OPSWAT.
Protecting the World's
Critical Infrastructure

MetaDefender for Microsoft 365

Gain advanced email protection against threats that bypass Microsoft 365 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 Microsoft 365, 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 Anti-Phishing 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 malicious behavior before they are received by a user. Proactive Data Loss Prevention rounds out the core email security technologies to secure sensitive data.

Key Insights

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

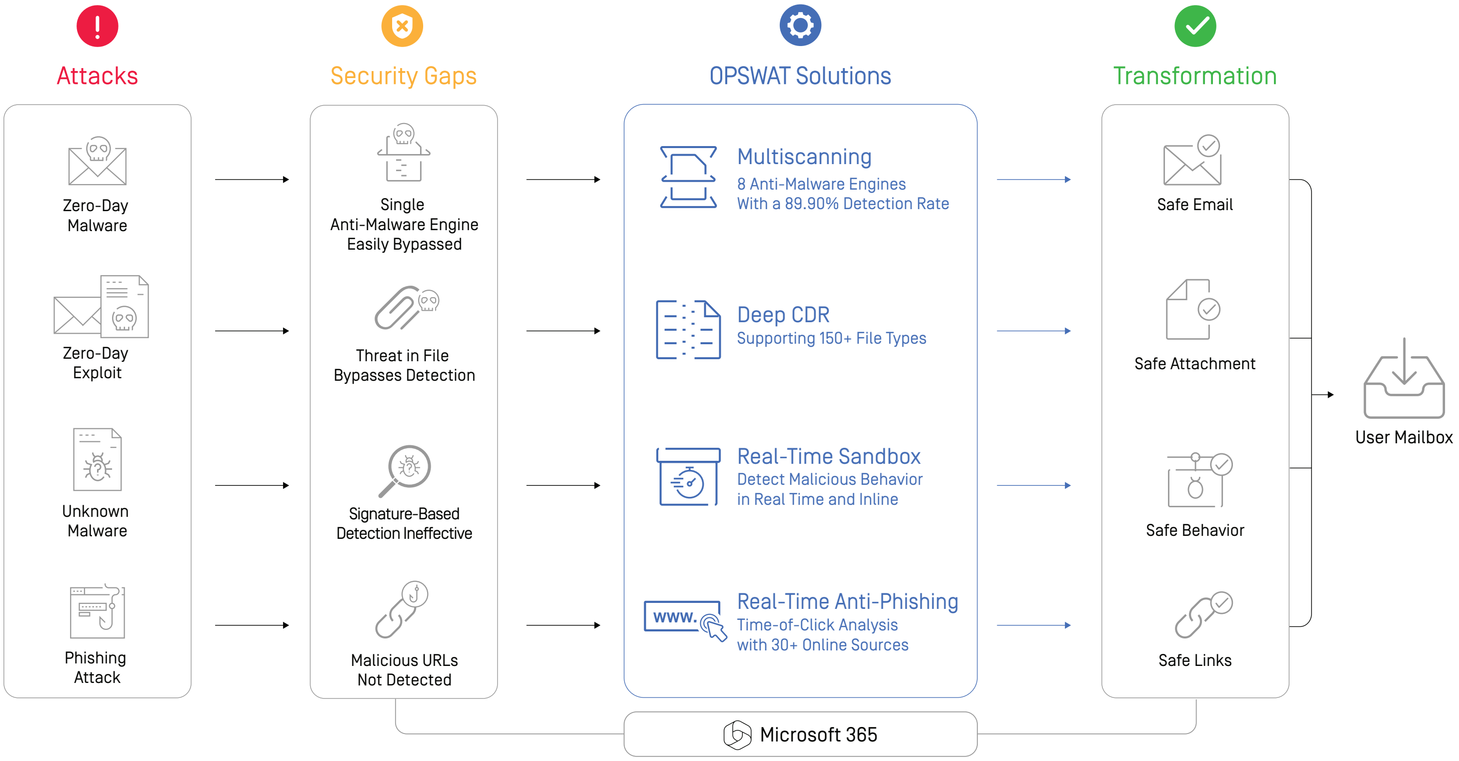
Avg. of 49 days to detect unknown malware, extends threat window

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
8 Anti-Malware Engines With a 89.90% 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

Microsoft 365

Microsoft 365 Security Gaps	OPSWAT MetaDefender for Microsoft 365	
Zero-Day Malware The challenge of zero-day malware attacks in Microsoft 365 arises from the limitations of single antivirus engines, disparate response times across vendors, and the occurrence of false positives.	**Multiscanning** Detects **89.90%** of Top 10,000 Threats	Multiscanning combines 8 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 M365 email security measures that do not detect threats in attachemnts..	**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	Multiple detection mechanisms and content-filtering technology ensures a 99.98% detection rate of spam and phishing attacks. URLs are rewritten and undergo reputation checks at the time-of-click via 30+ sources against sophisticated social engineering. Also features, QR code scanning & rewrite to enhance protection.
Data Loss Data leakage has the potential to inadvertently expose personal and protected business information.	**Proactive Data Loss Prevention** Stops Leakage & Supports **110+** 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.

Take The Next Step to Maximize Your Microsoft 365 Security

MetaDefender for Microsoft 365 adds advanced email security capabilities to all Microsoft 365 Enterprise packages.

Ready to take your email security posture to the next level?

Try it Now