

OPSWAT MetaDefender Kiosk Validation with DeltaV™ Systems

This document describes the use cases and tested environment for using the OPSWAT MetaDefender Kiosk solution with DeltaV™ systems for removable media security protection.



Table of Contents

What is a MetaDefender Kiosk	3
Benefits of MetaDefender Kiosk	3
Introduction	4
OPSWAT MetaDefender Kiosk Solution Overview	4
OPSWAT MetaDefender Kiosk and DeltaV Scenarios	8
Benefits of Removable Security Deployments	10
System Compatibility	10









What is a MetaDefender Kiosk?

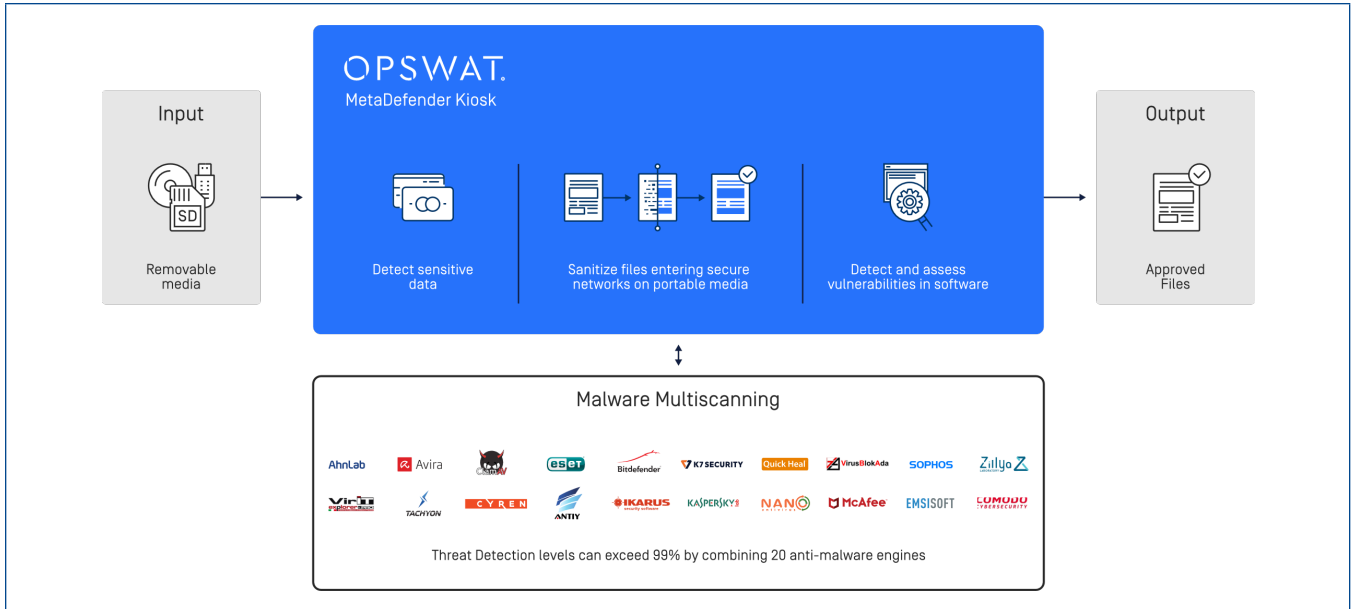
OPSWAT's industry leading MetaDefender Kiosk provides confidence, simplicity and visibility with enforceable removable media security processes that control inbound and outbound content across critical networks.

Protection in 3 Steps: Control the flow of data into and out of your organization

- Insert the removable media device into the MetaDefender Kiosk.
- MetaDefender Kiosk works as a media scanning station to check files from the device.
- Detailed report is generated after the scan is completed.

Benefits of MetaDefender Kiosk

	<p>Advanced threat detection: Scan files with multiscanning technology powered by over 30 antimalware engines with threat detection levels that can exceed 99%.</p>
	<p>Supports common media types: Scan over 15 types of removable media devices including but not limited to, USB Type A, USB Type C, Micro SD, floppy disk, CD, DVD, and more.</p>
	<p>Country of Origin check: Gain insights and create policies based on country of origin for files and content.</p>
	<p>File vulnerability assessment: Uncover vulnerabilities in installers, binaries, or applications before installation to plug any security holes.</p>
	<p>File Storage & Data Diode: Integrates seamlessly with MetaDefender Vault and NetWall, best-in-class secure data transfer and storage solutions designed for OT environments.</p>
	<p>Media Validation Agent: Validate digital signatures every time media is inserted into a device, blocking unscanned media from accessing your environment.</p>
	<p>Prevent Sensitive Data Leakage (DLP): Prevent potential data breaches and regulatory compliance violations by detecting and blocking sensitive data/personally identifiable information (PII) with OPSWAT's Proactive Data Loss Prevention (DLP) technologies.</p>
	<p>Clean & Reconstruct Suspicious Files: Remove suspect and superfluous data from common file types—including .doc and .pdf—outputting clean, usable files with Deep Content Disarm & Reconstruction (Deep CDR) capabilities.</p>



Introduction

Misuse of removable media represents an important cyber threat that also applies to Industrial Control Systems (ICS). Cybersecurity issues can still be initiated from “inside,” and removable media is a component that can facilitate insider threats.

Emerson recommends that USB ports and CD/DVD drives are disabled, which remains a best practice step in hardening DeltaV™ workstations and servers. However, a removable media security program can help to increase operational efficiency and security. If you require the day-to-day use of removable media, then OPSWAT MetaDefender Kiosk is a secure and compatible solution enabling use of removable media without exposing endpoints to malware within the DeltaV Area Control Network (ACN).

OPSWAT MetaDefender Kiosk Solution Overview

OPSWAT MetaDefender Kiosk helps protect your system by controlling the use of removable media to transfer data into, and out of, your DeltaV system. Media such as flash drives, DVDs, and a comprehensive list of encrypted USB devices (see <https://onlinehelp.opswat.com/kiosk/>) are processed by MetaDefender Kiosk. By simply inserting a media device into its appropriate drive, removable media with files that are deemed to be clean/allowed can be accessed by DeltaV stations. A detailed report of allowed/blocked content is displayed by the kiosk upon a successful scan of target removable media.

MetaDefender Kiosk is comprised of a hardened appliance station that offers different features (see <https://www.opswat.com/products/metadefender/kiosk>) and a Media Validation Agent – available to pair with a MetaDefender Kiosk – that runs on each DeltaV station that is scoped as part of the overall solution. Figure 1 (below) shows the different hardware options available for the kiosks.

Since the solution is based on digital certificates, users have the choice of managing clusters of MetaDefender Kiosks which will use different certificates or share the same certificates between multiple kiosks. This means that users can either be required to scan removable media content by a specific kiosk before connecting to a DeltaV workstation or, when sharing certificates, any existing kiosk can be used to validate removable media content.

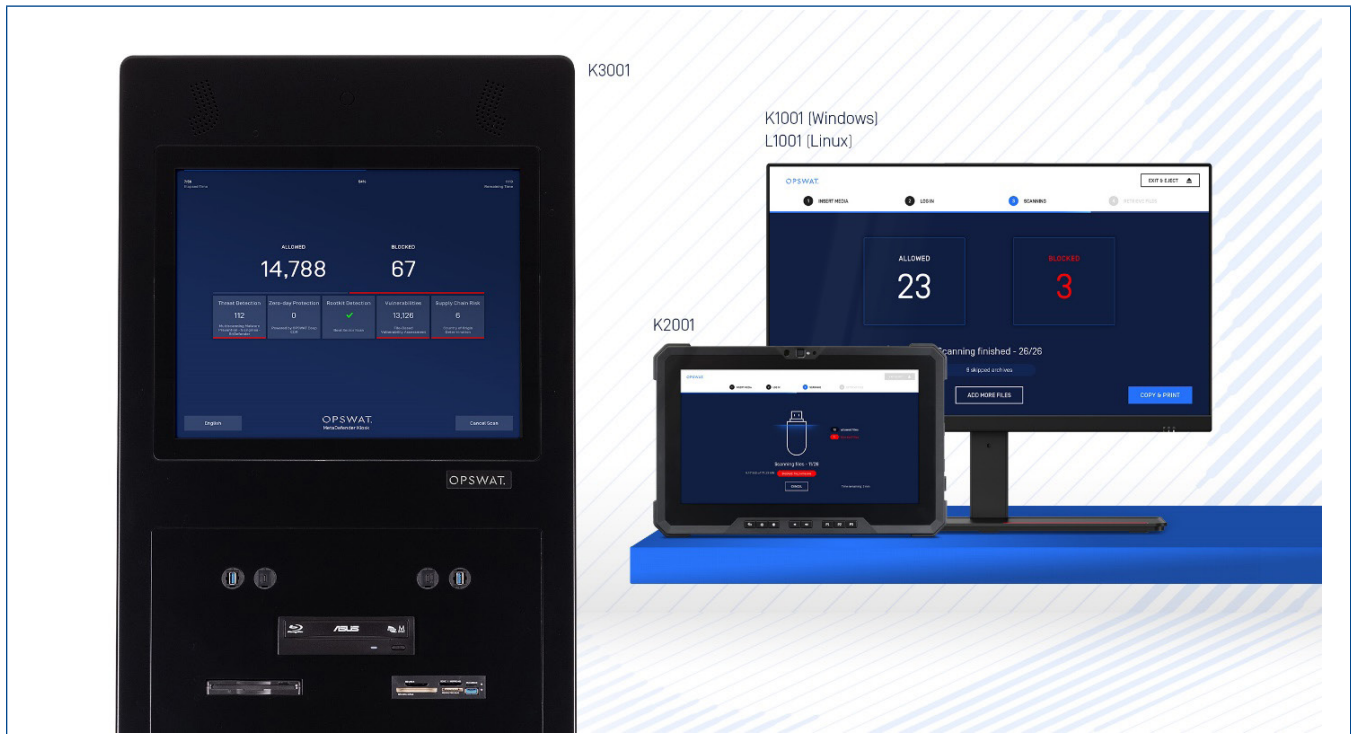


Figure 1. OPSWAT MetaDefender Kiosk Hardware Options (example only).

Hardened MetaDefender Kiosks can be purchased directly from OPSWAT with different software bundles that define the quantity and brand of antivirus engines* used to scan removable media. There is also an option to license the kiosks based on a-la-carte antivirus engines of your choosing. See the OPSWAT MetaDefender Kiosk options for more information about available bundles and a-la-carte options: <https://www.opswat.com/products/metadefender/kiosk>.

* Various threat prevention technologies are available with the MetaDefender solution such as CDR (Content Disarm and Reconstruction - data sanitization) and DLP (Data Loss Prevention) as additional solutions that can enhance the user experience. Please consult with OPSWAT directly for more information about these optional packages that can be added in combination with the OPSWAT MetaDefender Kiosk Validation solution.

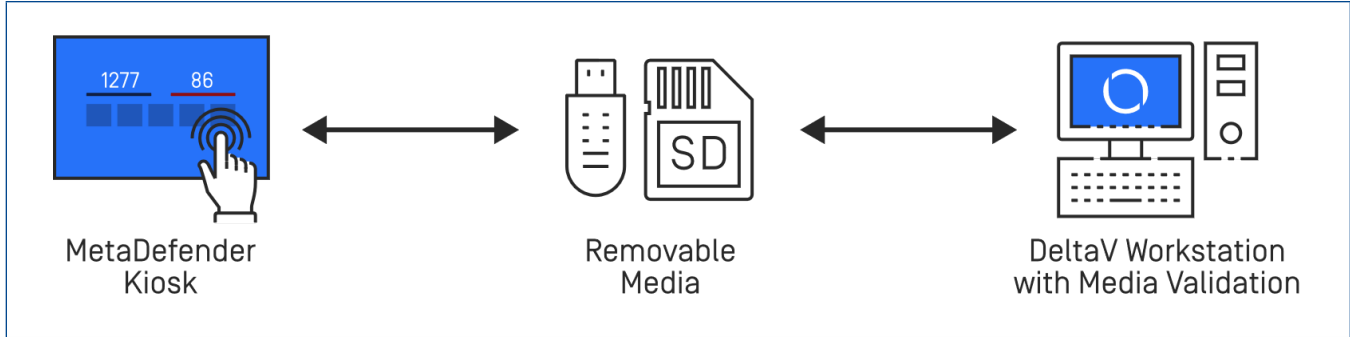


Figure 2. OPSWAT MetaDefender Kiosk Component.

Main Features:

- MetaDefender Kiosk will scan removable media for malware. Whenever malware is identified during a scan of removable media, access to that removable media will not be allowed on DeltaV workstations running the MetaDefender Media Validation Agent.
- MetaDefender Validation Agent will protect each DeltaV workstation where it is installed by only allowing removable media to be accessed if previously scanned and deemed clean by MetaDefender Kiosk.

The MetaDefender Kiosk is updated regularly to improve antivirus scan efficacy and this activity can be done offline (updates are loaded via USB into the kiosk) or online (when the kiosk is connected to a network with internet access). MetaDefender Kiosk updates are provided by OPSWAT directly and there are no OPSWAT files or updates available through Emerson's Guardian Support Portal, even for antivirus engines that may be related to what is offered by Emerson for the DeltaV stations. More information on installation with DeltaV control systems is detailed in the next section.

The Media Validation Agent is provided as an installer when the solution is acquired from OPSWAT. The agent needs to be installed on every DeltaV station where protection will be used. Along with Media Validation Agent, a digital certificate loaded on the kiosk, is installed on every DeltaV station where protection will be used. A self-signed certificate is provided with the solution, but Emerson highly encourages that a Certificate Authority-signed certificate is provided and managed accordingly by the user. Note that MetaDefender Kiosk does not need any communications with DeltaV stations for protection to work, and as you can see in Figure 3 (below), the only required connection for MetaDefender Kiosk is with the OPSWAT content server when the option for automatic updates is selected (Annual subscription to OPSWAT services is required to obtain support and updates for the MetaDefender Kiosk. Consult OPSWAT for options and pricing).

Emerson encourages customers to design engineered solutions for OPSWAT MetaDefender Kiosk with OPSWAT's help or from Emerson's Performance Services group, especially if you are not familiar with all the use cases for OPSWAT's solution and/or integration options with DeltaV. Please consult your local Emerson sales office for additional information about this solution offering.

The scanner stations, or kiosks, are hardened workstations running Microsoft Windows or Linux operating systems. Based on the selection of Windows or Linux, the user interface is tailored so that the console is limited to removable media scanning functions via a touchscreen interface. System administration will vary based on the operating system. For Windows, system administrators can exit the custom interface by entering valid credentials to access advanced configuration options. These settings are applied on each kiosk, and not as a group. Linux kiosks are managed via a central management portal as the Linux kiosks are hardened appliances.

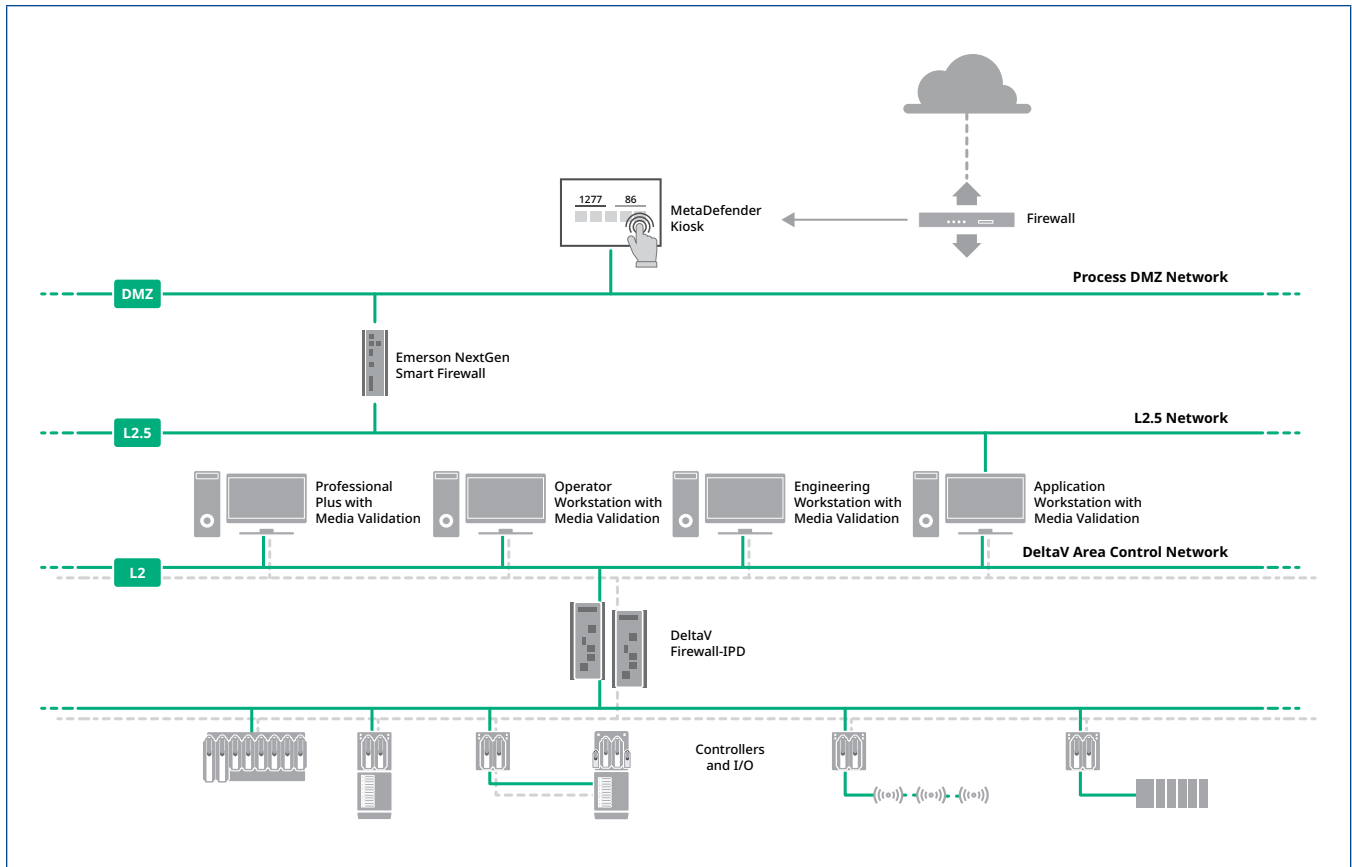


Figure 3. Reference Architecture highlights the OPSWAT MetaDefender Kiosk solution interfaced with a DeltaV system.

OPSWAT MetaDefender Kiosk and DeltaV Scenarios

Once deployed, the MetaDefender Kiosk will protect each DeltaV workstation, with Media Validation Agent is installed, by only allowing removable media to be accessed if previously scanned and deemed clean. With that in mind, the following use cases can be considered to further explain how protection is implemented as part of this solution:

- a) Removable media is first checked by the kiosk 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 accessed and modified by the DeltaV workstation where removable media is still connected, but removable media with modified content will not be accessible by other DeltaV workstations running the Media Validation Agent.

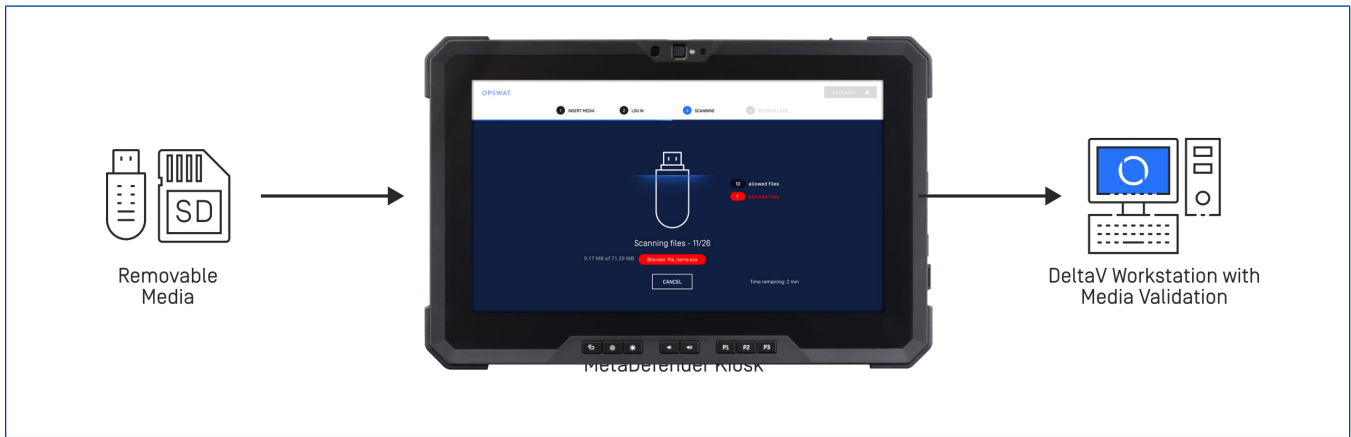


Figure 4. Scanning removable media prior to connecting it to the DeltaV workstation running the Media Validation agent.

- b) If the removable media content is modified, it will need to be re-scanned so that other DeltaV workstations running the Media Validation Agent can access the media contents.

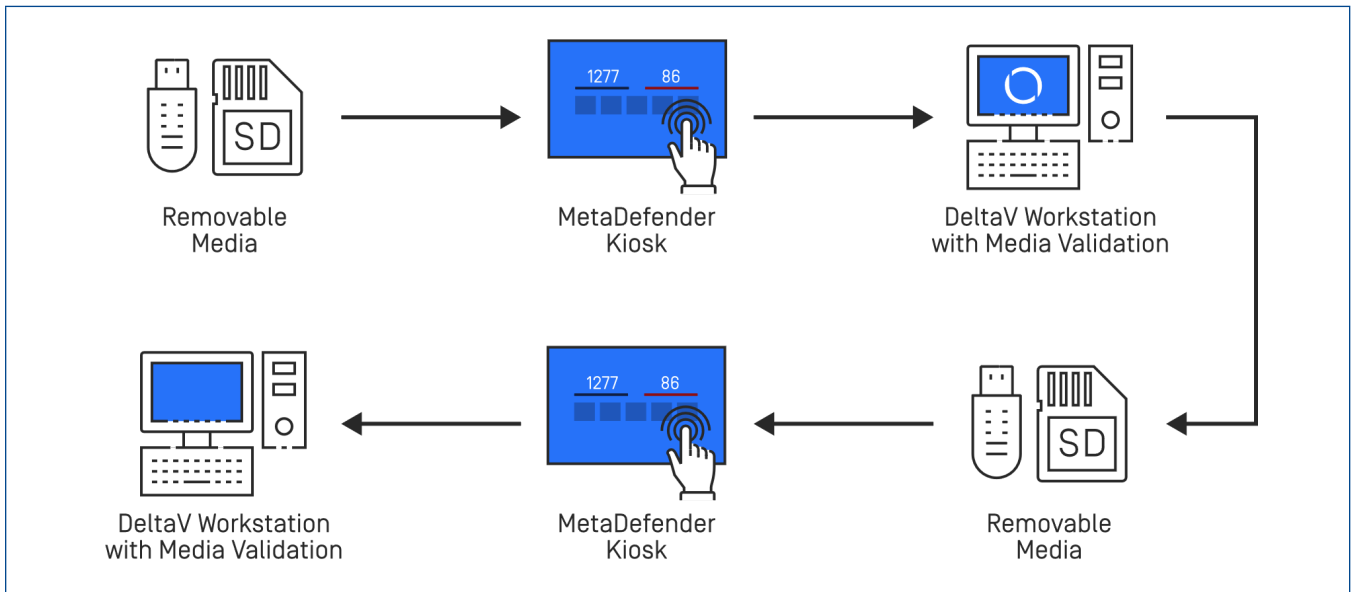


Figure 5. Re-scanning a removable media with modified content prior to connecting it to another DeltaV workstation also running the Media Validation agent.

c) The same behavior described on (b) above applies in case removable media content is modified by any computer other than DeltaV workstations and servers.

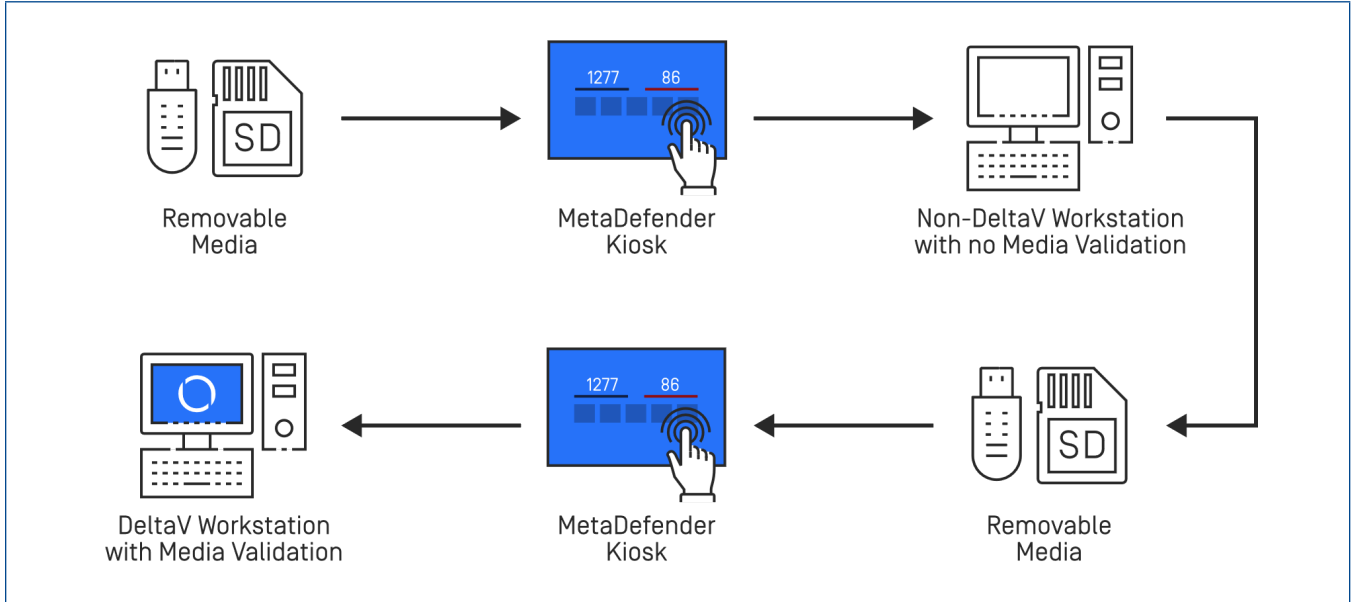


Figure 6. Re-scanning a removable media with content changed by a non-DeltaV workstation prior to connecting it to a DeltaV workstation running the Media Validation agent.

d) Removable media with modified content can be re-scanned multiple times and if deemed “validated” it will be fully accessible by any DeltaV workstation.

e) Whenever malware is identified during a scan, access to the removable media is not allowed on DeltaV workstations running the Media Validation Agent.



Figure 7. Different agent responses for removable media with ‘allowed’ or ‘blocked’ content.

Benefits of Removable Security Deployments

■ Advanced Threat Protection for OT Assets:

- Serves as a barrier to prevent USB devices containing malicious firmware/hardware from directly being able to connect to the OT endpoints.
- Scan removable media, files, patches, and updates for malware, vulnerabilities, and other suspicious content before it enters a critical domain.
- Protects critical assets and manufacturing systems from vulnerable software updates.
- Industry-leading anti-virus multi-scanning enables the simultaneous analysis of portable media threats with multiple antimalware engines, vastly increasing detection rates, decreasing outbreak times, minimizing false positives, and providing resilience.

■ Compliance:

- Placing OPSWAT MetaDefender Kiosks at key check point entrances, critical SCADA network locations, and research facilities to verify all media before use provides compliance with ISA/IEC NIST, NEI, NERC CIP and ISO/IEC requirements.
- All files in MetaDefender Vault are AES encryption secured, monitored, and checked for malware using 30+ anti-malware engines, and are then sanitized and quarantined based on configuration and workflow policies.

■ Data Loss Prevention:

- Vendors and contractors often need to extract files from a facility for debugging and analysis purposes. In this use case, the data flow can go to and from MetaDefender Vault. Outgoing data will start at the MetaDefender Vault and flow to the kiosk, where the authenticated and authorized user can extract the files using approved media. Data security and data privacy rules are enforced through pre-defined data redaction rules assigned to the relevant workflow
- All data transfers and workflow configuration changes are logged for detailed audit reporting.

To contact OPSWAT visit: <https://www.opswat.com/get-started>

System Compatibility

The OPSWAT MetaDefender Kiosk solution has been tested with DeltaV version 15.LTS and was included in the complementary products list for third-party product validation on a periodic basis. The expectation is that the solution is tested with major DeltaV versions, prior to their release, and that OPSWAT is the provider of such solution. OPSWAT is responsible for providing proposals, support, and software updates whenever required.

Although simple, the scope of the MetaDefender solution can expand beyond the use cases described in this whitepaper. The use cases tested with DeltaV systems include the installation of the Media Validation Agent on physical DeltaV stations and thin clients for DeltaV virtualization. Emerson recommends users to purchase the MetaDefender Kiosk as a solution including the design, implementation, and lifecycle support by reaching out to OPSWAT directly or through the Emerson's Performance Services organization.

Tests of the MetaDefender solution include the latest version of the Media Validation Agent installed on major versions of DeltaV system prior to their release. Emerson will not test versions of the Media Validation Agent on a periodic basis other than in preparation to release a major version of DeltaV software. See the list of complementary products in Emerson's Guardian Support Portal (Release Notes) for additional information about tested components mentioned in this whitepaper.

The OPSWAT MetaDefender Kiosk solution has been tested with DeltaV version 15.LTS and tests will continue for future major versions of DeltaV software. For backwards compatibility, please consult with your local Emerson sales support organization to get a validation services quote from Emerson's Performance Services organization.

The Emerson logo is a trademark and service mark of Emerson Electric Co. The DeltaV logo is a mark of one of the Emerson 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 diligent efforts were 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 designs or specifications of our products at any time without notice.

Contact Us
🌐 www.emerson.com/contactus

