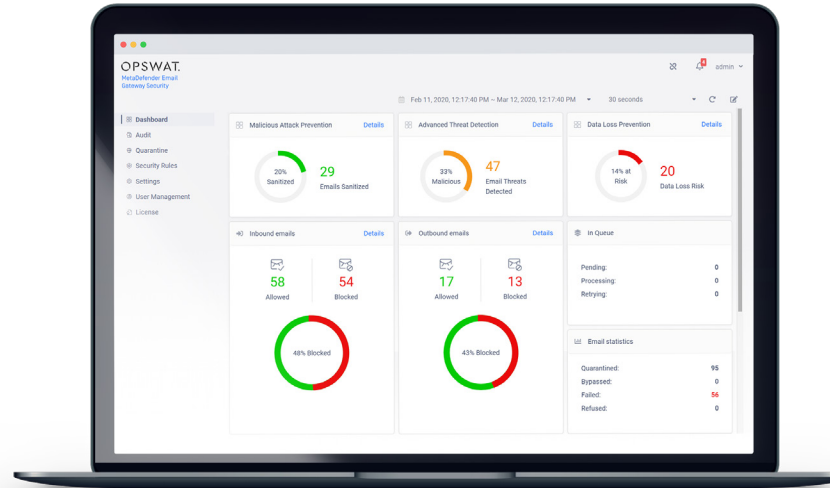


# MetaDefender® Email Gateway Security

Deliver trust to your inbox

Most malware is initiated through email. Links and attachments that appear safe can contain malicious content. Once accessed, malware replicates and spreads across the network.

MetaDefender Email Gateway Security examines every email and attachment, scans malicious content, reconstructs suspicious attachments and redacts sensitive data before it's delivered.



## Scan. Remediate. Deliver.

Advanced threats can bypass many malware detection applications used by email security solutions today.

The three best ways to combat email-originated malware?

1. Use as many anti-malware engines as possible,
2. Disarm and reconstruct attachment to prevent threats,
3. Check malicious behavior of links and neutralize.

MetaDefender Email Gateway Security—without affecting employee productivity—provides a value-added layer to legacy email gateways, neutralizing over 99% of malware in emails.

**MetaDefender Email Gateway Security delivers peace of mind, with no compromise.**

## Benefits

### Zero-Day Malware Prevention

Disarm unknown content and output clean, usable files

### Advanced Threat Prevention

Malware scanning of emails using 30+ engines

### Proactive antiphishing

Hyperlinks to unsafe URLs are replaced with plain text or redirected to reputation checks to prevent user misbehavior

### Prevent sensitive data loss

Detect, redact, or block sensitive data sent or received

### Comprehensive Inspection & Remediation

The entire email is processed: header, body, and attachments

### Disarm password-protected attachments

The most convenient solution to process encrypted attachments

### Secure Retrieval of Attachment for Outbreak Prevention

Upload attachments automatically to users' own secure storage for approval and outbreak prevention

# OPSWAT.

## MetaDefender Email Gateway Security

### Features

#### Prevent Malicious Emails

Sanitize over 85 common file types, and rebuild each attachment ensuring safe content and full usability.

#### Detect More Malware

Each email is analyzed with 30+ anti-malware engines using signatures, heuristics, and machine learning technologies to identify known and unknown threats.

#### Check Emails for PII

Content-checking the email headers, body and attachments for sensitive data before leaving or entering the organization.

#### Secure Storage of Attachments

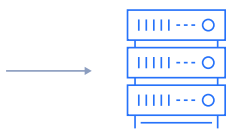
All attachments are delivered to an isolated storage for continuous malware scanning and outbreak prevention, released upon supervisor approval.

#### Dynamic Antiphishing

To uncover potential phishing attacks, embedded hyperlinks are replaced by actual plain-text URLs or re-routed for a reputation check.



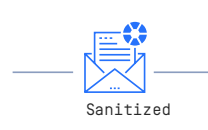
Internet



Gateway/MTA



OPSWAT.  
MetaDefender Email  
Gateway Security



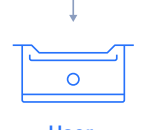
Sanitized



Mail server



OPSWAT.  
MetaDefender Vault



User  
mailboxes

### Email Processing Flow

End users only receive attachments that have been scanned and remediated. No harmful files are delivered to end-users. All integration offers a proper second line of defense for the email flow of your company.

- **Transport Agent** – When Microsoft Exchange Server available, emails are delivered through **Transport Agent**.
- **SMTP** – In cases of other email gateway availability (not Exchange), emails are delivered through **SMTP**.
- **x-Headers** – Used for communication purposes between MetaDefender Email Gateway Security and the **mail server**.

### Specifications

#### Supported Operating Systems

Microsoft Windows, 64 bit

#### Minimum Hardware Requirements

- **CPU:** Intel Core i5-8500 Processor, six-core embedded
- **RAM:** 32 GB DDR4
- **SSD:** 256 GB
- **NIC:** 1GbE

#### Integrations

- SMTP
- Exchange transport agent
- x-Headers

#### Performance

Up to 10,000 emails per hour

## OPSWAT.

Trust no file. Trust no device.

For evaluation purposes, MetaDefender Email Gateway Security offers three available options: **Out-of-Band Monitoring**, **Inline Monitoring** and **deploy via SPAN port**.