Application Whitelisting for DeltaV™ Systems

- Decrease risk with protection against zero-day malware
- Reduce time consuming patching cycles
- Automatically accept approved software
- Centralize cybersecurity management with McAfee® ePolicy Orchestrator

Application Whitelisting for DeltaV™ Systems allows for whitelisting applications as an integral part of the threat defense lifecycle.

Introduction

Application Whitelisting for DeltaV™ Systems software provides complete protection from unwanted applications and code — blocking advanced threats without requiring signature updates. It lets you consistently enable the known good, block the known and unknown bad, and properly administer new software. The dynamic whitelisting trust model reduces costs by eliminating expensive manual support requirements associated with other whitelisting technologies.

Application Whitelisting for DeltaV Systems, when properly installed on DeltaV workstations and servers, prohibits new software (i.e. malware) from executing on any node if that software has not been pre-approved for use with that station/server. Simply put, “zero-day” malware (i.e. malware not yet detectable by antivirus screener software) is prohibited from executing. Change Control software protects registry keys and important files from un-approved editing. A sophisticated attacker with onsite or remote access to your system (even with Whitelisting installed) could cause DOS or file corruption without this additional layer of protection.

Benefits

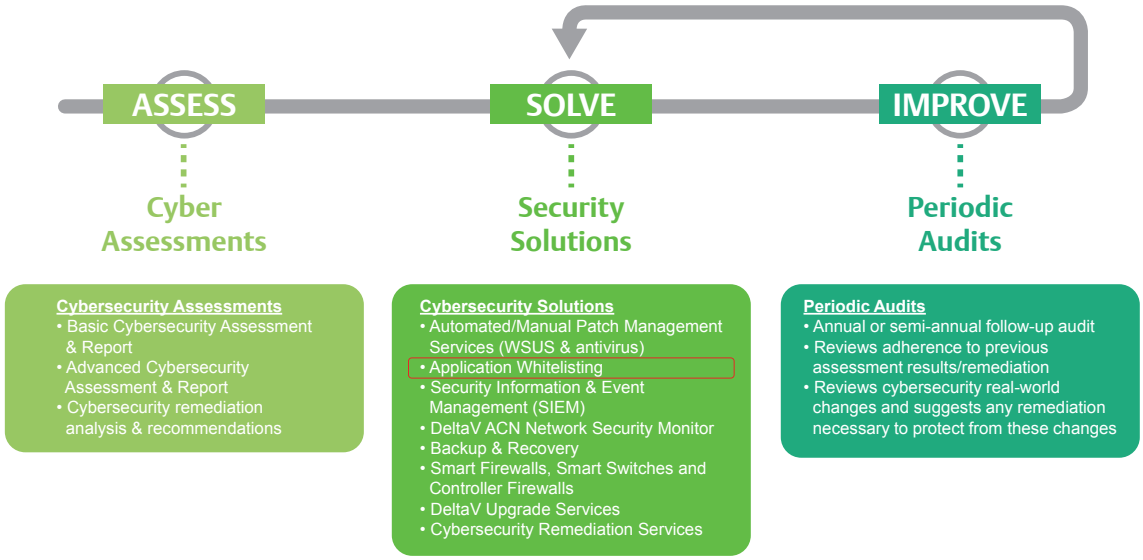
Decrease risk with protection against zero-day malware: Zero-day malware is a security threat to traditional antivirus (blacklisting) software because of the inherent delay between discovery and patching.

Whitelisting software takes the opposite approach to blacklisting, by automatically denying applications without prior authorization. Reduce risk from unauthorized applications and code by deploying whitelisting software for your control system endpoints.

Reduce time consuming patching cycles: Traditional antivirus products require regular patching to maintain security against newly discovered exploits. Whitelisting allows you to have endpoint protection without the need for constant patching.

Automatically accept approved software: Dynamic whitelisting allows trusted channels to automatically execute applications. A dynamic trust model eliminates the labor-intensive list management, and requires negligible cpu and memory usage.

This provides essential endpoint security while saving time and lowering ownership cost.



Centralize cybersecurity management with McAfee® ePolicy Orchestrator: True centralized management with a single local console offers greater visibility, simplifies operations, boosts IT productivity, unifies security, and reduces costs.

Inform security operations and empower actions with customizable notifications, while also educating desktop users about disallowed applications with informative pop-up messages.

As a result, you save time and money—with a more effective security program.

Service Description

Application Whitelisting for DeltaV Systems is a centrally-managed whitelisting solution that blocks unauthorized executables on DeltaV servers and workstations. It consists of several key products:

- **McAfee Agents**
  An agent downloads and enforces policies, and executes client-side tasks such as deployment and updating. The Agent also uploads events and provides additional data regarding each system's status and must be installed on each system node in your network that you wish to manage.
- **Application Control**
  Application Control software continuously protects systems from unknown, advanced persistent threats using centrally managed whitelisting software without manual monitoring. This solution uses a dynamic trust model and innovative security features that thwart advanced persistent threats — without requiring signature updates or labor-intensive list management typical of endpoint solutions.
- **Change Control (File Integrity)**
  Change Control software protects registry keys and important files from un-approved editing. A sophisticated attacker with onsite or remote access to your system (even with Whitelisting installed) could cause DOS or file corruption without this additional layer of protection.
- **McAfee ePolicy Orchestrator (McAfee ePO™)**
  McAfee ePO software provides flexible, automated management capabilities so you identify, manage, and respond to security issues and threats without compromising active process controls.
- **Emerson Support Service**
  Support service supplied through Emerson's Global Support Center (GSC). An annual license and service contract renewal is a part of the continued service.

What is McAfee ePolicy Orchestrator (McAfee ePO)?

McAfee ePO is a true centralized management platform with a single local console offering greater visibility, simplified operations, boosting IT productivity, unifying security operations for process control, and reducing overall cybersecurity costs. McAfee ePO provides a unified view of your security posture with drag-and-drop dashboards that provide security intelligence across endpoints and networks.

McAfee ePO simplifies security operations with streamlined workflows for proven efficiencies.

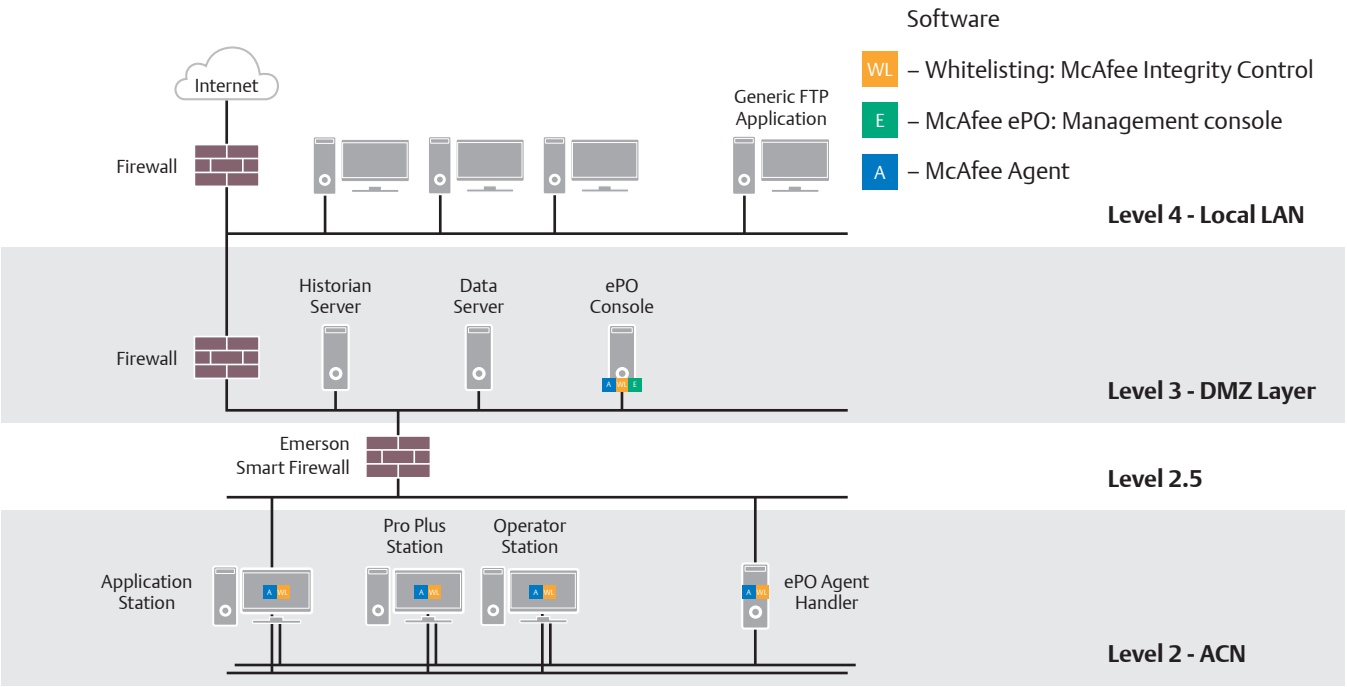
You define how McAfee ePO software should direct alerts and security responses based on the type and criticality of security events in your environment, as well as create automated workflows between your security and IT operations systems to quickly remediate outstanding issues. As a result, you save time and money — with a more effective cybersecurity program.

McAfee ePO shortens the time from insight to response through actionable dashboards with advanced queries and reports.

Finally, McAfee ePO allows IT personnel to observe/verify cybersecurity elements located on the control system without requiring assistance from operations personnel.

DeltaV System Compatibility

The deployment of Application Whitelisting for DeltaV Systems is compatible with 64-bit DeltaV versions v12.3.1 and above.



Example reference architecture for Application Whitelisting for DeltaV Systems on a typical DeltaV network.

Ordering Information

Description	Model Number
Application Whitelisting for DeltaV Systems	
Application Whitelisting for DeltaV Systems (1st-Year License/Subscription Service*)	
For **Workstations and Servers** with an active Guardian Support Contract	VE9127WY
For **Workstations and Servers** without an active Guardian Support Contract	VE9127WN
Application Whitelisting for DeltaV Systems (Annual License/Subscription Service Renewal)	
Application Whitelisting for DeltaV Systems Annual License/Subscription Service Renewal	
For **Workstations and Servers** with an active Guardian Support Contract	VE9127WY-RENEW
For **Workstations and Servers** without an active Guardian Support Contract	VE9127WN-RENEW

Related Products

- Endpoint Security for DeltaV Systems. This Emerson solution includes McAfee Endpoint Security software configured to work specifically for DeltaV out-of-the-box. This solution, when properly installed on DeltaV workstations and servers, detects and quarantines known malware using signature updates.

Not Supported Products

- Non-Emerson supplied McAfee Integrity Control Management software versions (i.e. Non-DeltaV versions) are not supported by Emerson Process Management.
- The Application Whitelisting for DeltaV Systems cannot be used in conjunction with Symantec™ antivirus solutions.
- This product cannot be used with 32-bit DeltaV versions.

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.emerson.com/whitelisting.**

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™