OPSWAT.

DATASHEET

METADEFENDER™

Cloud Email Security

MetaDefender Cloud Email Security removes threats from most attachments before they reach your users, augmenting Microsoft 365 without changing the workflow.

Key Insights

- **70.8%** of malicious emails are being removed by Microsoft Defender post-delivery, creating a window of exposure for active threats to invade systems[1]
- **127%** increase in multi-stage malware complexity[2]
- **$4.4M** global average cost of a data breach[3]
- **Up to 80%** of critical infrastructure organizations experienced an email-related security breach in the last 12 months[4]

Challenge

Modern file-based threats, zero-day exploits, and AI-generated threat campaigns often bypass conventional email security solutions. As a consequence, businesses have faced millions of dollars in losses. The global average cost of a data breach alone was $4.4M in 2025[3].

To address these shortcomings, MetaDefender Cloud Email Security has championed a multilayered approach to increase protection coverage through multiscanning, AI-powered malware prediction, sandbox dynamic analysis, and Deep CDR™ Technology. This prevention-first protection inspects and sanitizes attachments across inbound and outbound emails, before they reach your users and without affecting business continuity.

Zero-Day & AI-Generated Malware

Challenge: Signature-based detection fails against unknown threats, and AI-assisted techniques are accelerating the volume and variety of unseen variants. Detection coverage also varies by vendor geography and market focus, leaving regional blind spots.

Solution: Metascan™ Multiscanning applies up to 17 anti-malware engines with heuristics and machine learning to maximize detection coverage and reduce false positives. In case active content bypasses these AV engines, Predictive Alin AI predicts malicious intent pre-execution, delivering a file safety verdict in milliseconds. For threats that still evade detection, MetaDefender™ Aether extends inspection into behavioral analysis for unknown or evasive payloads, extracting IOCs correlated with threat intelligence.

Zero-Day Exploits

Challenge: Zero-day and unknown file-based exploits reach users before signature-based tools can respond. Password-protected files (such as financial records and compressed archives) are delivered uninspected, leaving active content threats intact.

Solution: Deep CDR™ Technology rebuilds files, removing active content, scripts, macros, and embedded objects. It also decrypts and sanitizes password-protected files while preserving full usability without creating noticeable email workflow delay.

1. Microsoft, March 2026
2. OPSWAT Threat Landscape Report, 2025
3. IBM, 2026
4. Osterman Research, 2024

METADEFENDER CLOUD EMAIL SECURITY

ATTACKS	SECURITY GAPS	OPSWAT SOLUTIONS	OUTCOME	
Zero-Day Malware	Single-engine scanning has lower detection rates than multiscanning	**Metascan Multiscanning** Up to 17 AV engines and up to 99.2% detection rate for top 10,000 threats for on-premises deployment	Safe attachment	User mailbox
Zero-Day Exploit	File-based exploits bypass standard defenses	**Deep CDR™ Technology** Sanitizes 200+ file types and scored 100% SE Labs CDR Protection score [SE Labs, 2024]	Safe file	
Unknown Malware	Signature-based detection fails for unknown malware	**MetaDefender Aether** Zero-day detection and behavioral analysis with a 99.9% detection rate*	Safe behavior	
AI-Generated Malware	Sandboxing every file is too slow for email flow	**Predictive Alin AI** Predicts file safety in milliseconds (P90: 50ms; P99: <100ms) and with a 0.1% false positive rate*	Safe verdict	
Encrypted Attachments	Password-protected files reach inboxes unscanned	**Decrypt and inspect password-protected attachments**	Safe delivery	

*: Based on OPSWAT's internal benchmark of randomly selected, real-world file samples collected from the community-driven filescan.io website, in cooperation with sample-sharing agreements.

Maximize your email security defenses today.

MetaDefender Cloud Email Security deploys in minutes. No hardware, no disruption to mail flow, fast time-to-protection for cloud-first environments.

Request a Demo

OPSWAT.
Protecting the World's Critical Infrastructure

opswat.com/get-started