OPSWAT.

DATASHEET

Turn Email Security into Compliance Proof

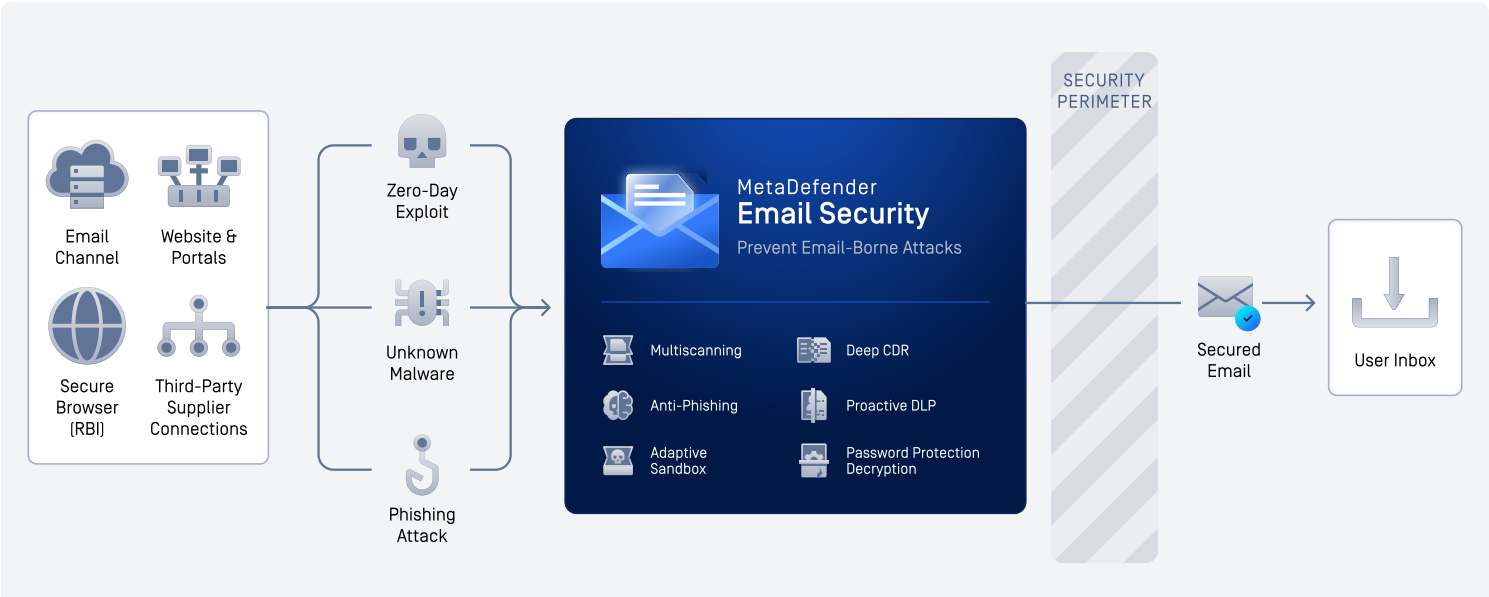
MetaDefender Email Gateway Security & MetaDefender Cloud Email Security

Support compliance requirements with prevention-first email security across on-prem and cloud deployments.

Email security has become a board-level compliance priority for CISOs, CROs, and cyber risk leaders in regulated industries. With shrinking reporting windows, supervisors expect timely responses and defensible evidence trails. Non-compliance leads to NIS2 fines reaching €10M or 2% of global turnover for essential entities, or GDPR penalties reaching €20M or 4% of global turnover; DORA exposes financial entities to administrative penalties under national supervisory regimes.

Where audits and regulatory reviews often find gaps

- **Residual inbox risk is hard to defend**. Post-delivery cleanup still leaves exposure windows and inconsistent outcomes difficult to justify in audit and supervisory review. Per Microsoft's own data, Microsoft Defender removes ~70% of malicious email post-delivery[1].
- **Evidence gaps slow incident reporting and weaken due diligence.** Encrypted attachments, fragmented logs, and unclear sanitization actions make it harder to demonstrate control effectiveness.
- **Hybrid coverage gaps increase regulatory and third-party risk.** Disjointed controls across on-prem and Microsoft 365 create inconsistencies that assessments increasingly scrutinize.



1. Microsoft, March 2026

OPSWAT's prevention-first technologies address the compliance gaps

MetaDefender™ Email Gateway Security (EGS)

Deployed on premises in front of existing mail servers at the SMTP/MX level, it reduces phishing, ransomware, and zero-day exploit risks before they reach inboxes by applying 30+ anti-malware engines, Deep CDR™ Technology, adaptive sandboxing, AI-powered malware prediction and Proactive DLP™ technology. Additionally, EGS sanitizes password protected emails automatically when a password is available or through a self-service portal in which the user can provide the password so that the file can be analyzed and sent to user sanitized and encrypted.

MetaDefender™ Cloud Email Security (CES)

Deployed in minutes on-cloud, it adds to Microsoft Defender, neutralizing known and unknown threats, including zero-days, without MX record changes. It combines up to 17 AV engines scanning, Deep CDR™ Technology and adaptive sandbox, sanitizing password-protected files through the self-service portal.

> "Working with MetaDefender Email Security helps us meet these compliance requirements by providing advanced threat prevention and data sanitization that ensures our network is secure.
>
> **Guy Elmalem**
> IT and Cyber Infrastructure Manager at Hapool Insurance Corporation, a privately owned insurance entity.

OPSWAT technologies mapped to compliance articles	Multiscanning (EGS + CES)	Deep CDR™ Technology (EGS + CES)	Proactive DLP (EGS)	Adaptive Sandbox (EGS + CES)
Digital Operational Resilience Act (DORA)	DORA Art. 9(2)	DORA Art. 9(3)(b)–(c)	DORA Art. 9(4)(a)	DORA Art. 9(1)
Network and Information Systems Directive 2 (NIS2)	NIS2 Art. 21(2)(b)-(e)	NIS2 Art. 21(2)(a)-(b)	NIS2 Art. 21(2)(a)	NIS2 Art. 21(2)(b)-(e)
General Data Protection Regulation (GDPR)	GDPR Art. 32(1)(b)	GDPR Art. 32(2)	GDPR Art. 32(2)	GDPR Art. 32(1)(d)

Why OPSWAT

- **Compliance readiness & evidence**: Documented inspection and sanitization outcomes (audit-friendly evidence trail) aligned to common regulatory requirements such as NIS2, DORA, GDPR, and 25+ additional frameworks. Full list at opswat.com/compliance.
- **Operational resilience**: Reduced SOC noise, encrypted attachment handling, consistent inspection outcomes.
- **Validated outcomes**: 99.2% detection rate for 30+ AV engines, 100% SE Labs Protection and Accuracy score (Deep CDR™ Technology), 99.9% efficacy rate (adaptive sandbox).

Ready to maximize your email security protection?

Schedule a Demo Today

OPSWAT.
Protecting the World's Critical Infrastructure

opswat.com/get-started