Email Security Comparison Guide

OPSWAT protects critical infrastructure and assumes that any email, file, or device entering or leaving an enterprise could be a risk. To do this, OPSWAT provides cyberthreat platforms that not only detect threats but also prevent them.

Aligned with Zero-Trust philosophy, OPSWAT launches a new version of MetaDefender Email Gateway Security product, which gives enterprises an easily integrated comprehensive approach for securing their emails, reaching out close to 100% known and unknown threat detection.

Features	OPSWAT Email Gateway Security	FireEye Email Gateway Security	Proofpoint Email Protection	Glasswall FileTrust™ for Email	Microsoft Exchange Online	Cisco Email Security	Mimecast Email Security	hMailServer
Deployment mode for Confidential Customer	Software	Cloud, on-premises and virtual	Cloud, on-premises and hybrid	SaaS	SaaS	Virtual appliance	SaaS	Software
Pricing scheme	Mailbox/Year	User-mailbox/Year	User/month	User/Year	User/Year	User/Year	User/Month	Unit
Email Threat Prevention								
Technology	✓ Deep CDR	–	–	✓ d-FIRST™	–	–	✓ SoleGATE / ZHARA	–
File types	✓ 85 file types: (Office docs, HTML, PDF, RTF)	–	–	✓ 42 file types	–	–	✓ 9 file types	–
File type conversion	✓	–	–	–	–	–	✓	–
Disarm URLs in attachments	✓	–	–	✓	–	✓	–	–
Reputation Check URLs	✓	✓	–	–	–	✓	✓	–
Password Protected Attachment	✓	✓ Only email scan, no user engagement	–	–	–	–	–	–
Advanced Threat Detection								
Anti-malware protection	✓	✓	✓	–	✓	✓	✓	✓
Engine count	✓ 30+ (McAfee, Symantec, Kaspersky...)	✓ 1 (Sophos)	✓ 1 (Proofpoint)	–	✓ 3	✓ 2 (not default)	✓ multiple AV engines	✓ 1
Data Loss Prevention								
Technology	✓ Proactive DLP	✓ Only with HELIX	✓ Email Data Loss Prevention (DLP)	–	✓ DLP	✓ DLP	✓ Content Control and DLP	✓ Regular expression matching
DLP direction – Inbound	✓	–	–	–	✓	–	–	✓
DLP direction – Outbound	✓	–	✓	–	✓	✓	✓	–
DLP enabled content	✓ 35 file types (PDF, JPEG, Office Docs)	–	–	–	✓ Only Office documents	✓ Only text	✓ Only text	✓ Only text
DLP features	✓ CCN, SSN, regular expression matching, redaction, watermarking	–	–	–	✓ Only Template matching	✓ Only Regular expression matching	✓ Only Regular expression matching, Fingerprinting	✓ Only Regular expression matching

OPSWAT.

Product Overview

MetaDefender Email Gateway Security enables enterprises to gain a critical level of protection typically missing from the industry.

Technologies

Industry best practices recommend combining the below four approaches to enhance your email security:

1. Using Proactive Antiphishing **(Dynamic and Static)** technology, the embedded hyperlinks are replaced by actual plain-text URLs or re-routed through Metadefender.com for a reputation check.
2. Proactive Data Loss Prevention **(Proactive DLP)** can prevent emails with sensitive content leaving or entering the organization by content-checking in the email body and attachments.
3. Deep Content Disarm and Reconstruction **(Deep CDR)** technology, preventing zero-day attacks and unknown threats. Attachments are sanitized over 85 common file types and rebuild each email attachment ensuring safe content and full usability.
4. Advanced threat prevention **(Multiscanning)** technology analyzes each email with 30+ anti-malware engines using signatures, heuristics, and machine learning technologies for the highest and earliest detection of known and unknown threats.

MetaDefender Email Gateway Security delivers peace of mind, with no compromise.
For more information, please visit: opswat.com/products/metadefender/email-gateway-security

Sources: www.fireeye.com, www.glasswall solutions.com, www.cisco.com, www.proofpoint.com, www.microsoft.com, www.mimecast.com
All information sources current as of 06-2020.

OPSWAT.
Trust no file. Trust no device.