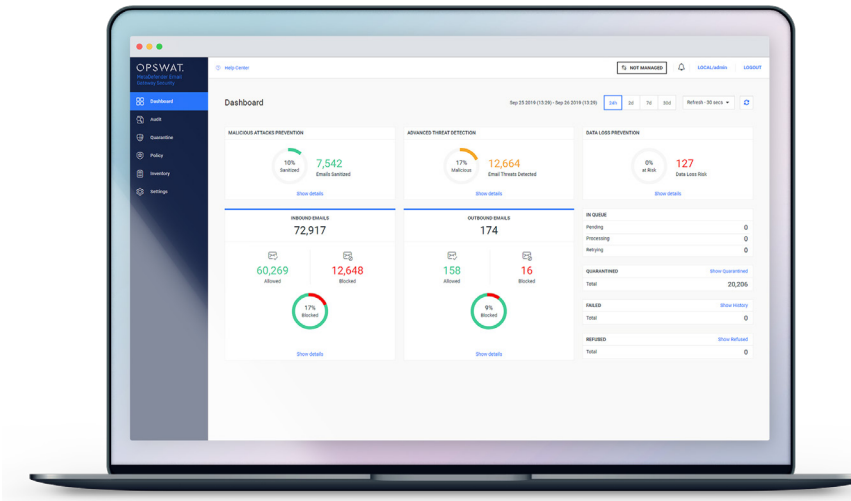
OPSWAT.

DATASHEET

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, scanning and addressing malicious content, before it's delivered.

Configure. Analyze. Address.

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

The two best ways to combat email-originated malware?

1. Sanitize data, to address threats before they occur.
2. Use as many malware engines as possible.

MetaDefender Email Gateway Security evaluates inbound and outbound emails, reconstructs suspicious attachments, and redacts sensitive content—while maintaining consistent email delivery flow. Hyperlinks to unsafe URLs are also replaced with plain text to prevent user misbehavior.

MetaDefender Email Gateway Security delivers peace of mind, without interrupting employee productivity.

Benefits

Sanitize Suspicious Files
Disarm unknown content and output clean, usable files

Industry-leading Multiscanning
Integrated multiscanning of 30+ engines

Disarm Malicious Links
Discover and neutralize harmful links, even if hidden, within the body of the email

Prevent Sensitive Data Leakage
Detect, redact, or block sensitive data sent or received

Safe URL Redirection
Determine reputation, understand malicious behavior, and quantify risk

Comprehensive Inspection & Remediation
The entire email is processed: header, body, and attachments—even if encrypted

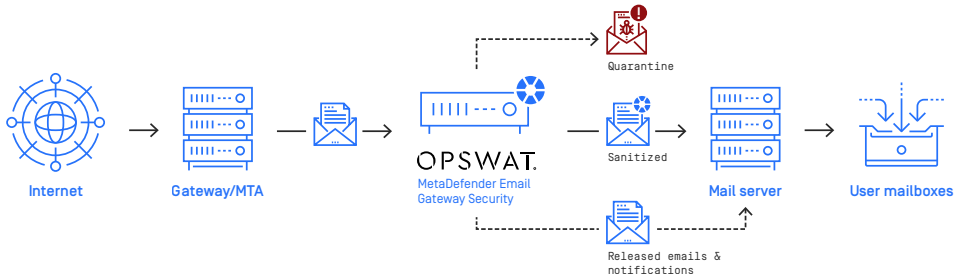
OPSWAT.

MetaDefender Email Gateway Security

Deployment Modes

Protection

For production environments seeking the highest level of email security. End users only receive attachments that have been scanned and remediated. No blocked files are delivered to end users.

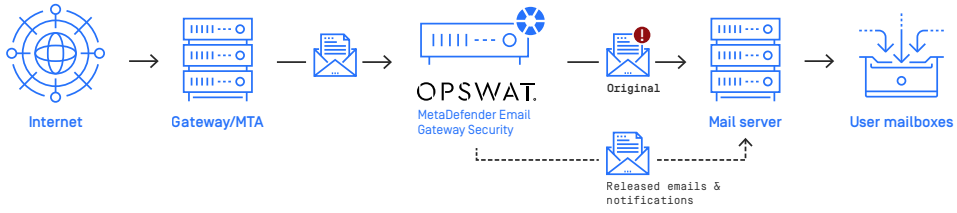


Out-of-Band Monitoring

End users receive original emails through standard conventions. A duplicate of every email is sent to MetaDefender Email Gateway Security for evaluation. The findings are sent to the end user separately via email. This deployment model is generally used as an initial step to evaluate the risk of existing environments, before full implementation and enforcement.

Inline Monitoring

Every email is sent to MetaDefender Email Gateway Security first. End users receive original unaltered emails through a secure channel. The findings are sent to the end user separately via email. This deployment model is generally used as an initial step to evaluate the risk of existing environments, before full implementation and enforcement.



Specifications

Supported Operating Systems

Microsoft Windows, 64 bit

Minimum Hardware Requirements

- **CPU:** 1 x 2.4 GHz, 4 core
- **RAM:** 8 GB DDR4
- **SSD:** 8GB + 0.5 GB per scan engine
- **NIC:** 1GbE

Deployment Model

On-site SMTP/Exchange

Performance

Up to 10,000 emails per hour

OPSWAT.

Trust no file. Trust no device.