OPSWAT.

MetaDefender™ Kiosk

Air-Gap Network Security and Compliance at the Point of Entry

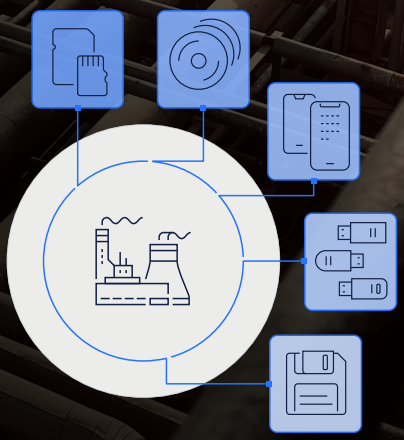
Once is all it takes.

The use of portable and removable media has increased data mobility and overall productivity within IT, OT, and SCADA infrastructures worldwide.

However, without audit, control, security inspection, sanitization, authorization, and authentication processes, the use of portable and removable media also increases cyber risk exposure to both air gapped and networked critical infrastructure systems.

Uncontrolled media can allow malware to penetrate our most critical systems as well as enable corporate secrets and private information to be extracted without authorization or knowledge.

How can you trust portable media entering and exiting your facilities?



Enforce Control and Trust at the Point of Entry

Protect Your Organization's Perimeter

MetaDefender Kiosk is a market-leading, trusted solution which enables secure, audited, authorized, authenticated, and controlled use of media within your most critical infrastructure.

Once inserted, MetaDefender Kiosk immediately scans for malware, vulnerabilities, and sensitive data.

Suspicious files can be quarantined, sanitized, and/or sandboxed for additional scrutiny. Sensitive files as well can be redacted.

Let MetaDefender Kiosk put control and trust back into your processes and productivity tools.

All-in-One

Our top cyber risk mitigation technologies packaged in one easy to use kiosk.

Regulatory and Standards Compliance

All processing, analysis, and file transfer information for media is audited, logged, consolidated, and provided in centralized dashboard reports as well as for Syslog/SIEM export. Complete integration with Active Directory for user authorization and activity tracking is provided.

Trusted Protection against Vulnerabilities

11% of Zero-day viruses go undetected by market leading vendor malware engines with heuristics enabled. Using only one vendor leaves the door wide open to compromise of your critical infrastructure, using up to four engines is also not enough. Only OPSWAT provides 30+ engines to enable trusted protection.

Data Loss Prevention (DLP)

MetaDefender Kiosk provides advanced DLP capabilities to help guard against extraction of confidential and sensitive data from client systems.

Deep Clean & Reconstruct Suspicious Files

Deep Content Disarm & Reconstruction (Deep CDR) capabilities actively remove suspect and superfluous data from common file types—including .doc and .pdf—outputting clean, usable files.

Boot Sector Scanning

Whether files are being imported into a secure environment or deployed as deliverables, MetaDefender Kiosk establishes a secure process that can be replicated globally.

Industry-leading Multiscanning

Portable media are the most common vehicle for infecting isolated environments. By combining up to 30+ anti-malware engines in a single scanning device, threat detection level scans exceed 99%.

OPSWAT.

Trust no file. Trust no device.

Easy to Set Up, Easy to Use

MetaDefender Kiosk 1000 series

L1001

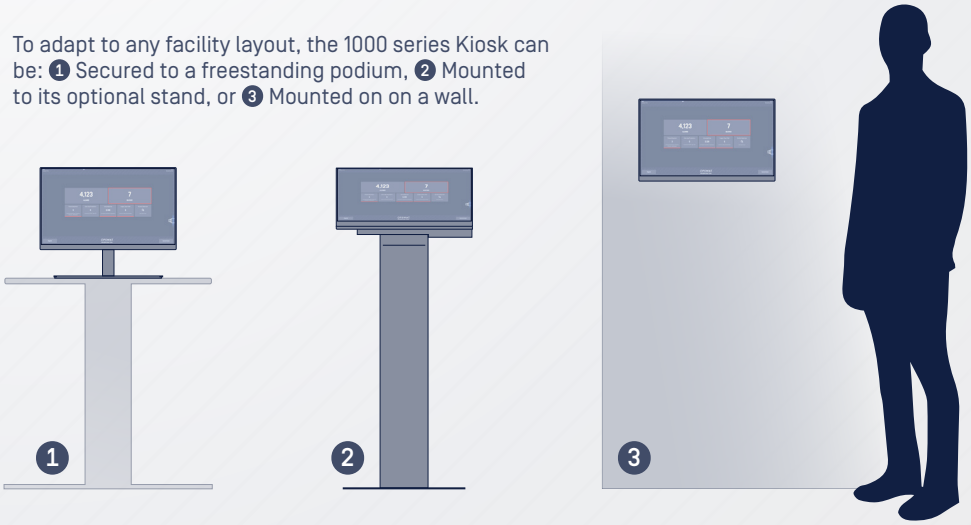
Secure, Portable, Easy to Use

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.

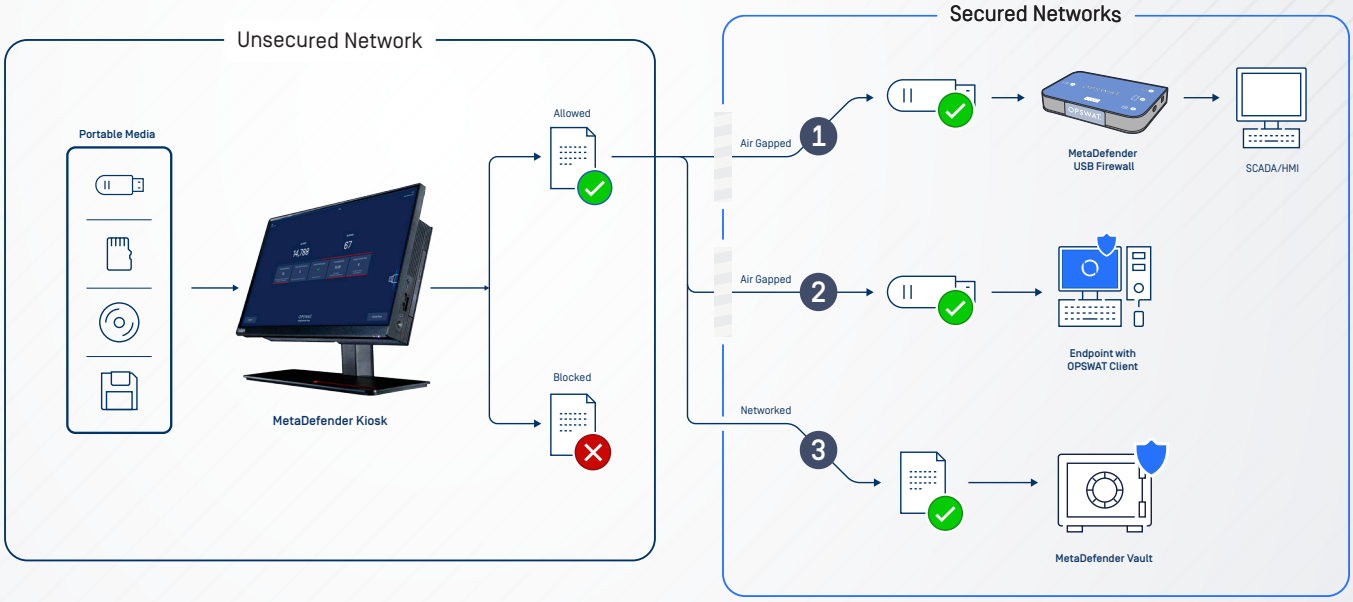
MetaDefender Kiosk enables you to authorize, authenticate, secure, and trust both the portable media and the hosted files entering and existing your facility.

To adapt to any facility layout, the 1000 series Kiosk can be: ❶ Secured to a freestanding podium, ❷ Mounted to its optional stand, or ❸ Mounted on on a wall.



Ideal in Any Cross-Domain Workflow

Integrations with OPSWAT products make MetaDefender Kiosk easy to adapt to your secured network requirements.



Potential Deployment Options

1 Deployed with USB Firewall

"No installation Required" USB Firewall that enforces a "closed loop" where only files that have been authenticated and/or sanitized by the Kiosk can enter your critical infrastructure.

2 Deployed with OPSWAT Client

OPSWAT's Policy Enforcement client software is fully integrated with the Kiosk functionality to enforce authentication and sanitization of files prior to authorized entry into your critical infrastructure.

3 Deployed with MetaDefender Vault

The OPSWAT Vault software integrates with MetaDefender Kiosk via a network to provide parallel processing and ticket based secure access to files from inside the facility. Additional integrated capabilities include tiered supervisory approvals for file access and transfer as well as secured bidirectional file transfer back to the Kiosk for authenticated, authorized, verified, redacted, and approved data extraction from critical infrastructure systems.

Key Features & Benefits

MetaDefender Kiosk lets you trust all portable media that enter or exit your facility.

MetaDefender Kiosk acts as a digital security guard—inspecting all media for malware, vulnerabilities, and sensitive data, and preventing unauthorized media and potential malware from accessing your environment.

20+ media types

2x USB Type A, 15-in-1 card reader, CD/DVD drive, and 3.5" diskette

Multiple File System & Virtual Disk Support

- FAT, NTFS, Ext, HFS+, and APFS
- VHD and VMDK

Manage All MetaDefender Products from One Plane of Glass

Includes Centralized Management, Dashboards, and Reporting for multi-Kiosk installations.

File Storage & Data Diode Integration

Seamless with MetaDefender Vault and best-in-class data diodes for secure storage and transmittal.

Secure Erase

Wipe portable media completely clean, before loading approved content.

OPSWAT Security Technologies

User-configurable workflows for Content Disarm and Reconstruction (CDR), Secure Data Extraction, and Data Loss Prevention (DLP).

Whitelist Support

Supports whitelisting by vendor, model, and ID.

Auditable and Customized Workflows

for file scanning, analysis, quarantine, sanitization, sandboxing, and transfer.

Media Validation Agent

Digital signature validation is conducted every time media is inserted, blocking access by unscanned media.

Multiple Authentication Methods

Including Active Directory integration.

Localizable Interface

International and custom language templates

Security and Compliance Solutions by OPSWAT

Network and Systems Protection, Data at Rest, Data in Transit, Policy Management, and Data Privacy

OPSWAT provides cloud, hybrid, and local solutions to enable standards and regulatory compliance. Their many solutions scopes includes Zero Trust Networking, Software Defined Perimeters, Network Access Control, Email Protection, Policy Enforcement, Systems and Endpoint Protection, Data Transfer and Data at Rest Authorization and Protection, and more. Compliance scopes include ISA/IEC 62443, HIPAA, AWIA, GDPR, HITRUST, ISO/IEC 2700X and others.

Critical Infrastructure needs OPSWAT Solutions

OPSWAT protects over a thousand companies from Ransomware and other critical infrastructure dangers. Protect your company now and talk to our experts.

OPSWAT.
Trust no file. Trust no device.

Trusted by over 1,000 large enterprises and government organizations worldwide

OPSWAT protects critical infrastructure. Our goal is to eliminate malware and zero-day attacks. We believe that every file and every device pose a threat. Threats must be addressed at all locations at all times—at entries, at exits, and at rest. Our products focus on threat prevention and process creation for secure data transfer and safe device access. The result is productive systems that minimize risks of compromise. That's why 98% of U.S. nuclear power facilities trust OPSWAT for cybersecurity and compliance.

OPSWAT.com/contact