

OPSWAT.

MetaDefender® for Secure Networks

Secure File Transfer Solutions

MetaDefender is used by organizations that require the highest level of security, including critical infrastructure, government agencies, and financial institutions, to enable a secure way to get files in and out of an organization, and prevent cyber security threats.

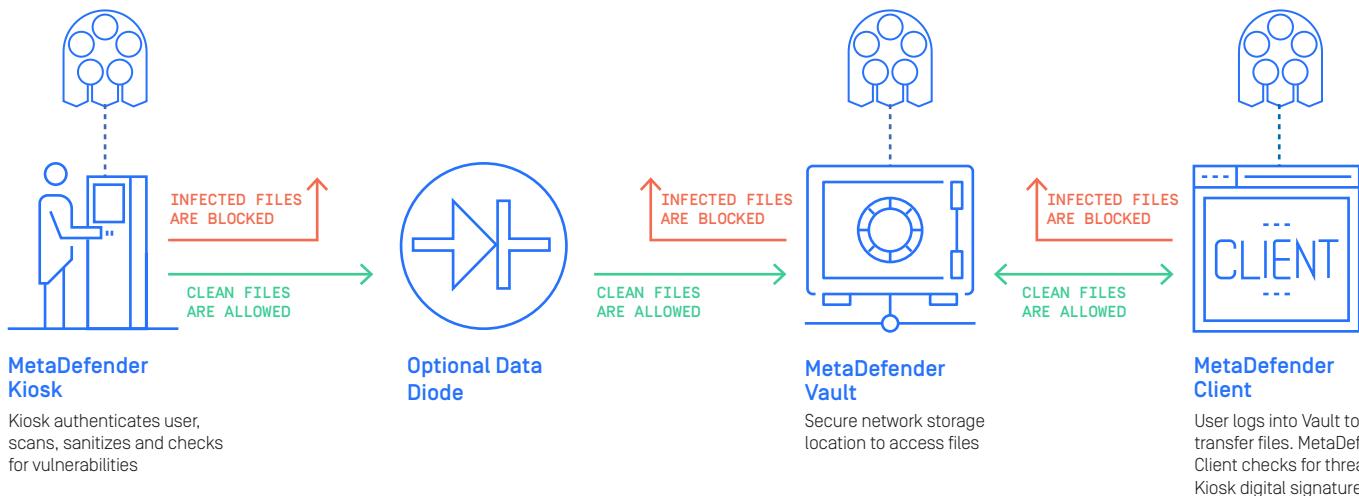
Maintaining isolated or air-gapped networks is challenging, due to stringent uptime requirements, regulations, and the risk of malware introduction via portable devices and media like USB drives and cell phones. In 2015, an attack on Ukraine's power grid left 700,000 people without power. How can critical infrastructure facilities ensure that malicious files stay out while still allowing portable media devices to be used?

MetaDefender enables you to create a secure end-to-end process for transferring files to and from your critical networks.

- Defend against attacks introduced through USB and other portable devices and media like SD Cards, CD/DVDs, and cell phones.
- Create granular security policies for file types and security processing based on users and roles.
- Enable visibility and auditing of file transfers.
- Prevent known and unknown threats using multi-scanning, data sanitization (CDR), and vulnerability detection.



Secure File Transfer



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.

MetaDefender Kiosk can leverage any of MetaDefender's core defense technologies but also includes product specific features such as User Interface [UI] localization, data diode integration, digital certificate signing, and file hash verification. MetaDefender Kiosk is used by the vast majority of US nuclear operators, making MetaDefender the leading hardware-based portable media detection and file sanitization solution for the US nuclear industry.

Features

- Customizable, multi-language user interface
- Seamlessly integrates with MetaDefender Vault
- Protect against threats in portable devices and media, including USB drives, SD cards, CD/DVDs, and cell phones
- Can digitally sign permitted files and media
- Ability to block or quarantine malicious files
- Support for encrypted media devices and device white listing
- Supports configurable workflows based on users or roles
- Provides enterprise-wide visibility into all devices accessing local networks and cloud applications, allowing for easy identification of security and compliance issues as well as detailed device information



DATA ENTERING ORGANIZATION

MetaDefender Client

Additional Threat Protection for the Endpoint

MetaDefender Client protects endpoints in your organization from USB-based threats. Portable media can be scanned and sanitized using MetaDefender's industry-leading threat prevention technology, supplementing existing antivirus and endpoint protection. MetaDefender Client can also verify the digital signatures that MetaDefender Kiosk has applied. This saves time and ensures that only files signed by the Kiosk at the perimeter can be used by the endpoint.

Features

- Secures the endpoint against portable media and device based attacks
- Blocks access to USB drives and other portable media devices until security conditions are met
- Supports the validation of digital signatures applied by MetaDefender Kiosk
- Provides a second layer of defense against threats by scanning the system with multiple anti-malware engines

MetaDefender Vault

Secure File Transfer and Storage

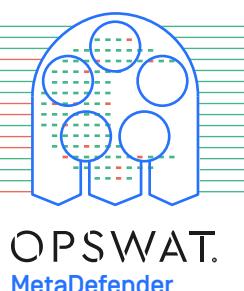
MetaDefender Vault is a protected network storage location that can sit anywhere on your network without requiring any hardware, and can be used with MetaDefender Kiosk for storing checked and processed files. The solution enables the transfer of secure files into and out of isolated networks, without the need to transport portable media into a facility. Guests or users can access all certified and checked files from MetaDefender Vault while leaving all USB drives at the perimeter. Checkpoints across isolated networks can be established strategically for visibility, audits, and malware prevention wherever necessary.

Features

- Easy installation and integration with MetaDefender Kiosk and Client
- Files can be transferred using a browser, so no special client software is required
- Can keep files locked for specific time periods to prevent outbreaks from time-based malware
- Administrator roles and granular logging for improved auditability
- Supervisor approval option places a human in the loop for reviewing scan results before unlocking uploaded files

The screenshot shows the OPSWAT MetaDefender Vault interface. The left sidebar has a dark theme with white text and icons. It includes sections for 'Files' (selected), 'Pending Approval', 'My Files', 'Users', 'Outbreak Prevention', 'Supervisor Approval' (which is checked), 'Settings', 'Notifications', and 'Audit'. A search bar at the top right says 'Search for filename'. The main area lists files with columns for 'FILENAME' and 'SCAN RESULT'. Some files are marked as 'Infected'. The interface is labeled 'Version 1.2.1.4114' at the bottom right. A note at the bottom says 'Showing 28 out of 28'.

FILENAME	SCAN RESULT
calendar.ics	Metadefender Core
mdicapsrv-4.2.3-1-support-1523484097.tar.gz	Processing
Mon_Apr_9_10-36-41_2018_allowed.zip	Metadefender Core
Mon_Apr_9_10-10-19_2018_allowed.zip	No Threat Detected
Mon_Apr_9_10-09-30_2018_allowed.zip	No Threat Detected
Mon_Apr_9_10-05-52_2018_allowed.zip	No Threat Detected
Mon_Apr_9_10-01-11_2018_allowed.zip	No Threat Detected
SOW for SCD Proxy EOL flash replacement.do...	Infected
nsResize.dll	Infected
FileHistory_1517299200_1517355331.csv	No Threat Detected
FileHistory_1517299200_1517355331 (1).csv	Not Scanned
IMG_0320 (1).jpg	No Threat Detected
Frank.jpg	No Threat Detected
IMG_0320.jpg	No Threat Detected
Fri_Apr_6_08-04-40_2018_allowed.zip	No Threat Detected
OESIS_V4_VMOD_SRC_4.3.2.493.tar	No Threat Detected
Standard MD 2017.pptx	No Threat Detected
OPSWAT 2018 Corporate Overview_January 2...	No Threat Detected



OPSWAT
MetaDefender

MetaDefender Benefits

Multi-Scanning - Scan with over 30 anti-malware engines using signatures, heuristics, and machine learning technology for the highest and earliest detection of known and unknown threats.

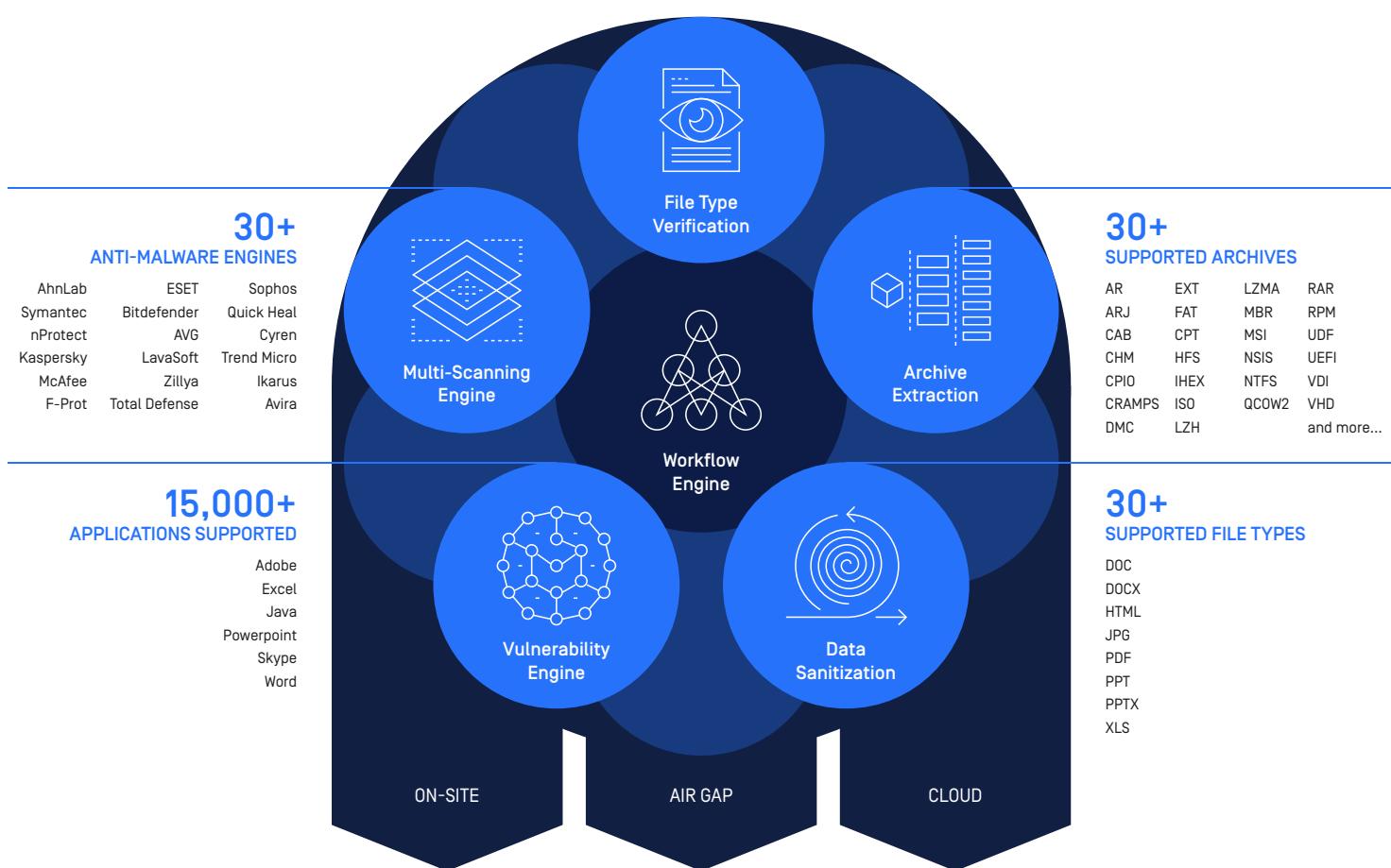
Data Sanitization (CDR) - Disarm over 30 common file types, and reconstruct each file ensuring full usability with safe content.

Vulnerability Scanning - Detect known vulnerabilities in over 15,000 software applications using over 1 billion hashes.

File Handling Options - Block, quarantine, or digitally sign and verify files.

File Type Verification - Ability to verify the file type and only allow approved file types to be copied over.

MetaDefender Architecture



OPSWAT.

Trust no file. Trust no device.

www.opswat.com