OPSWAT.

DATASHEET

MetaDefender Email Gateway Security

Advance Your Email Security Posture to the Max

Email continues to be the primary attack vector. and over 86% of malware is delivered via email,

Even worse, hackers use unknown exploits to remain hidden for extended periods of time, exploiting the vulnerabilities of business applications to deliver malicious payloads. Over 25000 such vulnerabilities are discovered every year, 75% of which have been in the wild for more than 2 years.

OPSWAT MetaDefender Email Security provides key capabilities to advance organizations' email security posture to the maximum, protecting against email-initiated sophisticated attacks, zero-day malware, and unknown threats.

Key Features

Anti-Phishing and Anti-Spam:
Emails are sent through multiple detection mechanisms and content-filtering technology to ensure a 99.98% detection rate of spam and phishing attacks. The URLs are rewritten to later reputation checks at the time of clicking, via 30+ sources against sophisticated social engineering.

Advanced Threat Protection:
The Multiscanning technology significantly improves the detection rates of zero-day malware and advanced threats by scanning emails with more than 30 AV engines, reducing the window of exposure to virtually zero. Beyond the traditional signature detection, Multiscanning leverages heuristics and machine learning engines to address unknown zero-day malware.

Sandboxing:
Using the unique emulation engines of the sandbox, MetaDefender Email Gateway Security is able to detect zero-day malware and hidden threats in various email attachments, such as macros in MS Office documents or PDF files.

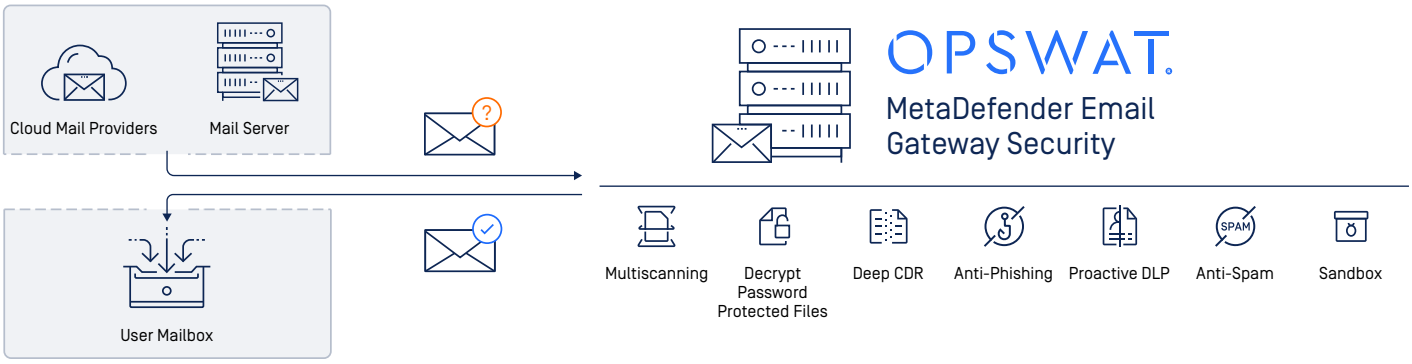
Data Loss Prevention:
Proactive DLP performs full email content auditing, including more than 40 file type checks, to ensure compliance while blocking or editing email content/files to prevent PII from being sent. It leverages the Optical Character Recognition (OCR) Technology to scan image files as well.

Zero-day Prevention:
Deep Content Disarm and Reconstruction (Deep CDR) is OPSWAT's advanced threat-prevention technology that protects organizations against attackers using unknown and Zero-Day exploits by sanitizing more than 120 file types and emails from malicious active content. Our approach is 30 times faster than the detection-based security measures.

Manage Password Protected Attachments:
Password-protected attachments are no exception, as our solution obtains the user's password for decryption so Deep CDR and Multiscanning can be applied.

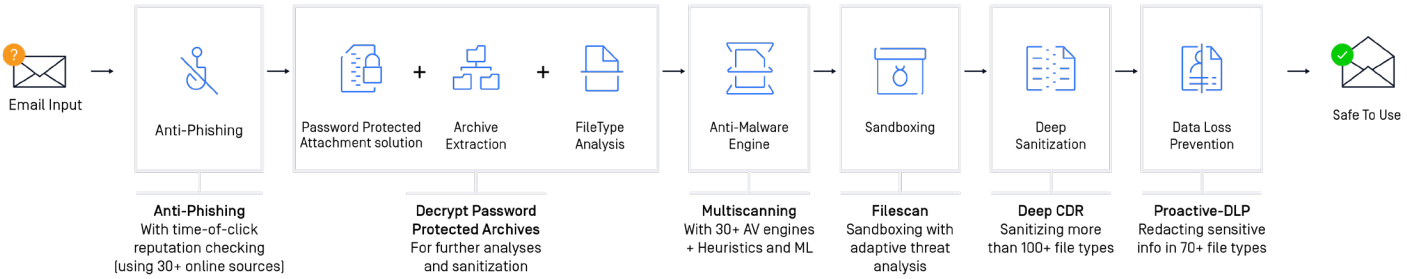
OPSWAT.

MetaDefender Email Gateway Security



Benefits

- Uncovering phishing attacks on multiple stages
- Protecting users from social engineering attacks, ensuring IT can rely less on user awareness
- Ensuring compliance with PCI and other regulations for emails and protecting PII data within companies
- Detecting malicious macros and hidden threats in real-time
- Increased the detection rate of unknown threats with the unique dynamic and static analysis technologies
- Reducing the Window of Vulnerability (WoV) against zero-day malware, thus effectively preventing malware outbreaks
- Protecting business productivity files by sanitizing document-based threats from attachments
- Decrypting password-protected files to apply all key features
- Effectively eliminating zero-day targeted attacks by relying on prevention rather than detection



Summary

Our goal is to protect organizations from email-initiated cyber-attacks. To that end, OPSWAT MetaDefender Email Gateway Security features key capabilities to maximize the protection and reduce security risks from your mailbox.

With key OPSWAT technologies such as Deep CDR, Multiscanning, Proactive DLP, and sandboxing, our solution effectively protects organizations against sophisticated attacks, including zero-day malware, phishing attempts, and unknown exploits. Our solution is also available as a cloud service.

Contact us