OPSWAT®

Protecting the World's
Critical Infrastructure

Scan to Learn More
About Our Solutions

OPSWAT.COM

OPSWAT.

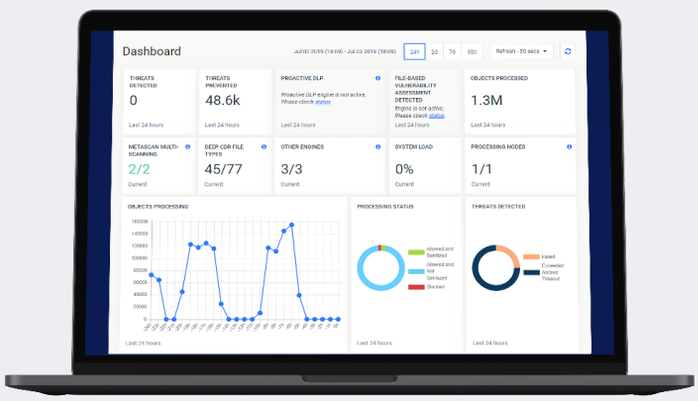
DATASHEET

MetaDefender Core®

Advanced threat prevention platform

No longer can your business rely solely on detection-based cybersecurity systems to provide adequate protection for your most valuable business assets, since zero-day malware learns how to bypass these defenses. Enterprises need to take more preventive approaches to combat advanced targeted attacks.

MetaDefender Core enables you to integrate advanced malware prevention and detection capabilities into your existing IT solutions and infrastructure for better handling common attack vectors: securing web portals from malicious file upload attacks, augmenting cybersecurity products, and developing your own malware analysis systems.capabilities and features.



> *"We evaluated sandboxes, AV vendors and cloud multiscanning vendors for our zero-day malware file upload challenge and chose Deep Content Disarm and Reconstruction from OPSWAT."*
>
> **Teza Mukkavilli**
> Head of Security, Upwork

Key Features and Benefits

Deep Content Disarm and Reconstruction (Deep CDR)

Rebuild over 100 common file types, ensuring maximum usability with safe content. Hundreds of file reconstruction options are available.

Multiscanning

Choose from over 30 leading antimalware engines in flexible package options. Proactively detects over 99% of malware threats by using signatures, heuristics, and machine learning.

File-Based Vulnerability Assessment

Scan and analyze binaries and installers to detect known application vulnerabilities before they are executed on endpoint devices, including IoT devices.

Proactive Data Loss Prevention (Proactive DLP)

Content-check 30+ common file types for personally identifiable information (PII) and redact or add watermark to this sensitive data before they are transferred.

100+ File Conversion Options

Keep files usable and intact through true "reconstruction" of file types or flatten files to less complex formats.

Custom Workflows

Create your own workflow for multiscanning and Deep CDR and customize the order and process in which files are handled.

Archive Extraction

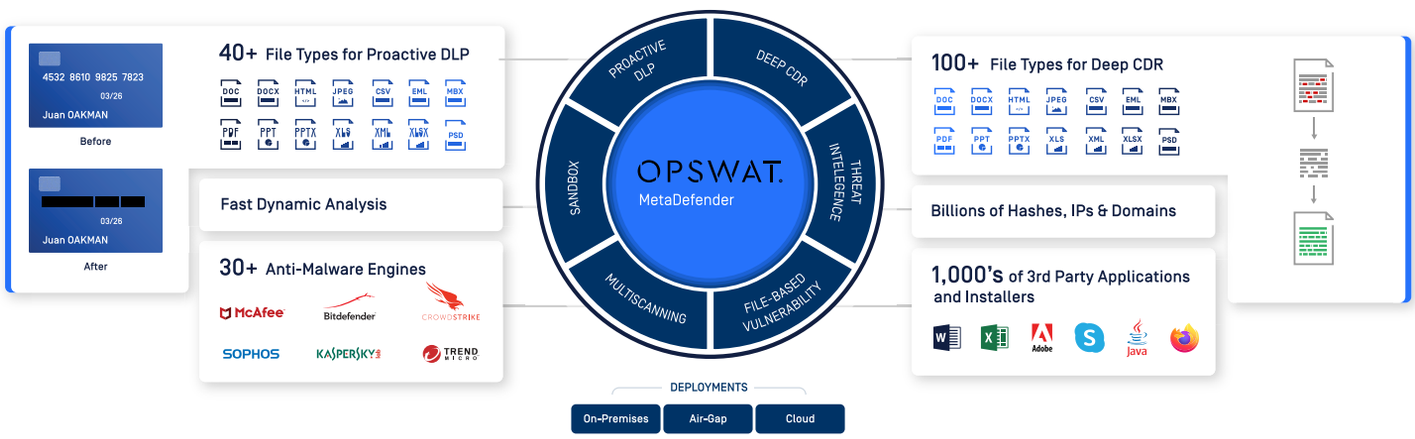
Multiscanning and Deep CDR for more than 30 types of compressed files. Archive handling options are configurable, and encrypted archives are supported.

File Type Verification

Verify over 4,500 file types to determine the actual file type based on the content of the file, not the unreliable extension to combat spoofed file attacks.

OPSWAT.

MetaDefender Core



Why MetaDefender Core

- Mitigating risks for your critical systems and preventing threats that may have bypassed defenses
- Protection for sensitive personally identifiable information from entering or leaving your organization
- Easy deployment on Windows or Linux servers in your environment, even if air-gapped, or using our software-as-a-service offering via MetaDefender Cloud
- Support for many programming languages, for integration into your environment via REST API
- Low total cost of ownership with ongoing maintenance using centralized management

About OPSWAT

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

For further information about MetaDefender Core
opswat.com/products/metadefender/api

To contact a technical sales representative
opswat.com/contact

OPSWAT.
Trust no file. Trust no device.

OPSWAT.

DATASHEET

MetaDefender® Email Gateway Security

Advance Your Email Protection

The majority of malware continues to be initiated through email attacks. Organizations are challenged by slow and often inefficient email security solutions. OPSWAT's new approach to email security delivers a higher level of effectiveness to protect your organization against advanced email attacks.

Key Features

Anti-Phishing and Anti-Spam:
Our advanced multi-step, anti-phishing approach prevents phishing, BEC, and Social Engineering attacks to better avoid human error. Real-time, smart link neutralization checks the reputation of the link when clicked.

Zero-Day Malware Prevention:
Our approach prevents advanced persistent threats (APTs) and zero-day threats. Identifying emails with suspicious behavior or content, including password-protected attachments, helps protect business productivity files in real time.

Advanced Threat Protection:
Multiscanning technologies and multiple anti-malware engines significantly increase early malware detection and reduce vulnerability time to virtually zero.

Proactive Data Loss Prevention:
Proactively prevent data leaks to ensure compliance, and block or redact email content/files to prevent PII from being sent.

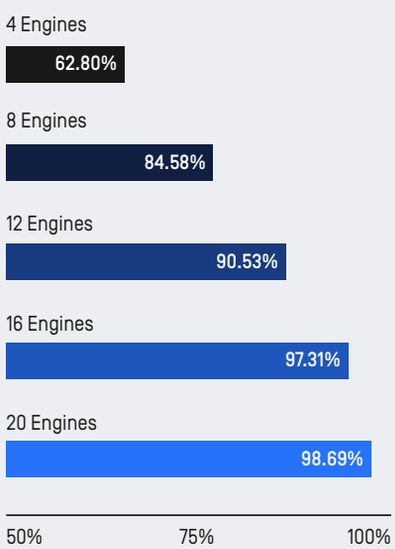
OPSWAT.

MetaDefender Email Gateway Security

Benefits

- Ensures IT can rely less on user awareness.
- Reduces the WoV (Window of Vulnerability) against malware.
- Protects business productivity files
- Effectively eliminates zero-day targeted attacks
- Significantly reduces downtime caused by advanced threats.
- Ensures compliance with PCI and other regulations and protects PII data.

Detection rates of top 10,000 threats with OPSWAT Multiscanning*



* Data shown above is representative of April 2022. Our Detection Efficacy Report is continually updated to reflect a 30-day period.

Visit MetaDefender Cloud | Reports (opswat.com) for the most recent report and information regarding the data collection.

Capabilities

Increase Detection of Advanced Threats

Advanced threat detection and prevention technology provide the highest detection rates. It analyzes each email with machine learning technologies by using up to 20 anti-malware engines (on-premise) and up to 24 anti-malware engines (cloud scanning option).

Reduce Window of Exposure

Multiscanning technology can combine multiple AV engine update windows, reducing the window of vulnerability (WoV) for companies. MetaDefender Core packages can significantly reduce exposure time to less than seven minutes enabling more efficient protection against the ever-increasing malware attacks.

Zero-Day Attack Prevention

Deep CDR disarms every email, including those with password-protected attachments, by removing potentially malicious content. Over 100 common file types are sanitized and only reconstructed, fully usable files are delivered.

Dynamic Anti-phishing

Dynamic, anti-phishing technology addresses attacks across multiple stages. A comprehensive solution applies advanced heuristic, neural network, and spear-phishing filters, as well as IP/sender and content reputation checks. Hyperlinks are naturalized and/or checked by the MetaDefender Cloud reputation engine.

Protect PII & Sensitive Data Loss

Proactive DLP helps to comply with industry regulations, such as PCI, HIPAA, GLBA, GDPR, and FINRA. It automatically detects 70+ file types including PDF and office documents and leverages Optical Character Recognition (OCR) technology to detect and redact sensitive information in images.

Summary

OPSWAT MetaDefender Email Gateway Security provides advanced email protection to ensure that business email communications are confidential, intact, and continuous to business and critical infrastructure by reducing the security risk and eliminating potential human error.

Contact us

OPSWAT.

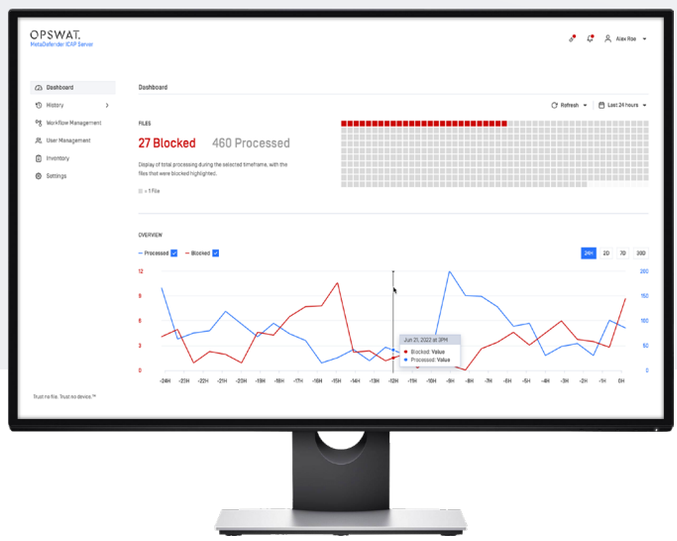
Trust no file. Trust no device.

OPSWAT.

DATASHEET

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.

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.

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

Key Features

Deep CDR (Content Disarm and Reconstruction) 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 (Data Loss Prevention) content-checks files for sensitive, private, and confidential data

File-Based Vulnerability Assessment technology detects application and file vulnerabilities before they are installed

OPSWAT.

MetaDefender ICAP Server

Integration

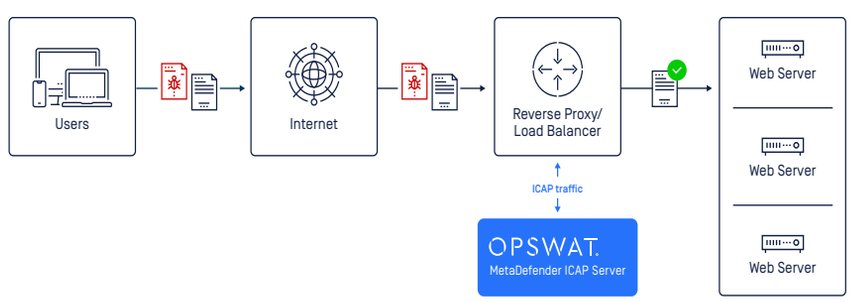
MetaDefender ICAP Server integrates with any product that supports the Internet Content Adaptation Protocol (ICAP) and can be installed at various intersection points to secure file transfers.

Specifications

Deployment Model	**Windows** Windows 10; Windows Server 2012, 2016, 2019 or newer (64-bit)	**Linux** Red Hat (7.x, 8.x); Ubuntu (18.04, 20.04); CentOS (7.x, 8.x); Debian (9.x, 10.x, 11.x)
Hardware Requirements	Minimum RAM: 2GB Minimum SSD: 2 GB + ~500MB x (number of managed scan engines)	
Supported Browsers	Chrome, Firefox, Safari, Microsoft Edge	
Ports	Inbound (1344, 8048), Outbound (8008)	
Supported File Systems	NTFS, FAT32, AFS, Linux EXT2, 3 & 4	
Deployment Model	Online/Offline, Physical/Virtual	

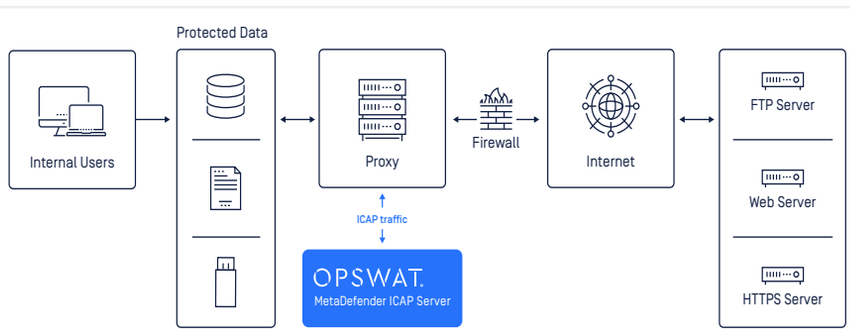
Forward Proxy / Web Gateway / Firewall
Screen web traffic before it reaches a secured network

Supports: Squid, ARA Networks JAGUAR5000, McAfee Web Gateway™, Fortinet FortiGate®



Reverse Proxy / Web Application Firewall / Load Balancer / Application Delivery Controller
Protect application web servers from malicious file upload

Supports: F5® Advanced WAF™, F5 Big-IP® ASM™, F5 Big-IP® LTM™, Citrix ADC, Avi Vantage (VMware), Symantec™ Blue Coat ProxySG

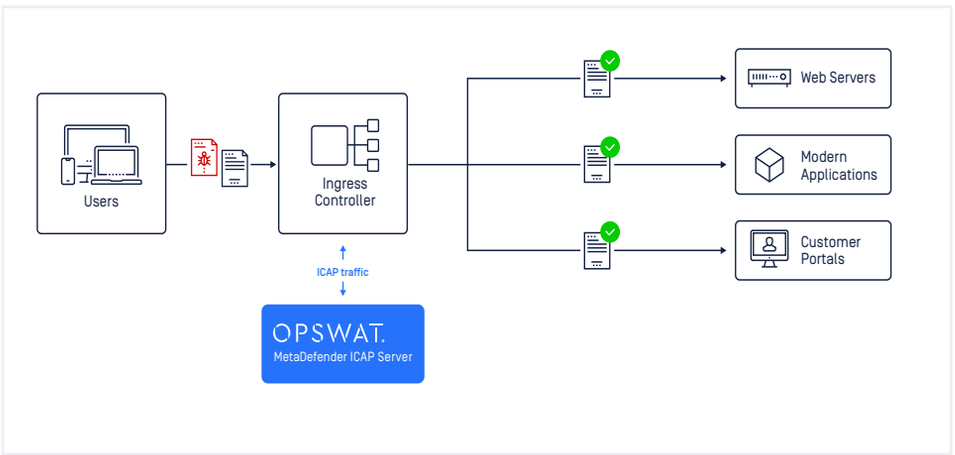


OPSWAT.

MetaDefender ICAP Server

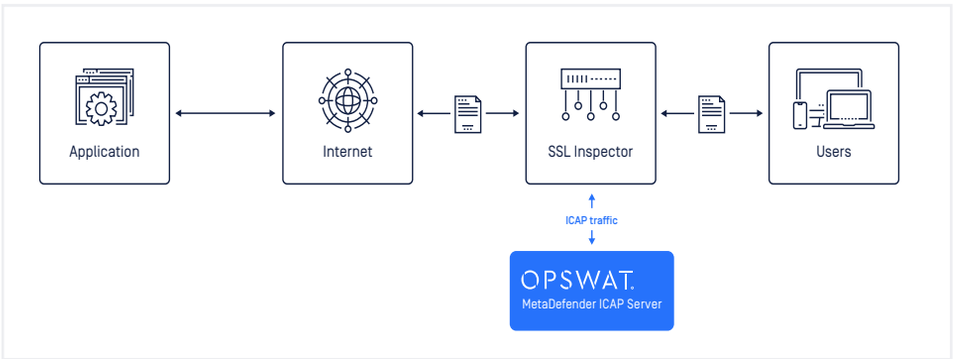
Ingress Controller
Inspect all incoming files for potential malicious files before they are admitted to applications deployed in containerized environments.

Supports: NGINX Plus, NGINX Open Source



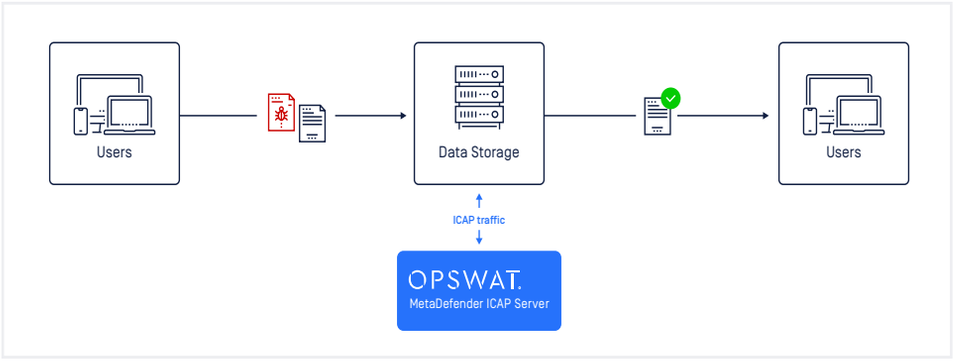
SSL Inspection
Integrate multiple security features at the point of decryption for efficient file-based threat prevention.

Supports: F5® SSL Orchestrator™, A10 Networks Thunder® SSLi®



Managed File Transfer (MFT)
Scan all file traffic as it moves through your data repositories

Supports: GoAnywhere MFT, Progress MOVEit, Axway B2Bi, Axway SecureTransport

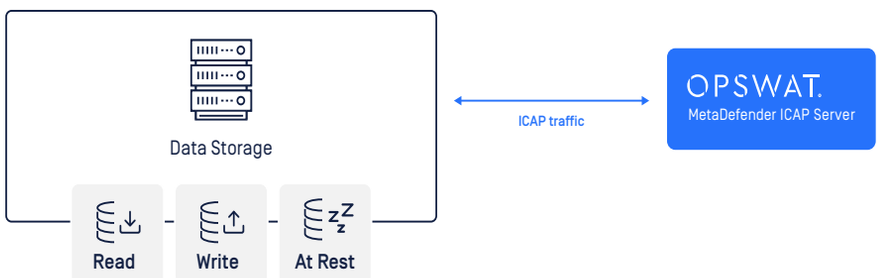


OPSWAT.

MetaDefender ICAP Server

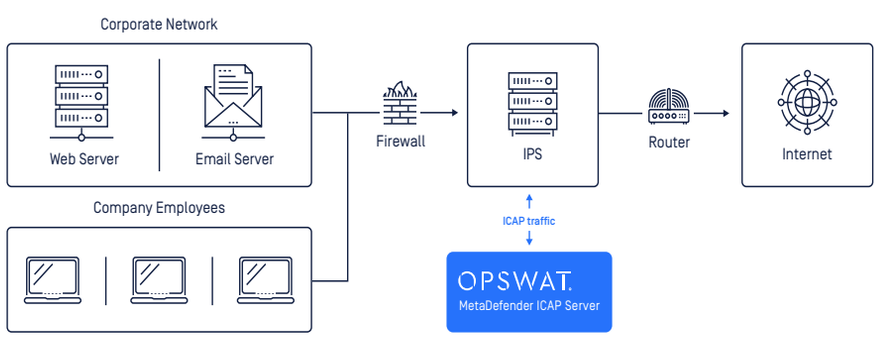
Storage Solutions
Quickly scan files in repositories on read, write, or at rest

Supports: Dell EMC Isilon OneFS, Nutanix Files, Huawei Oceanstor



Intrusion Prevention Systems (IPS)
Enhance the effectiveness of Intrusion Prevention/Detection Systems (IPS/IDS) by adding advanced threat prevention and vulnerability detection

Supports: Any IPS/IDS with ICAP client functionality



OPSWAT.
Protecting the World's Critical Infrastructure

Visit opswat.com/products/metadefender/icap for more information on MetaDefender ICAP Server. Schedule a demo with a cybersecurity expert at opswat.com/contact.

OPSWAT.

DATASHEET

MetaDefender® for Secure Storage

Secure Your Storage

Storage solutions facilitate access, sharing and collaboration. However, they leave the IT and Security departments in a blind spot when it comes to malware and sensitive data loss.

MetaDefender for Secure Storage offers a robust layer of protection for securing stored enterprise data such as files and images. It helps you prevent data breaches, downtime, and compliance violations in your cloud and on-premises storage.

Analyze. Remediate. Report.

Files from users in 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.

MetaDefender for Secure Storage lets you trust the data shared within your organization.

Benefits

Zero-day Threat Prevention

Disarm unknown content and output safe, usable files. OPSWAT's Deep CDR technology is focused on preventing an attack before it occurs. It can sanitize hidden or unknown malware from 80+ file types.

Advanced Threat Detection

Multiscanning from 10 leading anti-malware engines (Mcafee, ESET, Avira, K7 etc.) combining all detection mechanisms (signatures, heuristics, AI/NGAV) leaves little room for error.

Compliance Risk Mitigation

Detect, redact, or block sensitive data. OPSWAT's proactive DLP technology provides automated reporting and remediation for sensitive data loss to keep you in line with regulatory requirements such as HIPAA, PCI-DSS and GDPR.

Broad Integration Coverage

Box, Microsoft OneDrive, Amazon S3, Cloudian can all be seamlessly integrated so that you can start evaluating their health within minutes.

OPSWAT.

MetaDefender for Secure Storage

Features

Processing at scale

With one click - process the entire storage, new files only, or customize for specific files.

Automatic Reporting

See the status of your storage at a glance through automated reports emailed directly to you and your organization's stakeholders; or see it real-time via the comprehensive dashboard.

Flexible Scheduling

Choose a combination of real time processing and scheduling options that fit your organization's needs to keep your storage secure from Zero day threats and Advanced Persistent Threats.

Full auditibility

Monitor and log a history of user actions that can be easily exported for full transparency to facilitate corporate audits.

Automated Workflow

In addition to manual scheduling options, you have the ability to integrate processing into your business workflow via REST API.

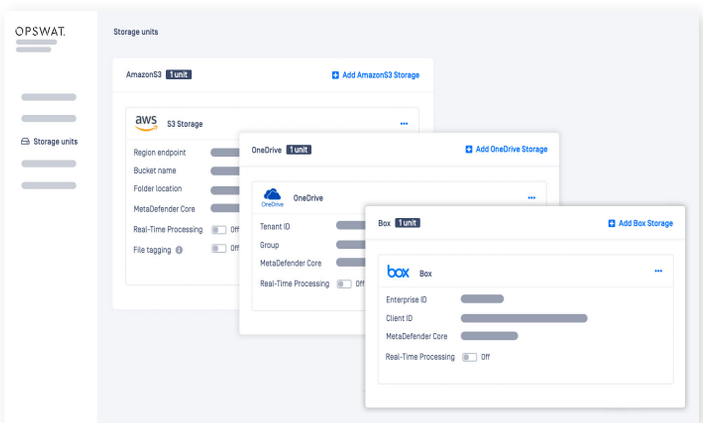
User Management

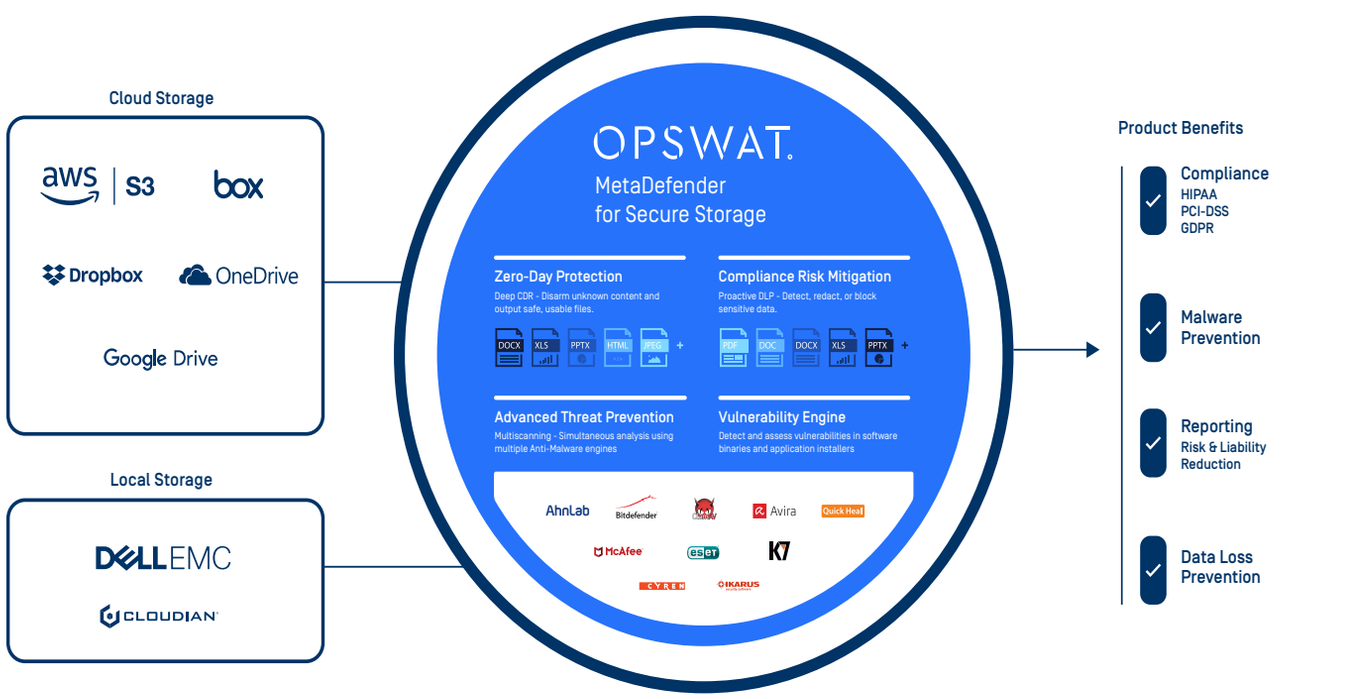
Enable your IT department to effectively manage compliance and data breach risks by giving role based (including 'read only') access to multiple administrators.

Integrations (Amazon S3, Box, and more)

Setup and configure multiple storage units within minutes to manage and secure all your data in one view.

- Integrate with all your Amazon S3 instances.
- Easily configure all your storage units from Box.
- Secure all your data stored in OneDrive and other collaboration solutions.





OPSWAT.

MetaDefender for
Secure Storage

How does OPSWAT minimize your compliance risk?

Regulatory requirements mandate the privacy and security of sensitive customer data.

- OPSWAT checks for any sensitive data that might be inadvertently exposed or maliciously targeted. Role based need to know access (including 'read only') minimizes violations of data privacy laws. Our products alert you to misuse, giving you visibility into suspicious or careless activity by your users. If this activity went undetected, it could put your organization at risk and result in significant regulatory fines and reputational loss.
- OPSWAT's advanced suite of technologies; including industry-leading Mutliscanning from 30+ anti-virus engines, Deep Content Disarm and Reconstruction for sanitization of all files, and Proactive Data Loss Prevention to detect and block sensitive data; helps to meet and exceed the mandated regulatory requirements.

Types of data that OPSWAT protects

- to meet **Payment Card Industry (PCI) Data Security Standards (DSS)** guidelines:
  - **Credit card number**

Risk of Non-compliance

According to PCI Compliance Blog (pcicomplianceguide.org/faq/#15) the penalties for non-compliance are:
The payment brands may, at their discretion, fine an acquiring bank $5,000 to $100,000 per month for PCI compliance violations. The banks will most likely pass this fine along until it eventually hits the merchant. Furthermore, the bank will also most likely either terminate your relationship or increase transaction fees. Penalties are not openly discussed nor widely publicized, but they can be catastrophic to a small business.

- to meet **General Data Protection Regulation (GDPR)** regulations:
  - **Personally identifiable Information (PII) of data subjects**
    - email
    - date of birth
    - phone number
    - passport number

Risk of Non-compliance

There are two tiers of administrative fine for non-compliance with the GDPR:

- Up to €10 million, or, in the case of an undertaking, 2% of annual global turnover – whichever is greater
- Up to €20 million, or, in the case of an undertaking, 4% of annual global turnover – whichever is greater

Fines for GDPR breaches are discretionary rather than mandatory. They must be imposed on a case-by-case basis and should be "effective, proportionate and dissuasive".

ec.europa.eu/info/law/law-topic/data-protection/data-protection-eu_en

- to prevent **Health Insurance Portability and Accountability Act (HIPAA)** violations:
  - **Social Security number**
  - **date of birth**
  - **phone number**
  - **address**

Risk of Non-compliance

Penalties for non-compliance are based on the level of negligence and can range from $100 to $50,000 per violation (or per record), with a maximum penalty of $1.5 million per year for violations of an identical provision. Violations can also carry criminal charges that can result in jail time.

hhs.gov/hipaa/for-professionals/compliance-enforcement/data/enforcement-highlights/index.html

OPSWAT.

Trust no file. Trust no device.

OPSWAT.

DATASHEET

Filescan Sandbox

Rapid. In-depth.

Why Filescan Sandbox?

The OPSWAT Filescan Sandbox integrates a wide range of state-of-the-art tools, services, and proprietary engines to identify Indicators of Compromise (IOCs) and quickly extract threats from files, documents, scripts, and URLs at scale. Using proprietary engines, it goes deeper than traditional static analysis tools providing actionable intelligence in a wide range of scenarios. With exceptional speed, it effectively minimizes the number of artifacts to sandbox, thus streamlining the otherwise time-consuming and resource-intensive process.

Filescan Sandbox employs a cutting-edge emulation engine capable of quickly deobfuscating and analyzing state-of-the-art, environment-aware malware in under 15 seconds. Additionally, it automatically cross-references any relevant Indicators of Compromise (IOCs), such as second stage, downloaded files or URLs, with comprehensive threat intelligence databases for accurate identification.

It integrates into diverse platforms and corporate systems through its straightforward RESTful HTTP-based API and open, agile architecture. The on-premises instance only requires a single server to enable the immediate processing of thousands of files and URLs per day. The web interface provides user-centric reports that are easy to understand and contain in-depth data.

Verified Technology

We are confident about our technology and actively seek feedback from users. As part of this effort, we operate a free community service at www.filescan.io, which undergoes rigorous scrutiny through thousands of daily scans. Our commitment to field testing against emerging malware and phishing threats creates a relevant and robust solution.

As passionate researchers, we frequently experiment with cutting-edge technology on the community platform, enabling us to adapt to the latest cybersecurity trends quickly— after thorough testing and validation, our technology transitions into our enterprise-grade commercial product.

Visit the OPSWAT Filescan documentation to learn more about integration and customization options.

Key Features

- Extract Indicators of Compromise (IOCs) from a wide range of executables, documents, scripts, and URLs.
- Emulates 90%+ of highly obfuscated state-of-the-art macro malware (VBA), VBS, PowerShell, Jscript, MSHTA, XSL, WSF.
- Improve detection of unknown malware with ML-powered Threat Intelligence Similarity Search.
- Simple and cost-effective, on-premises standalone deployment or private cloud.
- Rapid & deep analysis at a large scale (25K+ scans per day/ machine).
- REST API for automated integration and Single source of truth reputation endpoint.
- Single source of truth reputation endpoint
- Integrates with MetaDefender Core, MetaDefender Cloud, Palo Alto Cortex XSOAR, Splunk SOAR, VirusTotal, YARA, MITRE ATT&CK framework and more
- Clean and intuitive reports with in-depth data on demand and able to export in HTML, PDF, MISP, STIX.
- Designed, engineered, and maintained by experienced experts.

OPSWAT.

Filescan Sandbox

Example Hardware Setup

- Intel Xeon-E 2136 (12M Cache, 3.30 GHz)
- RAM 32GB DDR4 ECC 2666 MHz
- 2x SSD NVMe 256GB RAID

Note: this is an example system that would allow processing 25K files/ day with a retention period of 10 days.

Minimal Technical Requirements

- Ubuntu Server 20.04 LTS ("Focal Fossa")
- 8 vCPUs (Preferably 16 vCPUs)
- 16GB RAM (Preferably 32GB)
- 32 GB SSD Disk Space

Throughput / Hardware Requirements

The following table lists explanatory system specs with a retention period of 10 days:

Scans Per Day	Required System CPUs	Required System RAM	Required Storage per Retention Period
1000	4	4GB	256GB
2500	4	4GB	256GB
5000	4	4GB	256GB
10000	8	8GB	256GB
25000	16	16GB	256GB

Get in Touch

Start your free trial of Filescan at our community platform today. Need more privacy and want to learn about our on-premises offering? Please get in touch at sales@filescan.com.

OPSWAT.

DATASHEET

Filescan Sandbox

Sandbox Engine Features	Filescan	Vendor A	Vendor B	Vendor C	Vendor D
Render URLs and Detect Phishing Sites	✓	✓			
Extract and Decode Nearly All Malicious VBA Macros	✓		✓		
Analyze VBA Stomped Files Targeted for Any System	✓				
Shellcode Emulation (x86, 32/64)	✓				
Export MISP (JSON) and STIX Report Formats	✓		✓		
Extract and Analyze Embedded PE Files	✓				
Deobfuscate Javascript/VBS	✓		Limited		
Deobfuscate Powershell Scripts	✓		Limited		
Deobfuscate MSHTA Scripts	✓				
Parse METF Embed Equation Exploit Structure	✓				
Parse Malformed RTF Files	✓				
Parse Office Binary File Formats (BIFF5/BIFF8)	✓				
Parse Strict OOXML File Format	✓				
Automatically Decode Embedded Base64 Strings	✓				
Extract Annotated Disassembly	✓				
Decrypt Password Protected Office Documents	✓		✓		
Decompile Java	✓		✓		
Decompile .NET	✓		✓		
Calculate .NET GUIDs (Module Version/TypeLib Id)	✓	✓			
Classify Imported APIs	✓			✓	
MITRE ATT&CK Support (In-report and Search)	✓		✓	✓	
Render PDF Pages	✓	✓	✓		
Extract Embedded Files (eg: OLE2 from Word)	✓	✓	✓		
Automatically Tag Samples Based on Signatures	✓	✓	✓		
YARA Support	✓	✓	✓		✓
Generate Text Metrics (Average Word Size, etc.)	✓				
Detect Cryptographic Constants	✓				✓
Text Analysis (Guessed Language)	✓	✓			

OPSWAT.

DATASHEET

Filescan Sandbox

Sandbox Engine Features	Filescan	Vendor A	Vendor B	Vendor C	Vendor D
Map UUIDs to Known Associated Files / Metadata	✓		Limited		
Filter Strings and Detect Interesting Ones	✓		✓	✓	
Extract and Detect Overlay	✓			✓	✓
Integrated Allowlist	✓	✓	✓		
Detect Alternative IOCs (Emails, Bitcoin Address, etc.)	✓		✓		✓
Calculate Authentihash	✓	✓	✓		
Verify Authenticode Signatures	✓	✓	✓	✓	
Parse RICH Header	✓	✓	Limited	✓	✓
Calculate Entropy of Resources	✓	✓		✓	✓
Detect URLs, Domains and IP Addresses	✓	Limited	✓	✓	✓
Calculate Hashes of Resources	✓	✓		✓	✓
Calculate Imphash	✓	✓	✓		✓
Calculate SSDEEP	✓	✓	✓		✓
Extract PDB Information	✓	✓	✓	✓	
Detect TLS Callbacks	✓		✓	✓	✓
Resolve Known Import Ordinals to Names	✓		✓	✓	✓
Detect Anomalies (eg: Header Checksum Validation)	✓	Limited	✓	✓	✓
Query VirusTotal and MetaDefender Cloud for Reputation Checks	✓	✓	✓	✓	✓
Detect Packers (PEiD)	✓	✓	✓	✓	✓
Detect File Types	✓	✓	✓	✓	✓
Calculate Hashes of Sections	✓	✓	✓	✓	✓
Calculate Entropy of Sections	✓	✓	✓	✓	✓
Extract Strings from Executable	✓	✓	✓	✓	✓
Extract/Detect Resources	✓	✓	✓	✓	✓
Extract/Detect PKCS7 Certificate	✓	✓	✓	✓	✓

OPSWAT.

DATASHEET

MetaDefender® Vault

Storage you can trust

Transferring files into and out of any environment exposes systems to breach and infection.

Portable media are often used to conduct these transfers, bypassing security protocols.

MetaDefender Vault is a secure file storage and retrieval solution that protects critical files.

Secure. Approve. Access.

The moment files enter MetaDefender Vault, they are scanned for malware and vulnerabilities. Files are evaluated continuously, as virus definitions are updated. Suspicious files can be sanitized. Sensitive files can be redacted.

Rules can be created to block access to files for a pre-set containment period—to prevent latent outbreaks and zero-day attacks. Job function and approval sequences confirm who must authorize inbound and outbound files and who can access them.

MetaDefender Vault lets you trust the data that travels into, across, and out of your environment.

Benefits

Sanitize Suspicious Files

Disarm unknown content and output clean, usable files

File-based Vulnerability Assessment

Finds exploits before they reach your environment

Industry-leading Multiscanning

Integrated multiscanning of 30+ engines

Sensitive Data Block

Detect, redact, or block sensitive data

Language Localization

Global deployment, consistent experience

Policy Enforcement

Meet requirements for media-less environments

OPSWAT.

MetaDefender Vault

Features

Outbreak prevention through continuous scanning and optional time-specific quarantine

Supervisor approval & secure data workflow processes

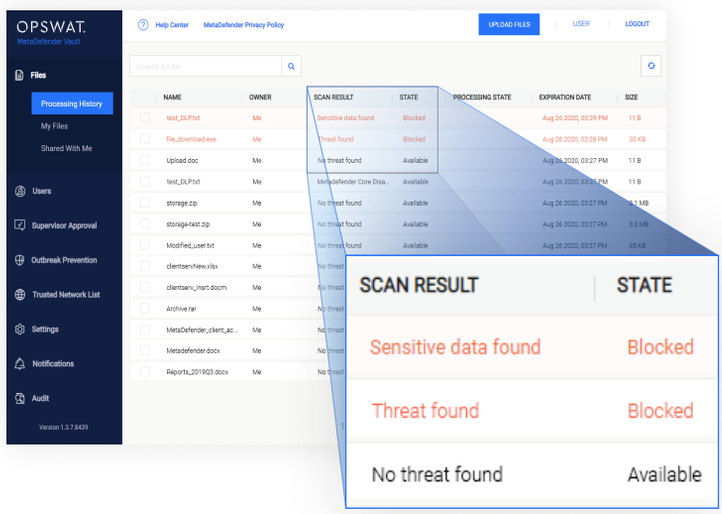
All stored files are encrypted with **Advanced Encryption Standard (AES)**

Direct integration with **Microsoft Active Directory** to speed user adoption

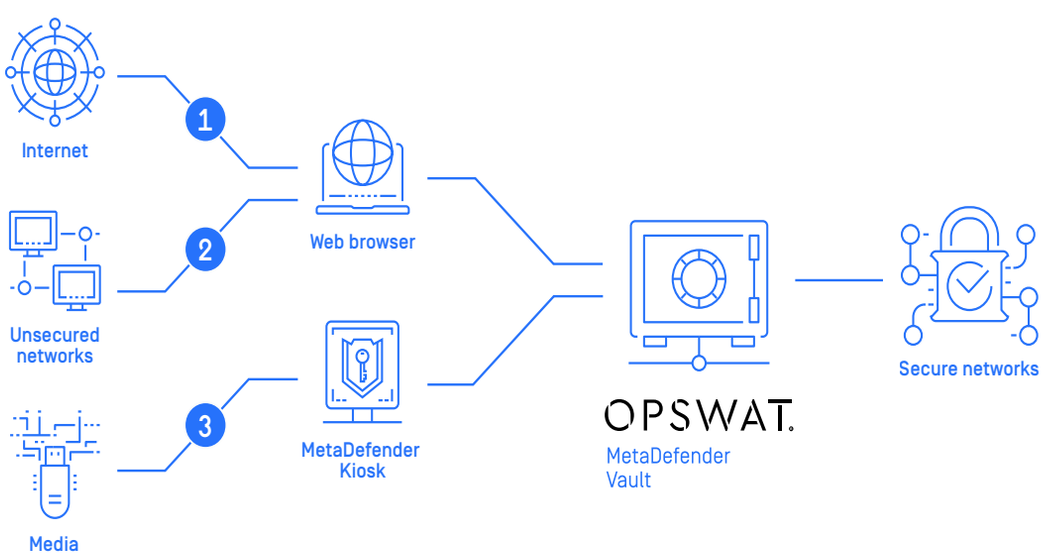
Storage and retrieval behaviors are logged and **fully auditable**

Integrates with **MetaDefender Kiosk** for portable media support and **MetaDefender Email** to sanitize attachments

End users can access Vault via an **internet browser**, removing the need for local software installation.



MetaDefender Vault secures data flow, with flexible deployment options



1. Navigate to MetaDefender Vault's web portal interface, and upload a file. Then access files safely via secure networks internally.
2. Transfer files in between low security and high security systems, using MetaDefender Vault as a secure hub.
3. Plug portable media into MetaDefender Kiosk, and access files through MetaDefender Vault. This process can also be reversed, to extract files.

OPSWAT.

Trust no file. Trust no device.

OPSWAT.com/contact

OPSWAT.

DATASHEET

MetaDefender® Drive

Trust you can hold in your hand

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 a MetaDefender Drive before a device enters a facility to inspect the device for malware before the device boots.

Isolate. Analyze. Address.

MetaDefender Drive creates a portable perimeter, anywhere maintaining an air-gap is critical. Once plugged into a USB port, the computer is booted safely from MetaDefender Drive, by running off of MetaDefender Drive's own operating system. This separation allows analysis without software installation, scanning the entire device for malware, vulnerabilities, and overall integrity. Deep forensic analysis is conducted on every possible file, and detailed threat reports pinpoint which files need to be removed and remediated.

Highlights

Multiscanning
Scans 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. Supports scanning while target system is online or offline.

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.

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

Multiple operating system support
Microsoft Windows, macOS and Linux.

Robust support for file systems
Supports NFTS, FAT32, APFS, or Linux ext2, ext3, ext4.

Central manageability
Options to connect to OPSWAT Central Management for reports and configurations from a single platform.

Tamper Proof
Device firmware is protected by a digital signature. The ruggedized housing is waterproof and tamper proof.

Data Privacy
Run on-premises for maximum privacy. No data is sent to the cloud.

OPSWAT.

MetaDefender Drive

Specifications	MetaDefender Drive Enterprise	MetaDefender Drive Advanced
Security Features		
Advanced Malware Scanning	Kaspersky, Ahnlab, Bitdefender, Avira, and K7	McAfee, ESET, Bitdefender, Avira, and K7
File-based Vulnerability Assessment	Included	Included
Proactive DLP	-	Included
Hardware Security		
Digital Security	Digitally Signed Trusted Secure Firmware (RSA-2048 Bit)	Digitally Signed Trusted Secure Firmware (RSA-2048 Bit)
Physical Security	FIPS 140-2 Level 2 compliant physical epoxy security encapsulation	FIPS 140-2 Level 2 compliant physical epoxy security encapsulation
Hardware Performance		
USB Write Speed	170MB/s	170MB/s
USB Type	USB 3.0	USB 3.0
USB Connector	USB Type A	USB Type A
Hardware Specification		
Physical Dimensions	2.9" x 0.8" x 0.4" 71mm x 19mm x 9mm	2.9" x 0.8" x 0.4" 71mm x 19mm x 9mm
TAA Compliant	Yes	Yes
Package Weight	38 g	38 g
Storage Temperature	-25°C to +85°C	-25°C to +85°C
Operating Temperature	0°C to 70°C	0°C to 70°C
Operating Humidity	20% to 90%	20% to 90%
Material	Aluminum	Aluminum
Shock Resistance	1000G maximum	1000G maximum
Vibration Resistance	15G maximum, peak-to-peak	15G maximum, peak-to-peak
Compatibility		
Computer Hardware Platform	Linux, Intel-based Macs from 2006-2017, Windows	
System Requirements	Windows® 7, 8, 8.1, 10 macOS X 10.8 Mountain Lion (or newer) Linux Debian 5 based (or newer), RHEL 6 based (or newer) Minimum 4GB RAM	

OPSWAT.

Trust no file. Trust no device.

OPSWAT.

DATASHEET

MetaDefender™ USB Firewall

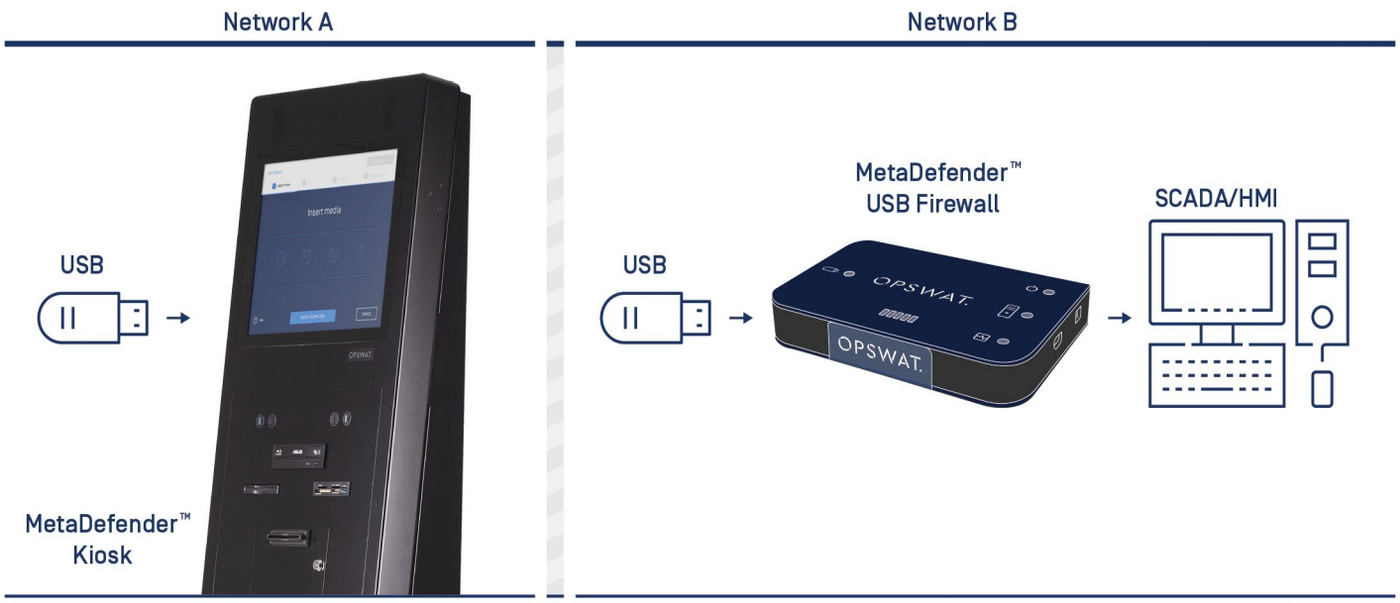
Providing another option for securing and controlling portable media use in Critical Infrastructure

For immediate 2021 release; the MetaDefender USB Firewall from OPSWAT provides yet another option for safely and securely leveraging the productivity advantages, flexibility, and convenience of portable media in IT or OT SCADA environments.

Complementing OPSWAT's MetaDefender Kiosk, MetaDefender Vault, and the OPSWAT Client for Windows, Linux, and Mac, the MetaDefender USB Firewall provides a plug-and-play, no install, no software footprint path to securing portable media; ensuring the boot sector and file contents of portable media are inspected, audited, sanitized, and approved prior to use.

Features

- Automatically blocks unprocessed or compromised files
- Boot Sector Protection
- Works with MetaDefender Kiosk Manifest to Audit Files
- No software install required
- Portable Media Security assists in Policy, Regulation, and Standards Compliance
  - NERC CIP, ISA 62443, NIST 800-53, NIST 800-82, ISO 27001



OPSWAT.

MetaDefender USB Firewall

Making the Case

Information Technology and Operational Technology (IT/OT) skilled personnel are in high demand. This has made it challenging to hire and retain internal teams. Many companies therefore default to outsourcing skilled contract labor. These contractors are required to support a great many client applications internally, in the cloud, and in the field. This support often requires an exchange of files with offsite sources in order to accommodate a variety of patching, updates, applications, and data analysis.

In lieu of VPN or internet access to the client facility or cloud, portable media has often filled the gap. Portable media devices have improved personnel, process, and technology environments worldwide through leveraging their productivity advantages, flexibility, and convenience. Unfortunately, portable media devices have also served as a transfer point for malware and intellectual property.

USB devices are consistently listed as one of the top cybersecurity vulnerabilities in IT as well as the OT environments of critical infrastructure. Many companies have therefore chosen to internally lock down or remove access to USB ports in order to reduce cyber risk. Some have also taken on the resource intensive task of issuing their own managed laptops to contractors. Regardless, the need for a secure exchange of files remains.

What if there was a way to safely and securely leverage the full productivity, flexibility, and convenience of portable media in an IT or OT environment? Effectively, what if you could have your cake and eat it too? The MetaDefender Kiosk and USB Firewall is the solution that delivers on this vision.

Technical Specifications

USB Media Type Support

- USB Type A
- USB 2.0 High speed

Minimum System Requirements

- Windows, Linux, Mac
- USB Type-A USB 1.0 or greater

Supported File Systems

- FAT, NTFS, Ext; VHD & VMDK

Material

- Aluminum and ABS

Physical Characteristics

- Dimensions : 125mm x 80mm x 23mm
- Weight : 460g

In the Box

- MetaDefender USB Firewall
- USB power adapter and cable
- USB Micro to Type A cable
- Protective case
- Quick start booklet
- Limited Warranty 1yr

Power

- Supply: 5V DC via USB Wall Adapter (minimum 2A)
- Active consumption: 1A @ 5V (5W)
- Standby consumption: 500mA @ 5V (2.5W)

Regulatory Compliance

- FCC
- CE
- RoHS/REACH

OPSWAT.

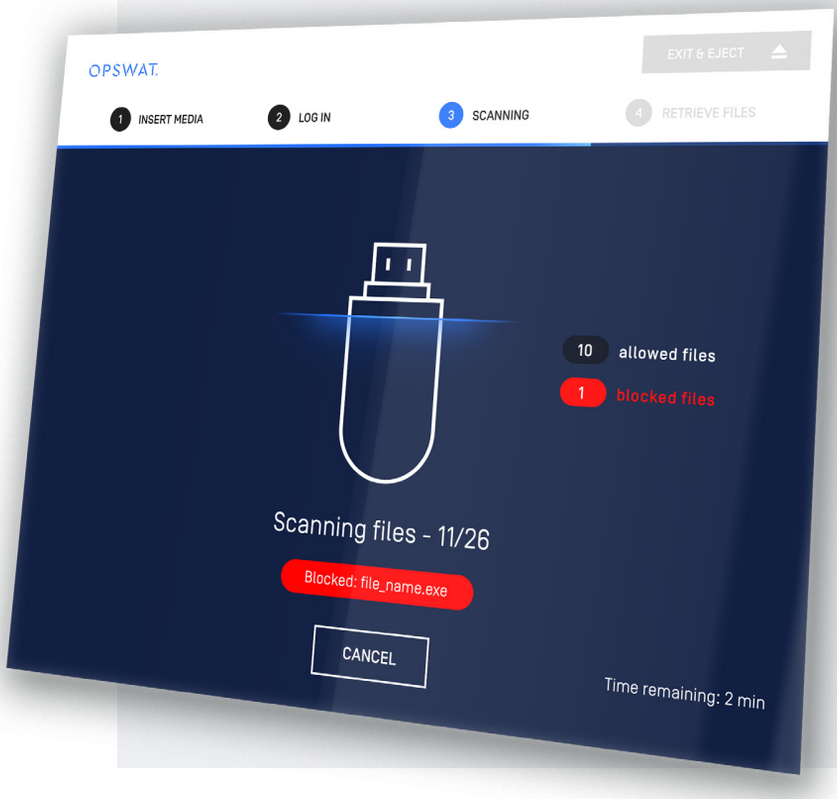
Trust no file. Trust no device.

OPSWAT.

DATASHEET

MetaDefender® Kiosk

Trust at the point of entry



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

Anytime 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.

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 Vault** for file storage and retrieval

OPSWAT.

MetaDefender Kiosk

Benefits

Clean & Reconstruct Suspicious Files

Disarm unknown content and output clean, usable files

Industry-leading Multiscanning

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

Prevent Sensitive Data Leakage

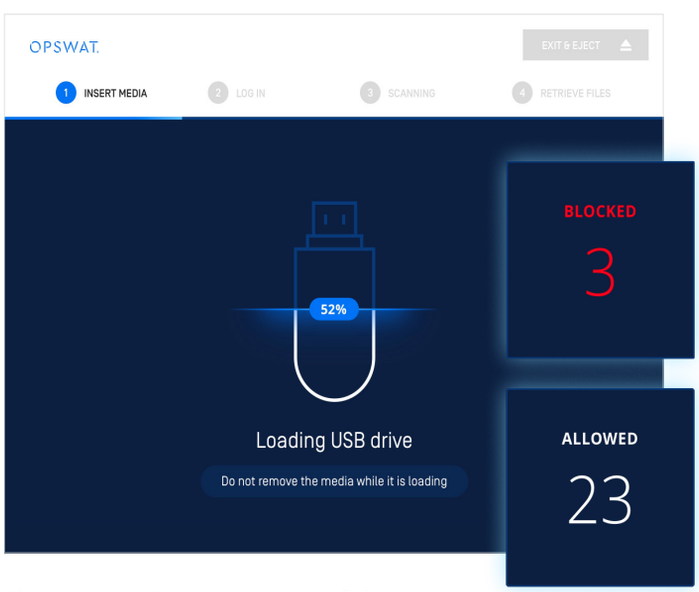
Detect, redact, or block sensitive data

Streamline Data Transfer

Global deployment, consistent experience

Meet Compliance

Fulfill regulatory requirements



After portable media is inserted into MetaDefender Kiosk, all files are scanned for malware and vulnerabilities. Malicious files are blocked. Suspect files can be cleaned. Only clean, safe portable media enter your environment.

Capabilities

Proactive Data Loss Prevention (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 Content Disarm & Reconstruction (Deep CDR)

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

Multiscanning

Proactively detects 99%+ of malware threats; integrates 30+ 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

OPSWAT.

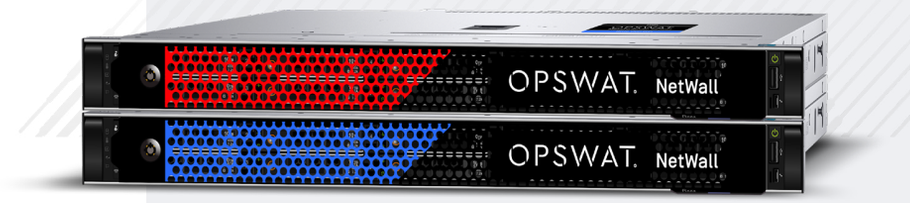
Trust no file. Trust no device.

OPSWAT.

DATASHEET

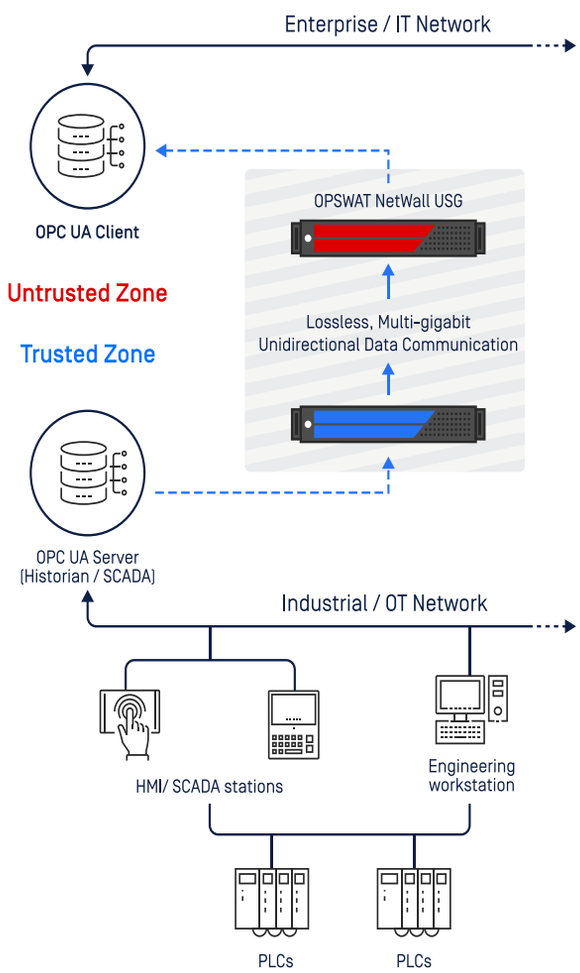
NetWall USG™

Unidirectional Security Gateway for Safe OT/IT Communications



OT Cybersecurity That No Firewall Can Match

OPSWAT NetWall USG (Unidirectional Security Gateway) 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. NetWall USG enforces one way data flows while guaranteeing payload delivery and preventing data loss and retransmission.



NetWall USG Assures No Way Back to the OT Network

Key Features

Guaranteed payload delivery with absolutely no data loss.

Anti-overrun control eliminates data overflow, retransmissions, and sync issues.

No return path: one-way data flows are enforced by a non-networked serial connection between the NetWall USG server pair.

Easy to deploy: preconfigured platform deploys quickly, seamlessly.

Simple to operate: ready for use in minutes after one-time initial setup. No firewall audit or configuration needed.

Highly scalable: choose 100 Mbit, 1 Gbit or 10 Gbit throughput—all software selectable.

Transparent to users: high-fidelity data replication means there is no need to alter work procedures of corporate users.

Enables regulatory compliance: for many requirements of Industrial Cyber Security standards, including 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 for ICS.

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

OPSWAT.

NetWall USG

Lossless, Unidirectional Data Communications

- Isolate OT/ICS assets against cyberattacks
- Prevent malicious C&C communications from the OT network
- Segment and protect networks, devices, historians, SCADA, DCS, HMIs, and PLCs
- Seamless integration with OPSWAT MetaDefender Kiosk and Vault
- Secure the transfer of software updates and other files to the protected domain

OPSWAT NetWall USG Specifications

PRODUCT DESCRIPTION	
NetWall USG is delivered as a preconfigured appliance, comprising of a pair of 19" 1U rack mounted servers (2U total). Includes a non-networked serial cable, USB security dongles and management console. Field upgradable by software licensing.	
PRODUCT PART NUMBERS	
NetWall USG 100 Mbps	MD-NW-UNI-100Mbps
NetWall 1 Gbps Upgrade	MD-NW-1Gbps-UG
NetWall 10 Gbps Upgrade	MD-NW-10Gbps-UG
PLATFORM SPECIFICATION	
Redundant Power Supplies	250W
Voltage	100-240VAC, auto ranging
Power Consumption	Typical ~150W
USB Interface	1 USB socket on each platform to connect provided USB crypto key
TESTED LATENCY*	
TCP data stream	0.6ms
UDP data stream	0.7ms
RELIABILITY	
MTBF	> 50,000 hours
FORM FACTOR	
Weight	2 units @ 27lb / 12.2kg each
Mounting	Rack mounting kit supplied

Broad Support for Unidirectional OT/IT Convergence

OPSWAT NetWall Unidirectional Gateway data replication solutions support a wide range of industrial OT and corporate IT protocols and applications.

Application and Protocol Support

Industrial Protocols

- Modbus
- OPC (UA, DA, A&E)
- MQTT-SN
- IEC104

IT Protocols

- UDP, TCP, HTTP, HTTPS
- Video/Audio stream transfer

IT Monitoring Applications

- Log Transfer, SNMP Traps, SYSLOG
- SIEM integration via SYSLOG

File/Folder Transfers

- FTP, SFTP, Folder and file transfers/copying
- Windows File Share, SMB, CIFS
- Antivirus updates, patch (WSUS) updates

OPSWAT.

Protecting the World's Critical Infrastructure

OPSWAT.

A Unified Zero-Trust Security Platform

The OPSWAT MetaAccess Zero-Trust Access Platform delivers security compliance, visibility, and control to every device and user accessing your enterprise resources. Based upon the Software Defined Perimeter Technology (SDP), a more robust alternative compared to VPN, it examines devices to make sure that they are secure, with the required security controls installed.

It then goes much deeper by doing a comprehensive device posture check including executing a risk and vulnerability evaluation with the ability to detect and fingerprint close to 10,000 third-party applications.

Once the MetaAccess Zero-Trust Access Platform has ensured that the endpoint device is compliant and secure, the user will be authorized through an integrated IAM (identity authorization management) solution. Their access to corporate resources is then permitted based on a policy of least-privilege access.

Supported Endpoints

- Windows - Windows 7 and above
  Windows Server 2008 and above
- MacOS - OSX 10.9 and above
- iOS - iOS 8.3 and above
- Android - Android 5.1 and above
- Debian-based Linux v4 (15.4.x) Ubuntu 16/Mint 18/Debian 8
- Red Hat-based Linux v4 (15.6.x) CentOS 7.14/Red Hat Enterprise 7/OpenSuse 11.4/Suse Enterprise 12.x/Fedora 27

Platform Modules

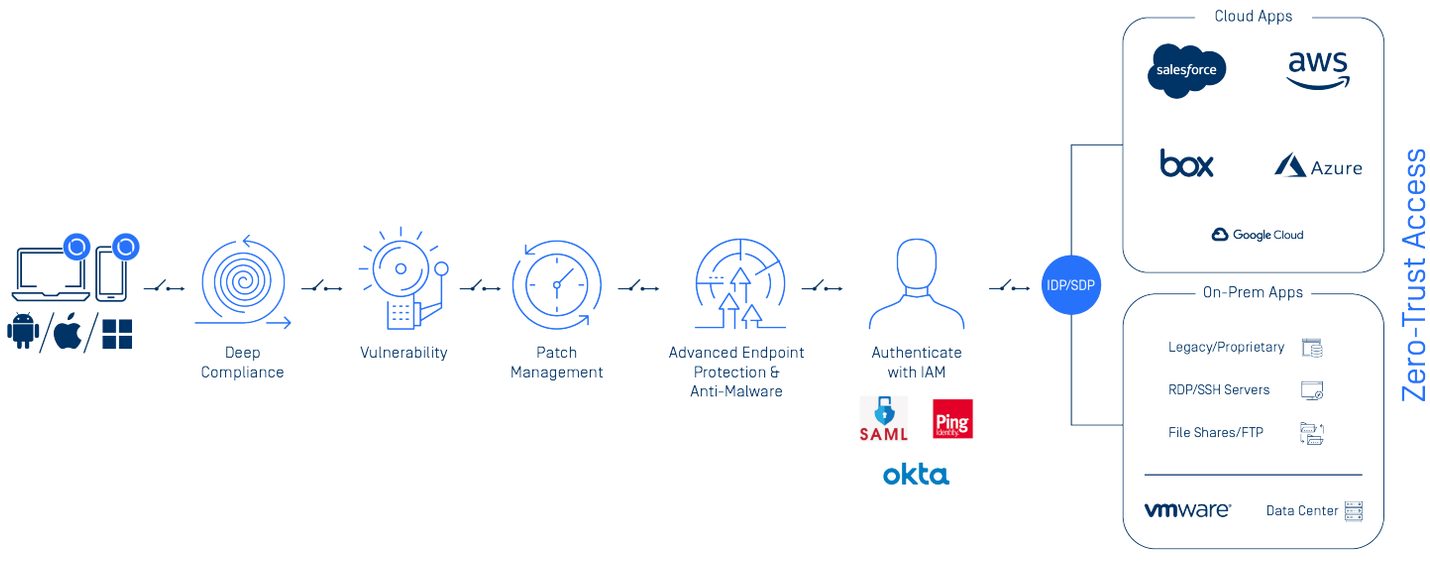
MetaAccess Platform and Compliance
Device posture checks to verify compliance to regulations and policy

Vulnerability Detection
Detection of more than 25K CVEs and OS security patch gaps

Patch Management
Automated patching of ~10K 3rd party apps

Advanced Endpoint Protection
Threat protection using 20+ AV engines, application control & privacy protection

Secure Access
User authorization (IAM) and least-privilege secure access to resources



SIEM syslog-ng sumo logic splunk>

OPSWAT.
Protecting the World's Critical Infrastructure

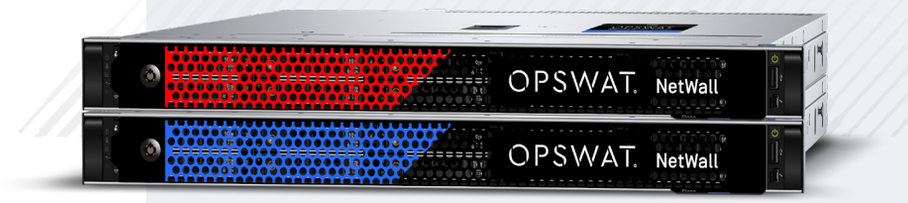
OPSWAT.com/contact

OPSWAT.

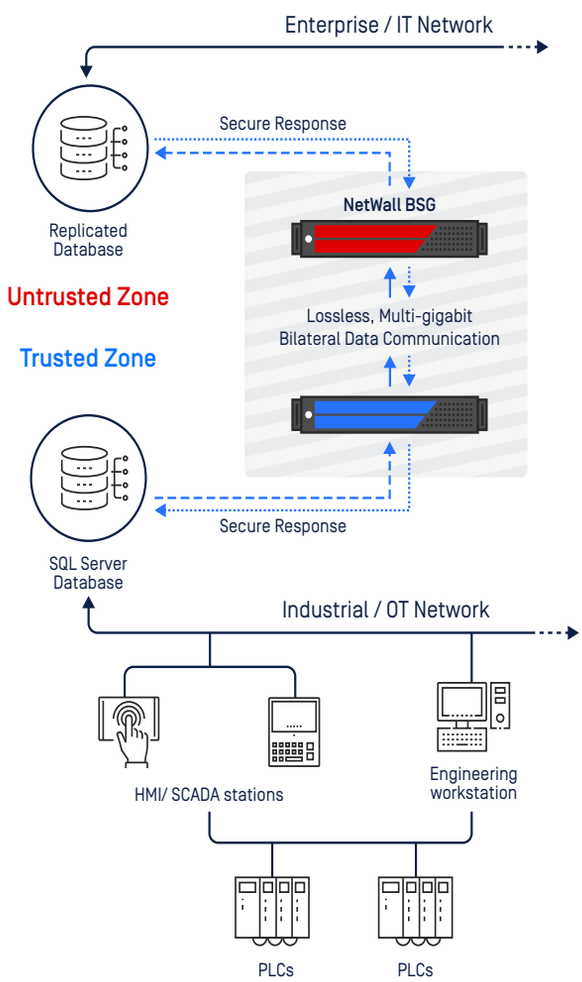
DATASHEET

NetWall BSG™

Bilateral Security Gateway for Safe OT/IT Communications



OPSWAT NetWall 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. NetWall 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.



Use NetWall BSG for OT Data Replication with Secure Response

Key Features

Guaranteed payload delivery with absolutely no data loss.

Anti-overrun control eliminates data overflow, retransmissions, and sync issues.

No return path: one-way data flows are enforced by a non-networked serial connection between the NetWall USG server pair.

Bilateral support mechanism permits data replies while enforcing full protocol break and physical isolation.

Easy to deploy: preconfigured platform deploys quickly, seamlessly.

Simple to operate: Ready for use in minutes after one-time initial setup. No firewall audit or configuration needed.

Highly scalable: Choose 100 Mbit, 1 Gbit, or 10 Gbit throughput—all software selectable.

Benefits

- Lossless, unidirectional OT to IT data communications
- Includes a unique mechanism to permit receiving data replies for select applications
- Isolates OT/ICS assets against cyberattacks
- Prevents OT network data exfiltration, malicious C&C communications
- Segments and protects networks, devices, historians, SCADA, DCS, HMIs, and PLCs

OPSWAT.

NetWall BSG

OPSWAT NetWall BSG Specifications

PRODUCT DESCRIPTION	
NetWall BSG is delivered as a preconfigured appliance, comprising of a pair of 19" 1U rack mounted servers (2U total). Includes a non-networked serial cable, USB security dongles and management console. Field upgradable by software licensing.	
PRODUCT PART NUMBERS	
NetWall BSG 100 Mbps	MD-NW-BIL-100Mbps
NetWall 1 Gbps Upgrade	MD-NW-1Gbps-UG
NetWall 10 Gbps Upgrade	MD-NW-10Gbps-UG
PLATFORM SPECIFICATION	
Redundant Power Supplies	250W
Voltage	100-240VAC, auto ranging
Power Consumption	Typical ~150W
USB Interface	1 USB socket on each platform to connect provided USB crypto key
TESTED LATENCY*	
TCP data stream	0.6ms
UDP data stream	0.7ms
RELIABILITY	
MTBF	> 50,000 hours
FORM FACTOR	
Weight	2 units @ 27lb / 12.2kg each
Mounting	Rack mounting kit supplied

Broad Support for OT/IT Convergence

OPSWAT NetWall Bilateral Gateway data supports a wide range of OT nad IT protocols and data replications, including applications requiring a response message.

Application and Protocol Support

Industrial Historian Replication

- GE Proficy Historian
- Aspentech IP21
- OSIsoft PI
- CanaryLab Historian + other Industrial Historians

IT Protocols

- UDP, TCP, HTTP, HTTPS
- Video/Audio stream transfer

Industrial Protocols

- Modbus
- OPC (UA, DA, A&E)
- MQTT-SN
- IEC104

IT Monitoring Applications

- Log Transfer, SNMP Traps, SYSLOG
- SIEM integration via SYSLOG
- GE OSM

Relational Database Replication

- Microsoft SQL
- Oracle Golden Gate + other RDB

File/Folder Transfers

- FTP, SFTP, Folder and file transfers/copying
- Windows File Share, SMB, CIFS
- Antivirus updates, patch (WSUS) updates

OPSWAT.

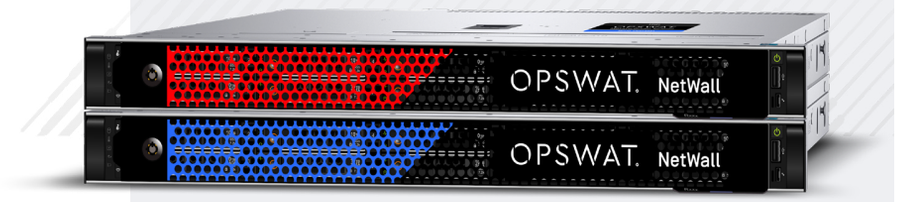
Protecting the World's Critical Infrastructure

OPSWAT.

DATASHEET

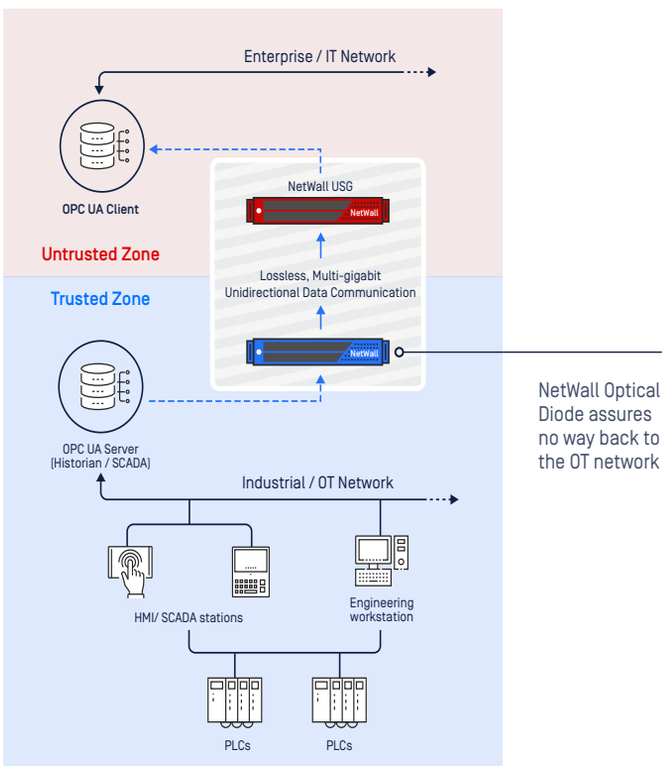
NetWall Optical Diode™

Unidirectional Security for Safe OT/IT Communications



Hardware-Enforced, Deterministic, One-Way Data Transfer Data Diode

In compliance with NEI and other cyber security controls, NetWall 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. NetWall 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.



Key Features

Highly Reliable Payload Delivery: Secure and reliable data delivery over a hardware enforced one-way optical connection.

No Return Path: One-way data flows are enforced by a non-networked serial connection between the NetWall server pair.

Easy to Deploy: Preconfigured platform deploys quickly, seamlessly.

Simple to Operate: Ready for use in minutes after one-time initial setup. No firewall audit or configuration needed.

Highly Scalable: Choose 100 Mbps, 1 Gbps, or 10 Gbps license. The Din Rail version starts at 10 Mbps and can be licensed to 100 Mbps.

Transparent to Users: High-fidelity data replication means there is no need to alter work procedures of corporate users.

Enables Regulatory Compliance: Meets many requirements of Industrial Cyber Security standards, including 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 for ICS.

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

OPSWAT.

NetWall Optical Diode™

Reliable Unidirectional Data Communications

- Isolates OT/ICS assets against cyberattacks
- Blocks any traffic originating from the IT network from entering the OT Network
- Segments and protects networks, devices
- Seamlessly integrates with OPSWAT MetaDefender, Kiosk, and Vault
- Secures the transfer of software updates and other files to the protected domain
- Optional OPSWAT MetaDefender Core integrates into NetWall for advanced malware prevention and detection

PRODUCT DESCRIPTION	
NetWall Optical Diode is delivered as a preconfigured appliance, comprising of a pair of 19" 1U rack-mounted or din rail mount servers (2U total). It includes a non-networked optical cable, USB security dongles, and it is field-upgradable by software licensing.	
ENVIRONMENTAL DIN RAIL SERVER	
Voltage	12 - 36 VDC
Power Consumption	Typically, 30W
USB Interface	1 USB socket on each platform to connect provided USB crypto key
ENVIRONMENTAL 1U SERVERS	
Power Supply	250W
Voltage	100 - 240 VAC, auto-ranging
Power Consumption	Typical ~150W
USB Interface	1 USB socket on each platform to connect provided USB crypto key
TESTED LATENCY*	
TCP Data Stream	0.6ms
UDP Data Stream	0.7ms
*Actual latency results may vary according to setup used, traffic characteristics and network topology.	
RELIABILITY	
MTBF	> 50,000 hours
FORM FACTOR - DIN RAIL	
Weight	2 units @ 2.2kg each
Mounting	Din Rail mounting
FORM FACTOR 1U SERVERS	
Weight	2 units @ 27lb / 12.2kg each
Mounting	Rack mounting kit supplied

Broad Support for Unidirectional OT/IT Convergence

OPSWAT NetWall Optical Diode data replication solutions support a wide range of industrial OT and corporate IT protocols and applications.

Application and Protocol Support

Industrial Protocols
- Modbus
- OPC (UA, DA, A&E)
- MQTT-SN
- IEC 104
- DNP3
- Pi historian replication

IT Protocols
- UDP, TCP, HTTP, HTTPS, SMTP
- Video/Audio stream transfer

IT Monitoring Applications
- Log transfer, SNMP Traps, SYSLOG
- SIEM integration via SYSLOG

File/Folder Transfers
- FTP, folder and file transfers/copying
- Windows file share, SMB, CIFS
- *Antivirus updates, patch (WSUS) updates*

OPSWAT.

Protecting the World's Critical Infrastructure

OTfuse™

Industrial Intrusion Protection System (IPS)

Device Level Intrusion Protection

Many industrial OT environments are built around a flat network design with very little practical segmentation. Simple user names and passwords are in widespread use and shared across operations teams and across multiple points of physical connectivity.

As a result, many OT networks lack internal security controls, putting OT assets at risk from unauthorized/ hostile use and unintended misuse. OTfuse™ establishes a crucial line of defense for OT hardware assets to protected OT networks, and without disrupting the work procedures of business stakeholders.

OTfuse is an industrial security appliance and intelligent Intrusion Prevention System (IPS) that sits in front of industrial endpoints to protect mission-critical PLC, VFD, DCS, and other network connected devices. Operating as a transparent OSI Layer-2 bridge, OTfuse automatically learns and enforces the normal operations of your plant environment and eliminates threats in real time.

It protects industrial assets from unauthorized config changes, device resets, device reads, logic updates, and message values.

OPSWAT offers an OTfuse Standard and OTfuse Lite versions. The OTfuse Standard appliance support up to 15 industrial device and the Lite version supports 3.

Easy and Automated Protection

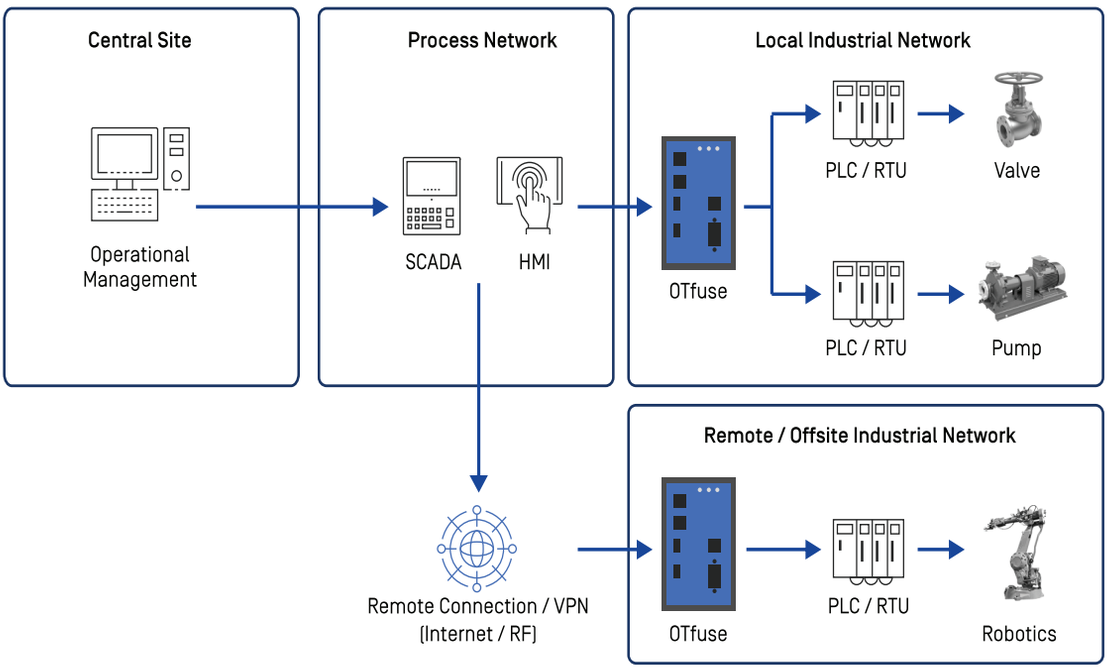
OTfuse installs easily at the cabinet level and self-learns your OT network subnets. No IP address is needed (except for management) and no reconfiguration of your existing network segmentation and subnet address scheme.

In real time, the appliance controls who is permitted to communicate using what protocol and command types and when.

As such, OTfuse supports the implementation of IEC62443-3 standard for segmentation and controlling the traffic flows between different zones in the industrial environment.

OPSWAT.

OTfuse



Protecting iFIX and Cimplicity Networks

OTfuse GE is an industrial network security appliance specifically engineered to understand and self-learn iFIX protocol communication patterns and prevent unauthorized communications from reaching GE iFIX assets. The appliance governs access to iFIX 6.x HMI and SCADA systems and maximizes protection for all the iClients in use across your deployment, making sure that unauthorized nodes cannot interact with the rest of the site.

OTfuse GE does the same for industrial networks whose HMI and SCADA systems use the GE Cimplicity communication protocol.

OTfuse GE Cybersecurity Features

OPSWAT provides five essential security controls to protect iFIX and Cimplicity HMI, SCADA, clients and view nodes as they interact with each other and the broader OT/IT network.

OPSWAT OTfuse GE

Network Risks	Real-time Security Protection	Control
Unknown nodes or clients	Alert and block attempt to add any node that interacts with or modifies iFIX system behavior	Rogue Node Detection
Unauthorized scanning or communication	Prevent network activity from detecting protected nodes	Reconnaissance Detection/ Prevention
Unintentional reconfiguration or update	Permit only read-type function codes on native iFIX or Cimplicity protocols except during admin-defined timeframe	Scheduled Maintenance Enforcement
Very high message rates (DoS)	Block IPs that exceed normal message rates	DoS/DDoS Protection
Fake devices	Direct enforcement of known IP and MAC addresses for trusted iFIX or Complicity SCADA nodes and clients	IP Spoofing Protection

OPSWAT.

Trust no file. Trust no device.

OPSWAT.

OTfuse

Application and Protocol Support

Supported Protocols	TCP, UDP, MODBUS, ETHERNETIP, S7COMM, SLMP, FINS, VNETIP, BACNET, DNP3, EGD
GE SCADA / HMI Software	CIMPLICITY, iFIX
GE Proprietary Protocols	DICOM, GE-ADL, GE-SDI, GE-SRTP, IEC60870, MMS

Specifications

Spec	OTfuse Standard, OTfuse GE	OTfuse Lite
Hardware Manufacturer	Lanner	CompuLab
Number of OT devices supported:	Up to 15	Up to 3
CPU	ATOM (E3845)	Celeron J3455
RAM	8GB	4GB
Storage	128GB	64GB SATA SSD
USB Interfaces	2 (1x2.0; 1/3.0)	4 (2x2.0 + 2x3.0)
Power Inputs	2 voltage inputs (redundant power)	1 twist lock input
Input Power Range	12-36 VDC power input	9-24V DC
Serial (Console)	Yes (1)	1 (optional, requires special cable)
Ethernet Ports	2/4 3 Gigabit	2 GbE
Bypass Pair {Qty}	Yes (1)	No
Operating Temp Range	Standard: -40°C to +75°C	-20°C to +40°C
Digital Input	No	No
Dimensions	146H/127D/78W (mm)	112H/84D/34W (mm)
Weight	1.45 kg	350 grams
Standard Certificates and Declarations	CE/FCC Class A/RoHS/ UL / C1 div II	UL lister for USA and Canada
Vibration 60068-2-6, test Fc	Yes	IEC TR 60721-4-7
EMC Interference Certification	EN55032:2015+AC:2016 Class A: EN55024:2010	n/a

OPSWAT.

DATASHEET

Neuralyzer™

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.

What We Offer

Neuralyzer 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. Neuralyzer can be operated without an expert skillset or training.

It provides unparalleled visibility into converged IT/OT operations and 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.

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

Benefits

- Addresses both IT and specific ICS threats to OT systems
- Easy to use and built for OT personnel
- Offers full visibility and management info into ICS Assets
- Timely and accurately informs you of any threats or anomalies on the network
- Supports regulatory requirements with wide and objective risk assessments
- Provides a unified view of operation, security, and compliance in a single pane of glass

OPSWAT.

Neuralyzer

USE CASES

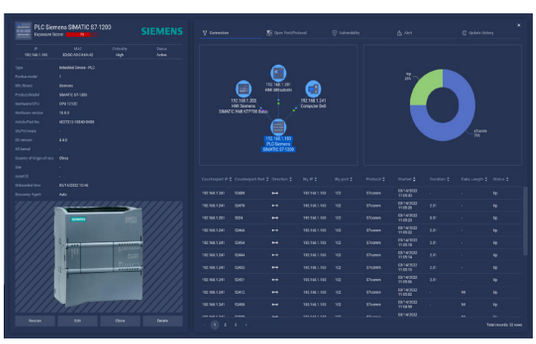
- Asset Inventory & Vulnerability Assessment
- Network Visualization & Monitoring
- Threat Detection & Response
- Exposure Assessment & Alert workflow

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



PART NUMBERS

Neuralyzer All-In-One Network Appliance	NEU-AIO-STD

SPECIFICATIONS

Networking	▪ 1 x Onboard RJ-45 Gigabit Ethernet Network Adapter ▪ 1 x Intel Wi-Fi 6E (6GHz) AX211 2x2 Bluetooth 5.2 Wireless Card ▪ 2 x Add-On USB 3.0 to RJ-45 Gigabit Ethernet Network Adaptor
Voltage	90 – 264 VAC, auto-ranging 47 Hz – 63 Hz
Power Consumption	220W (maximum)
Weight	15.06 lbs. (maximum)
Dimensions	13.54 in. (344.00mm) x 21.26 in. (540.20mm) x 2.07 in. (52.50)

Capabilities

- Rapidly Discover Devices and Build Asset Inventory
- Immediately Explore Connectivity and Visualize Network
- Continuously Monitor Network to detect Threats and Anomalies
- Constantly & Objectively Address OT Vulnerabilities and Risks
- Structured & Streamlined Risk Alert Workflow
- Global, regional & Industry Regulatory Compliance Reporting
- Comprehensive & Customizable Dashboard
- Simple Deployment, OT-Friendly and Easy to Use

OPSWAT.

Protecting the World's Critical Infrastructure

OPSWAT.com/contact

OPSWAT.

DATASHEET

MetaAccess® Zero-Trust Access Platform

Secure Access and Device Compliance

Zero-Trust Access (ZTA), an approach that considers all entities untrusted by default, is rapidly becoming the industry standard and being mandated by regulatory bodies including governments. Leveraging the latest ZTA technologies, OPSWAT's MetaAccess Zero-Trust Access Platform is a unified platform cloud solution for providing deep endpoint compliance, advanced endpoint protection, identity authorization, and secure access without hindering workflows.

Benefits

A Unified Multi-Function Platform Approach

Threat detection, vulnerability assessment, patch management, advanced endpoint protection, compliance, and incident response in one platform.

Zero Trust Security

Enable universal Zero-Trust security principles, including explicit verification and least-privileged access. Enforce verify-first, connect-second access.

Regulatory Compliance

Define and enforce security policies to comply with NERC, CISA, PCI, HIPAA, SOC2, SOX, GLBA, and GDPR. Create audit documentation and reports.

Enhanced User Experience

Mutual TLS encryption enables high-performance secure access. Self-remediation for quick issue resolution.

Flexible Deployment

No additional hardware or network integration required. Scalable and cost-effective licensing with 24/7 support.

Features

Device Posture Checks

Ensures compliance with regulatory and organizational endpoint policies, endpoint vulnerability assessment, and automated patch management. It also detects DLP (Data Loss Prevention) applications and blocks or removes unwanted software.

Anti-Malware Multiscanning

Provides advanced threat detection, greatly improving the odds of catching near zero-day threats by integrating more than 20 anti-malware engines.

Anti-Keylogging and Screen Capture Protection

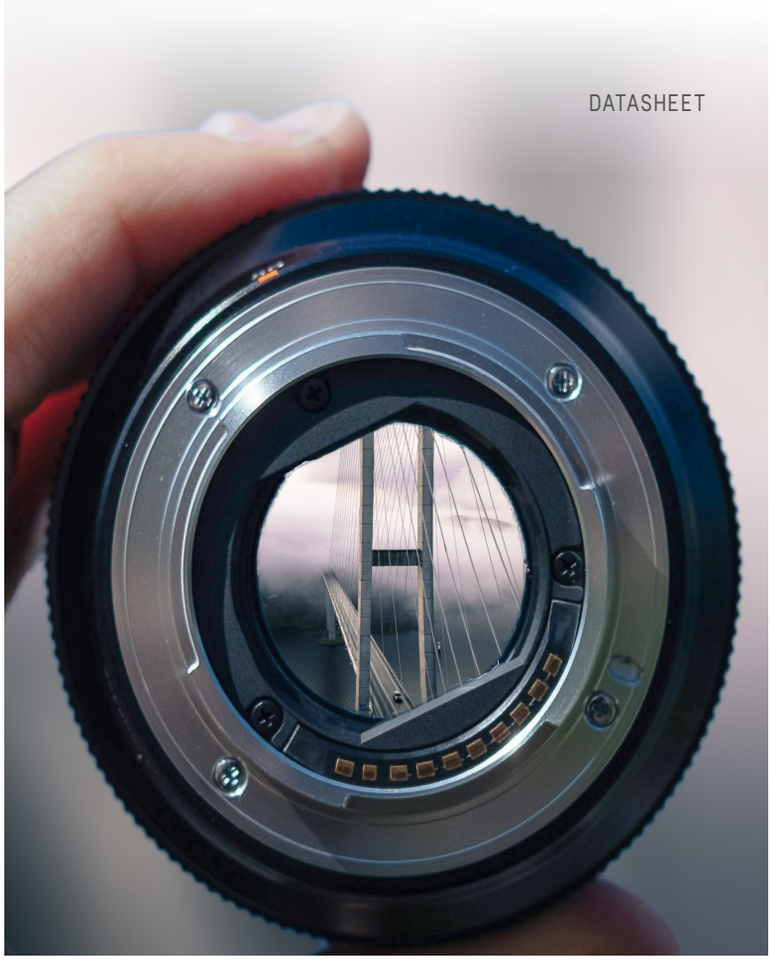
Encrypts keystrokes and prevents unauthorized screen capture recording and copy/paste to protect data.

Secure Access

Hides enterprise resources from the internet and internal networks to mitigate DDoS attacks, credential thefts, connection hijackings, and data loss.

OPSWAT.

DATASHEET



MetaAccess® NAC

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?

MetaAccess Network Access Control (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.

Visibility. Security. Control.

MetaAccess 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.

MetaAccess 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.

MetaAccess NAC delivers an industry-leading solution addressing critical security challenges facing your network with a streamlined implementation experience.

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.

OPSWAT.

MetaAccess NAC

Features

MetaAccess 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

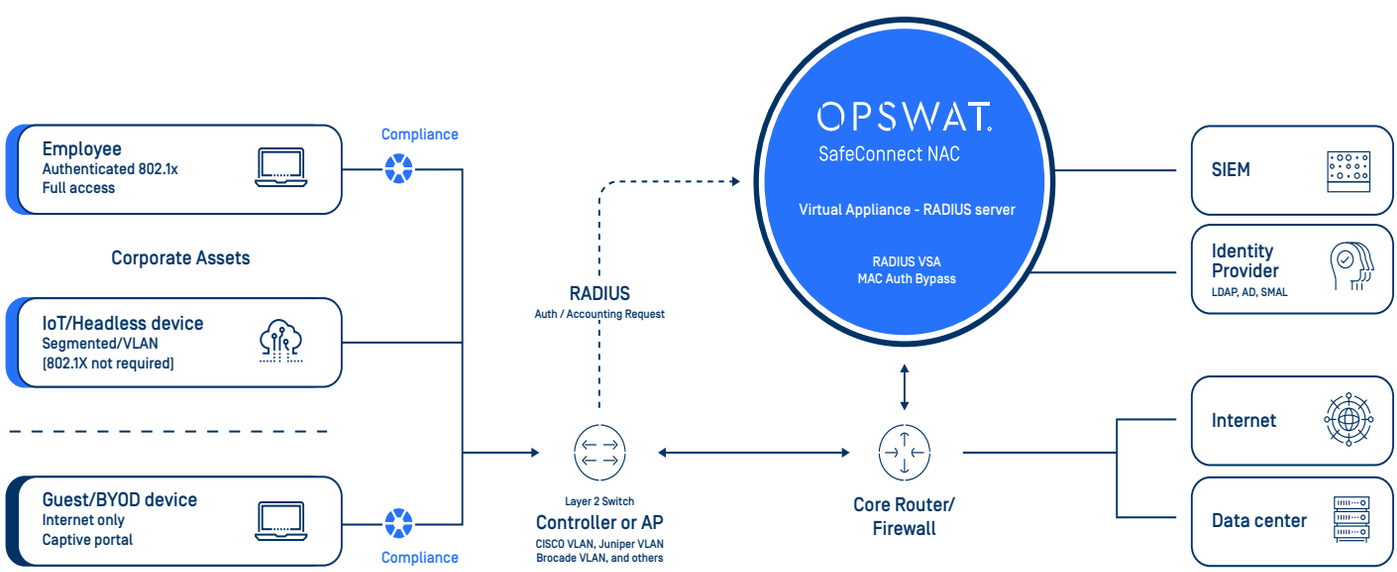
Capabilities

- 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

MetaAccess NAC 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*



OPSWAT.

Trust no file. Trust no device.

OPSWAT.

DATASHEET

MetaAccess OT™

Industrial-Grade Secure Remote Access for OT Assets

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

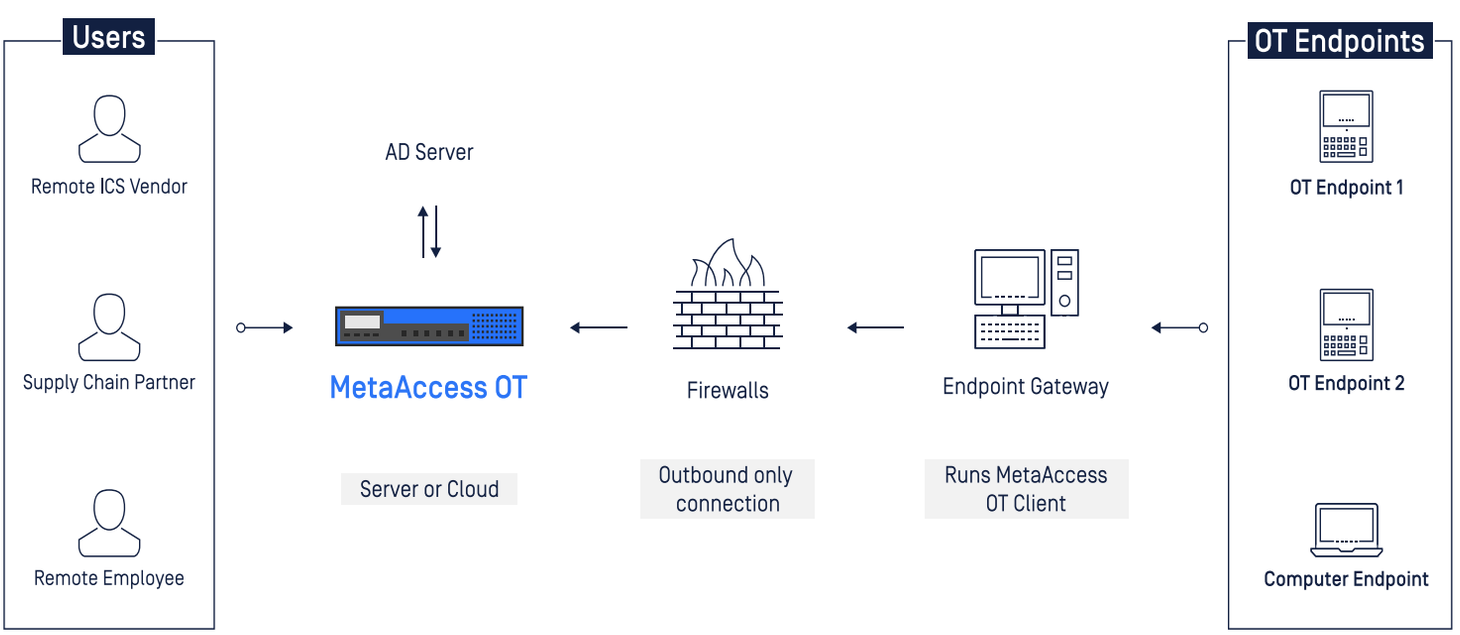
VPNs are typically the go-to solution for IT to provide remote access, but they're not designed for OT environments. With VPNs, it is all or nothing. Once a user gains access, they can see and inspect any asset on the OT network without supervision, and there is no way to terminate the session should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

OPSWAT MetaAccess OT 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. MetaAccess OT 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.



OPSWAT.

MetaAccess OT™

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.

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.

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.

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

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 (RDP).

Private cloud or on-prem deployment options
Go with a customer-dedicated AWS instance for maximum reliability, uptime, and performance. Or a standard 1U server (or VM) on-premises with separate management and administration interfaces.

Pay-as-you-go flexibility
Lower TCO with a flexible pricing model that scales with your business based on the number of concurrent users and endpoint servers.

Solution Comparison

Feature	MetaAccess OT	Software-Defined Networking Tools	VPNs
Native OT protocol support	Yes, including deep packet inspection	Port-level only	None
Session origination	Outbound only via TLS from customer to policy engine	Inbound or outbound, depending on product and vendor	Inbound through to perimeter firewalls
Session types	Highly granular single-user-to-single-service permissions	User-to-network permission defaults	Network-to-network permission defaults
Local use or AD users/groups	Yes	Yes	Yes

Native Policy Controls

	FINS	Modbus	OPCUA	S7	SLMP	RDP	Ethernet IP	VNC	HTTP HTTPS	ssh	telnet
Read-only	✓	✓	✓	✓	✓	✗	✗	✗	✗	✗	✗
Read-write	✓	✓	✓	✓	✓	✗	✗	✗	✗	✗	✗
No SQL injection	✗	✗	✗	✗	✗	✗	✗	✗	✓	✗	✗
No XSS	✗	✗	✗	✗	✗	✗	✗	✗	✓	✗	✗

OPSWAT.
Protecting the World's Critical Infrastructure

opswat.com/contact