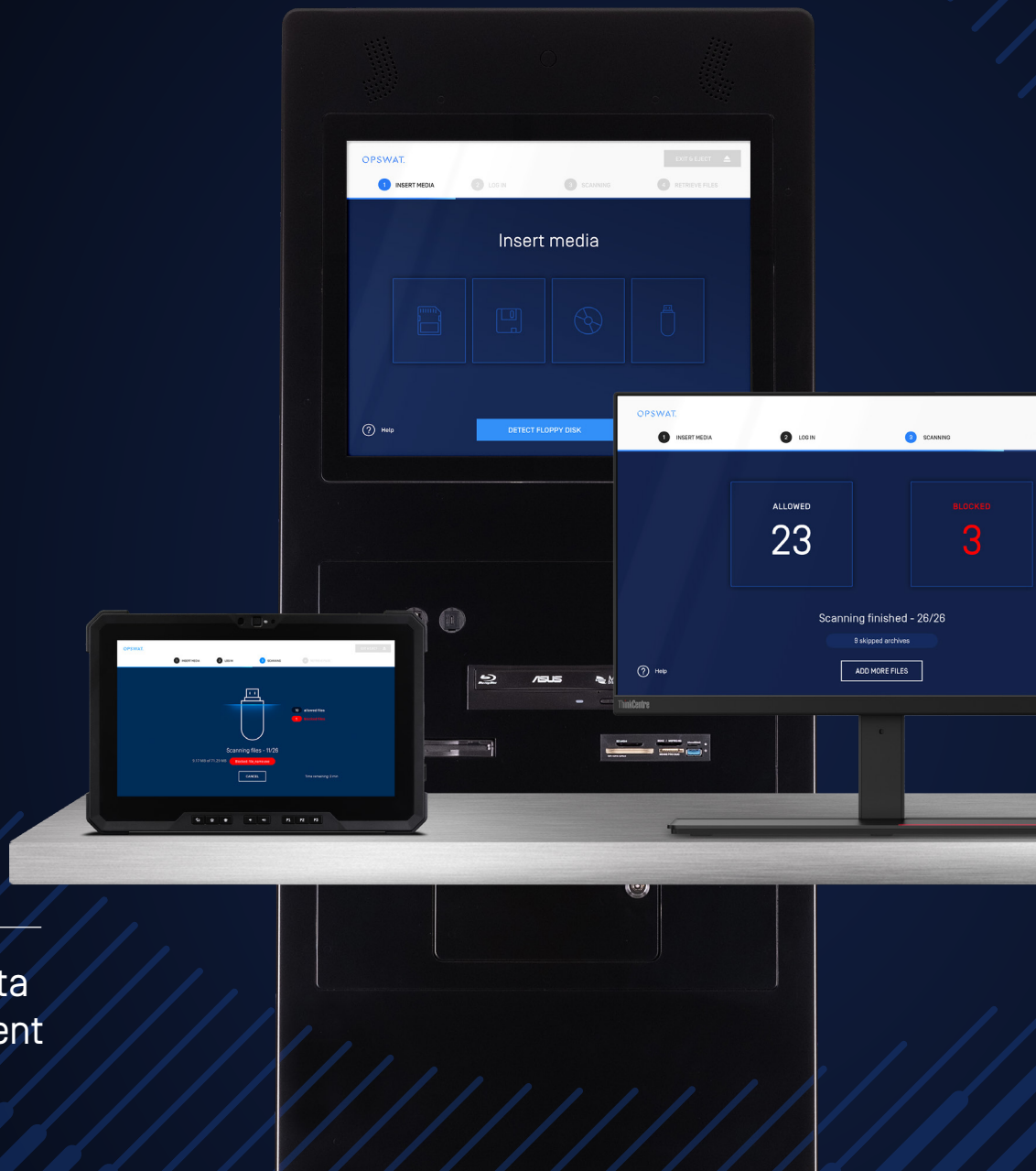


OPSWAT.

# METADEFENDER KIOSK™

Globally Trusted Removable  
Media Security



Protect the Flow of Data  
Into Your OT Environment



# Protecting Your Critical Network and Assets Against Removable Media Threats

Any time portable media accesses secure environments, critical infrastructure risks exposure to external threats.

Software updates, reporting, audits, and more all require external data sources—and as threats evolve, so too must the means necessary to protect your organization from them.

Additionally, you need a solution that stays compliant with regulations that are put into place to enforce security standards.





# OPSWAT. METADEFENDER KIOSK SERIES

Scan 20+ devices from  
USB-C to diskettes

Secure PLCs, HMIs, and  
engineering stations

Protect against vulnerabilities, zero-  
day threats, malware, and more

Enforce policies to ensure all devices  
are scanned before use

CD  
DVD  
Blu-Ray

3.5" Diskette

USB-A 3.0  
USB-C

SD  
Micro SD  
Compact Flash

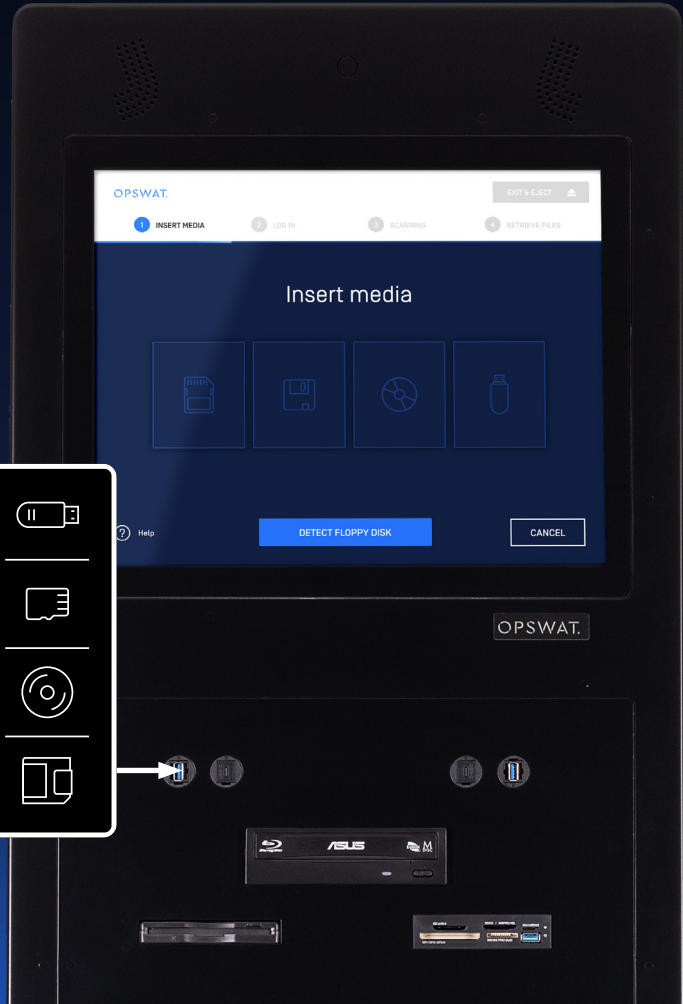


# Secure Your Critical Network

Control the flow of data into and out of your organization in three simple steps.

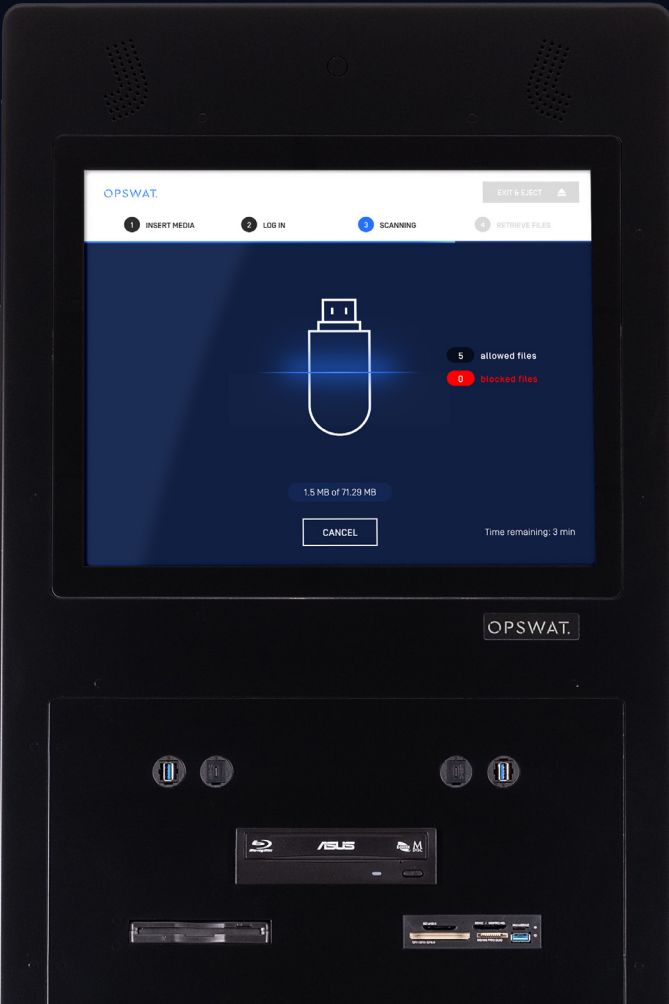
## 1 Insert Media

MetaDefender Kiosk accepts 20+ media types.



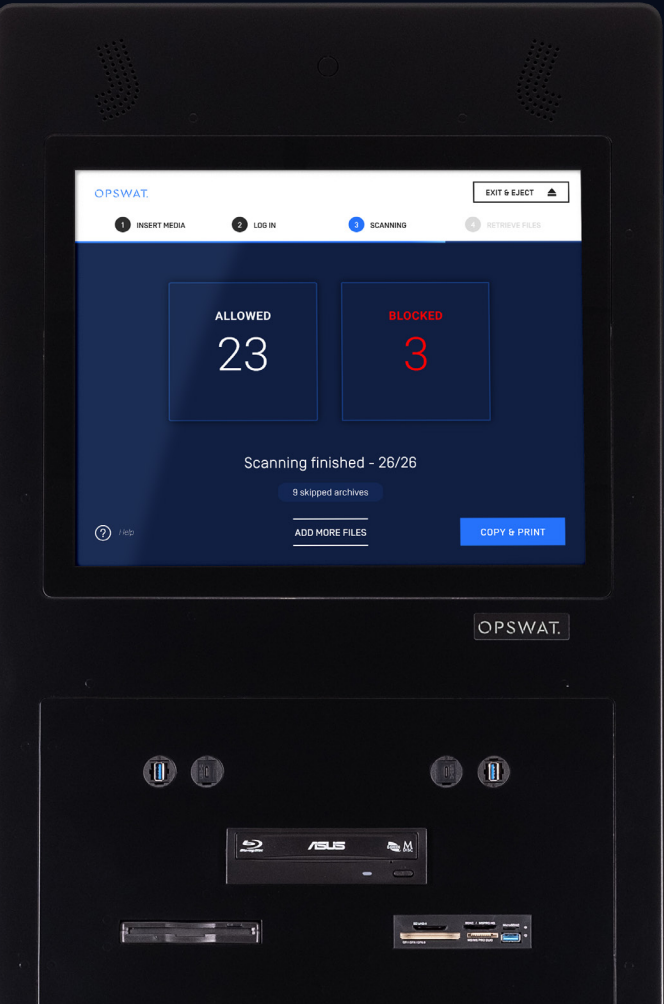
## 2 Process Files

MetaDefender Kiosk works as a media scanning station to check files from the device.



## 3 Review Results

A detailed report will be generated after the scan is completed.



# Keep it Protected



Advanced detection multiscanning with 30+ engines



File vulnerability check



Country of origin detection



Deep content disarm and reconstruction (CDR)



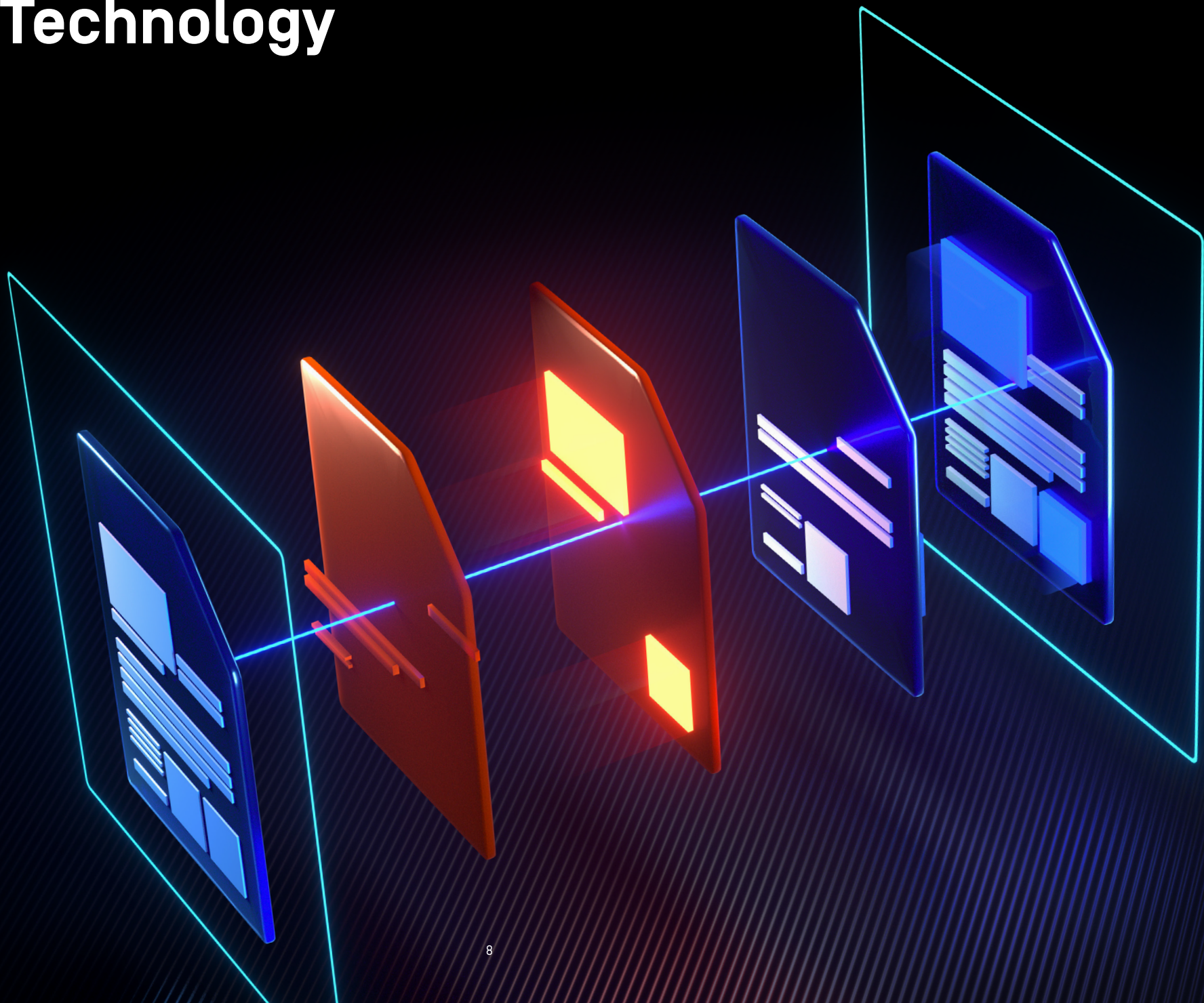
Data loss prevention (DLP)



Enforcement of scanning policies and visitor management



# Industry Leading Patented Technology



## Deep Content Disarm and Reconstruction

Deep CDR prevents known and unknown file-based threats, protecting against malware and zero-day attacks. Deep CDR regenerates safe, usable files and supports hundreds of file types.



## Vulnerability Detection

OPSWAT's File-Based Vulnerability Assessment technology detects application and file-based vulnerabilities before they are installed.



## Country of Origin Detection

Many organizations are experiencing heightened requirements to examine the supply chain security of software running on their systems, particularly ones from foreign adversaries. Automate binary scans on a target system and determine in which country the publisher resides.



## Multiscanning

Advanced threat detection and prevention technology increases detection rates and decreases outbreak detection times by simultaneously scanning files using 30+ anti-malware engines.





# Trust No File. Trust No Device.

- Enforce scanning security policies across your organization on premises and from the cloud
- Enhance the overall security and functionality of your air gap
- Improve visibility and management of removable devices
- Support a broad range of compliance requirement and regulations such as NERC CIP, NIST 800-53, and more

## A Digital Security Guard

MetaDefender Kiosk is available in multiple form factors to meet your portable media security needs and support compliance requirements including NERC CIP, NIST 800-53, and beyond.

It supports a variety of removable media types, including CD/DVD, 3.5" diskettes, flash memory cards, mobile devices, and USBs—even when encrypted—in an easy-to-use media scanning station. Once media is inserted, MetaDefender Kiosk immediately scans for malware, vulnerabilities, and sensitive data, ensuring that the media is safe to interact with your critical network.

## A Safeguard Against Unscanned Media

When data is scanned by MetaDefender Kiosk, it's given a digital signature to validate that it has been scanned. OPSWAT's Media Validation Agent works in turn with Kiosk, installed on Windows-based endpoints blocking all removable media missing the validation signature from interacting with devices on your network.

## Cybersecurity to Fit Your Needs

MetaDefender Kiosk is available in multiple configurations, each designed to meet the needs of critical infrastructure networks of various sizes, locations, and even those on the go in some of the harshest environments.



# Which Kiosk is Right for You?

**L-Series**

- Linux Operating System
- Enable automatic updates when few or no IT experts are on-site
- Turnkey quick to deploy and manage
- Fully hardened out of the box

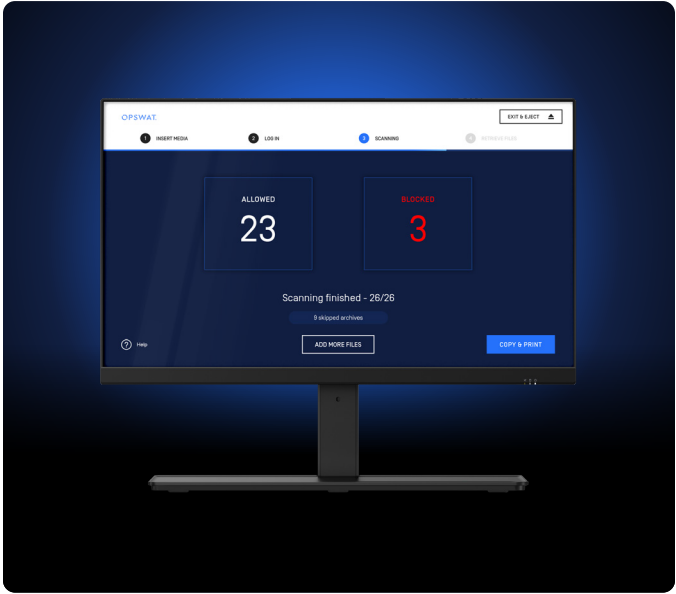
**K-Series**

- Windows Operating System
- Most comprehensive solution on the market
- Wide variety and number of engines available
- Visitor management with Active Directory support
- Support for the broadest range of removable media types



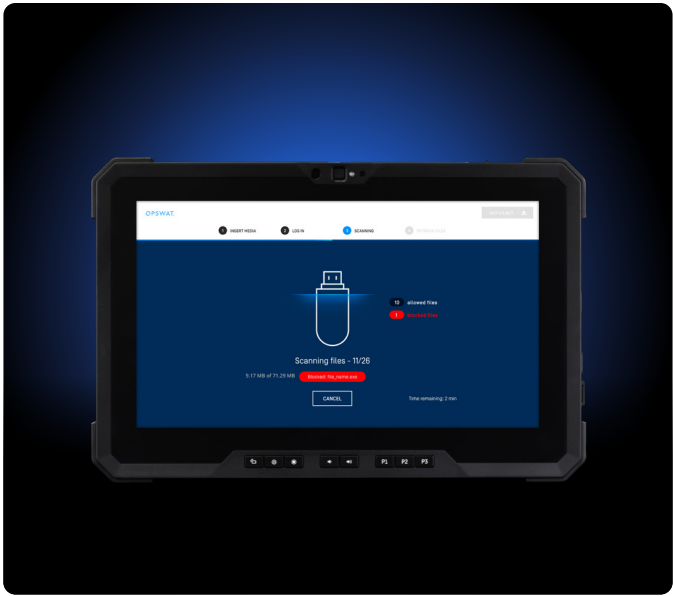
MetaDefender Kiosk  
**L1001**

The OPSWAT MetaDefender Kiosk L1001 is a Linux Kiosk providing enhanced security, high performance, and simplified maintenance. This all-in-one solution is a fully integrated appliance for critical infrastructure environments.



MetaDefender Kiosk  
**K1001**

The OPSWAT MetaDefender Kiosk K1001 is designed for desktop use or to be mounted on a wall or stand. This Kiosk occupies a smaller footprint providing removable media scanning where you need it.



MetaDefender Mobile Kiosk  
**K2100**

The OPSWAT MetaDefender Mobile Kiosk K2100 is a portable, powerful, and ultra-rugged solution designed for use in the harshest environments. The K2100 is ruggedized to military standards featuring a glove-touch screen and water resistance certifications allowing the secure use of portable and removable media in all conditions and environments.



MetaDefender Kiosk  
**K3001**

The OPSWAT MetaDefender Kiosk K3001 is our largest Kiosk capable of scanning the broadest range of media types. The K3001 is built with an industrial touchscreen and strong metal enclosure.

Built for a strong presence and establishing a culture of cybersecurity awareness at your site, the K3001 can be custom branded with your organization's logo or colors.

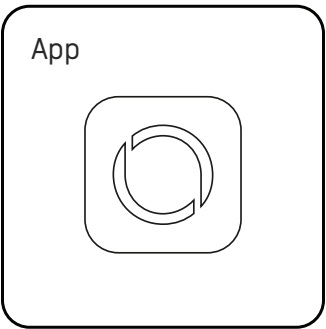
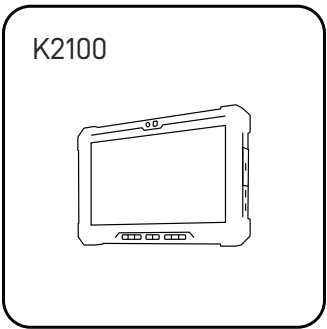
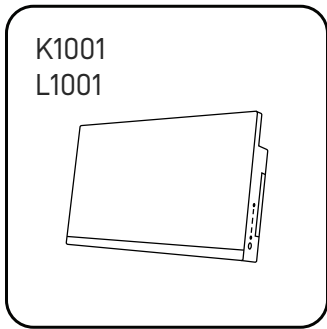
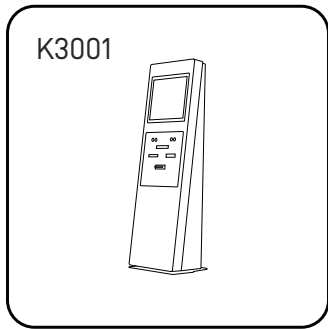
The K3001 can also be equipped with a printer to support compliance requirements.



MetaDefender Kiosk  
**App**

The MetaDefender Kiosk App is designed to be deployed on approved hardware providing additional flexibility for deployments.





Form Factor

**Free Standing**  
Ruggedized  
2mm high grade steel casing  
Tamper-resistant  
Powder Coated

**Table Stand**  
**Floor Stand**  
**Wall Mount**

**Mobile Tablet**  
Ultra-ruggedized  
**Floor Stand**  
**Dock**  
**Wall Mount**

**Application**  
Windows Operating System

Use Cases

**Larger presence**  
**More varied media types**  
**Customizable color and design**

**Smaller footprint**

**Portable**  
**Glove capable touchscreen**  
**For demanding environments**  
-20 to 145°F  
-29 to 63°C

**Flexible**  
Can be installed on a variety of endpoints

Media Support

**USB**  
2x Type-C  
2x Type-A  
**15-in-1 card reader**  
Secure Digital  
Micro SD  
Compact Flash  
**CD/DVD/Blu-Ray**  
**3.5" diskette**

**USB**  
1x Type-C  
1x Type-A  
**3-in-1 card reader**  
**CD/DVD**

**USB**  
1x Type-C  
1x Type-A  
**Micro SD**

Varies based on hardware



# Strengthen Your Cybersecurity Posture with the OPSWAT Suite of Solutions

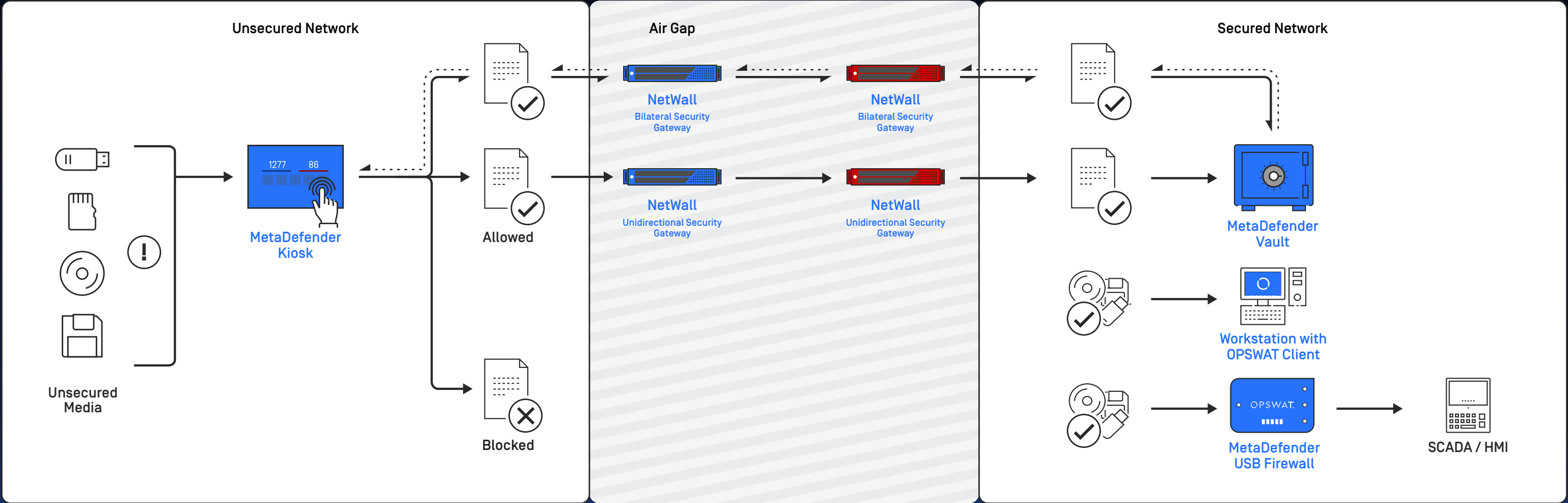
The best form of protection against any cyberthreat vector is a multi-layered, defense-in-depth approach. Deploy our kiosks with purpose-built technology to create an end-to-end enforceable solution that bolsters your cybersecurity posture.

**NetWall Unidirectional Security Gateway (USG)**  
Enable lossless, unidirectional data communications and secure transfer of software updates and other files to the protected domain.

**OPSWAT Client**  
Authenticate files and authorize access to prevent threat actors from modifying or introducing compromises files after validation at the OPSWAT kiosk. Centralize management and reporting of multiple MetaDefender solutions and Kiosk installations from a single pane-of-glass.

**MetaDefender Vault**  
Enhance the efficiency of OT Solutions with the parallel processing of files during client facility check-in and retrieval. Secured and audited bidirectional file transfers—with tiered supervisory approval—enables authenticated, authorized, and verified data extraction from critical networks. Enforce data loss prevention (DLP) policies during Vault-to-Kiosk transfers to proactively redact files found to contain protected data.

**MetaDefender USB Firewall**  
Enforce file authentication and media protection in isolated networks without any software installation.





GET STARTED

# Are you ready to put MetaDefender Kiosk on the front lines of your removable media security strategy?

Talk to one of our experts today.

Scan the QR code or visit us at:

[opswat.com/get-started](https://opswat.com/get-started)

[sales@opswat.com](mailto:sales@opswat.com)



**OPSWAT.**

Protecting the World's Critical Infrastructure

OPSWAT is an industry leader in critical infrastructure protection (CIP). 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 entry, at exit, 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 risk of compromise. That's why 98% of U.S. nuclear power facilities trust OPSWAT for cybersecurity and compliance.