

OPSWAT.

Protecting the World's Critical Infrastructure

Cybersecurity Solutions Built for Any Critical Network

OPSWAT.

Industry-Trusted Portfolio

From IT to OT and everything in between, OPSWAT's products and solutions can be integrated or deployed across every attack surface, providing unrivaled and simple to use, end-to-end cybersecurity at every level—from the cloud to the plant floor.

opswat.com/products

Software Solutions

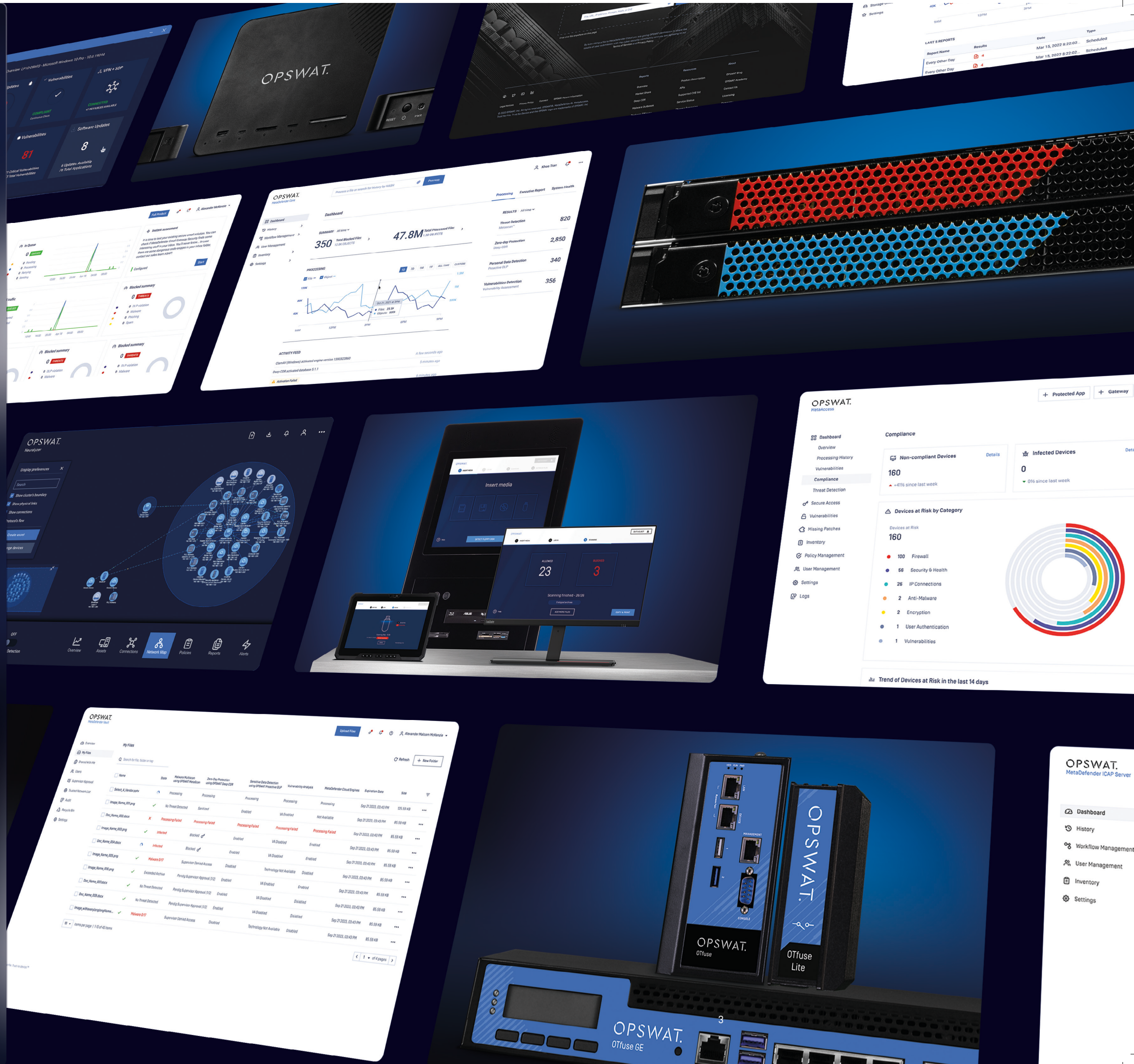
- MetaDefender Core
- MetaDefender ICAP Server
- MetaDefender Managed File Transfer
- MetaDefender Storage Security
- MetaDefender Email Security
- MetaDefender Sandbox
- MetaDefender IT Access
- MetaDefender Network Control Access

Hardware Solutions

- MetaDefender Kiosk
- MetaDefender Media Firewall
- MetaDefender Drive
- MetaDefender NetWall
- MetaDefender OT Security
- MetaDefender Industrial Firewall
- MetaDefender OT Access

OPSWAT Technologies

- Deeo CDR
- Multiscanning
- Proactive DLP
- Adaptive Sandbox

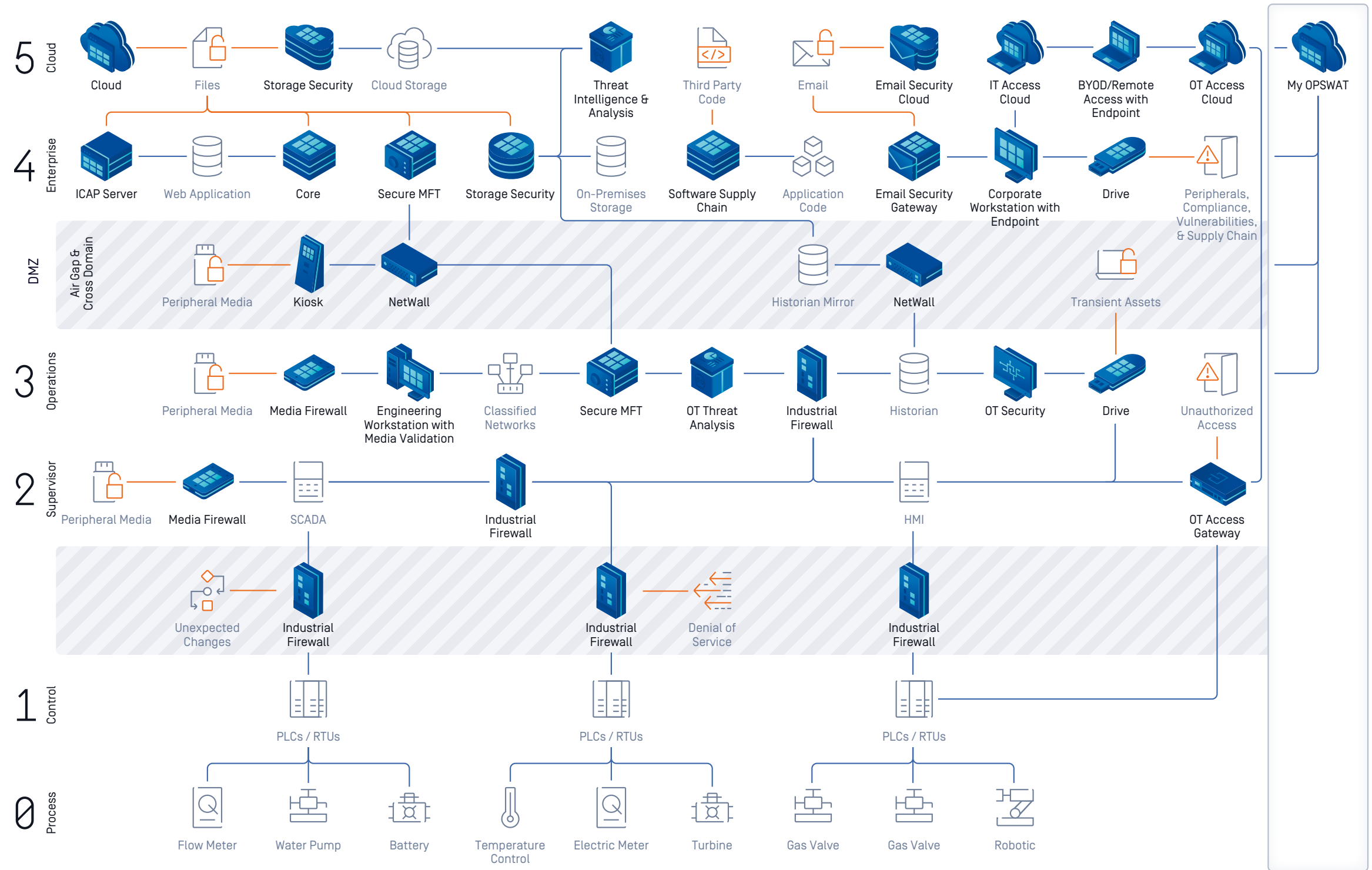


- Dashboard
- History
- Workflow Management
- User Management
- Inventory
- Settings

OPSWAT.

The MetaDefender™ Platform

OPSWAT has spent the last 20 years evolving our end-to-end cybersecurity platform to give public and private sector organizations the critical advantage needed to protect the most complex networks. Built on our "Trust no file. Trust no device."™ philosophy and integrated by design, we're solving our customers' challenges as their singular point of cybersecurity, creating critical lines of defense across every level of their infrastructure.



MetaDefender™ Core

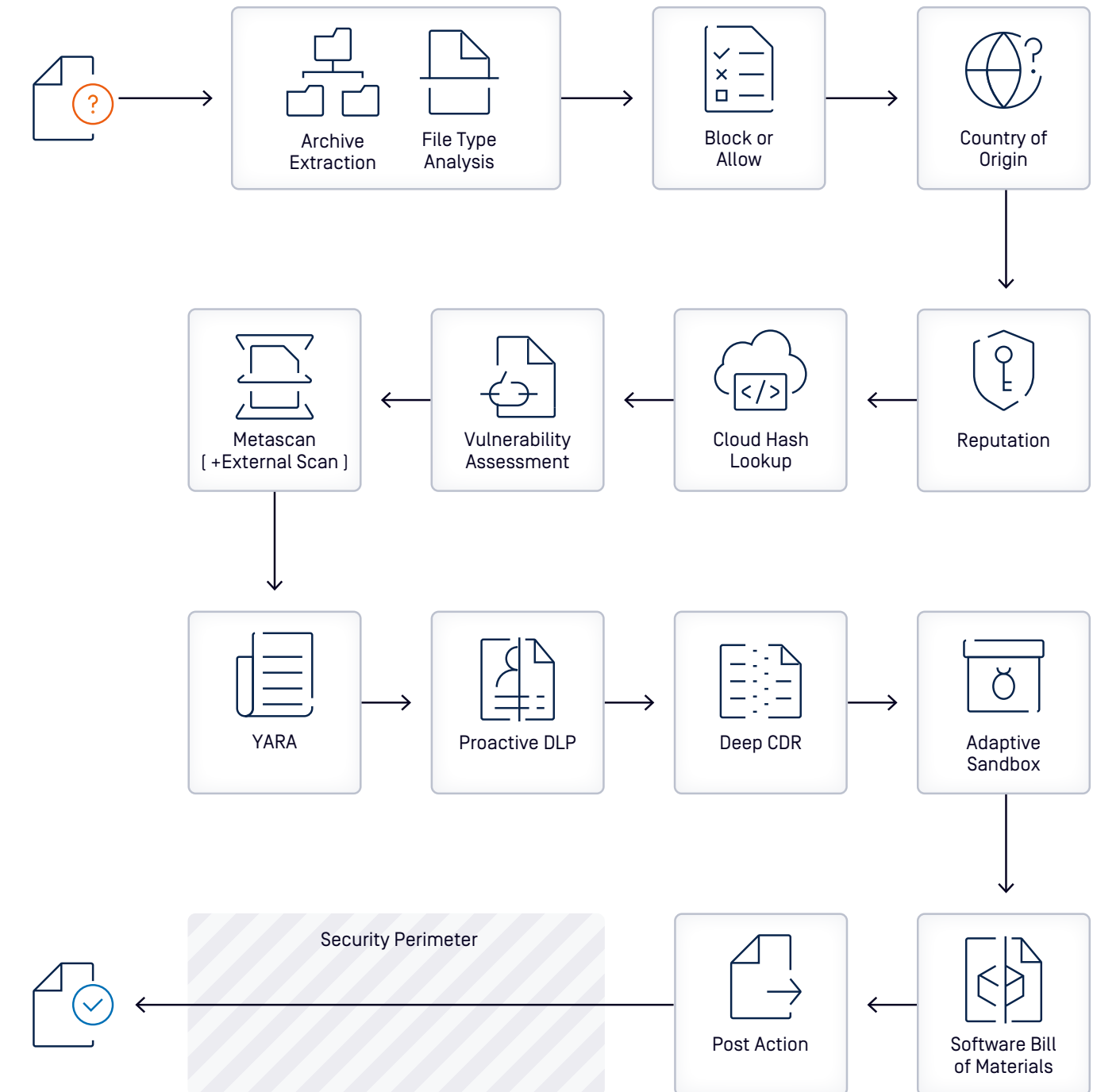
Advanced Threat Prevention Solution

With the growing threat of sophisticated, multi-layered, and zero-day attacks, business can no longer rely solely on detection-based cybersecurity systems to provide adequate protection for their most valuable business assets. Enterprises need to take more comprehensive and preventive approaches to combat advanced file-borne attacks.

MetaDefender Core integrates advanced malware prevention and detection capabilities into your existing IT solutions and infrastructure to handle common attack vectors by securing web portals from malicious file attacks, augmenting cybersecurity products, and developing malware analysis systems that adhere to company-specific policies.



MetaDefender Core Workflow



Why MetaDefender Core

Risk Mitigation

Proactively safeguard critical infrastructure and prevent potential threats that may have slipped past conventional defenses.

Data Protection

Ensure the security of sensitive data and confidential information by securing files in transit or at rest from file-borne attacks.

Versatile Deployment

Easily deploy on Windows or Linux servers within your environment, including air-gapped networks, or opt for our SaaS solution through MetaDefender Cloud.

Seamless Integration

Seamlessly integrate into your existing environment with support for multiple programming languages via REST API.

Cost-Effective Maintenance

Achieve low total cost of ownership (TCO) with centralized management for ongoing maintenance, saving valuable resources.

Flexible Containerization

Simplify integration and maintenance with flexible deployment in containerization environments, reducing TCO, addressing potential conflicts from hidden dependencies, and enabling scalability across various platforms and operating systems.

Key Features



Prevent Zero-Day and Advanced Evasive Malware

Deep CDR is a preventative technology that removes potentially malicious content from over 150+ file types. It validates, disarms, and regenerates safe-to-use files, eliminating advanced threats like APTs, zero-day attacks, and obfuscated malware before delivery.



Achieve Over 99% Threat Detection Accuracy

Multiscanning technology leverages 30+ leading anti-malware engines to proactively detect over 99% of malware threats. It combines signatures, heuristic analysis, and machine learning to identify file-borne threats.



Detect Application and File-Based Vulnerabilities

File-Based Vulnerability Assessment technology scans and analyzes binaries and installers to detect known application vulnerabilities before they are executed on endpoint devices, including IoT devices.



Adaptive Threat Analysis

Adaptive Sandbox is an emulation-based sandbox featuring threat agnostic analysis of files and URLs, identifying actionable indicators of compromise (IOCs) for incident response.



Prevent Regulatory Compliance Violations & Detect Adult Content

Proactive DLP prevents sensitive and confidential information in 110+ file types from leaving or entering the company's systems by content-checking files before they are transferred. This helps enterprises meet regulatory requirements like HIPAA, PCI-DSS and GDPR. Proactive DLP also detects adult content in images and offensive language in text using OCR, machine learning and AI technologies.



100+ File Conversion Options

Use the file type conversion functionality to flatten files to fewer complex formats.



Generate SBOM (Software Bill of Materials)

Generating SBOMs secures software supply chains by providing comprehensive component inventories for source code and containers.



Workflow Engine

Create multiple workflows to handle different security policies based on users and file sources.



Archive Extraction

Scan over 30 types of compressed files. Archive handling options are configurable, and encrypted archives are supported.



File Type Verification

Determine the actual file type based on the content of the file, not unreliable extensions, which can easily be spoofed.



Faster False Positives Remediation

Reputation Engine matches file hashes against database of known good and bad files and leverages advanced analyses to remediate false positives faster.

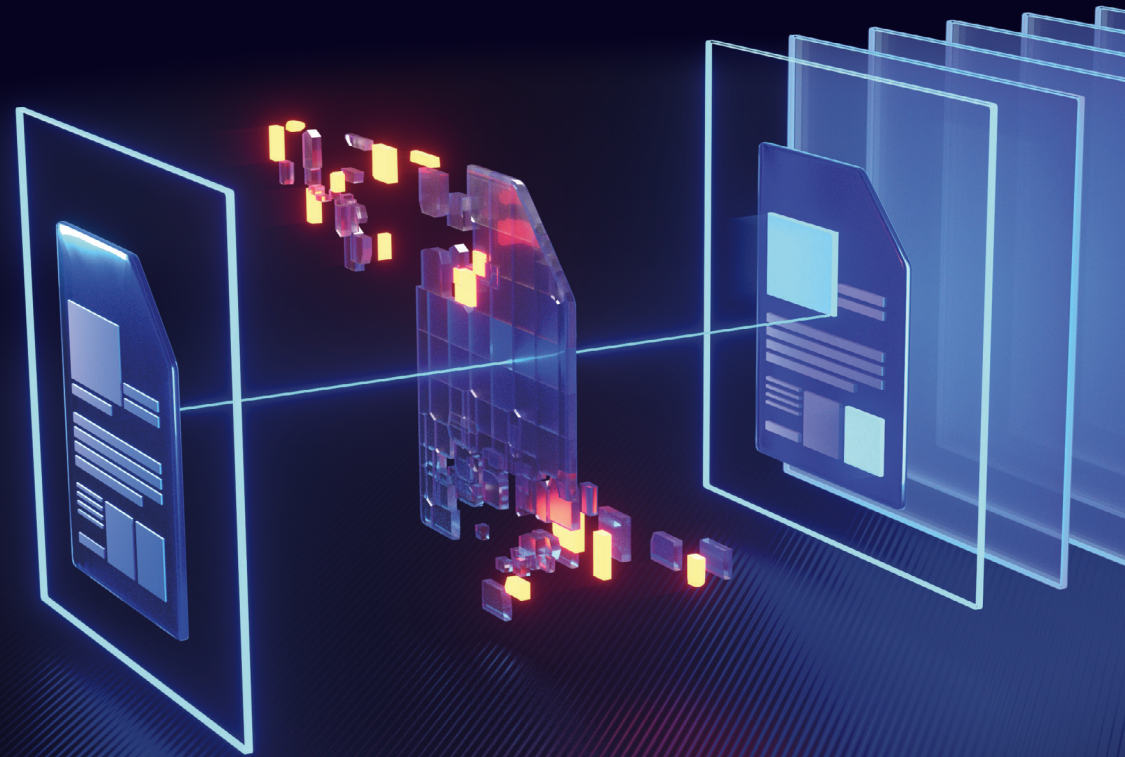


Country of Origin

Detect the geographic source of uploaded files including PE, MSI, and self-extract file types. By analyzing digital fingerprints and metadata, it can identify restricted locations and vendors. This enables automated filtering that blocks unauthorized access to sensitive data while ensuring compliance with data regulations across regions.

Deep CDR

Deep Content Disarm and Reconstruction (Deep CDR) technology protects from known and unknown file-borne threats by sanitizing and reconstructing files. Any possible embedded threats are neutralized while maintaining full usability with safe content.

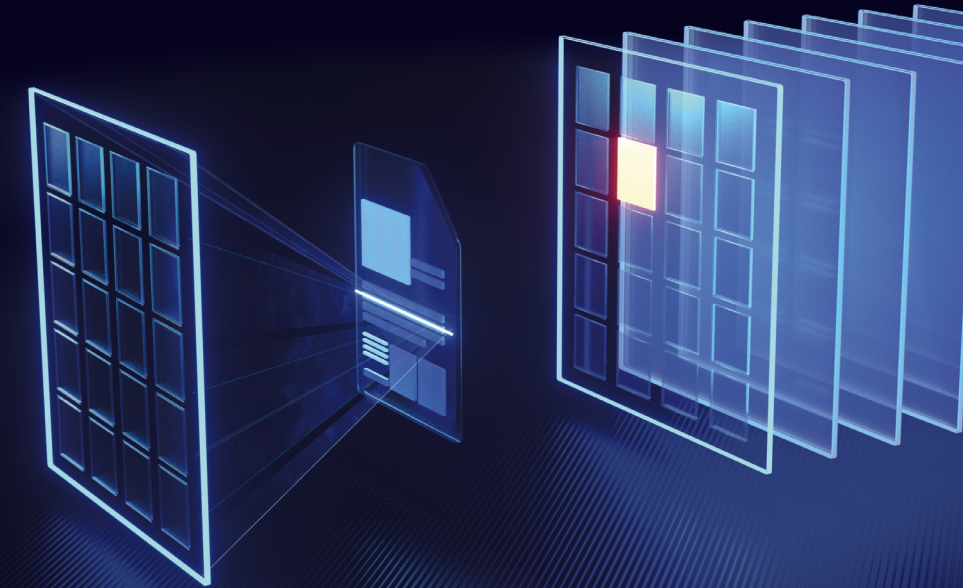


Industry-Leading Patented Technology

Our comprehensive platform is underpinned by patented foundational technologies that are trusted worldwide to secure critical networks. Purpose-built to protect critical environments, these technologies provide industry-leading advanced prevention against known and unknown threats, zero-day attacks, traditional malware, AI malware, and more.

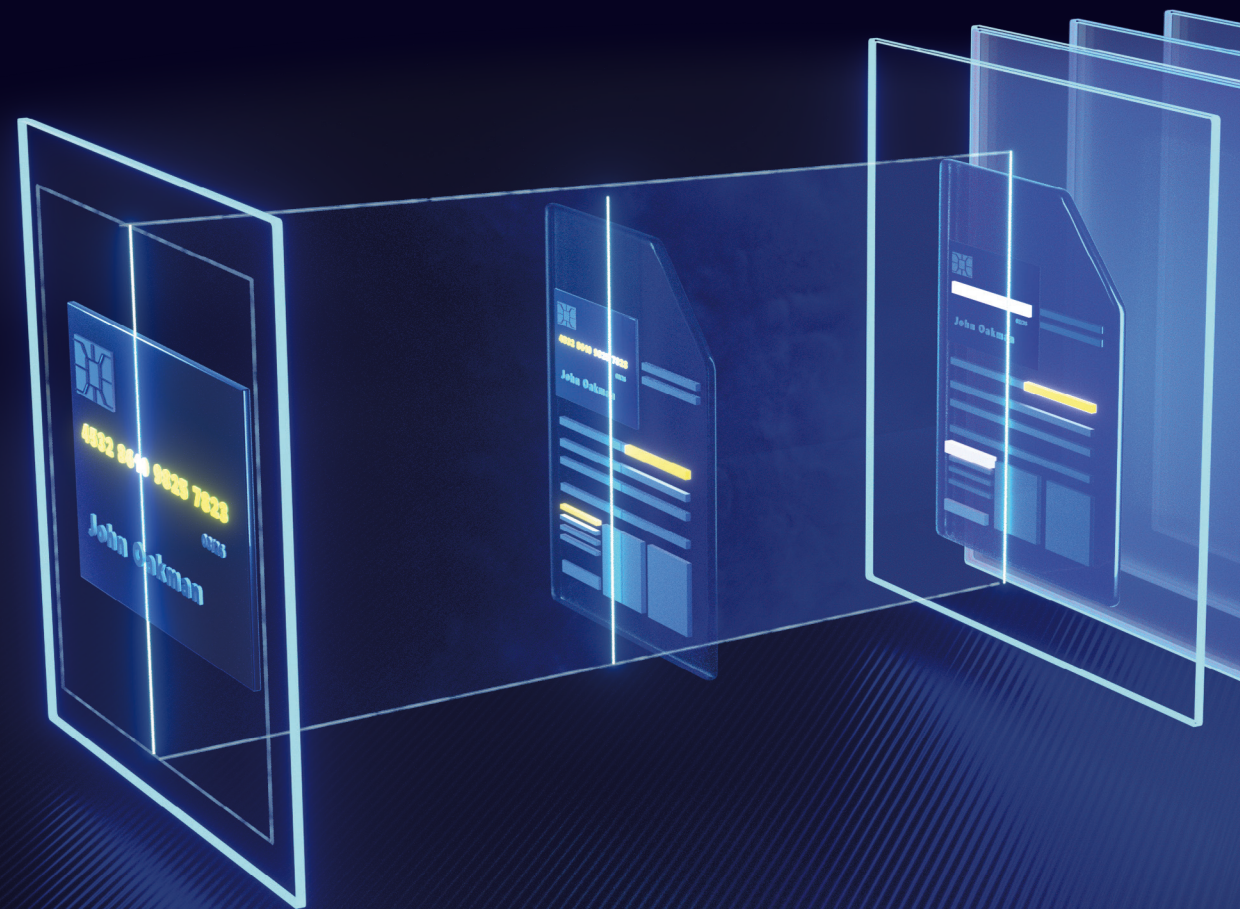
Multiscanning

Multiscanning technology leverages 30+ leading anti-malware engines and proactively detects over 99% of malware by using signatures, heuristics, and machine learning. This significantly improves detection of known threats and provides the earliest protection against malware outbreaks.



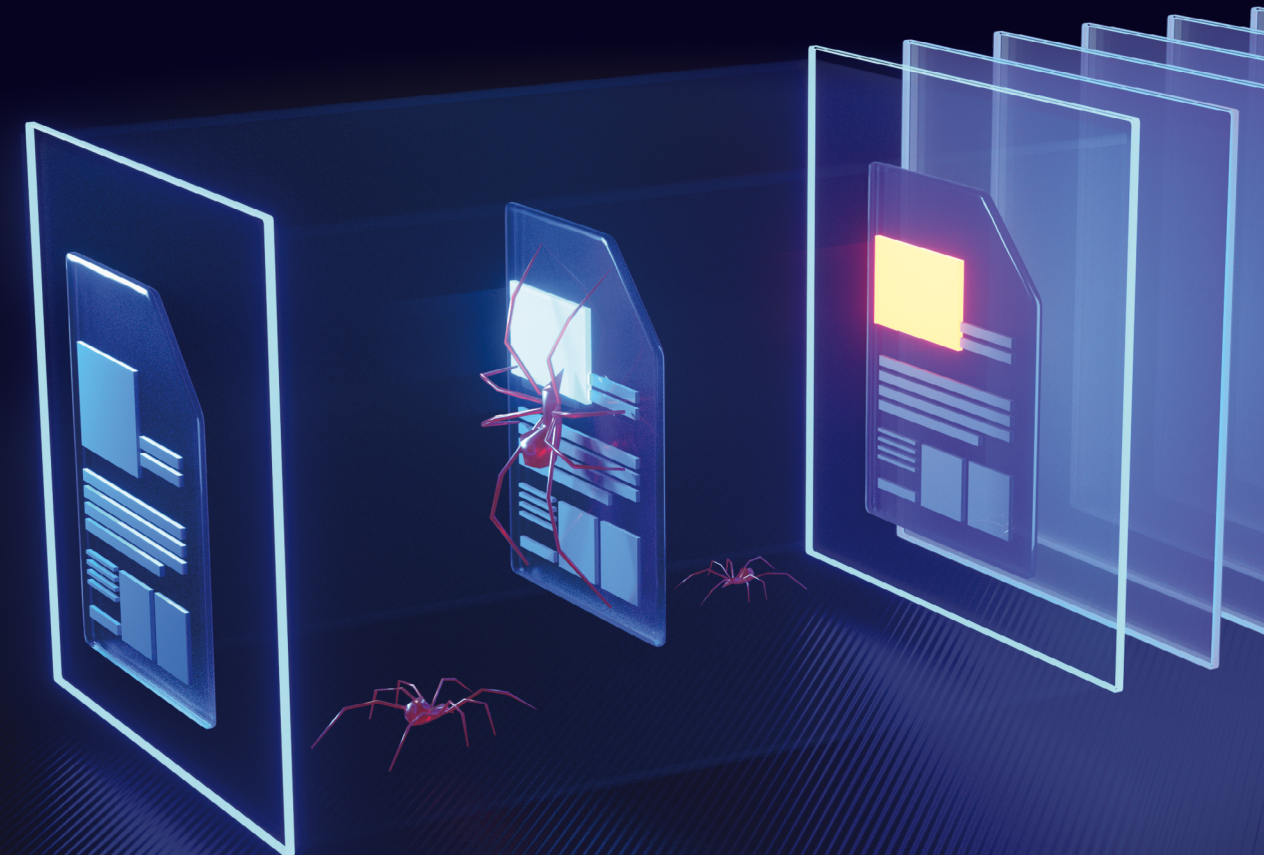
Proactive DLP

Proactive DLP helps prevent sensitive and confidential information in files from leaving or entering systems by content-checking files before they are transferred. This helps enterprises meet regulatory requirements like HIPAA, PCI-DSS, and GDPR.



Adaptive Sandbox

Next-Gen Sandbox offers a complete set of malware analysis technologies including, threat agnostic analysis of files and URLs, emulation of all targeted applications (Microsoft Office, PDF readers, and more), a focus on Indicator-of-Compromise (IOC) extraction, and Rapid Dynamic Analysis engine for targeted attack detection.



OPSWAT.

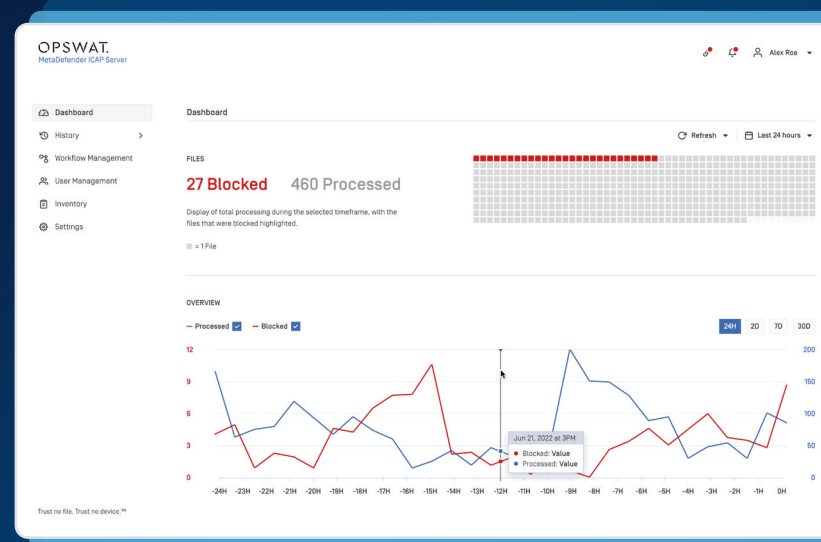
METADefENDER™

ICAP Server

Trust your network traffic

Cybercrime is a multibillion-dollar business. Criminals use files to sneak malware into otherwise secure systems. Negligent users may download innocent-looking files meant to steal or encrypt data. Right now, files containing threats or sensitive data might be unknowingly moving through your network traffic and into your organization's infrastructure.

To best secure network traffic from malicious file upload attacks and data leakage, organizations need a comprehensive solution that defends against malware and mitigates risks from data theft.



Benefits

- Leverage real-time comprehensive threat detection and prevention for network traffic
- Increase cost-efficiency with simple plug-and-play integration via any ICAP-enabled network devices
- Protect against zero-day threats and advanced targeted attacks
- Prevent sensitive data from entering or leaving the organization to mitigate data breaches and compliance violations
- Detect vulnerabilities in files before they are installed
- Customize policies, workflow and analysis rules to meet your unique security needs

Integration

MetaDefender ICAP Server integrates with any product that supports the Internet Content Adaptation Protocol (ICAP) and can be installed at various intersection points to secure file transfers.

Our Solution

MetaDefender ICAP Server addresses issues before they are a problem. It integrates into your existing network devices to provide an additional layer of security.

By combining multiple threat detection and prevention technologies, MetaDefender ICAP Server can analyze every file for malware, potentially malicious content, and sensitive data.

As a result, all suspicious files are blocked or sanitized before they are accessible to the end-users. Sensitive data is redacted, removed, or blocked, helping enterprises meet security compliance standards.

Key Features

-  **Deep CDR**
Prevents known and unknown file-borne threats and mitigates zero-day attacks
-  **Multiscanning**
Detects over 99% of malware using more than 30 anti-malware engines
-  **Proactive DLP**
Content-checks files for sensitive, private, and confidential data
-  **File-Based Vulnerability Assessment**
Detects application and file vulnerabilities before they are installed

Specifications

Supported Operating Systems	Windows Windows 10 Windows Server 2012, 2016, 2019 or newer (64-bit)
	Linux CentOS 7.x, 8.x, 9.x Red Hat Enterprise Linux 7.x, 8.x, 9.x Debian 9.x, 10.x, 11.x Ubuntu 18.04, 20.04, 22.04

Hardware Requirements	RAM: minimum 2GB free SSD: minimum 5GB free
-----------------------	------------------------------------------------

Supported Browsers	Chrome, Firefox, Safari, Microsoft Edge
--------------------	-----------------------------------------

Ports	Inbound: 1344 (ICAP), 8048 (Web Management Console and REST interface), 8043 & 8443 (NGINX) Outbound: 8008 (only if MetaDefender Core is installed on a remote system)
-------	---------------------------------------------------------------------------------------------------------------------------------------------------------------------------

Deployment Models	<ul style="list-style-type: none">• On-premises• Cloud• Physical/Virtual deployment:<ul style="list-style-type: none">○ Amazon Machine Images (AMI)○ Azure VMs• Containers:<ul style="list-style-type: none">○ Kubernetes○ Helm support is available for Amazon EKS (Elastic Kubernetes Service), AKS (Azure Kubernetes Service), and GKE (Google Kubernetes Engine)
-------------------	-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------

OPSWAT.



METADefENDER™

Managed File Transfer

Many organizations today rely on unmanaged and unsecured traditional file transfer solutions. These tools can produce significant challenges when integrating new workflows and additional data transfers into IT processes. Because these methods can compromise both security and operational efficiency, a new solution is needed to help achieve compliance and avoid the pitfalls of homegrown scripts.

MetaDefender Managed File Transfer empowers productivity by enabling the automation of file transfers and providing advanced security features, centrally managed through a single pane of glass.

1TB

Transfer files up to 1TB in size

150+

File types verified against zero-day exploits

99.93%

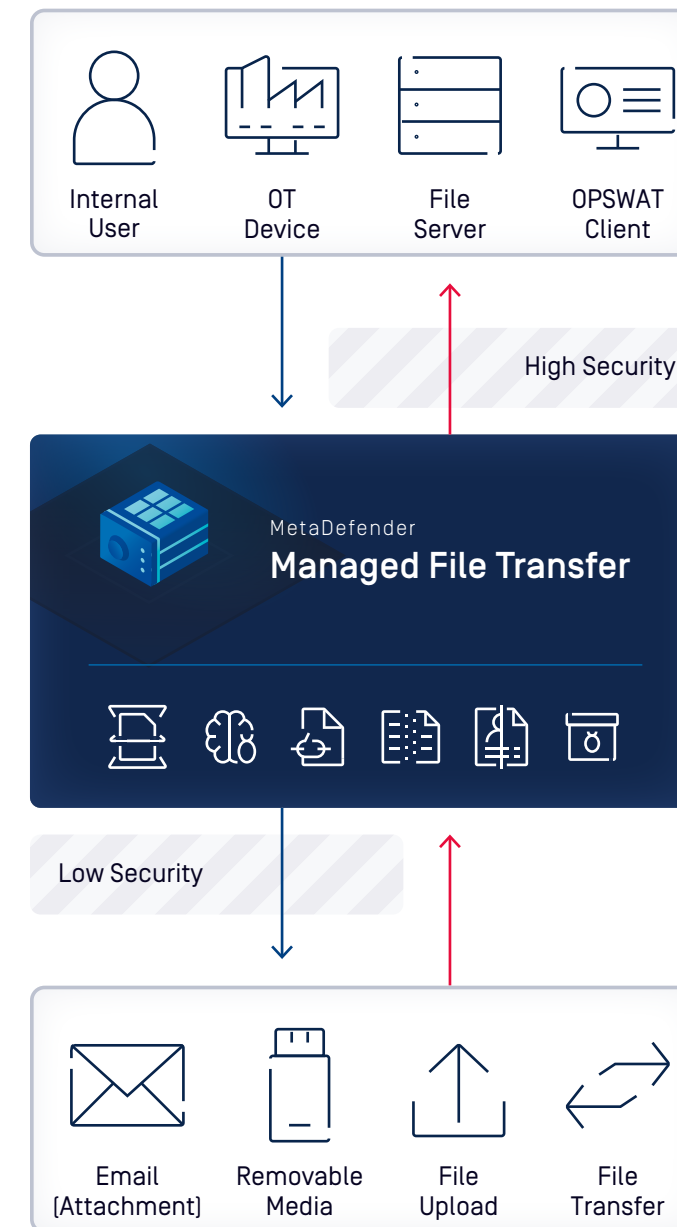
Zero-day malware detection and outbreak prevention

1B

Data points correlated to identify IT & OT vulnerabilities

MetaDefender Managed File Transfer ensures compliance, security, automation and centralized control to defend IT/OT networks and manage file engagement between Internal/External users and systems.

Powered by MetaDefender technologies, file transfers gain multi-layered protection with Multiscanning, Sandboxing, Deep CDR, Malware Outbreak Prevention and File-based Vulnerability Assessment.



Key Features

- Secure Manual & Automated Transfers**
 Advanced automation eliminates the need for manual transfers or home-grown scripts, ensuring efficient and streamlined file management, both internally and externally.
- Prevent Unknown Zero-Day Exploits**
 Deep CDR disarms active objects and unknown exploits in over 150 file types, delivering safe and usable files.
- Prevents Malware Outbreaks**
 Recurring file analysis by Multiscanning includes malware outbreak alerts.
- Powerful Zero-Day Malware Detection**
 Multiscanning uses up to 30 anti-malware engines with heuristics and AI/ML to ensure industry-leading detection of malware.
- Prevents Installation of Vulnerable Applications**
 File-based vulnerability assessment detects and correlates executable files with 3M+ hashes of vulnerabilities from 2.5K vendors.
- Regulatory Compliance**
 Built-in robust security measures include supervisor approvals, encryption and proactive data protection, helping to achieve compliance with industry regulations.
- Advanced Detection of Unknown Malware**
 An adaptive sandbox detects malicious behavior through rapid and in-depth file analysis, uncovering detection evasion and unknown threats.

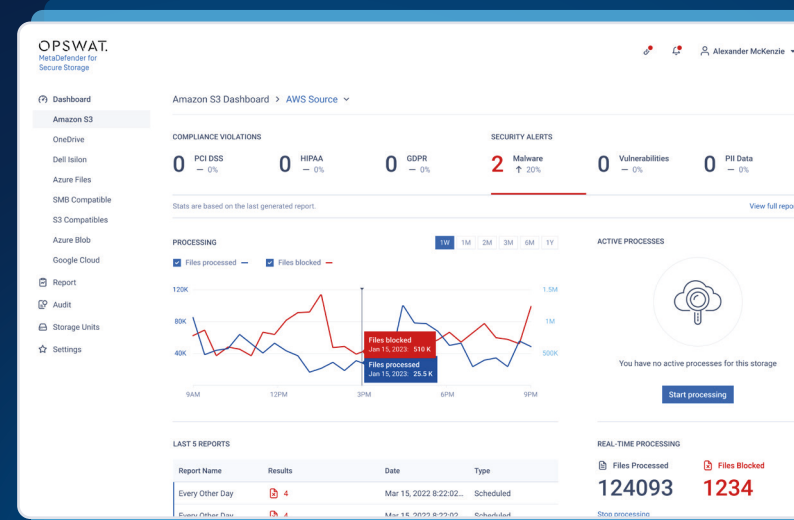
OPSWAT.

METADefENDER™

Storage Security

Secure Your Enterprise Data Storage

MetaDefender Storage Security offers a robust layer of protection for on-prem and cloud storage. It protects enterprise-stored data from data breaches, downtime, and compliance violations in storage and collaboration solutions like OneDrive, Box, Amazon S3, Microsoft Azure, Cloudian, Dell EMC, and any S3 or SMB compatible storage.



Key Features



Real-time Scan

Real-time processing ensures that files are processed as soon as they are uploaded. Real-time processing supports two handling types for files discovery:

- **Polling Handling:** Regular checks for new files to scan.
- **Event-based Handling:** MetaDefender Storage Security has a generic webhook endpoint that can be invoked through a serverless function from AWS, Azure, Alibaba Cloud, and Google Cloud Platform.



Scheduled Scan

Automatically check your storage for threats or vulnerabilities at a predetermined time and frequency.



File Tagging and Management

- Add information about file processing as tags to classify the contents of files quickly and find all malicious files with a <tag> for further analysis and forensics.
- Choose conditional steps to move files tagged as "Allowed," "Sanitized," or "Blocked."
- Apply Deep CDR (Content Disarm and Reconstruction) technology to files.
- Copy, move, and delete files after scanning according to the configuration [e.g. if the file is blocked or after it is sanitized].



Proactive Event Notification

- Notify specific individuals when critical events occur.
- Key Events include report generation, user registration, and file blocking.
- Ensure an immediate response with timely action and improved system management.
- Customizable notifications to relevant stakeholders increase operational efficiency and agility.



SIEM Integration

Integrate with SIEM systems seamlessly and quickly through an intuitive GUI and RESTful API.



Streamlined Report Management

- View all saved and scheduled reports in one centralized location.
- Easily track health trends or help meet audit requirements by periodically saving reports.
- Compare key indicators from previous scans to gauge trends, ensuring informed decision-making and proactive security management.

Scan. Sanitize. Store.

Files from users within the organization are scanned for malware and analyzed for potential data loss or unsolicited privacy data. Suspicious files can be sanitized, while sensitive data from files can be reported and redacted automatically.

Native integration with many cloud and on-premises storage services makes this solution easy to deploy. Automated and actionable audit reports give IT professionals full visibility into potential risks associated with users and services for quick remediation.

Share data within your organization confidently and securely with **MetaDefender Storage Security**.

Benefits

All-in-One Platform

- Integrate seamlessly into existing workflows, providing real-time or on-demand scanning across various storage repositories.
- Guard against zero-day threats and advanced targeted attacks using leading technologies.
- Multi-layered solutions deliver real-time threat detection and prevention to ensure comprehensive storage security measures.

Plug-and-Play Integrations

- Enhance cost-effectiveness with a simple plug-and-play integration.
- Configure and start scanning easily without needing storage admins.
- Seamlessly integrate with Amazon S3, SharePoint Online, Azure, any SMB or S3 compatible storage.
- Begin evaluating your storage within minutes.

Enhanced File Privacy

- Tailor policies, workflows, and remediation actions to fit your security needs.
- Aid compliance with regulatory requirements like PCI, HIPAA, GLBA, and FINRA.
- Prevent sensitive data breaches by controlling data entry and exit within the organization.

OPSWAT.

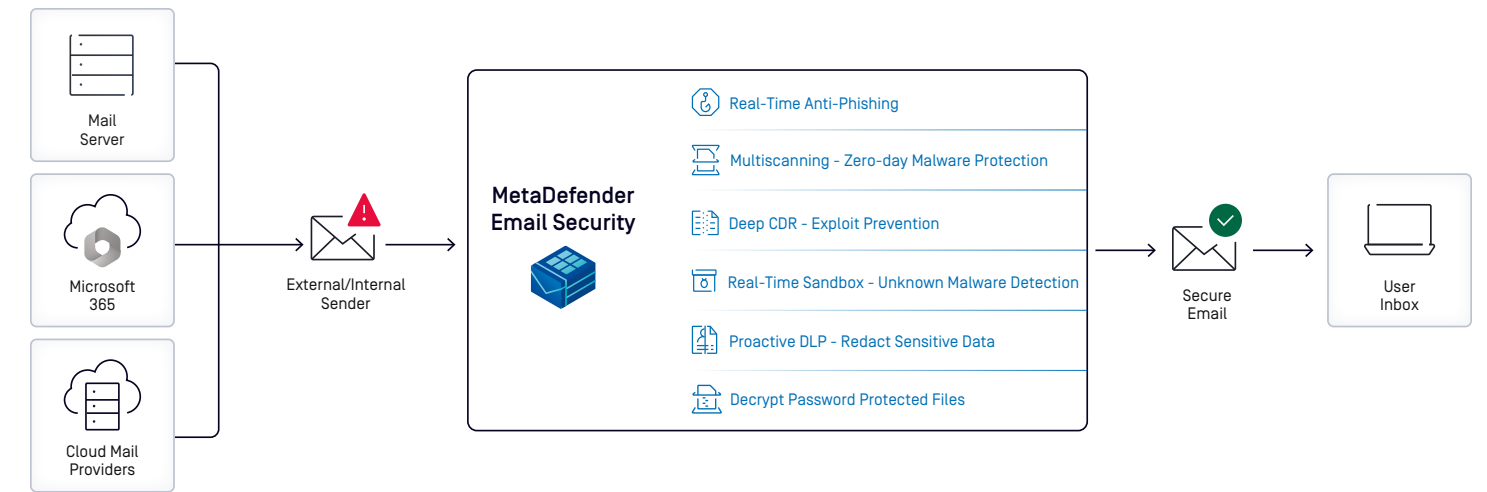
METADefENDER™

Email Security

Advance Your Email Security Posture to the Max

Email continues to be the primary attack vector, and over 86% of malware is delivered via email. Even worse, hackers use unknown exploits to remain hidden for extended periods of time, exploiting the vulnerabilities of business applications to deliver malicious payloads. Over 25000 such vulnerabilities are discovered every year, 75% of which have been in the wild for more than 2 years.

OPSWAT MetaDefender Email Security provides key capabilities to advance organizations' email security posture to the maximum, protecting against email-initiated sophisticated attacks, zero-day malware, and unknown threats.



Key Features



Anti-Phishing and Anti-Spam

Emails are sent through multiple detection mechanisms and content-filtering technology to ensure a 99.98% detection rate of spam and phishing attacks. The URLs are rewritten to later reputation checks at the time of clicking, via 30+ sources against sophisticated social engineering.



Advanced Threat Protection

The Multiscanning technology significantly improves the detection rates of zero-day malware and advanced threats by scanning emails with more than 30 AV engines, reducing the window of exposure to virtually zero. Beyond the traditional signature detection, Multiscanning leverages heuristics and machine learning engines to address unknown zero-day malware.



Sandboxing

Using the unique emulation engines of the sandbox, MetaDefender Email Security is able to detect zero-day malware and hidden threats in various email attachments, such as macros in MS Office documents or PDF files.



Data Loss Prevention

Proactive DLP performs full email content auditing, including more than 40 file type checks, to ensure compliance while blocking or editing email content/files to prevent PII from being sent. It leverages the Optical Character Recognition (OCR) Technology to scan image files as well



Zero-day Prevention

Deep Content Disarm and Reconstruction (Deep CDR) is OPSWAT's advanced threat-prevention technology that protects organizations against attackers using unknown and Zero-Day exploits by sanitizing more than 120 file types and emails from malicious active content. Our approach is 30 times faster than the detection-based security measures.



Manage Password Protected Attachments

Password-protected attachments are no exception, as our solution obtains the user's password for decryption so Deep CDR and Multiscanning can be applied.

Benefits

- Uncovering phishing attacks on multiple stages
- Protecting users from social engineering attacks, ensuring IT can rely less on user awareness
- Ensuring compliance with PCI and other regulations for emails and protecting PII data within companies
- Detecting malicious macros and hidden threats in real-time
- Increased the detection rate of unknown threats with the unique dynamic and static analysis technologies
- Reducing the Window of Vulnerability (WoV) against zero-day malware, thus effectively preventing malware outbreaks
- Protecting business productivity files by sanitizing document-based threats from attachments
- Decrypting password-protected files to apply all key features
- Effectively eliminating zero-day targeted attacks by relying on prevention rather than detection

Summary

Our goal is to protect organizations from email-initiated cyber-attacks. To that end, OPSWAT MetaDefender Email Security features key capabilities to maximize the protection and reduce security risks from your mailbox.

With key OPSWAT technologies such as Deep CDR, Multiscanning, Proactive DLP, and sandboxing, our solution effectively protects organizations against sophisticated attacks, including zero-day malware, phishing attempts, and unknown exploits. Our solution is also available as a cloud service.

Sandbox

Advanced Threat Analysis Platform

MetaDefender Sandbox Platform combines static and dynamic analysis with machine learning powered threat intelligence for highly accurate and rapid malware analysis. Our platform can analyze 25K+ files per day per machine. Enhance defensive capabilities, save time, and effectively hunt threats with advanced threat analysis.

MetaDefender Sandbox now features a brand new user interface with improved navigation and responsive design. Its future-proof framework allows seamless updates and enhancements.

Overview

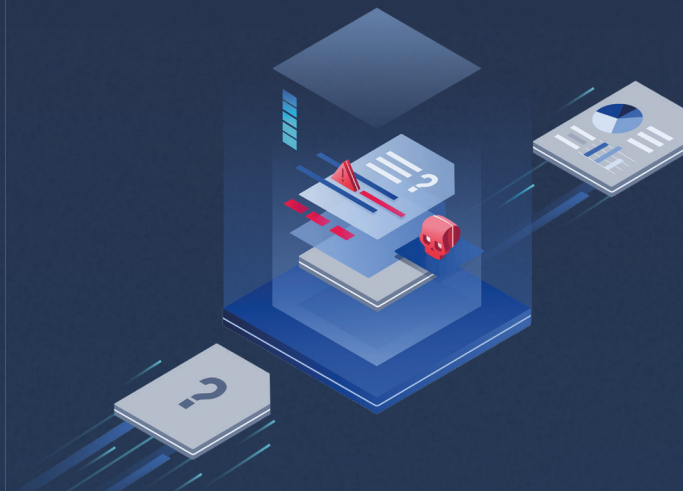
- Static analysis uses 30+ antivirus engines, Yara rules, and threat patterns for high-volume processing.
- Dynamic analysis virtually detonates malware with adaptive threat analysis to expose highly evasive malware and zero-day threats.
- Threat analysis accesses 50 billion+ hashes, IPS and domains, and includes threat actor attribution.
- Fully automated, zero-trust threat detection platform.

Traditional Sandbox



- Slow
- High Resource Use
- Detectable

Emulation Sandbox



- Fast
- Small Memory Footprint
- Adapts to Multiple Environments

Analysis Workflow

STAGE 1

Deep Structure Analysis

Deep Structure

Analysis Initial static file assessment and extraction of embedded active content.

- Analyzes 50+ different file types (e.g. LNK and MSI)
- Extracts artifacts, images, and more
- Automated decoding, decompilation, and shell code emulation
- Extracts VBA macro code from DWG
- Compiled Python unpacking and decompilation for PyInstaller, Nuitka, and py2exe
- Decompiled AutoIT Executables

STAGE 2

Threat Detection and Classification

Detect and classify threats using machine learning and decades of experience.

- Detects 290+ brands for ML-based phishing detection, even in offline environments
- Extracts and correlates a wide range of IOCs
- Detects malicious intent with 550+ generic behavior indicators
- ML-based similarity search detects unknown threats and malicious clusters
- Identify and extract configuration data (IOCs, C2 URLs, family version) from more than 18 malware families

STAGE 3

Adaptive Threat Analysis

Perform dynamic analysis on active content using adaptive threat analysis.

- Detonates targeted attacks via specific application stacks or environments
- Bypasses a wide range of anti-evasion checks
- Emulates JavaScript, VBS, PowerShell scripts
- Automatically adapts the control flow to detect unknown threats

STAGE 4

Threat Intelligence and Automation

Perform automated threat hunting and real-time threat identification using a wide range of integrations.

- Exports to MISP & STIX report formats
- Queries MetaDefender Cloud Reputation API
- Integrates with other open-source intelligence vendors
- Automatically generates YARA rules on a per threat basis
- Scans all artifacts with nearly 10,000 YARA rules

Platform Features

OPSWAT

- MetaDefender Core
- MetaDefender Cloud
- MetaDefender Threat Intelligence

SOAR

- MetaDefender Cloud Splunk SOAR
- Palo Alto XSOAR
- Assemblyline 4

Others

- MetaDefender Threat Intelligence Virus Total
- Python CLI
- SIEM (CEF Syslog)
- Chrome Extension
- Passive Email Scanning (IMAP)
- OpenAPI Specification (OAS)
- ChatGPT Executive Summary
- CIS Level 1 Compatible

Flexible Deployments

On-Premises (Example)

- Intel Xeon-E 2488 (24M Cache, 3.20 GHz, 8 cores)
- 32GB DDR5 RAM
- 2x SSD NVMe 256GB RAID

Note: example system processes 25K files/ day with a retention period of 10 days.

Cloud

- 5000 scans/day: m6a.xlarge
- 10000 scans/day: c6a.2xlarge
- 25000 scans/day: c6a.4xlarge

Learn more about the technical requirements [technical requirements](#)

OPSWAT.

METADefENDER KIOSK™

Kiosk Tower

Removable Media Security Kiosk

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

Any time 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.



CD
DVD
Blu-Ray

3.5" Diskette

USB-A 3.0
USB-C

SD
Micro SD
Compact Flash

Features

Built to Protect Critical Infrastructure
Advanced cybersecurity threat protection with OPSWAT Deep CDR, File-based Vulnerability Assessment, Threat Intelligence, and Proactive Data Loss Prevention, and 20 anti-malware engines. The K3001 supports most common portable media types, including floppy drives, with a variety of built-in media readers on the front of the kiosk.

Ready to Deploy
Each kiosk is pre-configured for your deployment with a region-specific power cord, power protection, and an uninterruptible power supply. The K3001 Premium comes standard with a pre-hardened operating system, pre-installed OPSWAT software, Ethernet, Wi-Fi, and mounting accessories.

Designed with Physical Security
Dual heavy-duty locks secure the main cabinet, and a separate heavy-duty lock secures a fully enclosed printer cabinet. Kiosks are keyed uniquely and specifically for your deployment. Internal floor mounting anchors ensure tamper-resistant permanent placement.

Ruggedized for Industrial Environments
Heavy-duty powder-coated steel enclosure with stainless steel and aluminum internal cabinetry is built to last. Active ventilation, low-profile antennae, and exterior sealed port for power and Ethernet make the K3001 Premium suitable for deployments in industrial and office locations.

Capabilities

Proactive DLP
Detects or blocks sensitive data/personally identifiable information (PII) from leaking by redacting it from 30+ common file types; PCI/DSS & GDPR compliant

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

Multiscanning
Proactively detects 99%+ of malware threats; integrates 20 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

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 Managed File Transfer** for file storage and retrieval

OPSWAT.

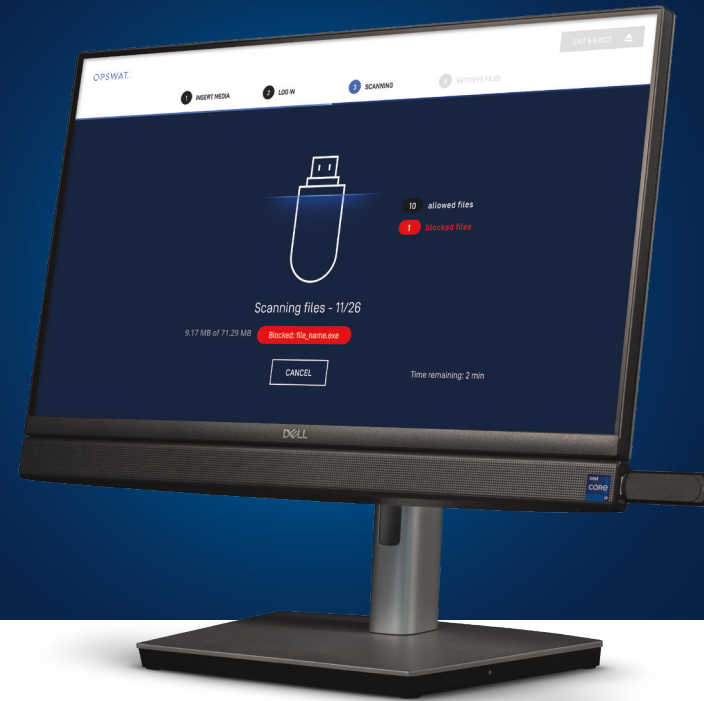
METADEFENDER KIOSK™

Kiosk Desktop

1002 SERIES

Removable Media Security Kiosk

Stop breaches at the point of entry and help your organization mitigate removable media threats and meet compliance, in one easy to use appliance. The MetaDefender Kiosk Desktop is out of the box and deployed in just minutes, protecting your network perimeter from the threats of portable media.



Key Features



Advanced Threat Detection

Scan files with multiscanning technology powered by over 30 anti-malware engines, threat detection levels can exceed 99%.



Country of Origin Check

Gain insights and create policies based on country of origin for files and content.



File Vulnerability Assessment

Uncover vulnerabilities in installers, binaries, or applications before installation to plug any security holes.



File Storage & Data Diode

Integrates seamlessly with MetaDefender Managed File Transfer, NetWall, and best-in-class data diode providers for secure data transfer and storage.



Media Validation Agent

Validate digital signatures every time media is inserted into a device, blocking unscanned media from accessing your environment.



Supports Common Media Types

USB Type-A, USB Type-C, SD, Micro SD, and CD/DVD



Prevent Sensitive Data Leakage (DLP)

Prevent potential data breaches and regulatory compliance violations by detecting and blocking sensitive data/personally identifiable information (PII).



Clean & Reconstruct Suspicious Files

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



Multiple File System & Virtual Disk Support

FAT, NTFS, Ext, HFS+ & APFS; VHD & VMDK.



Secure Erase

Wipe portable media completely clean, before loading approved content.

Additional Features

Mount and scan virtual disks: VHD and VMDK.

Block unscanned media from accessing your environment with the OPSWAT Media Validation Agent.

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

Hardened OS incorporates File Integrity Monitoring.

Integrates seamlessly with MetaDefender Managed File Transfer for file storage and retrieval.

Benefits

Clean & Reconstruct Suspicious Files

Disarm unknown content, prevent zero-day threats, and output clean, usable files.

Industry-leading Multiscanning

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

Prevent Sensitive Data Leakage

Detect, redact, or block sensitive data.

Streamline Data Transfer

Global deployment, consistent experience.

Compliance and Regulations

Fulfill regulatory requirements and ensure IT can rely less on user awareness. OPSWAT supports standards and regulatory national and international compliance requirements to include NIST, HIPAA, PCI DSS, GDPR, NERC CIP, NEI 18-08, ISA/IEC, and ISO/IEC.

Summary

OPSWAT MetaDefender Kiosk Desktop is an all-in-one risk mitigation solution combining durable hardware with OPSWAT's industry-leading security software. The Kiosk Desktop is versatile and fast, scanning up to 13,000 files/minute and supports a wide variety of peripheral ports and slots including USB-A, USB-C, SD, MicroSD, and CD/DVD.

Hardware

CPU	14th generation Intel® Core™ i9
RAM	32GB
Storage	1TB M.2 SSD OPA

Scanning Performance

Speed	Up to 13,000 files/minute
-------	---------------------------

Connectivity

Ports	6x USB-A* 1x USB-C 1x CD/DVD 1x SD/Micro SD**
-------	--------------------------------------------------------

Physical

Weight	14.9 lbs. (6.7kg)
Country of Origin	Mexico

Environmental

Operating Thermal Range	32°F to 95°F [0°C to 35°C]
Storage Humidity	0% to 95%
Operating Humidity	10% to 90%

Regulatory

Environmental Compliance	FCC Class A CE Mark
--------------------------	------------------------

Computing

Operating System	Windows and Linux available
------------------	-----------------------------

Features may vary by OS
*1x plus 5x additional on back
**Micro SD requires standard adapter sold separately

OPSWAT.

METADefENDER™

Kiosk Mini

Removable Media Security

The Kiosk Mini is a versatile, powerful, rugged, and accessible solution for protecting critical systems against uncontrolled removable media and malware, allowing the secure use of peripheral media in a wide array of environments. Designed for ease-of-use, the built-in battery and screen provides the end user with a simple entry point for popular types of portable media, protecting critical environments against threats wherever it is needed.



Key Features



Advanced Threat Detection

Scan files with multiscanning technology powered by over 30 anti-malware engines, threat detection levels can exceed 99%.



Country of Origin Check

Gain insights and create policies based on country of origin for files and content.



File Vulnerability Assessment

Uncover vulnerabilities in installers, binaries, or applications before installation to plug any security holes.



File Storage & Data Diode

Integrates seamlessly with MetaDefender Managed File Transfer, NetWall, and best-in-class data diode providers for secure data transfer and storage.



Media Validation Agent

Validate digital signatures every time media is inserted into a device, blocking unscanned media from accessing your environment.



Supports Common Media Types

USB Type-A, USB Type-C, SD, Micro SD, and CF



Prevent Sensitive Data Leakage (DLP)

Prevent potential data breaches and regulatory compliance violations by detecting and blocking sensitive data/personally identifiable information (PII).



Clean & Reconstruct Suspicious Files

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



Multiple File System & Virtual Disk Support

FAT, NTFS, Ext, HFS+ & APFS; VHD & VMDK.



Secure Erase

Wipe portable media completely clean, before loading approved content.

Additional Features

Mount and scan virtual disks: VHD and VMDK.

Block unscanned media from accessing your environment with the OPSWAT Media Validation Agent.

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

Hardened OS incorporates File Integrity Monitoring and Application Whitelisting.

Integrates seamlessly with MetaDefender Managed File Transfer for file storage and retrieval.

Benefits

Clean & Reconstruct Suspicious Files

Disarm unknown content, prevent zero-day threats, and output clean, usable files.

Industry-leading Multiscanning

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

Prevent Sensitive Data Leakage

Detect, redact, or block sensitive data.

Streamline Data Transfer

Global deployment, consistent experience.

Compliance and Regulations

OPSWAT helps support regulatory standards and national and international compliance requirements to include NIST, HIPAA, PCI DSS, GDPR, NERC CIP, NEI 18-08, ISA/IEC, and ISO/IEC.

Summary

OPSWAT MetaDefender Kiosk Mini is an all-in-one risk mitigation solution combining durable hardware with OPSWAT's industry-leading security software. The Kiosk Mini is versatile and supports a wide variety of peripheral ports and slots including USB A 3.1, USB C, SD, FC, and MicroSD.

Hardware

CPU	12th generation Intel® Core™ i7
RAM	32GB
Storage	256GB M.2 OPAL

Connectivity

Ports	2x USB-A 2x USB-C 1x SD 1x Micros SD 1x CF
-------	--------------------------------------------------------

Physical

Weight	13.24lbs (6kg)
Country of Origin	Mexico

Environmental

Operating Thermal Range	-20°F to 145°F [-29°C to 63°C]
Storage Humidity	5% - 95%
Operating Humidity	10% - 95%

Regulatory

Environmental Compliance	MIL-STD-810H IEC 60529 MIL-STD-461G ANSI/ISA.12.12.01 certification
--------------------------	------------------------------------------------------------------------------

Product specs may vary and not be exactly as shown

OPSWAT.

METADEFENDER™

Kiosk Stand

Removable Media Security

The OPSWAT MetaDefender Kiosk Stand is a powerful enhancement for VESA mountable MetaDefender Kiosk appliances, expanding the accessibility, presentation, and operability of the Kiosk solutions you already trust.



VESA-mountable Kiosk appliance not included

Key Features



Ease-of-Use

The Kiosk stand is easily compatible with all VESA mountable Kiosks including the K-1001, L-1001, K-2100 Mobile Kiosk, and Kiosk Mini.



Port Expansion

Increase the types of media your existing Kiosk can scan by adding Blu-Ray, CD, Floppy, SD, MicroSD, Mini SD, HDD, and CF ports.



Lockable HDD Bay

Lock hard drives in place with the Kiosk Stand for more secure scanning.



Customizable

Wrap the Kiosk Stand with your organization's logo and colors for a more personalized touch in shared spaces.

Benefits

Clean & Reconstruct Suspicious Files

Disarm unknown content and output clean, usable files.

Industry-leading Multiscanning

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

Prevent Sensitive Data Leakage

Detect, redact, or block sensitive data.

Streamline Data Transfer

Global deployment, consistent experience.

Compliance and Regulations

OPSWAT helps support regulatory standards and national and international compliance requirements to include NIST, HIPAA, PCI DSS, GDPR, NERC CIP, NEI 18-08, ISA/IEC, and ISO/IEC.

Summary

OPSWAT MetaDefender Kiosk stand expands the operability and presence of existing MetaDefender Kiosk removable media risk mitigation solutions, combining durable hardware with OPSWAT's industry-leading security software. The Kiosk stand adds support for additional media types to any VESA mountable MetaDefender Kiosk.

Hardware

Ports	Blu-Ray CD Floppy Diskette SD, Micro SD, Mini SD CF Lockable HDD Bay	Bays	3
		Mounting	VESA Compatible



OPSWAT.

METADefENDER™

Media Firewall

Next-Level Removable Media Security Enforcement for Critical Systems

The MetaDefender Media Firewall appliance is a critical component in a defense-in-depth removable media cybersecurity strategy for IT host systems and/or OT SCADA environments.






OPSWAT's MetaDefender Media Firewall works in conjunction with MetaDefender Kiosk acting as a simple, plug-and-play appliance to secure host systems from the threats of removable media-borne cyberattacks. The pre-installed default configuration ensures the boot sector and file contents of inserted portable media are inspected, audited, sanitized, and approved prior to use.



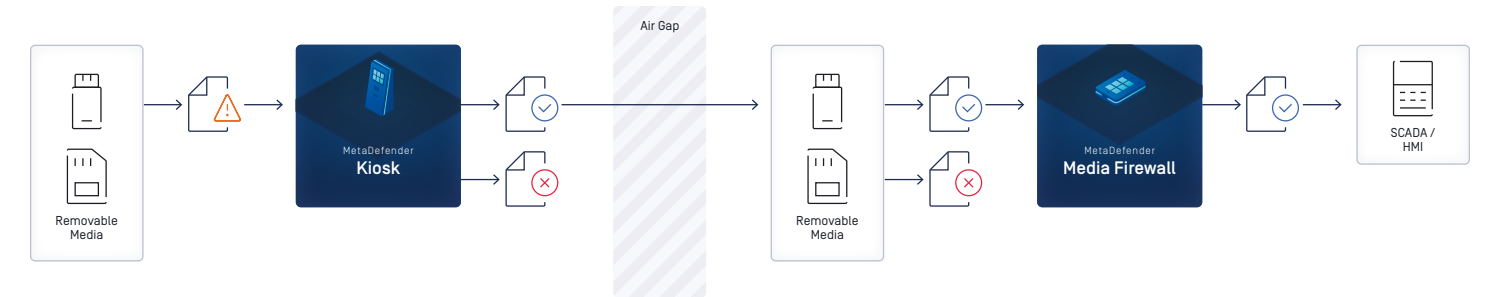
A Critical Advantage

Removable media threats are consistently listed as one of the top cybersecurity vulnerabilities for IT and OT environments alike by analysts. Many organizations have therefore chosen to internally lock down or entirely disable USB ports to reduce risk, but for some, that's simply not feasible. With the flexible and easy-to-use implementation of MetaDefender Media Firewall and MetaDefender Kiosk, organizations can focus on maximizing productivity while staying secure from the threats posed by removable media.

Key Features

-  Plug-and-play appliance that requires no software installation on the host computer
-  Provides boot sector protection
-  Locally managed using host system without ethernet, or remotely managed over ethernet with myOPSWAT.com
-  As a prerequisite, Media Firewall requires that portable media is first scanned by MetaDefender Kiosk
-  Assists in policy, regulation, and standards compliance with NERC CIP, NIST 800-53, ISA 62443, ISO 27001, and more

MetaDefender Media Firewall Working Flow



Specifications

Media Type Support	
Front Side	1x USB 3.0 Type-C 1x USB 3.0 Type-A 1x SD card slot 1x Micro SD card slot 1x Compact Flash card slot
Connectivity	
Rear Side	1x USB 3.0 Type-C (connect to host system) 1x RJ45 1GE LAN (management port) 1x USB 3.0 Type-A (remote management over Wi-Fi dongle) 1x 12V DC jack or 24V DC jack
I/O Transfer Throughput	USB 2.0 speed @ 26 Mbps
Power	Input: 100-240V AC -1.0A 50Hz-60Hz Output: 12V DC 3.0A 36W
Software	
Operating System	Linux 5.10
Firmware	MetaDefender Media Firewall firmware image
Management	Local: using host system, without ethernet On-premises: OPSWAT Central Management using ethernet Cloud: MyOPSWAT.com using ethernet
Host System Requirements	Windows, Linux, Mac USB Type-A (1.0 or greater)
Supported File Systems	FAT, NTFS, EXT
Supported File Size	Up to 64 GB
Hardware	
CPU	Quad Cortex-A53 ARM 1.8GHz
RAM	8 GB LPDDR4
Environmental	
Operating Temperature	-5 to +40°C (23 to 104°F)
Physical	
Dimensions	180mm (W) x 45mm (H) x 200mm (D)
Weight	1.068kg
Mounting	VESA 75
Tamper Detection	Tamper detection tape
Material	Metal and ABS
LEDs	5x on front side per I/O 1x on front side for power
Refer to MetaDefender Media Firewall User Guide for more.	
What's in the Box	
Power	12V DC 36W power supply AC power cord
Cables	6ft USB Type-C to Type-A cable 6ft RJ45 CAT 6 ethernet cable
Instruction	Quick Start Guide
Regulatory	
Safety	CE, UL, cUL
EMC	FCC, IC, VCCI, UKCA

OPSWAT.

METADEFENDER™

Drive Series

Transient and Stationary Device Threat Scanning

Even the most isolated, air-gapped networks provide access to external devices. Any transient device, like a laptop, is a prime target for malicious attacks. Security procedures can utilize MetaDefender Drive before a device enters a facility to inspect the device for malware before the device boots.

Scan an offline x86 server within your IT or OT network before deploying it to ensure no malicious software is embedded within the server kernel space, user space, firmware and drive installs and upgrades.



Features

Bare Metal Laptop or Server Multiscanning

Scan a laptop or server from bare metal to user space files and directories with multiple anti-malware engines using signatures, heuristics, and machine learning to proactively detect known and unknown threats.

Flexible Workflow

Full system or custom scan for specific file path.

Central Manageability

Option to connect to My OPSWAT for reports and configurations from a single platforms.

File-Based Vulnerability Assessment

Detects known vulnerabilities in more than 20,000 software applications with a patented file-based approach.

Proactive DLP

Detect sensitive and confidential data such as credit card, social security numbers in documents, images and videos.

Country Of Origin Detection

MetaDefender Drive checks the device's software and flags anything that may violate country of origin compliance.

Encrypted Disk Support (Including Microsoft BitLocker)

Detects encrypted volumes and prompts for a password, confirming that encrypted files are scanned. Supports LUKS-based encryption and macOS FileVault.

Backup

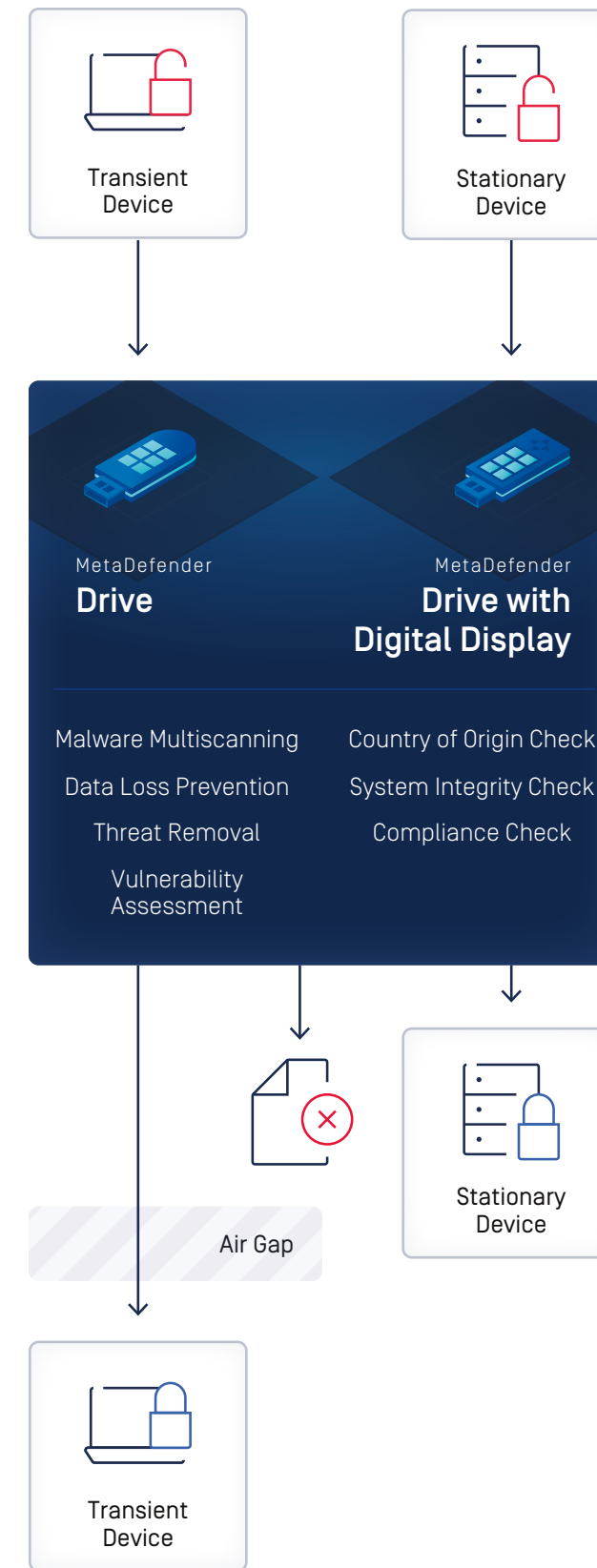
Ability to backup unit to the same state before scanning or threat removal

Threat Removal

Ability to remove files with threat after scan is completed.

Digital Display and LED Indicator Components

The scanning report and detailed alerts show on the LCD and LED light, enhancing the overall user experience.



Isolate.
Analyze.
Address.

MetaDefender Drive securely boots from the USB port of a laptop or server. MetaDefender Drive provides operating system separation that allows analysis without software installation, scanning the entire device for malware, vulnerabilities, and overall integrity. Deep forensic analysis is conducted on every possible file, memory boot sectors, peripheral drivers, kernel space and user space and detailed threat reports pinpoint which files need to be removed and remediated.



Zero-Trust Secure Bare Metal Boot Scan



No Software Installation Required



Support for UEFI/GPT Legacy BIOS



Scan Stationary and Transient Assets



Advanced Threat Removal Technology



Security Compliance Ready

OPSWAT.

METADefENDER™






Unidirectional Security Gateway





For Safe OT/IT Communication

MetaDefender Unidirectional Security Gateway (USG) assures uncompromising security for OT/IT communications, providing access to real-time OT data and enabling secure IT-OT data and file transfers without the risk of introducing security threats to critical OT production networks and assets. MetaDefender USG enforces one way data flows while guaranteeing payload delivery and preventing data loss and retransmission.

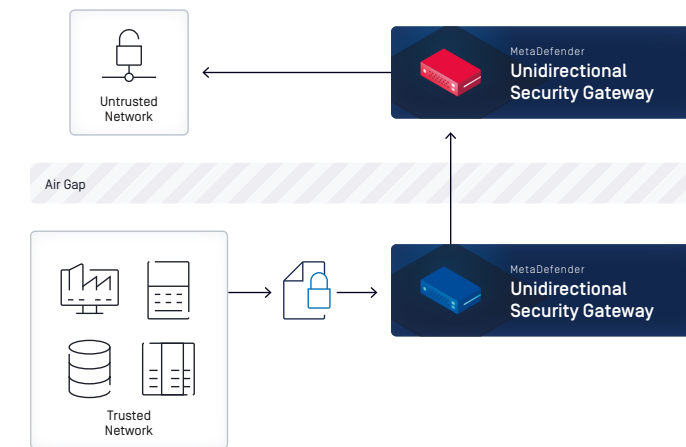


Key Features

-  **Guaranteed Payload Delivery**
Absolutely no data loss.
-  **Anti-Overrun Control**
Eliminate data overflow, retransmissions, and sync issues.
-  **No Return Path**
One-way data flows are enforced by a non-networked serial connection between the USG server pair.
-  **Easy to Deploy**
The preconfigured platform deploys quickly and seamlessly.
-  **Simple to Operate**
Ready for use in minutes after one-time initial setup with no firewall audit or configuration needed.

-  **Scalable**
Choose 100 Mbps, 1 Gbps, or 10 Gbps throughput—all software selectable.
-  **High-Availability**
With the purchase of a second USG, enable high-availability configurations (active/standby).
-  **Transparent to Users**
High-fidelity data replication means there is no need to alter work procedures of corporate users.
-  **Industrial Cybersecurity Compliance**
NERC CIP, NIST ICS/CSF/800-82/800-53, IEC 62443, NRC 5.71, CFATS, ISO 27001/27032/27103, ANSSI, IIC SF, and more. Protects against industrial attack techniques outlined by MITRE ATT&CK.

Deployment



MetaDefender Unidirectional Security Gateway assures no way back to the OT network

Benefits

- Airtight protection for OT/ICS-to-IT communication
- Secure, segmented, unidirectional data paths
- True protocol break, non-routable connection
- Assured delivery with no data loss
- Easy deployment and operation
- Prevent malicious C&C communications from the OT network
- Protect networks, devices, historians, SCADA, DCS, HMIs, and PLCs
- Seamless integration with MetaDefender Kiosk and Managed File Transfer
- Secure the transfer of software updates and other files to the protected domain

Electrical

Redundant Power Supply	250W
Voltage	100-240VAC, auto ranging
Power Consumption	150W typical

Hardware

Dimensions	2x 19 x 1.75 x 15.75" (483 x 44 x 400mm)
Weight	2x 27lb (12.2kg)
Operating Temp	32 – 131°F (0 – 55°C)
MTBF	>50,000 hours
Mounting	1U rack kit included

Other Specifications

Connectivity	2x USB for connecting provided crypto keys
Tested Latency ¹	0.6ms TCP, 0.7ms UDP

Protocol & Certification

Industrial	Modbus OPC (UA, DA, A&E) MQTT IEC104 DNP3 AVEVA PI historian ICCP
IT	UDP, TCP, HTTP, HTTPS, SMTP Video/audio stream transfer
IT Monitoring	Log Transfer SNMP Traps SYSLOG SIEM integration via SYSLOG Screen view
File System	FTP, FTPS, SFTP Folder and file transfer/copy Windows File Share SMB, CIFS Antivirus updates Patch (WSUS) updates
Certification	Common Criteria EAL 4+ ² FCC/CE/UKCA

¹ Actual latency results may vary according to setup used, traffic characteristics, and network topology.
² Certification ending

OPSWAT.

METADefENDER™

Bilateral Security Gateway








For Safe OT/IT Communication

MetaDefender Bilateral Security Gateway (BSG) supports real-time replication and transfer of historians and SQL databases without compromising the security and integrity of your critical production systems. BSG strictly enforces one-way data flows. It also employs a proprietary bilateral mechanism to handle data replies needed by SQL databases and industrial historians hosted in your OT environment, which is completely transparent and requires no change to application configurations or work procedures.

Benefits

- Lossless OT to IT data communications
- Includes a unique mechanism to permit receiving data replies for select applications
- Isolates OT/ICS assets against cyberattacks
- Assures reliable database replication with no database synchronization issues.
- Segments and protects networks, devices, historians, SCADA, DCS, HMIs, and PLCs

Key Features

- 
Guaranteed Payload Delivery
 Absolutely no data loss.
- 
Anti-Ovrrun Control
 Eliminate data overflow, retransmissions, and sync issues.
- 
No Return Path
 One-way data flows are enforced by a non-networked serial connection between the BSG server pair.
- 
Bilateral Support
 A mechanism permits data replies while enforcing full protocol break and physical isolation.
- 
Easy to Deploy
 The preconfigured platform deploys quickly and seamlessly.
- 
Simple to Operate
 Ready for use in minutes after one-time initial setup with no firewall audit or configuration needed.
- 
Scalable
 Choose 100 Mbps, 1 Gbps, or 10 Gbps throughput.



Use MetaDefender Bilateral Security Gateway for OT data replication with secure response

Electrical

Redundant Power Supply	250W
Voltage	100-240VAC, auto ranging
Power Consumption	150W typical

Hardware

Dimensions	2x 19 x 1.75 x 15.75" (483 x 44 x 400mm)
Weight	2x 27lb (12.2kg)
Operating Temp	32 - 131°F (0 - 55°C)
MTBF	>50,000 hours
Mounting	1U rack kit included

Other Specifications

Connectivity	2x USB for connecting provided crypto keys
--------------	--------------------------------------------

Tested Latency¹

1. Actual latency results may vary according to setup used, traffic characteristics, and network topology.

Protocol & Certification

Industrial	Modbus OPC (UA, DA, A&E) MQTT IEC104 ICCP
Industrial Historian	GE Proficy Aspentech IP21 AVEVA PI CanaryLab Other historians
IT	UDP, TCP, HTTP, HTTPS, SMTP Video/audio stream transfer
IT Monitoring	Log Transfer SNMP Traps SYSLOG SIEM integration via SYSLOG GE OSM Screen view
Relational Database	Microsoft SQL Oracle Golden Gate Other relational databases
File System	FTP, FTPS, SFTP Folder and file transfer/copy Windows File Share SMB, CIFS Antivirus updates Patch (WSUS) updates
Certification	FCC/CE/UKCA

OPSWAT.

METADefENDER™

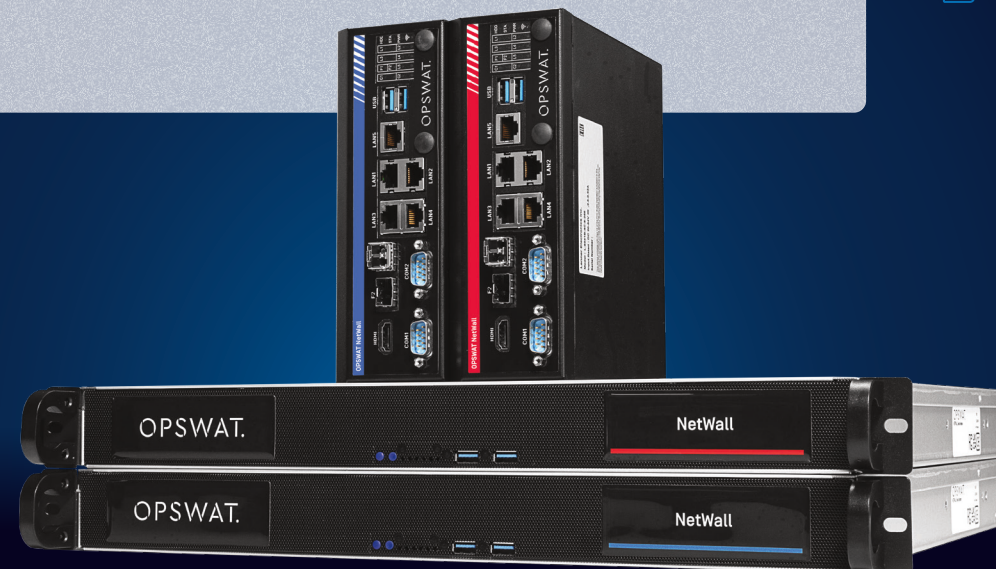
Optical Diode

For Safe OT/IT Communication

In compliance with NEI and other cyber security controls, MetaDefender Optical Diode serves as a deterministic isolation device which protects critical assets while allowing multiple data types to be transferred concurrently. The hardware-enforced, one-way optical link between the source and destination servers reliably transfers data over a non-routable protocol, ensuring complete security from network-borne threats. Optical Diode provides access to real-time OT data and enables secure IT/OT data and file transfers without the risk of introducing security threats to critical OT production networks and assets.

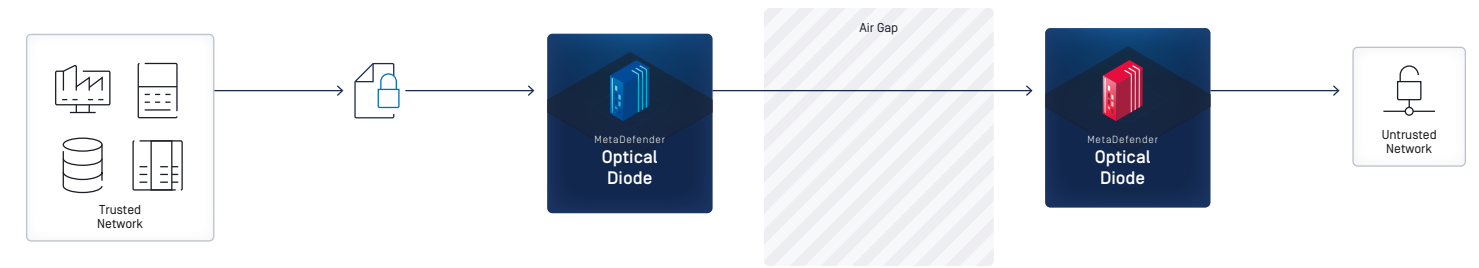
Benefits

- Airtight protection for OT/ICS-to-IT communication
- Secure, segmented, unidirectional data paths
- True protocol break, non-routable connection
- Redundant optical connection for unsurpassed reliability
- Easy deployment and operation
- Seamlessly integrates with MetaDefender Kiosk, Core, and Managed File Transfer

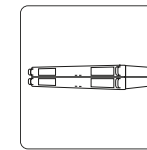


Key Features

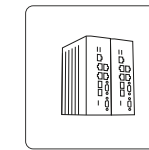
- No Return Path**
 One-way data flows are enforced by a unidirectional optical connection between the Optical Diode server pair.
- Easy to Deploy**
 The preconfigured platform deploys quickly and seamlessly.
- Simple to Operate**
 Ready for use in minutes after one-time initial setup with no firewall audit or configuration needed.
- Scalable**
 Choose 100 Mbps, 1 Gbps, or 10 Gbps license. The DIN Rail version ranges from 10 Mbps to 50 Mbps.
- High-Availability**
 With the purchase of a second Optical Diode, enable high-availability configurations (active/standby).¹
- Transparent to Users**
 High-fidelity data replication means there is no need to alter work procedures of corporate users.
- Industrial Cybersecurity Compliance**
 NEI 13-10, NERC CIP, NIST ICS/CSF/800-82/800-53, IEC 62443, NRC 5.71, CFATS, ISO 27001/27032/27103, ANSSI, IIC SF, and more. Protects against industrial attack techniques outlined by MITRE ATT&CK.



MetaDefender Optical Diode assures no way back to the OT network



1U



DIN Rail

Electrical

Redundant Power Supply	250W	✘
Voltage	100-240VAC, auto ranging	12-36VDC
Power Consumption	150W typical	30W typical

Hardware

Dimensions	2x 19 x 1.75 x 15.75" (483 x 44 x 400mm)	2x 2.5 x 7.32 x 6.3" (65 x 186 x 160mm)
Weight	2x 27lb (12.2kg)	2x 4.85lb (2.2kg)
Operating Temp	32 to 131°F (0 to 55°C)	-40 to 158°F (-40 to 70°C)
MTBF	>50,000 hours	
Mounting	1U rack kit included	No additional hardware needed

Other Specifications

Connectivity	2x USB for connecting provided crypto keys
Tested Latency ²	0.6ms TCP, 0.7ms UDP

Protocol & Certification

Industrial	Modbus OPC (UA, DA, A&E) MQTT IEC104 DNP3 AVEVA PI historian ICCP
IT	UDP, TCP, HTTP, HTTPS, SMTP Video/audio stream transfer
IT Monitoring	Log Transfer SNMP Traps SYSLOG SIEM integration via SYSLOG Screen view
File System	FTP, FTPS, SFTP Folder and file transfer/copy User-defined file polling interval Transfer priority based on date/time and filename Windows File Share SMB, CIFS Antivirus updates Patch (WSUS) updates
Certification	Common Criteria EAL 4+ ³ FCC/CE/UKCA

1. Available on 1U model only.
 2. Actual latency results may vary according to setup used, traffic characteristics, and network topology.
 3. Certification pending.

OPSWAT.

METADefENDER™

OT Security

Rethink OT Cybersecurity

Visibility into OT environments continues to be a major challenge and risk vector for organizations. OT environments are inherently heterogeneous and quite often consist of decades-old devices from multiple vendors. The ability to have full visibility into assets and what is happening on the network is key to any effective OT cybersecurity program.



Capabilities

- Rapidly Discover Devices and Build Asset Inventory
- Smart Asset Profiling
- Active and Passive Threat Monitoring
- Continuously Monitor Network to detect Threats and Anomalies
- Constantly & Objectively Address OT Vulnerabilities and Risks
- Structured and Streamlined Risk Alert Workflow
- Centralized Patch Management
- Global, regional & Industry Regulatory Compliance Reporting
- Comprehensive & Customizable Dashboard
- Granular Access and Controlled User Permissions

What We Offer

MetaDefender OT Security addresses risks to OT systems from both traditional IT and specific ICS threats. It is extremely simple to deploy and easy to use with OT-native UIs. MetaDefender OT Security can be operated without an expert skillset or training.

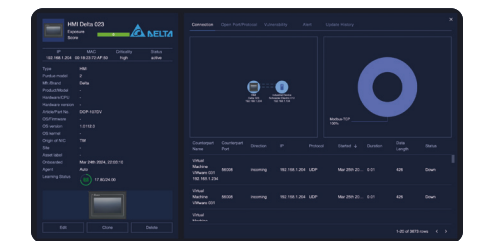
Designed for enterprise-level deployments, MetaDefender OT Security provides unparalleled visibility into converged IT/OT operations. It also delivers deep situational awareness of threats throughout the network.

It helps to protect your critical assets by maximizing your visibility, security, and control across your entire operations while staying compliant with regulatory requirements.

MetaDefender OT Security leverages AI technologies to gain knowledge of the unique attributes and requirements of OT environments.

Benefits

- Complete asset visibility and centralized security management for geographically dispersed networks
- Streamlines incident response and expedites remediation
- Easy to use and deploy. Built for OT personnel
- Timely and accurately informs you of any threats or anomalies on the network
- Supports regulatory requirements with wide and objective risk assessments
- Scalable across OT environments at an Enterprise level
- Provides a unified view of operation, security, and compliance in a single pane of glass
- Seamless integration with MetaDefender Industrial Firewall & IPS



Use Cases

- Asset Inventory & Vulnerability Assessment
- Network Visualization & Monitoring
- Threat Detection & Response
- Exposure Assessment & Alert workflow

Realtime, AI-based analytics Engine

- Behavioral Anomaly Detection
- Asset's Changes Detection
- Unusual Communication Detection
- Violation of Security Policies Detection

Deep Network Analysis & Device Fingerprinting

- Deep Network Traffic Dissection
- Knowledge of OT Devices & Protocols
- Proprietary ICS Fingerprinting & Vulnerability

OPSWAT.

METADefENDER™

Industrial Firewall

Industrial Firewalls for Mission-Critical Networks

MetaDefender Industrial Firewall is a network security solution designed to protect multi-layered, mission-critical networks. These firewalls are engineered to protect ICS (industrial control systems), OT (operational technology), and SCADA (supervisory control and data acquisition) systems from cyberthreats.



Industrial Firewall for Operations

MetaDefender Industrial Firewall for Operations is a high-performance, ruggedized firewall, built to effectively block anomalous activities on the network thereby ensuring your network remains secure and compliant against evolving cyberthreats.



Features FLM (Firewall Learning Mode) with ML (Machine Learning) capabilities to monitor and learn network traffic, automatically generating security policies.



Implements Protocol Specific DPI rule sets to block anomalies, zero-day threats, and DOS/DDOS attacks.



Equipped with 4 high-speed Ethernet ports and powered by stateful packet inspection for robust security.

Technical Specifications

Product Description

Type	Industrial Firewall for Operations
Description	Industrial Firewall with DIN Rail Mounting
Port Type and Quantity	3x 2.5 GbE RJ45 ports + 1 SFP
Port Speeds	3x 2.5 GbE RJ45, 1x 1GbE SFP

More Interfaces

USB Interface	2x USB 3.1 Gen 2
Serial Interface	HMI

Hardware

CPU	Intel X6425E
Encryption	TPM 2.0 via SPI
Memory	8GB
Storage	128GB

Power Requirements

Operating Voltage	Dual 12 - 36VDC
Power Consumption	60W
Power Supply	Phoenix contact 3-pin connector with lock

Approvals

Basic Standard (EMC)	CE, FCC
Safety of Industrial Control Equipment	UL 62368
Hazardous Locations	C1D2

Reliability

MTBF	15 Years
Warranty	5 Years + extended option 3 years

Ambient Conditions

Operating Temperature	-40°C to +70°C
Storage/Transport Temperature	-40°C to +70°C
Relative Humidity (non-condensing)	5% to 95%

Mechanical Construction

Dimensions (W x H x D)	143.94 x 134.9 x 64 mm
Mounting	DIN Rail
Enclosure	Aluminum with DIN clip
Weight	1.05kg
Protection Class	IP50

Software

Software version	OPSWAT Industrial OS (3.0.0)
Security	Firewall rules (incoming/outgoing, management), DoS prevention, Protocol Specific DPI (Deep Packet Inspection): Firewall Learning Mode (FLM) - L2
Routing	Port-based routing, IP masquerading, 1-to-1 NAT, port forwarding
Management	Local Web UI for configuration SSH, CLI
Diagnose	LEDs (Power, HDD Status, System Status), Log File, Syslog
Configuration	Web Interface, Command Line Interface (CLI)
Protocols	HTTPS, NTP (Client), DNS, Syslog
Redundancy Functions	N/A

Supported Protocols

Industrial Protocols

MODBUS	VNETIP	PROFINET IO (DCE/RPC)
ETHERNET/IP	BACNET	GOOSE
S7COMM	DNP3	SV
SLMP	EGD	EtherCAT Layer2
FINS	PROFINET DCP	OPC-UA (unencrypted)

GE Protocols

CIMPLICITY	DICOM	GESRTP
IFIX	MMS	GEADL
IEC-60870-5-104	GESDI	BN3500

OPSWAT.

METADefENDER™

IT Access

Securing the New Perimeter

The digital business landscape is continuously evolving, and with it, the need to protect it from a rapidly changing world of evolving threats. No longer are employees tied to a desk, nor are applications tethered to devices. The traditional network perimeter has expanded; so too should your ability to defend it.

Traditional threat-facing security infrastructure will have its place in networks for years to come. Alongside these legacy technologies emerges the Software Defined Perimeter, and the security around it will bring speed and agility to the enforcement of security policy regardless of the location of the user, the information or the workload.



The Software Defined Perimeter

A traditional enterprise network with its fixed perimeter and walled-off architecture has largely allowed the devices, applications and services within it to remain secure from external threats. BYOD, IoT and SaaS models have all tested this traditional infrastructure by introducing blind spots in visibility and control of users and devices.

Secure Access Software Defined Perimeter (SDP) renders an organization's critical IT infrastructure "invisible" or "dark"—meaning no DNS information or IP information is visible, and protected application resources cannot be detected from the Internet or other internal networks.

After all, you can't hack what you can't see.

Secure Access is a single platform providing Advanced Endpoint Compliance and Secure Remote, Cloud and On-Premise Access to your network, applications and data. This Data Sheet focuses on the Software Defined Perimeter capabilities and features.

Features

Secure Access SDP's **Zero-Trust Access** model hides enterprise resources from the Internet and internal networks, and offers more secure "verify-first, connect second" authentication.

Multi-Factor Authentication and Identity Access Management integration delivers a streamlined, consistent user experience.

As a customer-provisioned cloud offering, SDP **deploys rapidly and comes with 24/7 support**, offering you maintenance-free security.

Includes **cloud-hosted SDP gateway connector** for Public Cloud SaaS applications.

On a **VMware virtual appliance or AWS AMI instance**, protect private cloud and internally hosted applications.

Benefits

Easy to Install

No additional hardware or network integration required; rapid deployment and maintenance-free with 24/7 support.

Zero-Trust/Least-Privileged

Greater security with Verify-First, Connect Second access to public & private cloud applications.

Mutual TLS Encryption

Easier to deploy, high-performance VPN per-session application access.

Control Beyond Your Perimeter

Prevent data loss from devices accessing your cloud application and data from outside your network perimeter.

Decreases Network Attack Surface

Hide your applications from the Internet and corporate networks to mitigate DDoS attacks, credential theft, connection hijacking & data loss.

Advanced Endpoint and Secure Access Compliance Checks

PCI, HIPAA, SOC2, SOX, GLBA, & GDPR compliant security controls.

Predictable & Cost Effective

SaaS annual subscription model with term commitment discounts.

Use Cases

Legacy VPN Replacement

Zero-Trust security at a fraction of the price, without the throughput degradation that comes with VPN encryption

Beyond-Perimeter Cloud Access

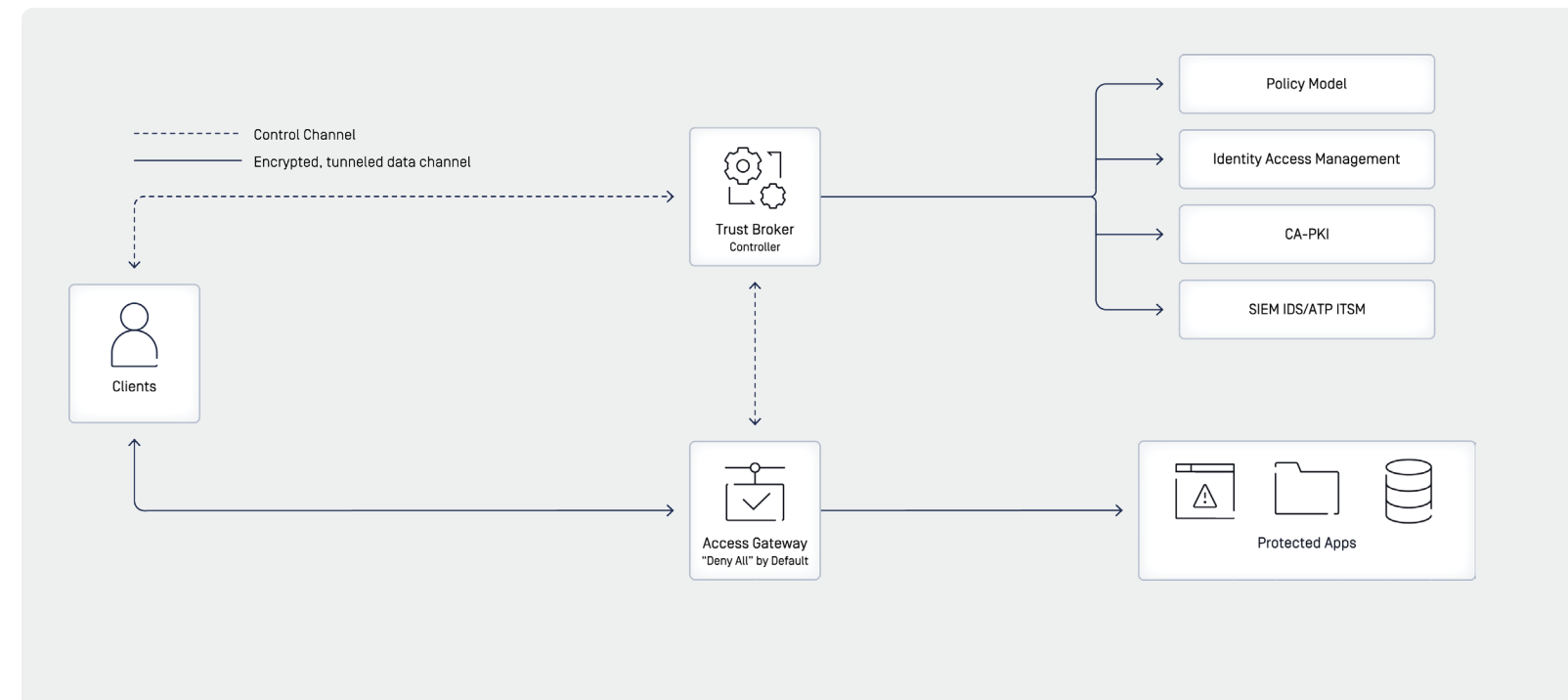
Secure access to your public and private cloud resources from devices outside of the network perimeter with mutual TLS encryption

Protect Critical Applications & Data

Seamlessly integrate with existing network access control offerings for policy-driven access to exactly the data and applications needed, regardless of connection location

Components

- **SDP Client** – available for Windows, macOS, iOS and Android devices; can be distributed to managed devices or downloaded as part of the BYOD onboarding process.
- **SDP Controller** – cloud-hosted trust broker between the SDP Client and security policy controls such as IAM providers, Issuing Certificate Authority and Device Compliance.
- **SDP Gateway** – termination point for mutual TLS VPN connection from the Client, the Gateway is provided with the Client's IP address and Certificates after the identity of the requesting device has been verified and the authorization of the user has been determined by the Controller.



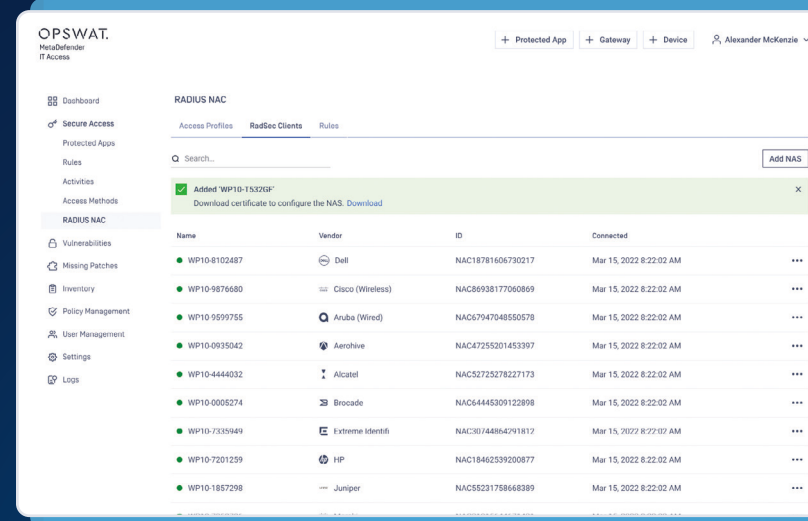
OPSWAT.

METADefENDER™

Network Access Control

The volume and diversity of devices accessing business-critical network resources represent an increasing challenge for today's IT organizations. How can you easily block unknown devices from the network, while maintaining a positive experience for devices that belong? And how do you know which devices meet your security standards?

MetaDefender NAC, formerly SafeConnect, automates device security compliance and network access assignment policies by gathering a wealth of real-time and historical device information. This allows for granular and more timely security decisions when it counts.



Benefits

Real-Time Visibility and Security

Complete visibility to all devices on both wired and wireless networks with authentication or blocking. Security assessment and enforcement for Windows, macOS and mobile devices.

Flexible Enforcement Options

The only solution on the market that offers either RADIUS-based enforcement that requires no VLAN changes or a unique Level 3 option that negates 802.1X requirements.

Streamlined User Authentication

Intuitive user access for guests, vendors and employees with a fully customizable self-registration portal.

Contextual Intelligence

Gain greater visibility into device types in context with the network, and publish that information to other security utilities to automate enforcement and remediation.

Remote Installation, Training, and Deployment

Remote deploy and install; includes 24x7 proactive monitoring & support, nightly backups and pushes of new devices, OS & Antivirus, automated updates.

Specifications For Standard VM

Appliance Specifications	SafeConnect VMWare Enforcer
VMWare Version*	ESXi 5.1 or newer
Virtual Hardware Version	Minimum version 8
CPU	2 quad-core CPUs [2-3Ghz]
Memory	16 GB minimum
Hard Drive Storage	300 GB minimum
Appliance Scalability	Up to 25,000 devices
Network Interface	Gigabit NIC

* Hyper-V and Azure also supported

Capabilities

- Port Level Control
- Role-Based Access Control
- Agentless Device Profiling
- Acceptable User Policy (AUP) Enforcement
- Custom Policy Builder
- Guest and IOT Self-Registration
- Flexible Network Integration Options
- Contextual Intelligence Publishing
- Application Usage Policies

Visibility. Security. Control.

MetaDefender NAC automates device security compliance and network access assignment policies based on identity role, device type, location, and ownership and gathers a wealth of real-time and historical context-aware device information that allows for more timely and informed security decisions.

MetaDefender NAC also addresses the daunting task of correlating mobile and IOT device information and user identity over time and across network segments for regulatory compliance, security forensics; and enabling identity-based firewall, web content, SIEM, and bandwidth management policies.

MetaDefender NAC delivers security, visibility, and control to every device accessing your network and cloud applications.

Features

MetaDefender NAC has an integrated **RADIUS server** which can stand alone or proxy to an existing RADIUS solution.

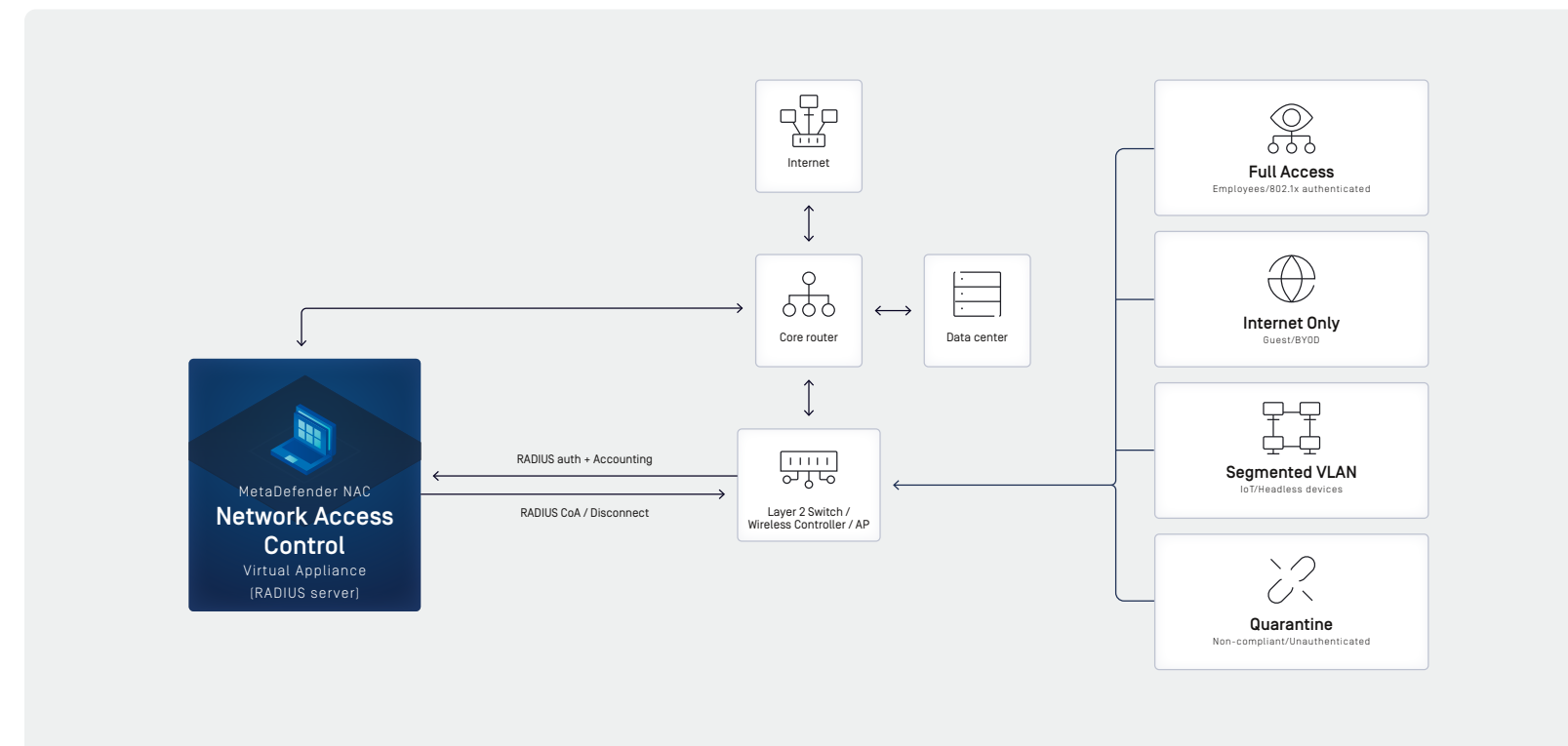
Simplify **Device Remediation** with an intuitive captive portal that guides the user back onto the network without intervention

Gain visibility into all connected device types, brands, OS and other characteristics with **Agentless Device Profiling**

IoT Device Registration associates an identity to browserless devices, allowing for granular access policies to mitigate security vulnerabilities

Provide secure guest access to wired or wireless networks with a selection of three **Guest User Self-Registration** models

Remote 24x7 Proactive Monitoring Support is remotely managed for you, and includes daily remote backups, software upgrades, problem determination/resolution ownership



OPSWAT.

METADEFENDER™

OT Access

Industrial Secure Remote Access

Establish Granular Visibility and Control Down to the Asset, Protocol, and User

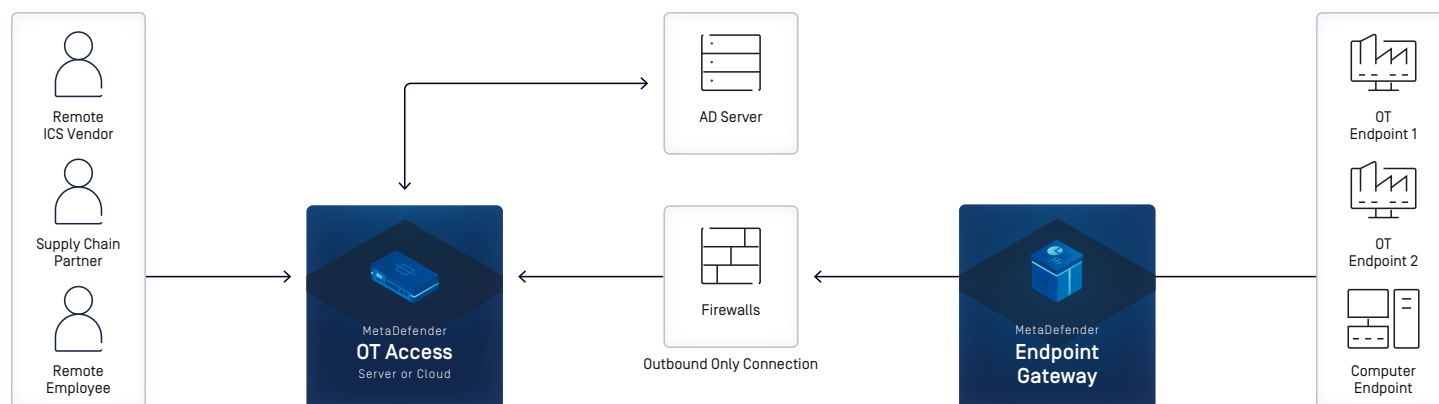
VPNs are typically the go-to solution for IT to provide remote access, but they're not designed for OT environments. With VPNs, it is all or nothing. Once a user gains access, they can see and inspect any asset on the OT network without supervision, and there is no way to terminate the session should something go wrong. OPSWAT's MetaDefender IT-OT Access solution eliminates this risk.

It enforces a logical line-of-sight protection model where users can only access what they are authorized to see across their connection and nothing else.

One Platform to Secure All Remote Access to Industrial Assets

Say goodbye to managing multiple remote access platforms, and lengthy user onboarding processes. MetaDefender IT-OT Access delivers secure remote access to all third parties, OEM, and remote users through one centralized platform, without the gaps that traditionally come with VPN solutions. More importantly, it significantly reduces the attack surface of your operational network—and risks posed by remote users.

There's no simpler way to establish a single, supervised, and secure line-of-sight entry point for remote users that require access to your OT assets.



Key Features

One Secure Solution for All

Simplify remote access with one software solution for all third party, OEM, and remote user access. No hardware required.

Easy Deployment

Set up in less than a day, with far fewer complications compared to standard VPNs.

Flexible Deployment Options

Use our multi-tenant instance for the absolute fastest onboarding experience, or go with a dedicated AWS instance for maximum isolation, reliability, and performance.

Run our software on a VM platform of your choice, or we can send you a 1U rack-mountable appliance with the software pre-installed.

Seamless Integration

Natively integrate with Microsoft Active Directory for seamless authentication of users and groups, including employees, third-party suppliers, contractors, and industrial equipment manufacturers.

Deep Packet Inspection

Monitor session duration, provide read/write/program level policies, and instantly block any user or session that violates a policy.

Granular Access

Customize access of every session down to the protocol, user activity, and role to ensure OT assets and network are not remotely manipulated outside the line of sight.

Best-in-Class Device Posture Checks

Ensure that any device granted remote access to your OT environment complies with your organization's security policies using OPSWAT's industry leading OESIS framework.

Secure Password Sharing

Keep passwords hidden from users without restricting access with 2-factor authentication.

No Firewall Compromises

Connect through a fully-encrypted, outbound-only TLS service registration tunnel without any firewall reconfiguration. No risk of pre-auth attacks, which are common for VPNs recently.

Continuous Monitoring

Supervise, enforce (policies), or terminate any session instantly.

Session Recording

Every session is thoroughly logged for compliance [syslog] and auditability [syslog and RDP session recordings].

METADEFENDER OT Access		VPNs	
Feature			
Native OT protocol controls	✓ Including deep packet inspections	✗	
Connection origination	Outbound only via TLS from site to server	Inbound through perimeter firewall	
Permission type	Granular single-user to single-user	Course Single-user to whole-network	
	Read-Only	Read-Write	No SQL Inject No XSS
Native Policy Controls			
FINS	✓	✓	✗
Modbus	✓	✓	✗
OPCUA	✓	✓	✗
S7	✓	✓	✗
SLMP	✓	✓	✗
RDP	✗	✗	✗
Ethernet IP	✗	✗	✗
VNC	✗	✗	✗
HTTP(S)	✗	✗	✓
ssh	✗	✗	✗
telnet	✗	✗	✗

GET STARTED

Put OPSWAT on the front lines of your cybersecurity strategy.

Talk to one of our experts today.

Scan the QR code or visit us at:

opswat.com/get-started

sales@opswat.com



OPSWAT.

Protecting the World's Critical Infrastructure

For the last 20 years OPSWAT, a global leader in IT, OT, and ICS critical infrastructure cybersecurity, has continuously evolved an end-to-end solutions platform that gives public and private sector organizations and enterprises spanning Financial Services, Defense, Manufacturing, Energy, Aerospace, and Transportation Systems the critical advantage needed to protect their complex networks from cyberthreats.

Built on a "Trust no file. Trust no device." philosophy, OPSWAT solves customers' challenges like hardware scanning to secure the transfer of data, files, and device access with zero-trust solutions and patented technologies across every level of their infrastructure.

OPSWAT is trusted globally by more than 1,700 organizations, governments, and institutions across critical infrastructure to help secure their devices, files, and networks from known and unknown threats, zero-day attacks, and malware, while ensuring compliance with industry and government-driven policies and regulations.

Discover how OPSWAT is protecting the world's critical infrastructure and securing our way of life; visit www.opswat.com.