GUIDE

MetaDefender Kiosk Deployment Guide

OPSWAT.

SECTION **1.0**

Recommended Deployment of MetaDefender Kiosk(s)

OPSWAT's MetaDefender Kiosk product is deployed by organizations to scan portable media and detect and prevent threats contained on such media and prevent their introduction to secure networks and systems. The intention of this document is to outline OPSWAT's recommended deployment for MetaDefender Kiosk systems within power plants. Specifically, this covers the deployment of MetaDefender Kiosk systems to meet the requirements for handling digital media.

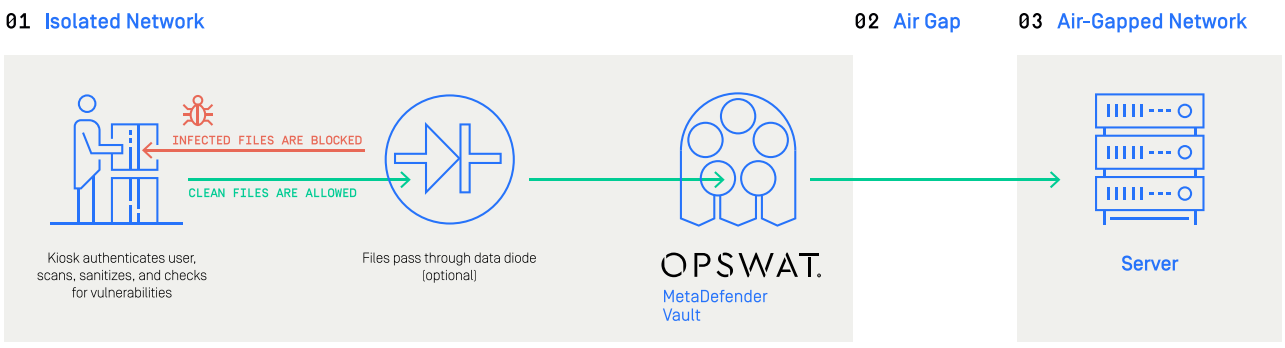
Requirements in NERC CIP-010-02 R4 (For Electrical Plants Only)

MetaDefender can help utilities meet the following requirements of NERC CIP-010-02 R4.

- Transient Cyber Asset(s) Managed by the Responsible Entity
- Transient Cyber Asset(s) Managed by a Party Other than the Responsible Entity
- Removable Media

Requirements taken from CIP-010-2 — Cyber Security — Configuration Change Management and Vulnerability Assessments, Attachment 1

Recommended Deployment Diagram



SECTION **2.0**

MetaDefender Kiosk Deployment Options

For each deployment aspect below, OPSWAT has recommendations for different deployment options. In many cases, there are multiple deployment options that have trade-offs between security, usability, cost, or all three. When different options are available an attempt is made to describe the trade-offs between the different options.

Beginning with MetaDefender Core 3.12.1 and MetaDefender Kiosk 3.3.4 OPSWAT includes a 'High Security' workflow by default with the product installation. These workflows can be used as a starting point and modified for the needs of a specific MetaDefender deployment.

Distributed vs. Standalone Deployment Model

MetaDefender Kiosk and MetaDefender Core can be installed either on the same system or on separate systems that are accessible over a network. Although both options are secure, OPSWAT recommends considering the following advantages of each.

Advantages of a Distributed Deployment Model

01. The MetaDefender Kiosk system can be protected by a system imaging product (see the System Imaging section below) without the loss of anti-malware definitions (see the Upgrading Anti-malware Engine Definitions section below) that have been applied to the MetaDefender Core component
02. Separation of the MetaDefender Kiosk and MetaDefender Core components mean that if one system is compromised it is limited to that system
03. If multiple MetaDefender Kiosks are using the same MetaDefender Core the anti-malware definitions only need to be updated on the MetaDefender Core server. This allows the definitions to be updated on a more frequent basis which increases the security against new outbreaks and zero-day attacks
04. MetaDefender Core servers can be located in a different physical location than the MetaDefender Kiosk system. This has multiple advantages:
    a. The MetaDefender Core system can be located in a more easily accessible area and thus be updated with anti-malware definition updates more frequently
    b. If the MetaDefender Kiosk system is physically compromised it does not affect the MetaDefender Core system

Advantages of a Standalone Deployment Model

01. No networking infrastructure or configuration is required

02. Kiosks can be relocated without any additional modifications

Network Traffic Restrictions

These recommendations are only applicable if the MetaDefender Kiosk systems are networked. The following functionality of MetaDefender Core and MetaDefender Kiosk require network access to other systems:

- Remote configuration of MetaDefender Core and Kiosk
  - Application of anti-malware engine definition updates to MetaDefender Core
  - Changes to workflows
  - Other configuration change
- Distributed Deployment of MetaDefender Core and Kiosk
  - Transfer of files to be scanned
  - Retrieval of scan results
- Post Scan File Handling
  - Upload of files from MetaDefender Kiosk to MetaDefender Vault (if configured as a file handling option in workflows)
  - Copying of files from MetaDefender Kiosk to a network path (if configured as a file handling option in workflows)

OPSWAT recommends restricting the allowed traffic to only that necessary for the functionality needed in a deployment. OPSWAT recommends using a product designed for this purpose to tightly restrict the traffic that is allowed. OPSWAT can provide recommendations on specific products that have been tested with MetaDefender for compatibility. If such a device is not used, OPSWAT recommends restricting network traffic to only the ports required for operation of the MetaDefender Kiosk systems using Windows Firewall as well as restricting traffic to specific trusted MAC addresses.

System Imaging

For the most security, OPSWAT recommends using a product capable of restoring Kiosk images to a known good point. MetaDefender Kiosk provides the option to restart the kiosk after each scanning session. When combined with a system restore product, this is the most secure configuration setting. If business requirements make restarting the kiosk after each session unfeasible, a scheduled task can be set to restart the kiosk systems on a regular basis (e.g. every night) so that they are restored at that time. OPSWAT can recommend vendors that provide system restore functionality.

- If a system restore product is installed on the kiosk, all configuration changes will be lost every time the system is restarted. If configuration changes are needed on the system, the system must first be put into an 'configurable' state for the changes to be made and then a new image taken with the updated configuration. This is also true for upgrades to newer versions of MetaDefender Kiosk or any patches that have been applied to the software.
- If MetaDefender Core is installed on the same system as MetaDefender Kiosk all updates will be lost upon system restore. This includes all anti-malware engine definition updates that have been applied. See the section on the advantages and disadvantages of choosing a distributed vs standalone deployment model.
- All scan logs that are stored on the system will be lost upon system restore. To maintain logs, MetaDefender Kiosk must be configured to save session logs to another system.

MetaDefender Kiosk Hardening

OPSWAT recommends following the instructions in the MetaDefender Kiosk user guide to harden the MetaDefender Kiosk systems.

SECTION **2.0**

Maintenance Policy

Updating Anti-Malware Engine Definitions

01. MetaDefender Core anti-malware engine definitions should be updated by following the instructions in the MetaDefender Core documentation

02. For downloading offline definition updates, OPSWAT recommends using the MetaDefender Update Downloader

03. OPSWAT recommends updating the anti-malware engine definitions as often as is possible, preferably daily

Upgrading MetaDefender

01. MetaDefender Core and MetaDefender Kiosk should be upgraded by following the upgrade instructions in the product documentation

02. OPSWAT recommends that when possible all deployments should be on the latest versions of MetaDefender Core and MetaDefender Kiosk. For more information on OPSWAT's support policy for specific versions of MetaDefender Core and Kiosk please refer to OPSWAT's MetaDefender support policy

03. When systems are upgraded it is recommended that the configuration settings from the previous installation are exported and archived so that they are available in case systems need to be restored to a previous version

04. OPSWAT recommends always upgrading both MetaDefender Core and MetaDefender Kiosk at the same time

SECTION **3.0**

Configuration Options

User Authentication and MetaDefender Kiosk Workflows

MetaDefender Kiosk enables authentication of users before starting a scanning session. OPSWAT recommends enabling user authentication for the following reasons.

- Identification of which user scanned each piece of media that was scanned by MetaDefender Kiosk for audit purposes
- Usage of different user profiles for different groups of users (see section on Multiple User Profiles)

MetaDefender Kiosk supports the use of custom authentication modules, which allow each organization to integrate their authentication method (e.g. RFID card, badge scanner, IC card, etc) with their MetaDefender Kiosk. This allows an organization to link scan sessions to their existing authentication systems. Depending on the authentication system used, a custom authentication module may have to be developed for deployment. Contact OPSWAT for more information on what a specific system would require.

Multiple User Workflow Profiles

OPSWAT recommends configuring multiple user workflow profiles to process files from different users. Each workflow should be configured to restrict the types of files to the minimum those users are expected to need to complete their jobs. File types that are more risky (e.g. EXEs or Archive files) should be limited to the users that are expected to bring in those types of files and need them to complete their work and should be blocked for all other users.

Authentication and MetaDefender Vault

If files are being uploaded to a MetaDefender Vault server after scanning there are two options for uploading the files:

01. **Upload to a Vault user account -** This is an option if the user credentials are available to the MetaDefender Kiosk system. This would most likely be the case if MetaDefender Kiosk and MetaDefender Vault are both on the same network and are using the same Active Directory server for authentication.
02. **Upload to a Vault guest user account -** This is an option to create a guest user account that is used for a specific file upload. This can be used when either user credentials are not available to MetaDefender Kiosk or there are guest users scanning files on the MetaDefender Kiosk.

Data Sanitization

Data sanitization is the process of removing potentially dangerous objects within files or modifying the files to neutralize threats, even if they are not detected by any anti-malware products. MetaDefender Core's data sanitization technology allows administrators to specify that certain types of files are sanitized even if no threat is detected. Although this results in greater security and a reduction in the risk to unknown threats, there is a tradeoff in that the usability of sanitized files is sometimes less than the original file.

- For the highest level of security, OPSWAT recommends that data sanitization is applied to all document and image types that are supported unless the potential loss of usability in those files is too great for business reasons

Options for Networked Environments

The most secure option if the MetaDefender Kiosk system is on a network is to upload the files to a MetaDefender Vault server. The advantages of uploading to MetaDefender Vault is that the files can be uploaded to a specific user's account or a guest account, and access is limited to that user. All file uploads and downloads are tracked, and an audit log is available for compliance officers to see when files were uploaded and downloaded from the server. This can help to track when files are accessed in a network and by whom. If MetaDefender Vault is not used, files can also be copied to a network share into a directory tied to the user who authenticated on the MetaDefender Kiosk system.

Option for Non-networked Environments

If the MetaDefender Kiosk system is not deployed on a network OPSWAT recommends using the functionality to copy clean files to user provided media, allowing original media to not be used on the secure network. OPSWAT would recommend either copying to pre-approved media that is only used in the secure network or to static media, such as CDRs. If copied to pre-approved rewritable media, such as USB drives, OPSWAT recommends a policy to wipe that media after use and before the next time the media is used as the destination media. MetaDefender Kiosk's wipe functionality can be used for this purpose.

Session Logging

MetaDefender Kiosk supports three types of logging of individual scan sessions. All three can be enabled or disabled independently of each other.

01. **Save session log to a text file** - Saves a text log for each session to the default log directory or a directory specified by the administrator, however if the files are saved locally they will not be retained if the system is restored as recommended in the System Restore section above.

02. **Save session log to scanned media** - Saves the text log for a session to the media that was scanned. This allows a record of the scan to be saved on the media that was scanned, however a file will not be written if the original media is read-only.

03. **Send session log to e-mail recipient** - This allows all scan logs to be collected into a single e-mail account, however it does require that the MetaDefender system has access to a mail server to send the e-mail.

SECTION **4.0**

Common Questions about MetaDefender Kiosk

01 . How many MetaDefender Kiosk systems are needed in a deployment?

We believe that the appropriate number of units would be the number required to give end users a chance to scan media however and wherever they are bringing it into a secure area. So, if there are three entrances a kiosk can be located at each entrance. If employees and/or visitors are also expected to scan media that is already within the secure area then a kiosk should also be in a location that is convenient for users to access within the secure area.

02 . What are the recommended physical locations for MetaDefender Kiosk systems to ensure steady availability to all end-users?

We recommend that MetaDefender Kiosk stations are located at all entrances to secure areas, and that users are required to scan any portable media before bringing them into secure areas.

03 . Which organization functional unit should be the owner of the MetaDefender Kiosk systems (to maintain, update, etc.)?

The appropriate department should be the one that is able to handle definition and software updates to the MetaDefender Kiosk systems. The necessary skills include basic Windows operating system knowledge as well as comfort with configuration and deployment of secure networks.

04 . Do you recommend deploying MetaDefender Kiosk in a standalone or distributed environment? What are the pros and cons of different deployment options?

A majority of our current customers have deployed MetaDefender Kiosk systems as standalone systems not connected to any network. Although this is a secure deployment option, we think that the most secure solution is to deploy MetaDefender Kiosks on an isolated network, with multiple MetaDefender Kiosk systems using a shared backend MetaDefender Core server.

The advantages of this deployment model are the following:

i. The MetaDefender Core server can be located in a central location that is physically easier to access to apply engine definition updates

ii. The MetaDefender Core server can be on a high performance server so that better scanning performance can be achieved versus standalone systems

iii. A single centralized MetaDefender Core server can have more scanning engines than multiple standalone MetaDefender Core servers at the same total cost

iv. The MetaDefender Kiosk systems can be restored to a known ‘clean’ state if necessary without losing engine definitions that have been applied

The disadvantage of going with a distributed deployment is maintenance of the network and the existence of the central MetaDefender Core server but we generally feel that the benefits listed above outweigh the additional costs.

05 . How frequently should anti-malware engine definitions be updated?

We recommend updating the engine definitions as often as is possible, preferably once a day if it is feasible. The ability to update virus definitions more frequently is a major advantage to having a distributed deployment model with a central MetaDefender Core server.

06 . How do you recommend laptops or tablets are scanned for threats?

Devices such as laptops or tablets can be scanned with our MetaDefender Client product on an isolated network. This client can be run on the device either when the system is already running or can be included on a 'boot' or 'live' CD or USB that is used to boot the system into a limited operating system.

07 . Can MetaDefender Kiosk detect BadUSB?

With BadUSB based attacks, the USB device has been modified to act as a different type of device (e.g. a keyboard or other peripheral) instead of a flash USB drive. Since this is done at a firmware level, there is no way for the system, and the MetaDefender Kiosk software, to know that is is anything besides the type of device it is identifying itself as, however just as the MetaDefender Kiosk UI is hardened against being compromised by a physical keyboard it would protect against a 'fake' keyboard or other input device that a BadUSB device is pretending to be.

08 . Does MetaDefender Kiosk provide any protection when the kiosk UI is not running?

If the MetaDefender Kiosk software is not running there is no additional protection on the system provided by MetaDefender Kiosk.

09 . Is it possible for malicious code to compromise the Kiosk UI?

OPSWAT is not aware of any way that a client can be compromised.

10 . If the Kiosk UI is compromised is there a way for the Servre to be compromised as well?

If the Kiosk were to be compromised, it does have system or network access to the server. What OPSWAT would recommend as the most secure deployment option would be have MetaDefender Kiosk and MetaDefender Core on separate systems on the same isolated network, and a device restricting network traffic between the Kiosk and the Core server to restrict traffic between the Kiosk and the server to only the traffic necessary for scanning. OPSWAT can recommend devices to provide this functionality.

11 . Is it possible for malicious code to be written to the MetaDefender Core server and compromise the server?

All files are written to the temporary directory, which can optionally be set to the RAM drive, and then removed after scanning so they will not remain on the server.

12 . If multiple MetaDefender Kiosk systems are deployed on the same isolated network could a compromised MetaDefender Kiosk system compromise other MetaDefender Kiosk systems?

OPSWAT is not aware of any way that a MetaDefender Kiosk system could compromise another MetaDefender Kiosk system on the same network. However, for additional security, having a device that restricts traffic to only that required for scanning files can be added between the MetaDefender Kiosk system and the network. OPSWAT can recommend devices that provide this functionality.

13 . If a MetaDefender Kiosk system is compromised could it infect media being scanned?

OPSWAT is not aware of any way the Kiosk could be compromised to act in this fashion, however for additional security the Kiosk could be restored to a known 'clean' state after each scanning session. OPSWAT can provide recommendations on tools that can be used to provide this functionality.

14 . If a MetaDefender Core server is compromised could it infect media being scanned?

The MetaDefender Core server does not interact with the media being scanned in any way.

15 . What provisions/safeguards are in place to assure that an infected file is not skipped during a scan session either because a scan was cancelled or because a user did not select that file to be scanned?

If any files are not scanned on the media, either because the user cancels a scan or because they browse to select the files that are to be scanned, within the scan session log is a notification that the entire media was not scanned. OPSWAT also recommends that the functionality of copying to user provided media or to a MetaDefender Vault server is used to ensure only files that have been scanned without any threats detected are used on a secure network.

16. Is there any known instance where a MetaDefender Kiosk system has been compromised in the past?

OPSWAT is not aware of any deployed MetaDefender Kiosk system that has been compromised.

SECTION **5.0**

About OPSWAT

OPSWAT is a global cyber security company that has provided security solutions for enterprises since 2002. Trusted by over 1,000 organizations worldwide, OPSWAT prevents data breaches and malware infections by eliminating security risks from data and devices coming into an organization. MetaDefender by OPSWAT is a powerful advanced threat detection and prevention platform, offering data sanitization (CDR), vulnerability assessment, multi-scanning, heuristics, big data, and additional threat protection technologies for a solution that is not solely based on detection. MetaAccess by OPSWAT is a cloud-based access control solution that helps enforce endpoint compliance and prevents contamination of cloud applications by blocking potentially compromised or noncompliant devices from accessing SaaS applications.

To learn more about OPSWAT's innovative and unique solutions, please visit http://www.opswat.com