Email Security Comparison Guide

Email security is standard practice in most enterprises. Yet over 90% of malware continues to be initiated through email[1]. To inform decision-making, OPSWAT provides a quick overview of the primary email protection technologies, as well as a comparison of the major providers.

Industry best practices recommend combining two approaches to email security:

1. **Multiscanning**—use as many engines as possible to maximize malware detection rates.
2. **Content Disarm and Reconstruction (CDR)**—eliminate superfluous or suspect data by cleaning attachments, to prevent latent and zero-day attacks.

Although most enterprises scan for malware to address detection, many use only one or just a few detection engines. Far fewer use data sanitization for prevention—to address threats before they occur.

Malware Scanning / Multiscanning

Malware scanning inspects each file for threats. Detection rates vary dramatically, based on the malware's sophistication, purpose (economic, political, criminal), malware type (Ransomware, Trojan, Adware, Malware, Phishing), and rarity. Since no single anti-malware engine is effective 100% of the time, by combining multiple engines, known as multiscanning, detection rates can approach 100%.

Content Disarm & Reconstruction (CDR)

Most files include data elements that are empty or innocuous. Increasingly, attackers have exploited these vacant areas to hide malware. Data sanitization takes a file, cleans it, and creates a new, usable file. This process has become known as content disarm and reconstruction (CDR). CDR focuses on preventing an attack before it occurs, even if the attack is hidden or unknown. As with multiscanning, the more file types a CDR solution supports, the better.

	Anti-malware protection	Number of engines
Check Point [2]	Check Point Anti-Spam & Email Security Software Blade	1
Cisco [3]	Sophos and/or McAfee	1-2
Microsoft [4]	Microsoft Exchange Online Protection / Advanced Threat Protection	Multiple, # unknown
Mimecast [5]	Mimecast Targeted Threat Protection – Attachment Protect	Multiple, # unknown
OPSWAT [6]	MetaDefender Email Gateway Security	30+

OPSWAT.

Supported CDR File Types

	Microsoft	Cisco	Check Point[7]	Mimecast[8]	OPSWAT[9]
doc	⊗	⊗	✓	✓	✓
docx	⊗	⊗	✓	✓	✓
xls	⊗	⊗	✓	✓	✓
xlsx	⊗	⊗	✓	✓	✓
ppt	⊗	⊗	✓	✓	✓
pptx	⊗	⊗	✓	✓	✓
pdf	⊗	⊗	✓	✓	✓
dot	⊗	⊗	⊗	✓	✓
xlt	⊗	⊗	⊗	✓	✓
pot	⊗	⊗	⊗	✓	✓
rtf	⊗	⊗	⊗	✓	✓
docm	⊗	⊗	⊗	✓	✓
dotx	⊗	⊗	⊗	✓	✓
dotm	⊗	⊗	⊗	✓	✓
xlsm	⊗	⊗	⊗	✓	✓
xlsb	⊗	⊗	⊗	✓	✓
xltx	⊗	⊗	⊗	✓	✓
xltm	⊗	⊗	⊗	✓	✓
csv	⊗	⊗	⊗	✓	✓
potx	⊗	⊗	⊗	✓	✓
pptm	⊗	⊗	⊗	✓	✓
potm	⊗	⊗	⊗	✓	✓
pps	⊗	⊗	⊗	✓	✓
ppsm	⊗	⊗	⊗	✓	✓
ppsx	⊗	⊗	⊗	✓	✓
odt	⊗	⊗	⊗	✓	✓
ott	⊗	⊗	⊗	✓	✓
7z	⊗	⊗	⊗	✓	✓
gz	⊗	⊗	⊗	✓	✓
rar	⊗	⊗	⊗	✓	✓
xz	⊗	⊗	⊗	✓	✓
zip	⊗	⊗	⊗	✓	✓
tar	⊗	⊗	⊗	✓	✓
vsdx	⊗	⊗	⊗	⊗	✓
vssx	⊗	⊗	⊗	⊗	✓
vstx	⊗	⊗	⊗	⊗	✓

	Microsoft	Cisco	Check Point[7]	Mimecast[8]	OPSWAT[9]
vsdm	⊗	⊗	⊗	⊗	✓
vssm	⊗	⊗	⊗	⊗	✓
vstm	⊗	⊗	⊗	⊗	✓
vsx	⊗	⊗	⊗	⊗	✓
vtx	⊗	⊗	⊗	⊗	✓
vdx	⊗	⊗	⊗	⊗	✓
htm/html	⊗	⊗	⊗	⊗	✓
mht	⊗	⊗	⊗	⊗	✓
hwp	⊗	⊗	⊗	⊗	✓
jtd	⊗	⊗	⊗	⊗	✓
jtdc	⊗	⊗	⊗	⊗	✓
xml	⊗	⊗	⊗	⊗	✓
xml-doc	⊗	⊗	⊗	⊗	✓
xml-docx	⊗	⊗	⊗	⊗	✓
xml-xls	⊗	⊗	⊗	⊗	✓
vcs	⊗	⊗	⊗	⊗	✓
ics	⊗	⊗	⊗	⊗	✓
jpg	⊗	⊗	⊗	⊗	✓
bmp	⊗	⊗	⊗	⊗	✓
png	⊗	⊗	⊗	⊗	✓
tiff	⊗	⊗	⊗	⊗	✓
svg	⊗	⊗	⊗	⊗	✓
gif	⊗	⊗	⊗	⊗	✓
wmf	⊗	⊗	⊗	⊗	✓
emf	⊗	⊗	⊗	⊗	✓
dwg	⊗	⊗	⊗	⊗	✓
dxf	⊗	⊗	⊗	⊗	✓
dwf	⊗	⊗	⊗	⊗	✓
3ds	⊗	⊗	⊗	⊗	✓
dae	⊗	⊗	⊗	⊗	✓
u3d	⊗	⊗	⊗	⊗	✓
drc	⊗	⊗	⊗	⊗	✓
rvm	⊗	⊗	⊗	⊗	✓
wmv	⊗	⊗	⊗	⊗	✓
mp4	⊗	⊗	⊗	⊗	✓
eml	⊗	⊗	⊗	⊗	✓

Superior Security—MetaDefender Email Gateway Security

Industry leading email security solutions optimize detection together with prevention. That's why MetaDefender Email Gateway Security uses 30+ malware engines to examine file attachments and every link embedded in the email body—resulting in malware detection that approaches 100%.

OPSWAT's Deep CDR technology is used to sanitize 80+ file types, resulting in clean, usable files. This capability delivers protection without compromising productivity.

All information sources current as of 09-2019

1 Source: https://purplesec.us/resources/cyber-security-statistics/
2 Source: https://www.checkpoint.com/products/anti-spam-email-security-software-blade/
3 Source: https://www.cisco.com/c/en/us/products/collateral/security/cloud-email-security/solution-overview-c22-739909.html
4 Source: https://docs.microsoft.com/en-us/office365/securitycompliance/anti-spam-and-anti-malware-protection
5 Source: https://www.mimecast.com/products/email-security-with-targeted-threat-protection/attachment-protect/
6 Source: https://www.opswat.com/technologies/multiscanning
7 Source: https://www.checkpoint.com/products/threat-extraction/
8 Source: https://community.mimecast.com/docs/DOC-1023#jive_content_id_Supported_File_Types
9 Source: https://www.opswat.com/technologies/data-sanitization

OPSWAT.

Trust no file. Trust no device.

© 2019 OPSWAT, Inc. All rights reserved. OPSWAT®, MetaDefender® and MetaAccess® are trademarks of OPSWAT, Inc.