

# MetaDefender<sup>®</sup> Kiosk

Trust at the point of entry

Can you trust every file that enters or exits your facility?

Anytime portable media accesses secure environments, critical infrastructure risks exposure. Software updates, reporting and audits all require external data sources.

MetaDefender Kiosk acts as a digital security guard—inspecting all media for malware, vulnerabilities, and sensitive data.

## Insert. Process. Access.

MetaDefender Kiosk accepts multiple form factors, including CD/DVD, 3.5" diskettes, flash memory cards, mobile devices, and USBs—even when encrypted.

Once inserted, MetaDefender Kiosk immediately scans for malware, vulnerabilities, and sensitive data. Suspicious files can be sanitized. Sensitive files can be redacted.

**MetaDefender Kiosk lets you trust all portable media that enters or exits your facility.**

Multi-language localization

Encrypted USB support

Audit receipt printing

20+ media types

Rebranding & custom graphics



## Additional Features

Support **multiple file systems**: FAT, NTFS, Ext, HFS+ & APFS

Mount and scan **virtual disks**: VHD and VMDK

**Media Validation Agent** blocks unscanned media from accessing your environment

Wipe portable media completely clean with **secure erase** option, before loading approved content

**Hardened OS** incorporates File Integrity Monitoring and Application Whitelisting

Integrates seamlessly with **MetaDefender Vault** for file storage and retrieval

# OPSWAT.

## MetaDefender Kiosk

### Benefits

#### Clean & Reconstruct Suspicious Files

Disarm unknown content and output clean, usable files

#### Industry-leading Multiscanning

Integrated 30+ anti-malware engines dramatically outperform single scan technologies

#### Prevent Sensitive Data Leakage

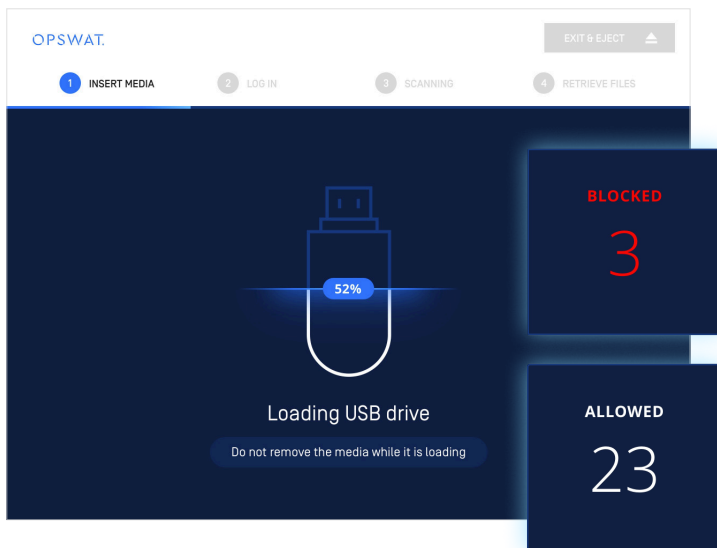
Detect, redact, or block sensitive data

#### Streamline Data Transfer

Global deployment, consistent experience

#### Meet Compliance

Fulfill regulatory requirements



After portable media is inserted into MetaDefender Kiosk, all files are scanned for malware and vulnerabilities. Malicious files are blocked. Suspect files can be cleaned. Only clean, safe portable media enter your environment.

### Capabilities

#### Proactive Data Loss Prevention (Proactive DLP)

Detects or blocks sensitive data from leaking by redacting it from 30+ common file types; PCI/DSS & GDPR compliant

#### Deep Content Disarm & Reconstruction (Deep CDR)

Removes suspect and superfluous data from common file types, such as .doc and .pdf

#### Multiscanning

Proactively detects 99%+ of malware threats; integrates 30+ malware engines by using signatures, heuristics and machine learning

#### File-based Vulnerability Assessment

Detect known exploits in 20,000+ software applications before they are installed

#### Threat Intelligence & Sandbox Data

New threats are updated in real-time; in-the-wild reputation analysis is conducted on every suspicious file

## OPSWAT.

Trust no file. Trust no device.