Endpoint Security for DeltaV™ Systems

- Decrease risk with intelligent, adaptive scanning
- Utilize advanced anti-malware protection
- Identify, remediate and secure your DeltaV™ system from cybersecurity risks through actionable threat forensics
- Centralize cybersecurity management with optional Trellix® ePolicy Orchestrator
- Open, extensible endpoint security framework

Endpoint Security for DeltaV™ Systems allows for ease in responding to and managing of the threat defense lifecycle.

Introduction

Endpoint Security for DeltaV™ Systems software utilizes elements of the Trellix Endpoint Protection Suite of products to provide endpoint protection (antivirus protection) for key DeltaV system components.

Endpoint Security for DeltaV Systems integrates core functions such as essential security to block advanced malware, control data loss and compliance risks caused by removable media into a single, manageable environment ideal for safeguarding traditional desktops and other systems that have limited exposure to Internet threats.

With the Managed Version, you can correlate threats, attacks, and events from the endpoint, network, data security as well as compliance audits to improve the relevance and efficiency of security efforts and compliance reports a single integrated management platform across all these security domains. Accelerated time to protection, improved performance, and effective management empower security teams to resolve more threats faster with fewer resources.

Two different versions of Endpoint Security for DeltaV Systems may be ordered: Managed or Unmanaged. The Managed Version includes the ePolicy Orchestrator (ePO). We also offer this solution in the Unmanaged Version, which does not include the ePO and is targeted for smaller DeltaV systems. Please read on for more details on both options.

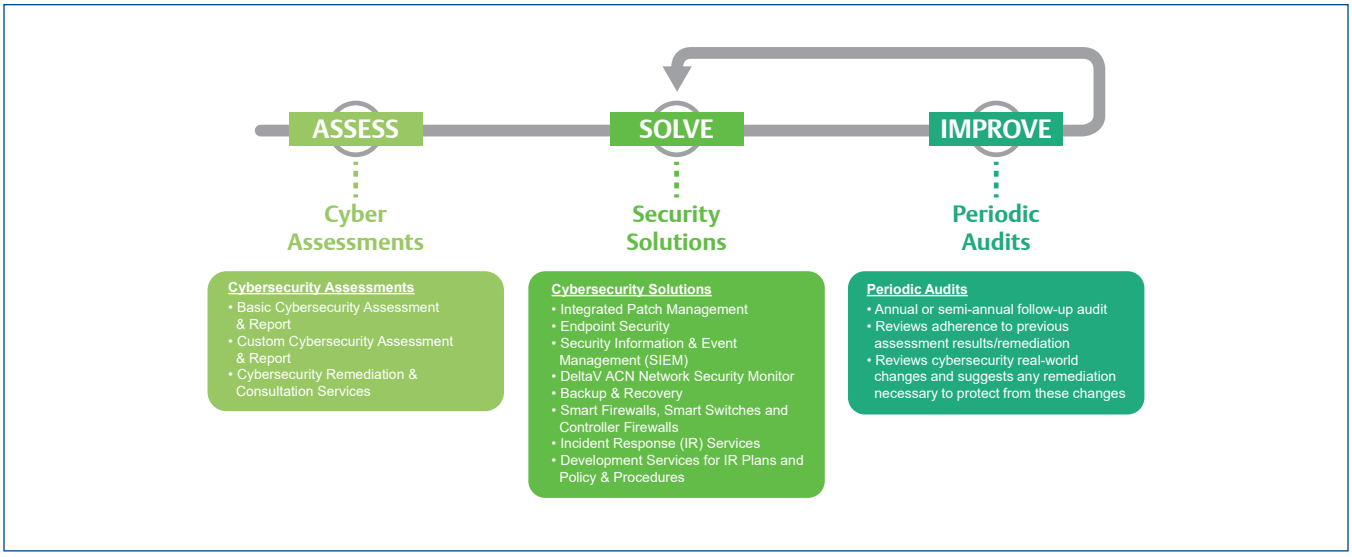
Benefits

Decrease risk with intelligent, adaptive scanning: Improves performance and productivity by bypassing scanning of trusted processes and prioritizing suspicious processes and applications. Adaptive behavioral scanning monitors, targets, and escalates as warranted by suspicious activity.

Utilize advanced anti-malware protection: Protects, detects, and corrects malware fast with a new anti-malware engine that is efficient across multiple devices and operating systems.

Identify, remediate and secure your DeltaV system from cybersecurity risks through actionable threat forensics: With the Managed Version, administrators can quickly see where infections are, why they are occurring, and the length of exposure to understand the threat and react more quickly.

Centralize cybersecurity management with Trellix® (ePO): True centralized management with a single local console offers greater visibility, simplifies operations, boosts IT productivity, unifies security, and reduces costs. As a result, you save time and money—with a more effective security program.



Open, extensible endpoint security framework: Integrated architecture allows endpoint defenses to collaborate and communicate for a stronger defense. Results in lower operational costs by eliminating redundancies and optimizing processes. Trellix Endpoint Security for DeltaV Systems seamlessly integrates with other Trellix and third-party products to reduce protection gaps.

Solution Description

What does Endpoint Security for DeltaV Systems provide?

Figure 2 illustrates the process by which Endpoint Security for DeltaV Systems handles the introduction of new executables and how it protects your DeltaV workstations and servers. Once files have been downloaded to a workstation or server, these files are published to the antivirus software resident on the agent. The software scans the new file and determines whether it is a malicious file or not. Malicious files are deleted and action logged while “clean” files are available for use.

Service Description

Agent-based policy auditing scans your endpoints to ensure that all policies are up to date. Organizations can measure compliance to best practice policies as well as to key industry regulations.

- Configuration is driven through the optional Trellix ePO management console.
- Trellix ePO provides visibility through dashboards and reports.
- Trellix Unmanaged Version will still have the Trellix agent but each endpoint’s policy is individually enforced directly at the endpoint.

Endpoint Security for DeltaV Systems includes the following elements:

- **Endpoint Security Software**
  - Enables customers to respond to and manage the threat defense lifecycle of protected devices.
  - Proves for the automated downloading of approved signature files to DeltaV workstations and servers based on your site’s update policies.
- **Trellix ePO Software (included with Managed Version only)**
  - Trellix ePO software provides flexible, automated management capabilities so you identify, manage, and respond to security issues and threats without compromising active process controls.
- **Trellix 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.
- **Emerson Support Service through Guardian Support Service**
  - Support service is supplied through Emerson’s Global Support Center (GSC).
  - Delivers a monthly Emerson-tested and approved signature file for use with DeltaV systems.
  - Delivers all software/updates and complete support for the Emerson delivered Endpoint Security for DeltaV Systems.

What is Trellix ePolicy Orchestrator (Trellix ePO)?

Trellix ePO Managed Version 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. Trellix ePO provides a unified view of your security posture with drag-and-drop dashboards that provide security intelligence across endpoints and networks.

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

You define how Trellix 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 IT/security and process operations systems to quickly remediate outstanding issues. As a result, you save time and money — with a more effective cybersecurity program.

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

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

Just as secure as the solution described above you may now order that same protection and security without the (ePO). When deploying Endpoint Security for DeltaV Unmanaged at site you still benefit from the same industry leading defense but with a smaller footprint. The Trellix Unmanaged option is targeted for the smaller DeltaV systems and won't need the separate server class machines required for the ePO and Agent Handler.

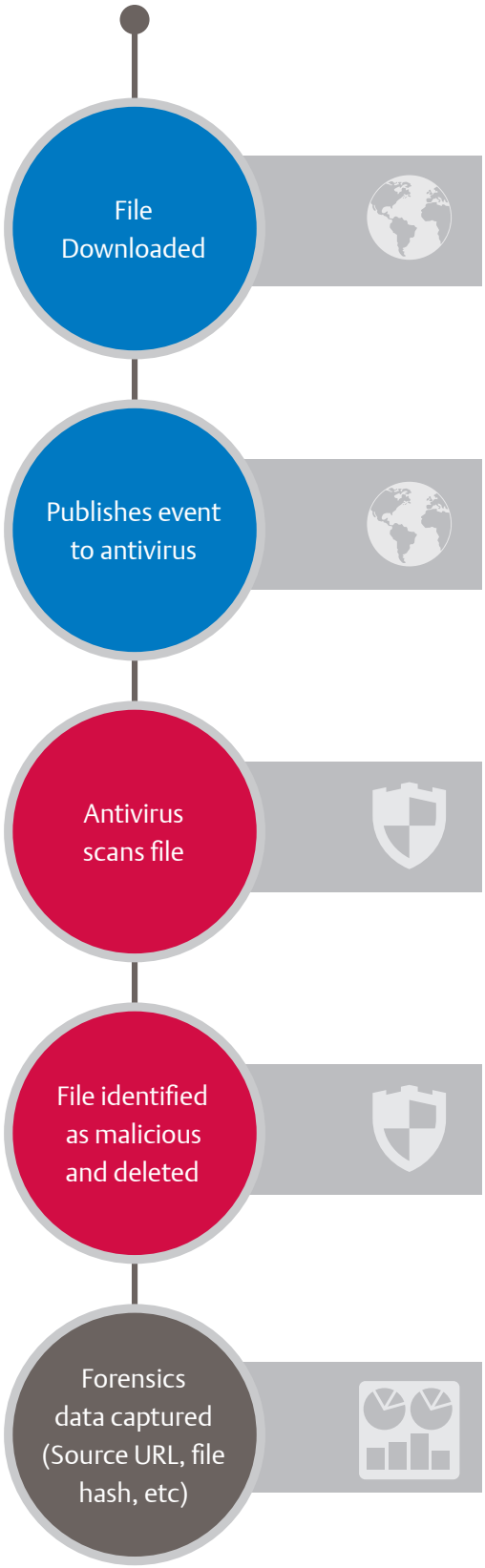
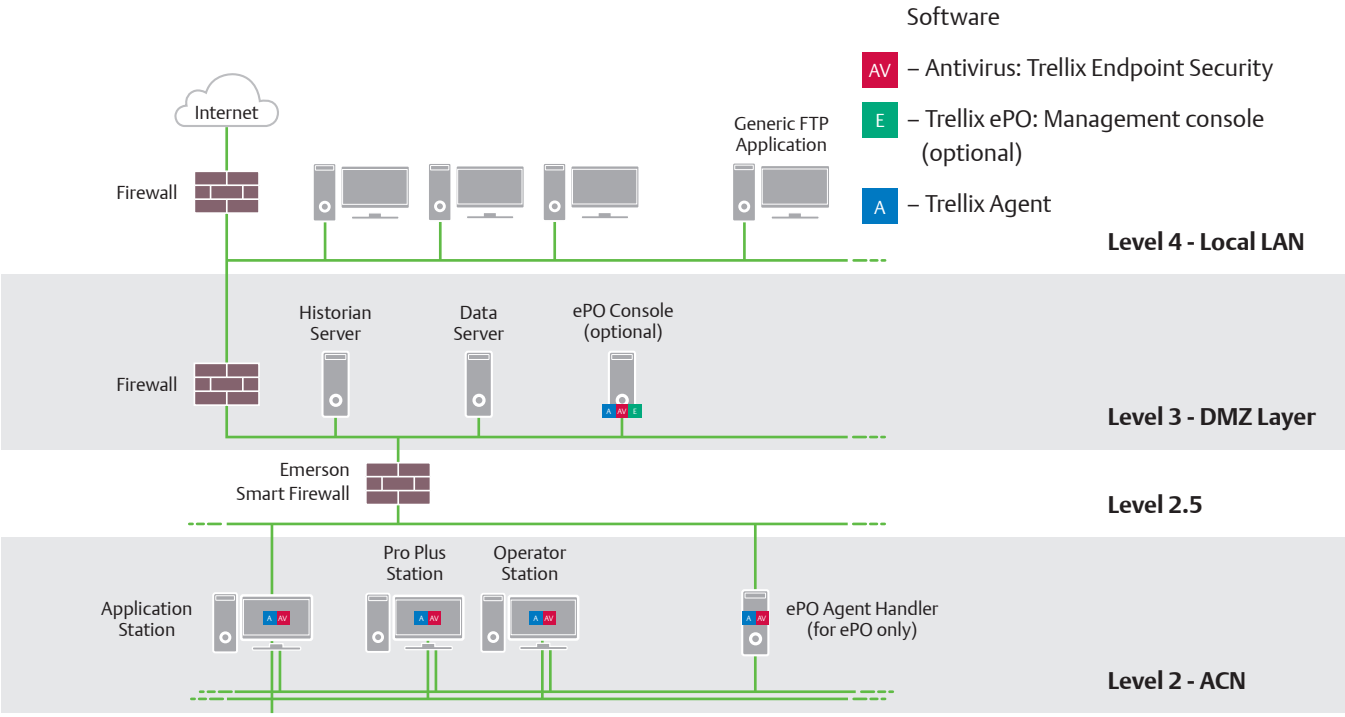


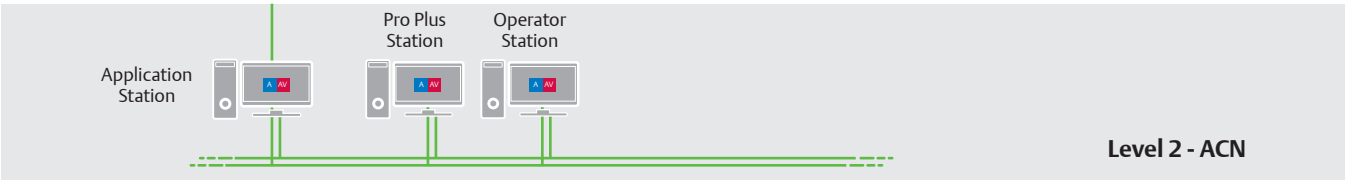
Figure 2. *How Trellix Endpoint Security 10 handles malicious file downloads from the Internet.*

DeltaV System Compatibility

The deployment of Endpoint Security for DeltaV Systems software is compatible with the currently supported DeltaV releases. Please consult the Complementary Products List for full details.



Example reference architecture for Endpoint Management for Managed DeltaV Systems on a typical DeltaV system.



Example reference architecture for Endpoint Management for Unmanaged DeltaV Systems on a typical DeltaV system.

Ordering Information

Description	Model Number
Endpoint Security Management Service for DeltaV Systems	
Endpoint Security Management Service for DeltaV Systems (1st-Year License/Subscription Service*)	
For Workstations and Servers with an active Guardian Support Contract	VE9126WY
For Workstations and Servers without an active Guardian Support Contract	VE9126WN
For Workstations and Servers Unmanaged with an active Guardian Support Contract	VE9126WYUM
For Workstations and Servers Unmanaged without an active Guardian Support Contract	VE9126WNUM
Endpoint Security Management Service for DeltaV Systems Media Pack	
Endpoint Security for DeltaV Systems, Media Pack Only**	VE9126M
Endpoint Security Unmanaged for DeltaV Systems, Media Pack Only**	VE9126UM
Endpoint Security Management Service for DeltaV Systems Annual License/ Subscription Service Renewal	
For Workstations and Servers with an active Guardian Support Contract	VE9126WY-RENEW
For Workstations and Servers without an active Guardian Support Contract	VE9126WN-RENEW
For Workstations and Servers Unmanaged with an active Guardian Support Contract	VE9126WYUM-RENEW
For Workstations and Servers Unmanaged without an active Guardian Support Contract	VE9126WNUM-RENEW

**1st-Year subscription service pricing cannot be pro-rated. Any pro-rating will be done in the renewal year.*

***1 media pack is required per site.*

Related Products

Application Whitelisting for DeltaV Systems - This Emerson solution includes Trellix Application Whitelisting software configured to work specifically with DeltaV out-of-the-box. This solution, when properly installed on DeltaV workstations and servers, blocks unauthorized executables on servers, corporate desktops, and fixed-function devices.

Products Not Supported

- Non-Emerson supplied Trellix Endpoint Security versions (i.e. Non-DeltaV versions) are not supported by Emerson.
- This product cannot be used in conjunction with Symantec™ Endpoint Protection antivirus solutions.
- This product cannot be used with 32-bit DeltaV versions.

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

Contact Us
www.emerson.com/contactus

DeltaV™

EMERSON™