OPSWAT

Metadefender®

KIOSK

What is Metadefender Kiosk?

As cyberattacks become more sophisticated and digital control systems increase in complexity and levels of automation, it is crucial to prevent threats from impacting critical infrastructure operations. Most critical infrastructure OT systems are isolated from cloud-connected IT networks, making portable media a primary cyberattack vector that must be secured. Likewise, "high security" networks such as those of government agencies are highly secured but also highly targeted.

For these environments, the need to control the flow of files and data into and out of the network to protect against threats and sensitive data leaks is paramount. Metadefender Kiosk protects organizations by acting as a checkpoint for incoming data on USB drives and other media devices, providing the ability to assess, control, and sanitize files before they enter a secure network, as well as identify and restrict vulnerabilities on applications that could be exploited. Today, Metadefender Kiosk is the de facto standard for securing ICS environments in the North American nuclear industry by enabling secure data transfer processes into and out of these high security, air-gapped networks.

Metadefender Kiosk Features

Scan files

including archives and compressed files, with more than 30 leading anti-malware engines

Remove embedded threats

in files with OPSWAT's patented and industry-leading data sanitization (CDR) technology

Detect vulnerabilities

in application binaries being brought in with the Metadefender Vulnerability Engine

Define flexible security policy workflows

for different user/AD groups

Block

based on file size, file type, or anti-malware scan results

Use domain or system accounts

to easily authenticate users

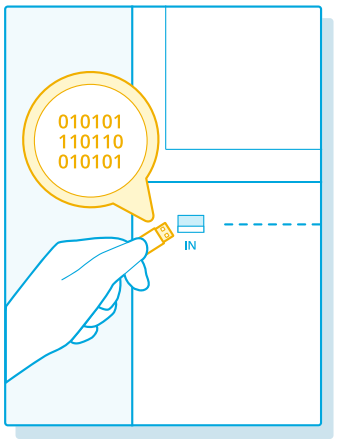
Analyze file type

to validate file content and prevent spoofing

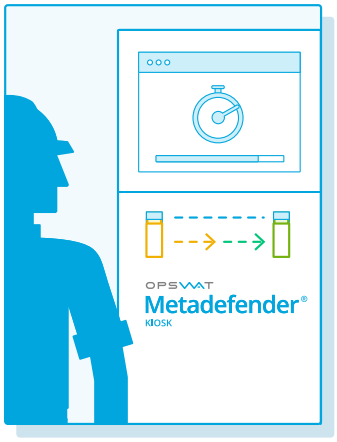
How Metadefender Kiosk Works

Metadefender Kiosk and its associated components or options (see below) can be configured in various ways to enable a fluid, secure, and guest- and employee-friendly file transfer and USB use policy and system. Depending on your organization's requirements, optional 3rd-party data diode solutions may also be incorporated.

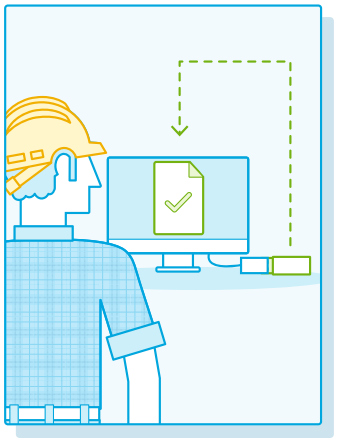
INSERT



PROCESS



ACCESS



Metadefender Kiosk Product Family

Metadefender Core

Metadefender Kiosk uses Metadefender Core, OPSWAT's back-end multi-scanning solution, to scan files for malware threats and sanitize files using its patented data sanitization (CDR) technology. Metadefender Core can be installed on the same system as Metadefender Kiosk, or a single Metadefender Core server can service multiple Metadefender Kiosk systems over a network.

Metadefender Secure File Transfer

Metadefender SFT can be added on to Kiosk environments to securely store files after they have been scanned. After files have been scanned, they can be uploaded to a Metadefender SFT server, which can act as a secure file vault for access by authenticated user accounts or unique guest accounts.

Metadefender Client

Metadefender Client can complement Metadefender Kiosk's capabilities by monitoring endpoints for any use of USB devices and scanning those devices before they are used on the endpoint. Metadefender Client can also be used to validate media that has previously been scanned by Metadefender Kiosk.

Why Metadefender Kiosk?

Portable media and USB
file scanning checkpoint for high-security networks

Enables a secure process
for safely moving files to secure media or network locations

Auditable record
of who brought in what data and when

About OPSWAT

OPSWAT is a global cyber security company providing solutions for enterprises since 2002 to identify, detect, and remediate advanced security threats from data and devices coming into and out of their networks. Trusted by over 1,000 organizations worldwide for this secure data flow, OPSWAT prevents advanced security threats across multiple channels of file transfer and data flow with flexible options of Metadefender® solutions and API-based development and threat intelligence platforms.