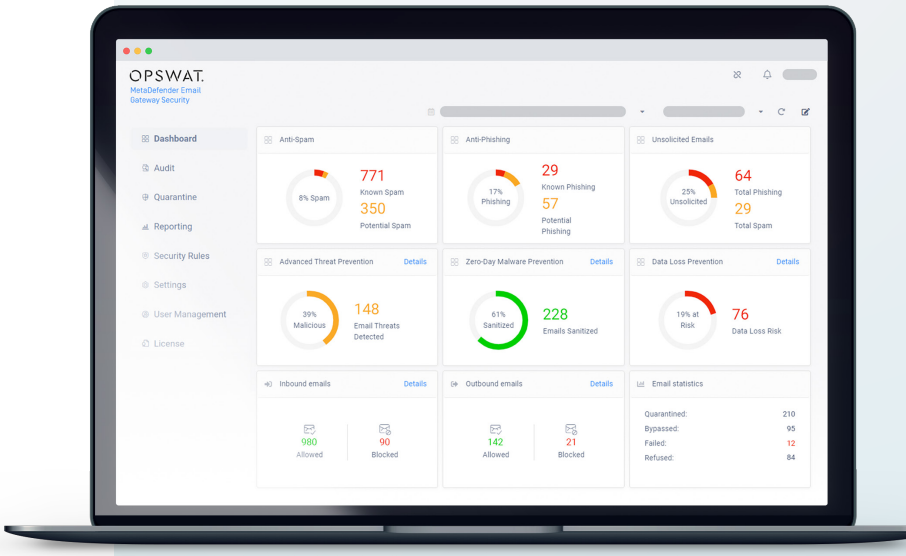
OPSWAT.

DATASHEET

MetaDefender® Email Gateway Security

Deliver trust to your inbox



Scan. Remediate. Deliver.

MetaDefender Email Gateway Security addresses all cybersecurity threats on emails and offers advanced threat prevention, while significantly decreasing malware outbreak detection time (to virtually zero).

It neutralizes attachments before they are delivered to prevent zero-day attacks, using the best-of-breed anti-spam and anti-phishing engines to prevent spam outbreaks and phishing attacks.

Protect your business by ensuring email security

Advanced threats can bypass most malware detections. Cyberattacks have become more sophisticated, and spear-phishing and targeted attacks are taking advantage of the weakest link—human error. User awareness can't be the last line of defense.

MetaDefender Email Gateway Security examines every email (header, body) and attachment. It prevents unknown threats, by sanitizing and removing any possible embedded threats in email attachments. Combining the values of multiple anti-malware engines increases the detection rate to 99%.

Benefits

Cost-effective, with no need to deploy multi-layered email security.

Significantly reduce downtime taken by advanced threats, by sanitizing emails from the zero-day threats.

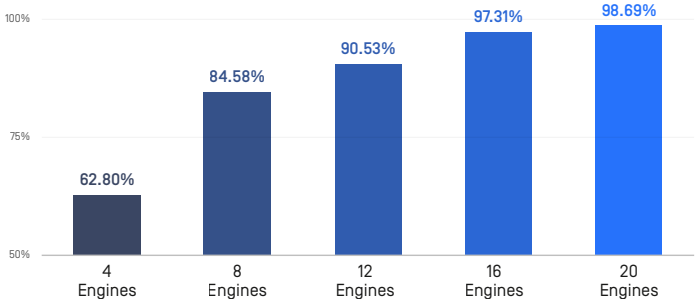
Simplify operation, along with delivering one email security solution for all kinds of threats.

Improve protection efficiency by gaining a 99% detection rate of malware with up to 35 AV engines.

Reduce exposure / vulnerable time against email threats with Multiscanning.

Protect users from harmful URLs by using an AI-based anti-phishing engine.

Detection rates of top 10,000 threats with OPSWAT Multiscanning



OPSWAT.

MetaDefender Email Gateway Security

Key Features

Advanced Threat Detection

The Multiscanning technology analysis each email with signatures, heuristics, and machine learning technologies by using up to 20 anti-malware engines (on-premise) and up to 35 anti-malware engines (by cloud scanning option). Our advanced threat detection and prevention technology provides the highest detection rates and decreases outbreak detection times.

Zero-day Attack Prevention

Deep CDR disarms every email body and attachment by removing potentially malicious content, only the reconstructed, fully usable files will be delivered. Sanitize over 100 common file types, including password-protected attachments, 30x faster than sandboxes.

Protect From Spam Outbreaks

Anti-spam technology is one of the most efficient in the market by providing the highest detection rate (over 99%) and close to zero (0.00%) false-positive rate. It examines the content of emails with multi-threading and concurrency scanning through a wide range of blacklists and applies image-filter detection to identify matches in different fingerprints to prevent real-time spam outbreaks.

Specifications

Performance
Up to 10,000 emails per hour

Supported Operating Systems
Microsoft Windows, 64 bit

Minimum Hardware Requirements

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

Dynamic Anti-phishing

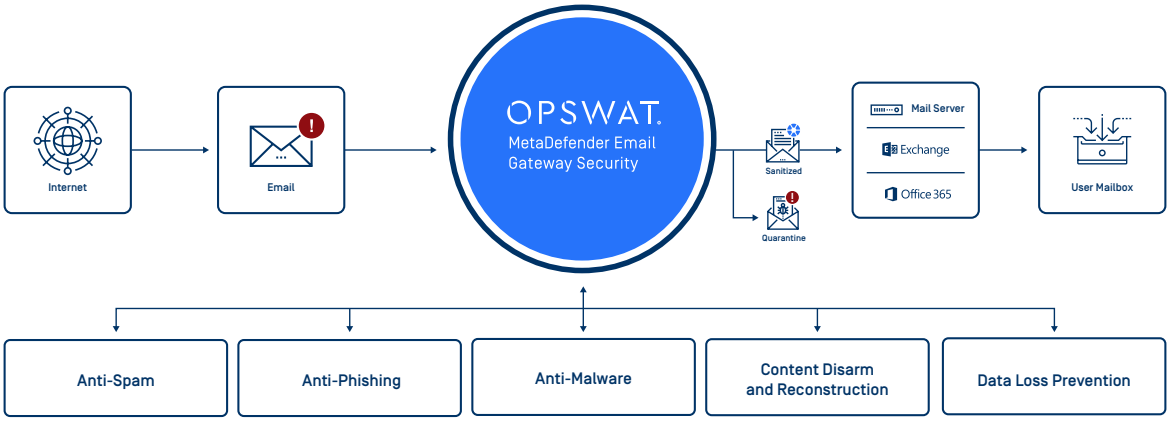
The dynamic anti-phishing technology addresses phishing attacks on multiple stages. A comprehensive solution that applies advanced heuristic, neural network, and spear-phishing filters as well as IP/sender and content reputation checks. Hyperlinks are naturalized and/or checked by the MetaDefender Cloud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

Protect PII & Sensitive Data Loss

The Proactive DLP helps to comply with industry regulations, such as PCI, HIPAA, GLBA, GDPR, and FINRA. Prevents sensitive content from accidentally entering or leaving your organization. Automatically redacts 40+ file types including PDF and office documents. Leverages Optical Character Recognition (OCR) technology to detect and redact sensitive information in images and documents.

Email Processing Flow

Every email (header, body) and attachment (including password-protected files) are examined with industry-leading anti-spam and Multiscanning engines, as well as sanitized and rebuilt to remove all potentially malicious content. End-users only receive emails and attachments with safe content and full usability.



OPSWAT.

Trust no file. Trust no device.