

# OPSWAT.

## MetaDefender® Email Security

### Stop Email Threats that Evade Sandboxes

MetaDefender Email Security protects against email borne threats that evade sandboxes and bypass advanced threat protection solutions such as those offered with Office 365 and G Suite. Using industry-leading multi-scanning and data sanitization, also known as content disarm & reconstruction (CDR), MetaDefender Email Security prevents zero-day attacks and unknown threats as well as providing close to 100% known threat detection, without affecting email server performance.

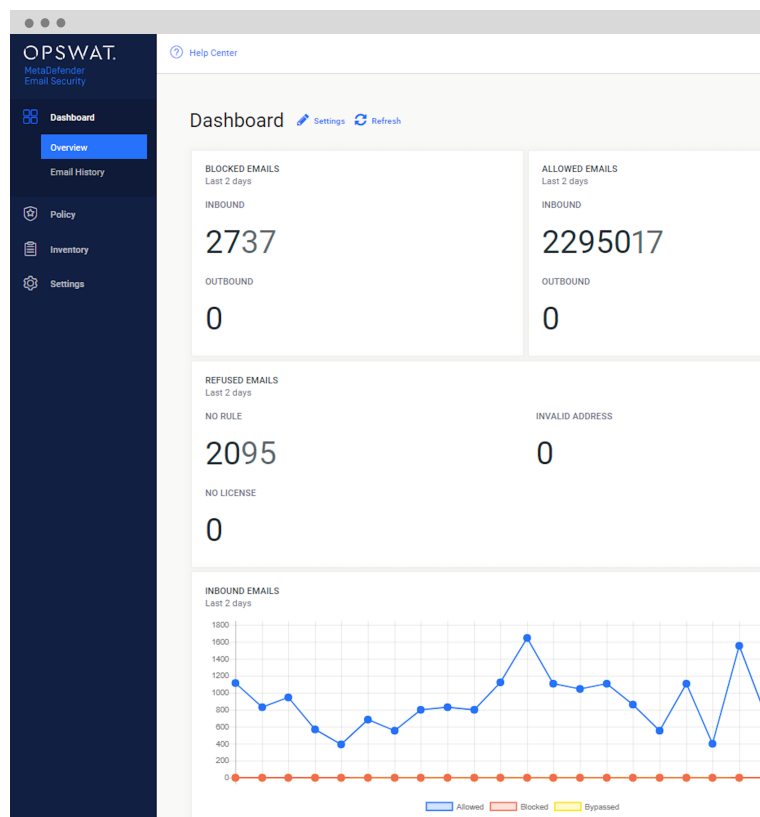
### Benefits

**Neutralize Malicious Emails** - Removes unknown and zero-day threats from the email body and attachments using OPSWAT's industry-leading Data Sanitization (CDR) technology.

**Detect More Email Malware** - Scans with 30+ anti-malware engines using signatures, heuristics and machine learning for the highest and earliest detection of known and unknown threats.

**Flexible Deployment** - Integrates with on-site email servers such as Exchange, as well as cloud email services such as Office 365, G Suite and hosted Exchange and any secure email gateway.

**High Performance** - Offers fast scanning without affecting email performance. Scalable to any email volume with MetaDefender's built-in high-performance architecture.



*"We use OPSWAT's MetaDefender as one of the tools in our arsenal that protects our email users against advanced malware threats. We've been using the product for many years now. OPSWAT's multi-engine scanning technology is fast, easy to integrate, and has been highly effective in our pursuit of offering the best security available to our customers. OPSWAT has been a great company to work with and I highly recommend them."*

Chris Cain  
VP of New Technologies, AppRiver

# MetaDefender Email Security Features

**Data Sanitization (CDR)** - Disarm over 30 common file types, and reconstruct each file ensuring full usability with safe content.

**Multi-Scanning** - Choose from over 30 anti-malware engines in flexible package options.

**Sanitize Hyperlinks** - Remove embedded hyperlinks in emails and display actual URLs.

**Quarantine Emails** - Block or quarantine emails, with real-time threat monitoring.

**High Performance** - High-performance architecture with load balancing.

**Role Based Configuration** - Active Directory and LDAP group-based administrative roles.

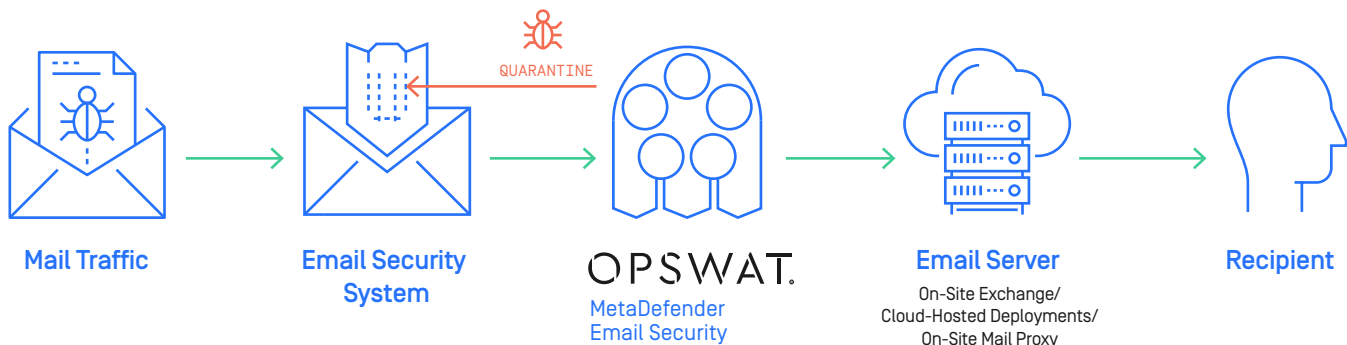
# Flexible Deployment in your Environment or in the Cloud

**On-Site Exchange** - MetaDefender Email Security can be installed on the Exchange Server or on a different machine as an SMTP Proxy and can work in conjunction with any other email security gateway.

**Cloud-Hosted Deployments** - MetaDefender Email Security can function as an SMTP proxy for cloud solutions such as Office 365, G Suite and hosted Exchange, and works in conjunction with any other email security gateway.

**On-Site Mail Proxy** - MetaDefender Email Security can function as an SMTP proxy for any email server in your environment and is compatible with any other email security gateway.

**System Requirements** - 64-bit platform, 4 core CPU, 4 GB RAM, 16 GB free hard disk space with Microsoft Windows 7, 8/8.1, 10 or Microsoft Windows Server 2008 R2, 2012/2012 R2 or 2016.



# OPSWAT.

Trust no file. Trust no device.

[www.opswat.com](http://www.opswat.com)