OPSWAT.

Protecting Digital Trust Across Banking, Financial Services, and Insurance Communications

Financial institutions are under pressure to protect digital trust while keeping customer, payment, and operational workflows moving. In 2025 alone, the average breach cost in financial services was **USD 6.29 million**. Critical sectors account for **62% of AI-driven breaches studied**, with financial services among the most targeted, according to IBM.

One common risk connects them all: **trusted communications carrying untrusted content**. Email and collaboration channels move the files, approvals, and reports that financial operations depend on. Attackers know this. They use legitimate-looking messages and files to steal credentials, deliver malware, and disrupt operations.

That makes communication security a core part of digital trust, compliance, and operational resilience.

Key Security Priorities for Financial Institutions

- **Protect Digital Identities and Customer Trust:** Reduce exposure to credential theft, mailbox takeover, and account compromise.
- **Secure High-Trust Financial Workflows:** Keep malicious files, links, and sensitive information out of payments, approvals, customer servicing, and daily operations.
- **Protect Sensitive Financial and Personal Data:** Reduce the risk of exposing customer, financial, and confidential business information through email and file-sharing channels.
- **Strengthen Operational Resilience:** Reduce disruption from ransomware, malware, and email-borne attacks.
- **Regulatory Compliance:** Strengthen controls and audit activities related to malware prevention, data protection, phishing mitigation, and operational resilience.

Secure Email Workflows from Known, Unknown, and AI-Scaled Threats

MetaDefender™ Email Security helps prevent threats before they reach users, inboxes, and business processes. It adds layered protection without noticeable delays, shrinking the exposure window and reducing the need for post-delivery remediation.

- Neutralizes potentially malicious content across 200+ file types while preserving usability with Deep CDR™ technology.
- Automatically processes password-protected email attachments by detecting passwords in the email body, sanitizing the file, and delivering a functional safe version to the inbox without manual validation.
- Improves detection coverage with 30+ anti-malware engines and an over 99% detection rate through Metascan™ Multiscanning.
- Identifies suspicious file behavior and previously unseen threats without sandbox detonation through AI-powered malware detection with Predictive Alin AI.
- Prevents zero-day attacks that traditional security tools miss through MetaDefender Aether™'s emulation-based Adaptive Sandbox.
- Detects, redacts, and anonymizes sensitive data across 125+ file types with Proactive DLP™.
- Helps block credential harvesting, malicious links, and phishing attempts.
- Supports operational resilience and audit activities related to DORA, NIS2, GDPR, and more.

Customer Results in Financial Services

A top bank in Taiwan used MetaDefender Email Security with Multiscanning and Deep CDR to strengthen protection against phishing-delivered malware and advanced file-based threats.

"Because we deployed Deep CDR technology into the email channel, they [the bank] are very confident to say that there is almost a 95% reduction of malware from the email channel."

Lambert Lin
Information Security Consultant

Secure Communications. Stronger Resilience.

See how MetaDefender Email Security can help protect the communications and files behind digital identity, payments, and customer operations.

Scan QR code to book a meeting

OPSWAT.
Protecting the World's Critical Infrastructure