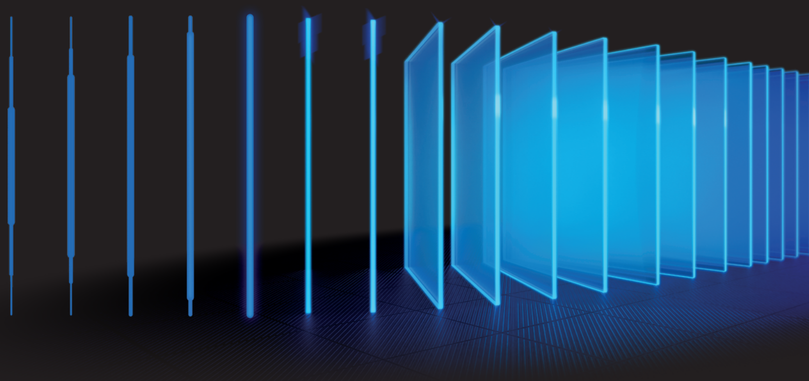
OPSWAT

Protecting the World's
Critical Infrastructure



MetaDefender for Email Exchange Server

Gain advanced email protection against threats that bypass native security

Email continues to be the top cybersecurity threat vector. In fact, 87% of spear phishing attacks bypass perimeter security - according to a CISA Analysis report.

To address these evolving threats, OPSWAT offers MetaDefender for Email Exchange Server, delivering a unique suite of capabilities for the most advanced threats.

By integrating cutting-edge technologies such as Multiscanning, Deep Content Disarm and Reconstruction, and Real-time Antiphishing technologies, detection rates are maximized for unknown and zero-day malware, phishing and exploits.

Additionally, the power of a Real-time Adaptive Sandbox outpaces traditional security measures by neutralizing threats before they are received by a user. Proactive Data Loss Prevention rounds out the core email security technologies to secure sensitive data.

Challenges

#1 cybersecurity threat vector is email, delivering **92% of malware**

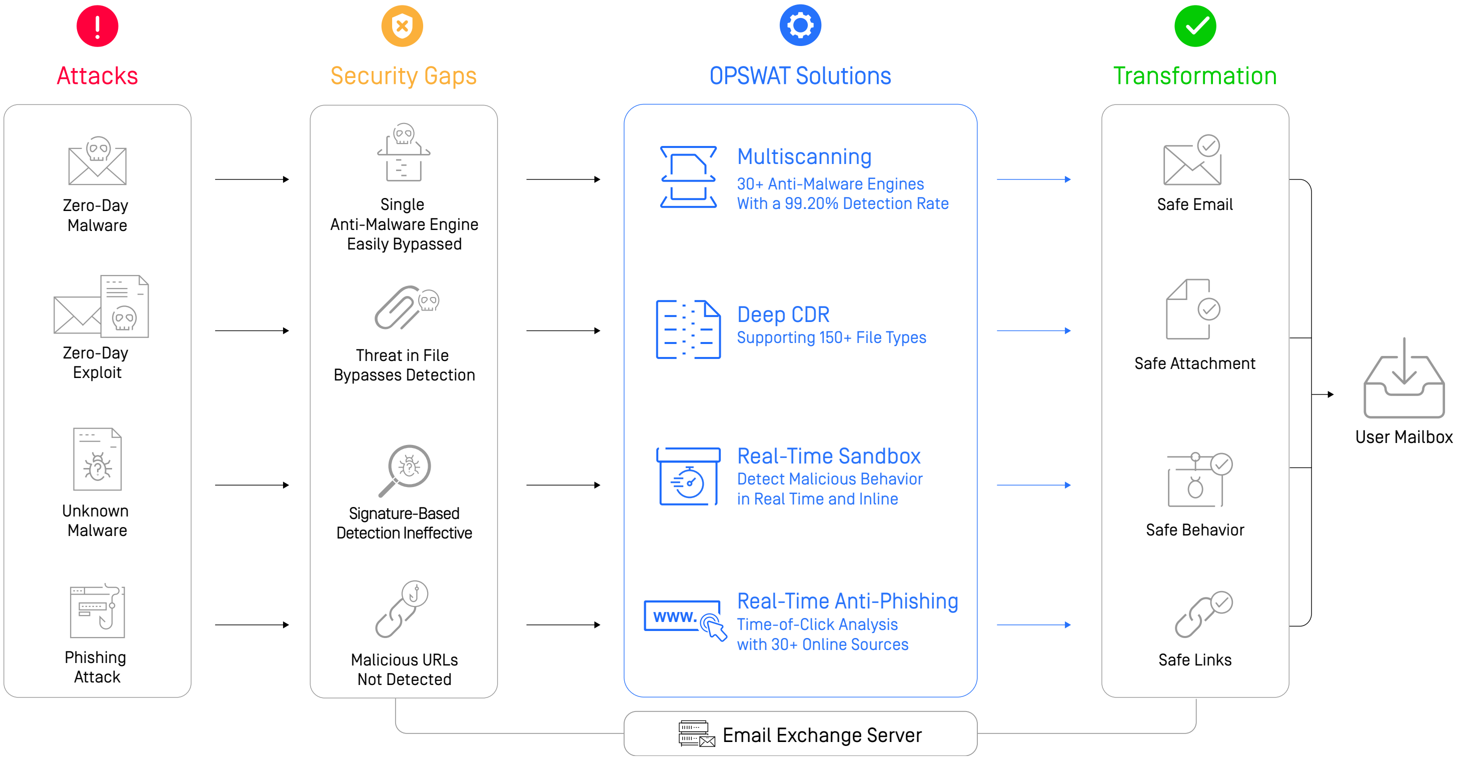
Avg. of 49 days to detect unknown malware, extends threat window

109M new malware instances yearly

Top attachments containing threats are common **Office documents**

Average cost per data breach in 2023 was **$4.45M** [IBM Research]

26,447 vulnerabilities discovered in 2023



Attacks

Zero-Day Malware

Zero-Day Exploit

Unknown Malware

Phishing Attack

Security Gaps

Single Anti-Malware Engine Easily Bypassed

Threat in File Bypasses Detection

Signature-Based Detection Ineffective

Malicious URLs Not Detected

OPSWAT Solutions

Multiscanning
30+ Anti-Malware Engines With a 99.20% Detection Rate

Deep CDR
Supporting 150+ File Types

Real-Time Sandbox
Detect Malicious Behavior in Real Time and Inline

Real-Time Anti-Phishing
Time-of-Click Analysis with 30+ Online Sources

Transformation

Safe Email

Safe Attachment

Safe Behavior

Safe Links

User Mailbox

Email Exchange Server

Email Exchange Server Gaps	OPSWAT. MetaDefender for Email Exchange Server	
Zero-Day Malware The challenge of zero-day malware attacks arises from the limitations of single antivirus engines, disparate response times across vendors, and the occurrence of false positives.	**Multiscanning** Detects **99.20%** of Top 10,000 Threats	Multiscanning combines over 30 anti-malware engines, enhanced by heuristics and machine learning. This approach significantly enhances threat detection.
Zero-Day Exploits Unknown and zero-day exploits pose a significant risk as they can evade native security measures that do not detect threats in attachments.	**Deep CDR** Identifies, Sanitizes & Neutralizes Threats in **150+** File Types	Deep Content Disarm & Reconstruction (Deep CDR) responds by detecting and neutralizing these elusive threats, reconstructing all file content, and performing deep image sanitization and steganography prevention.
Unknown Malware Unknown malware bypasses signature-based detection and remains a threat when analyzed offline by traditional sanboxes.	**A Real-Time Sandbox** Detects Malicious 10X Faster **Real-Time & Inline**	A Real-Time Adaptive Sandbox dynamically detects malicious behavior, provides rapid and in-depth threat analysis, and focuses on targeted attack detection and IOC extraction. Protection is performed in real time, before the email is received by a user.
Phishing & Credential Harvesting Social engineering and phishing attacks often slip through traditional security defenses, utilizing URL hiding and credential harvesting tactics.	**Real-Time Anti-Phishing** Uses Time-of-Click Analysis **30+** Online Sources	Real-Time Anti-Phishing provides a multilayered detection strategy incorporating advanced heuristics, machine learning and Time-of-Click analysis for link reputation checks with 30+ online sources.
Data Loss Data leakage has the potential to inadvertently expose personal and protected business information.	**Proactive Data Loss Prevention** Stops Leakage & Supports **70+** File Types	Proactive DLP safeguards PHI and PII data, detects inappropriate content and language, and utilizes OCR to automatically redact sensitive information. This proactive measure is crucial for maintaining compliance and protecting against data breaches.

Benefits:

MetaDefender for Email Exchange Server

Reduce human error by uncovering potential phishing attacks at multiple stages

Effectively eliminate zero-day targeted attacks by relying on prevention rather than detection

Reduce the Window of Vulnerability (WoV) against malware, effectively preventing malware outbreaks

Protect business productivity files by removing document-based threats from attachments

Increase the effectiveness of malware detection to provide advanced email protection from internal and external threats

Real-time detection of malicious content and unknown threats in attachments

Protect users from social engineering attacks, ensuring IT can rely less on user awareness

Ensure compliance with PCI and other regulations for emails and protecting PII data within companies

Increase the detection rate of unknown threats with the unique dynamic analysis technology

Take The Next Step to

Maximize Your Email Exchange Server Security

Get Started

OPSWAT.

Protecting the World's Critical Infrastructure

OPSWAT protects critical infrastructure (CIP). Our goal is to eliminate malware and zero-day attacks. We believe that every file and every device pose a threat. Threats must be addressed at all locations at all times—at entry, at exit, and at rest. Our products focus on threat prevention and process creation for secure data transfer and safe device access. The result is productive systems that minimize risk of compromise. That's why 98% of U.S. nuclear power facilities trust OPSWAT for cybersecurity and compliance.

Rev. January 11, 2024 2:37 PM