Network Security Monitor (NSM) for DeltaV™ Systems

- Detect advanced threats
- Increase security awareness
- Accelerate response time
- Maintain uncompromised availability

Network monitoring provides continuous advanced threat detection capability.

Introduction

Your control system network is used to direct critical infrastructure, transmit confidential recipes and produce valuable products. To protect this network, best practices have traditionally prescribed a layered architecture and prevented visibility into the network. But advanced targeted attacks are on the rise, and perimeter security measures may not be enough. Traditional firewalls and intrusion prevention systems (IPS) struggle to detect application-layer threats, hidden payloads and lateral movements.

Continuous network monitoring solves these challenges by shifting the perspective inwards. Rather than covering your external perimeter attack surface, continuous network monitoring helps identify advanced threats within your control system layer. Traditional firewalls and IPS have only one chance to block an advanced threat. But network monitoring provides continuous advanced threat detection capability.

Most network monitoring solutions detect anomalies based on network flows; however, Network Security Monitor for DeltaV™ Systems looks deeper into network behavior. This means you can fully inspect application contents to detect malicious, covert traffic, such as an executable embedded inside a PDF document.

Network Security Monitor for DeltaV Systems addresses your increasing cybersecurity challenges:

- Achieving visibility into your network behavior
- Discovering advanced threats
- Maintaining system availability

Network Security Monitor for DeltaV Systems works in concert with your Security Information and Event Management (SIEM) for DeltaV Systems, allowing you to correlate network traffic with events. The combined solution will move your detection capabilities beyond the limits of log and event management.

With this solution you can:

- Improve your defensive posture
- Reduce dwell time of advanced threats
- Mitigate risk and minimize potential loss
- Enable compliance with emerging standards

Benefits

Detect Advanced Threats: Detect advanced threats by discovering anomalies within protocols, applications and file transfers. Application-layer inspection detects anomalies by decoding application sessions to Layer 7. This technology improves anomaly detection by looking beyond network flows. Network flows will only discover anomalies when floods and big data leaks occur.

Increase Security Awareness: Network Security Monitor for DeltaV Systems can provide you with the most relevant network behavior from the DeltaV Area Control Network (ACN). Emerson's available comprehensive set of rules, alerts and dashboards can help you analyze network traffic on the control system layer.

Achieve the deepest level of real-time visibility into your network usage.

Accelerate Response Time: Network monitoring provides the granular visibility you need to discover attacks before it's too late. Real-time alerting enables a proactive response from your security team. Reduce the time for attackers to plan, move laterally, and extract data by discovering and responding to attacks more quickly.

Maintain Uncompromised Availability: Each of your DeltaV Smart Switches can be enabled for port mirroring, which copies the packet transmissions for the appliance to monitor network traffic passively. This avoids application interference and ensures there is no compromise to your DeltaV system availability and performance.

Service Description

Architectural Consultation: Because every customer has their own network architecture, the service begins with a network architecture consultation to ensure the best overall deployment for your organization. Emerson best practices ensure your network is both secure and compatible with the Network Security Monitor for DeltaV Systems.

Installation Services: On-site installation service is provided to ensure the appliance is configured properly to collect network traffic from the DeltaV Smart Switches.

Customization: Emerson's certified specialists can optionally assist with customizing rules, alerts, dashboards, and automated report generation depending on your security policies and compliance requirements.

Training Services: Network Security Monitor for DeltaV Systems puts you in the driver seat to monitor the DeltaV Area Control Network. Emerson certified specialists can train your local engineer or IT personnel to monitor the appliance and understand the alerts.

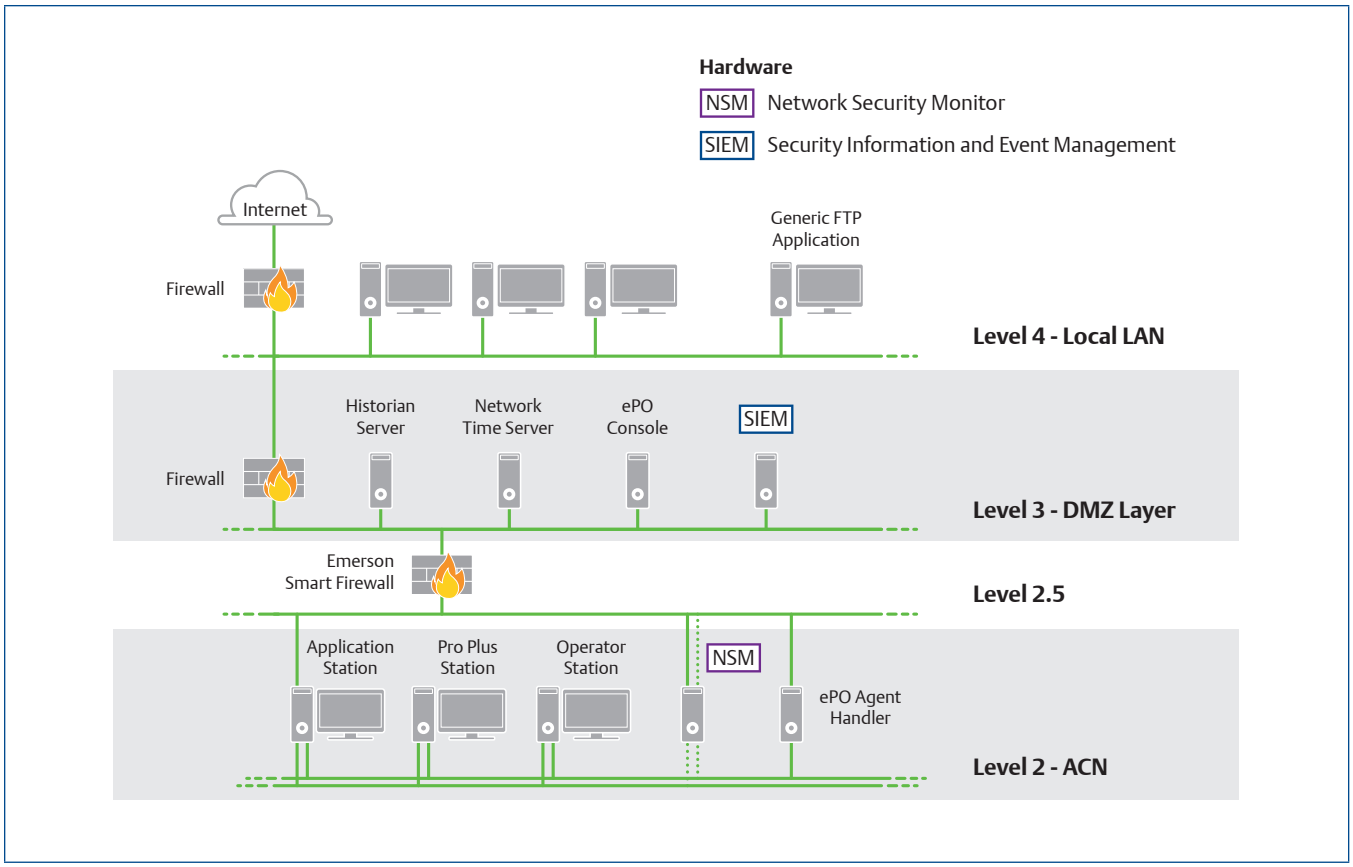
Maintenance Services: Maintenance visits are typically purchased in a bank of service hours to routinely check the DeltaV network traffic patterns and correlated events. Certified engineers can also investigate anomalies and help identify potentially malicious activity.

Configuration Updates: Emerson will update the configurations, dashboards and rules as needed to improve security visibility of your DeltaV System assets. The annual support subscription ensures that you will have access to the latest updates. Emerson SME support and call escalation to Trellix are also included.

Incident response: Emergency on-site services are also available to provide expert investigation and forensic analysis.

System Compatibility

The deployment of Network Security Monitor (NSM) for DeltaV Systems software is compatible with the currently supported DeltaV releases. Please consult the Complementary Products List for full details. The Security Information and Event Management (SIEM) for DeltaV Systems is required. A firmware update is required to enable port mirroring for your DeltaV Smart Switches.



Example reference architecture for NSM for DeltaV Systems on a typical DeltaV network.

Virtualized Option

The virtualized NSM for DeltaV Systems requires a VMWare ESXi host server. The virtual machine is available in two classes, depending on the size of your DeltaV System:

- Small – for use with smaller DeltaV Systems
- Medium – for use with most DeltaV Systems.
  Please note: If the customer requires a physical NSM appliance, then this must be ordered from Trellix as a direct buy-out. The physical appliance subscription support part number VE9129GxMD-S must be ordered and maintained annually for Emerson support.

Ordering Information

Description	Model Number
Network Security Monitor (NSM) for DeltaV Systems	Please Contact Your Local Emerson Sales Office
One Year Warranty and Support for NSM for DeltaV Systems	Please Contact Your Local Emerson Sales Office
Installation Services	Please Contact Your Local Emerson Sales Office

For inquiries and ordering information, please contact your local Emerson sales office. Prior to order acceptance, Emerson will issue a written proposal for your review and approval to ensure that scope, deliverables, timing, and budget meet your needs and expectations. Standard solution support is only offered to installs and upgrades currently performed by Emerson certified SIEM professionals.

Related Products

NSM for DeltaV Systems is part of Emerson's suite of Trellix Solutions for DeltaV Systems. Consider the following complementary products to get the most out of your NSM for DeltaV Systems:

- Endpoint Security for DeltaV Systems
- Application Whitelisting for DeltaV Systems

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

Legal Disclaimer:

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.

Contact Us
www.emerson.com/contactus

DeltaV™

EMERSON™