

OPSWAT.

# MetaDefender® Kiosk

Checkpoint for Portable Media

MetaDefender Kiosk is a checkpoint for detecting and stopping security threats before they enter an isolated network. The Kiosk can be deployed at strategic locations throughout your organization where employees or guests may be entering with USB drives or other portable media that could contain malicious files.

## Benefits

### Secure Workflow

Create a secure end-to-end process for transferring files to and from your critical networks. Prevent known and unknown threats using multi-scanning, data sanitization (CDR), and vulnerability assessment.

### Scan Portable Media to Prevent Threats

By multi-scanning files with 30+ anti-malware engines using signatures, heuristics and machine learning, MetaDefender Kiosk significantly improves detection of known and unknown threats.

### Sanitize High-Risk Files

Our Content Disarm and Reconstruction (CDR) 'disarms' over 30 different file types, removing all potentially malicious content.

### Flexible Hardware Deployment Options

Can be deployed on standard x86 hardware running Windows 7 or later. Complete turn key hardware solutions are also available in multiple size footprints.

*"Our MetaDefender kiosks give us the added confidence in our ability to help keep our network malware-free. With the multi-scanning software provided by OPSWAT, we don't have to rely on definitions from a single antivirus engine to catch every threat [...] the kiosks have proven highly effective in protecting our systems."*

Ed Koeller, Security Analyst, Ameren



# MetaDefender Kiosk Features

**Content Disarm and Reconstruction (CDR)** Disarm over 30 common file types, and reconstruct each file ensuring full usability with safe content.

**Multi-Scanning** Choose from over 30 leading anti-malware engines in flexible package options. Third party anti-malware licenses are included.

**Vulnerability Assessment** Detect known vulnerabilities in over 20,000 software applications using over 1 billion hashes.

**Customizable User Interface** Fully customizable with over 50 custom settings, eight languages out-of-the-box, and support for localization into other languages.

**MetaDefender Vault Integration** Secure access to files that have been sanitized by Kiosk to create a complete and cost-effective secure data workflow process.

**Granular Policies** Configurable workflows based on users or roles, types of portable media being used, and file types being processed.

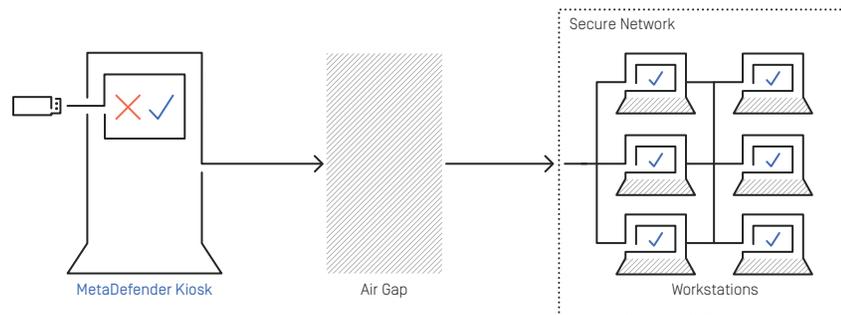
**Advanced Features** Kiosk supports your secure workflow with flexible authentication options, printed and electronic manifests, and detailed transaction logs for audit and compliance.

MetaDefender supports the following portable media types: USB devices, CDs, DVDs, Blu-rays, card readers, SD cards, and floppy disks. MetaDefender can also unlock encrypted USB devices with the password.

## MetaDefender Kiosk in Action

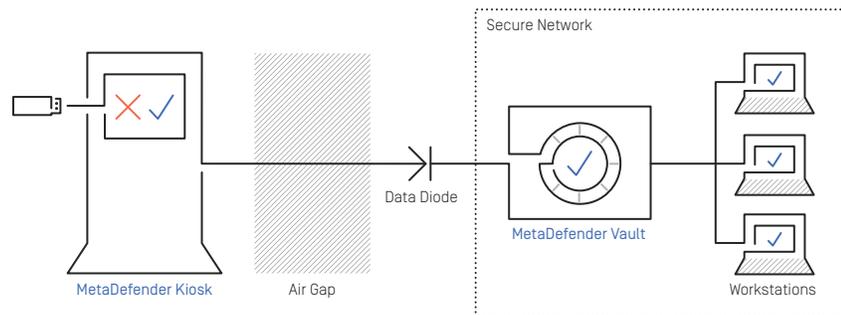
### Kiosk Air Gap Use Case

Kiosk authenticates user, performs multiscanning and CDR on the portable media, checks for vulnerabilities, and a printed and digital manifest is generated. Portable media is carried past the air gap by a user with a printed receipt.



### Kiosk Air Gap with Data Diode and Vault Use Case

Files are transferred through an air gap over optical cables through a one-way data diode to MetaDefender Vault. This combined solution supports a very robust secure file transfer and storage workflow with low Total Cost of Ownership (TCO).



Minimum system requirements: 64-bit machine, 4 core CPU, 4 GB RAM, 10 GB free hard disk space, Microsoft Windows 7, 8/8.1, 10 or Microsoft Windows Server 2008 R2, 2012/2012 R2 / 2016.

[Schedule a demo at opswat.com/contact](https://www.opswat.com/contact)

# OPSWAT.

Trust no file. Trust no device.

[www.opswat.com](https://www.opswat.com)