OPSWAT.

DATASHEET

METADEFENDER™

Email Gateway Security

Prevention First: Multi-Layered Email Security for Critical Infrastructure

As the market shifts toward cloud-only models, many highly regulated organizations still need on-premises email security they can rely on. MetaDefender Email Gateway Security delivers multilayered, pre-delivery protection for customers who require control, data sovereignty, and resilience in on-premises and air-gapped environments.

Key Insights

- AI-generated phishing surged 14x in late 2025, reaching 56% of phishing attempts by December 2025.[1]
- PDF attachments leading to CAPTCHA-gated phishing sites increased 365% in March 2026.[2]
- The mean time organizations took to identify and contain a breach is 241 days.[3]

Challenge

Attackers now iterate at speed, through the boost of artificial intelligence. In highly regulated and critical infrastructure environments, a successful email attack can mean operational disruption, regulatory exposure, and costly remediation.

Deployed at the SMTP/MX level, MetaDefender Email Gateway Security applies multilayered, inline protection before threats reach the inbox, neutralizing phishing, ransomware, zero-day threats, and sensitive data loss.

Prevention-first protection for advanced email threats

Challenge: Legacy defenses struggle with AI-generated phishing, malicious URLs, evasive attachments, and ransomware delivered through everyday files.

Solution: Real-time anti-phishing, multiscanning, Deep CDR™ Techonology, sandboxing, AI-powered malware detection, and Proactive DLP work together to reduce user exposure and strengthen attachment-level protection before threats reach the inbox.

Attachment security without operational disruption

Challenge: In highly regulated industries, delays to critical email attachments can disrupt normal operations.

Solution: MetaDefender Email Gateway Security processes every attachment including encrypted attachments, through successive security layers before delivery, applying deeper analysis only where files require it. The result: legitimate attachments move through quickly, while suspicious or opaque files receive the additional scrutiny they warrant, without slowing mail flow.

1. Hoxhunt, Phishing Trends Report 2026
2. Microsoft, Q1 2026 Trends and Insights
3. IBM, Cost of a Data Breach Report 2025

METADEFENDER EMAIL GATEWAY SECURITY

Threats	Why Legacy Defenses Fall Short	MetaDefender Email Gateway Security Approach
Phishing, Malicious URLs & Social Engineering	Static URL feeds and single-layer filtering miss modern phishing tactics and credential harvesting.	Real-time anti-phishing uses machine learning, sender checks, and on-arrival and time-of-click analysis.
Known Malware, Ransomware & File-Borne Threats	Single-engine detection leaves gaps, slower response, and more false positives.	30+ anti-malware engines, heuristics, and machine learning improve coverage before threats reach users [Metascan™ Multiscanning].
Zero-Day Exploits & Active Content in Attachments	Detection alone cannot reliably stop active content hidden in business files, and disguised documents.	Deep CDR™ Techonology preemptively neutralizes active content in 200+ file types by inspecting, sanitizing and regenerating safe usable files without business disruption.
Encrypted & Password-Protected Attachments	Most vendors either deliver or block encrypted files without inspection, creating a window of vulnerability or disrupting business operations.	Identifies passwords in emails to automatically run files through the CDR process. If the password cannot be found, the recipient can provide it through a self-serve portal without adding pressure to the SOC team.
AI-Powered Malware	AI-generated threats are designed to evade static inspection and conventional signature-based analysis.	Predictive Alin AI delivers malware verdicts in less than 100 ms without sandbox detonation, while MetaDefender Aether™ adds dynamic behavioral analysis with a 99.9% zero-day detection rate, providing rapid, in-depth inspection for suspicious files and unknown threats.
Sensitive Data Leakage & Compliance Risk	Threat blocking alone does not inspect outbound email, redact sensitive information, or enforce policy.	Proactive DLP™ across 125+ file types detects, redacts, and protects sensitive data to support compliance.

Protect email, attachments, and sensitive data before threats reach the inbox.

Request a Demo

OPSWAT.
Protecting the World's Critical Infrastructure

©2026 OPSWAT Inc. All rights reserved. OPSWAT, MetaScan, MetaDefender, MetaDefender Vault, MetaAccess, Netwall, OTfuse, the OPSWAT Logo, the O Logo, Trust no file, Trust no device, and Trust no file. Trust no device. are trademarks of OPSWAT Inc.