected to the workstation's USB port including all files, folder and subfolders. Files can be freely changed and accessed by the DeltaV Workstation where the removable media is still connected to, but changed content will not be accessible by other DeltaV Workstations running the Blue Coat ICSP Agent without re-scanning at the Blue Coat Scanner Station.

Figure 3 — *Scanning a removable media prior to connecting it to the DeltaV workstation running the Blue Coat ICSP agent.*

b. If the removable media content is changed, the removable media will need to be re-scanned in order to allow the changed content to be accessible by other DeltaV Workstations running the Blue Coat ICSP Agent. In case the removable media is not re-scanned, only the unchanged and scanned content will be accessible – all changed or new files/folders will not be accessible by other DeltaV Workstation.

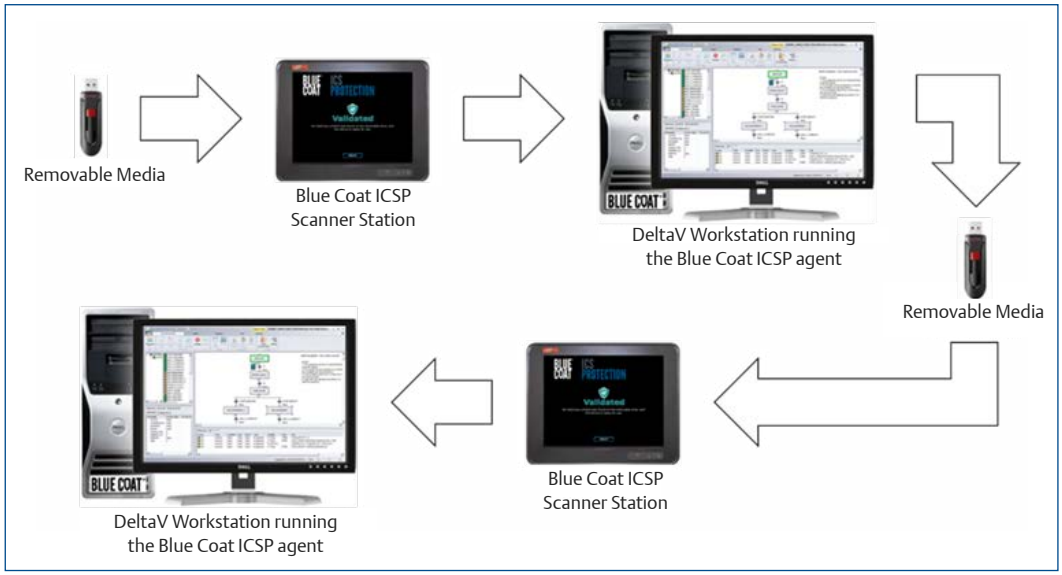

Figure 4 — *Re-scanning a removable media with changed content prior to connecting it to another DeltaV workstation also running the Blue Coat ICSP agent*

c. Same behavior described on (b) above applies in case removable media content is changed by any computer other than DeltaV workstations and servers. Previously scanned removable media are freely accessible on computers that are not running the Blue Coat ICSP agent.

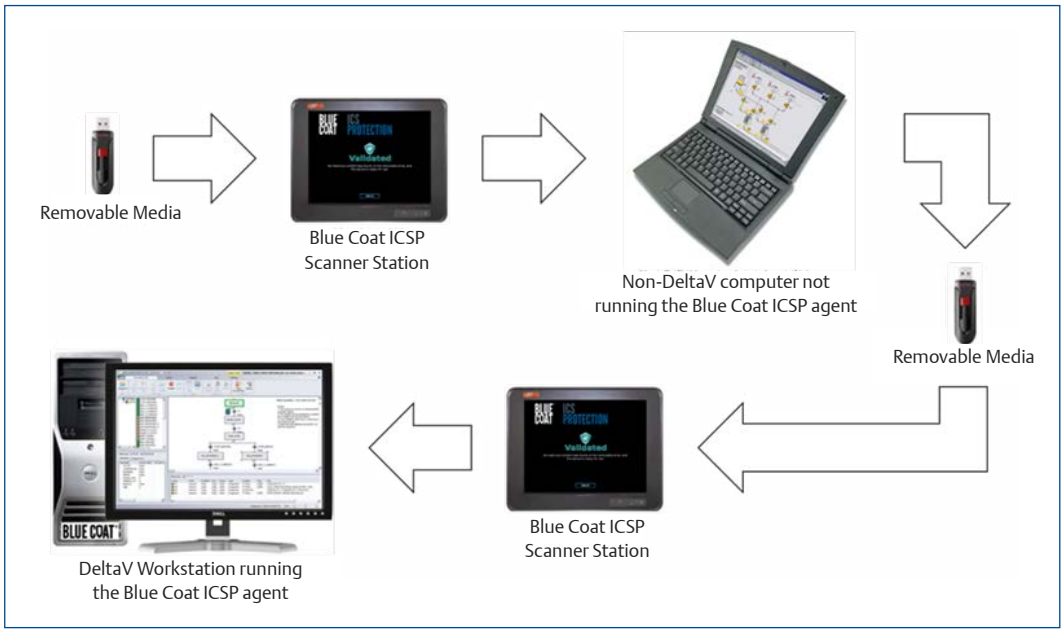

Figure 5 — *Re-scanning a removable media with content changed by a non-DeltaV workstation prior to connecting it to a DeltaV workstation running the Blue Coat ICSP agent.*

d. A removable media with changed content can be re-scanned multiple times and if deemed 'validated' (malware free) will be fully accessible by any DeltaV Workstation running the Blue Coat ICSP agent.

e. Whenever a malware is identified during a scan, the whole removable media unit will be flagged 'infected' and will not be allowed to even connect to a DeltaV Workstation – access is denied in this case. The removable media will need to be cleaned using any preferred malware cleaning application (including Blue Coat's malware cleaner), re-scanned, and deemed 'validated' (malware free) to be accessible again on DeltaV Workstations.

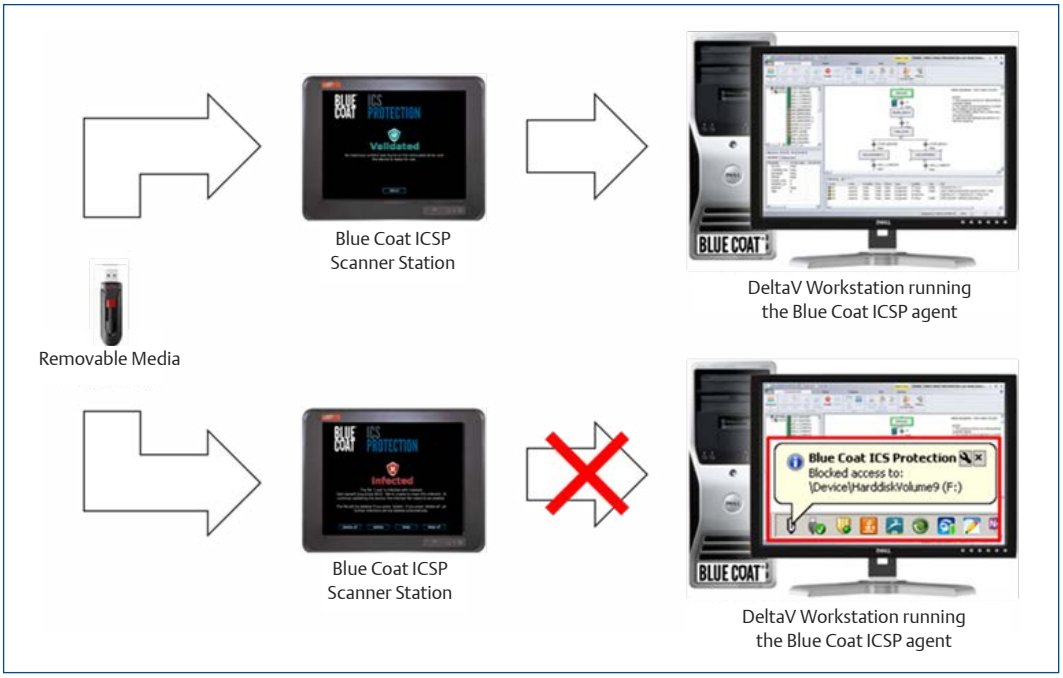

Figure 6 — *Different agent actions for 'validated' and 'infected' removable media scenarios.*

During setup phase, the Scanner Station can be configured to also set an expiration time for the scan duration. By default, no expiration is set therefore the scan is valid until content is changed. If expiration is set, even if the content has not changed the validity of the scan will be also based on time since last scan.

System Compatibility

Blue Coat ICSP is a DeltaV complementary product. In this product designation we will continue to test the agent with future versions of DeltaV so it remains supported as new DeltaV versions are released. Testing would be done using the latest version of the Blue Coat ICSP agent at the time of the DeltaV version testing. Tested versions and their supported status are documented as part of every DeltaV Release Notes within Emerson's Guardian Support Knowledge Base.

During the life of a DeltaV version we expect the users to only install the version of agent that is tested with that version or versions of DeltaV. If the agent is updated or revised during the life of the DeltaV version, installed any testing of the new agent for support of installed DeltaV systems is at the discretion of Emerson.

The Blue Coat ICSP is supported on DeltaV v13.3.1 and higher.

Blue Coat ICSP Agent Installation

The installation and setup of the agent is accomplished using the standard documentation provided by Blue Coat. No special DeltaV related installation or setup activities are required. Please refer to the Blue Coat ICSP user guide available at **https://bto.bluecoat.com/** for additional information.

Blue Coat ICSP Scanner Station Update Process

Similar to any anti-malware application, the Blue Coat ICSP Scanner Station shall be kept up to date based on the updaters provided by Blue Coat. The update process can be done offline or online:

- The offline process requires a computer to be connected to the Blue Coat server which will validate the user's license key and provide the updater files to be loaded on a removable media that will be used to update the Scanner Station.
- The online process requires that the Scanner Station is connected to the Blue Coat server to download the updater files when requested by the user.

Please refer to the Blue Coat ICSP user and admin guides at **https://bto.bluecoat.com/** for additional information.

Test Results

In order to validate support for the Blue Coat ICSP use on DeltaV Workstations, an initial setup has been considered to allow multiple use cases to be tested including, but not limited to, the following tasks:

- Blue Coat Scanner Station online and offline updating processes
- Blue Coat ICSP agent installation on all tested DeltaV Workstations
- Network setup to allow multiple scenarios testing
- Preparation of multiple types of removable media (scanned, not scanned, etc.)

The following test cases were validated with DeltaV:

- Localization: DeltaV system languages (English, French, Japanese and Russian)
- Scope of testing: DeltaV physical workstations, thin client stations, DeltaV virtual machines and mobile devices for the Wireless Mobile Workforce solution (Panasonic Toughbooks and Toughpads)
- USB ports: USB 2.0, USB 3.0, USB shared over Microsoft Remote Desktop Services, USB/IP port converter
- Devices not affected by the Blue Coat ICSP (non-storage USB devices): keyboard, mouse, touchscreen devices, external CD/DVD drive, smart card readers, DeltaV license dongle
- Use cases:
    1. Setup – offline updates
    2. Setup – online updates
    3. Setup – agent installation
    4. Copying files – DeltaV endpoint to non-protected workstation
    5. Copying files – Non-protected workstation to DeltaV endpoint
    6. Copying files – Infected file to DeltaV endpoint
    7. Copying files – DeltaV endpoint to non-protected workstation via smartphone
    8. Scanned files for DeltaV – USB access (all DeltaV files)

Identified Issues and Limitations

There were issues identified when tests were performed with the Blue Coat ICSP solution for DeltaV systems as highlighted below:

- Blue Coat Malware Protection is not supported on DeltaV Workstations/Servers. Emerson provides Endpoint Security for DeltaV systems (powered by Intel McAfee), or as an alternative the Symantec Endpoint Protection has been tested with DeltaV systems.
- If Blue Coat ICSP is used, Emerson recommends that only removable media is allowed to connect to the DeltaV workstations. This is preferably set up via Windows Group Policies and detailed instructions are available in the Guardian Support Knowledge Base (KBA# NK-1600-0336).
- Blue Coat ICSP is only supported on DeltaV system v13.3.1 and higher. Tests were successfully performed on all DeltaV supported operating systems, however Blue Coat has not yet officially released support for their solution running on Windows 10 / Windows Server 2016.
- The Blue Coat Scanner Station is unable to scan removable media with 1TB available storage space containing 300GB data or more. This issue is being evaluated by Blue Coat.
- Media Transfer Protocol (MTP) is not supported by the Blue Coat ICSP solution. Latest smartphones can connect to newer workstations via this protocol, hence bypassing the Blue Coat ICSP protection. If the Blue Coat ICSP solution is used, Emerson recommends that portable devices (MTP specific) are denied via Windows Group Policies and detailed instructions are available in Emerson's Guardian Support Knowledge Base (KBA# NK-1600-0336).

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 Attacks. 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.

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/deltav

DELTAV™

EMERSON™