

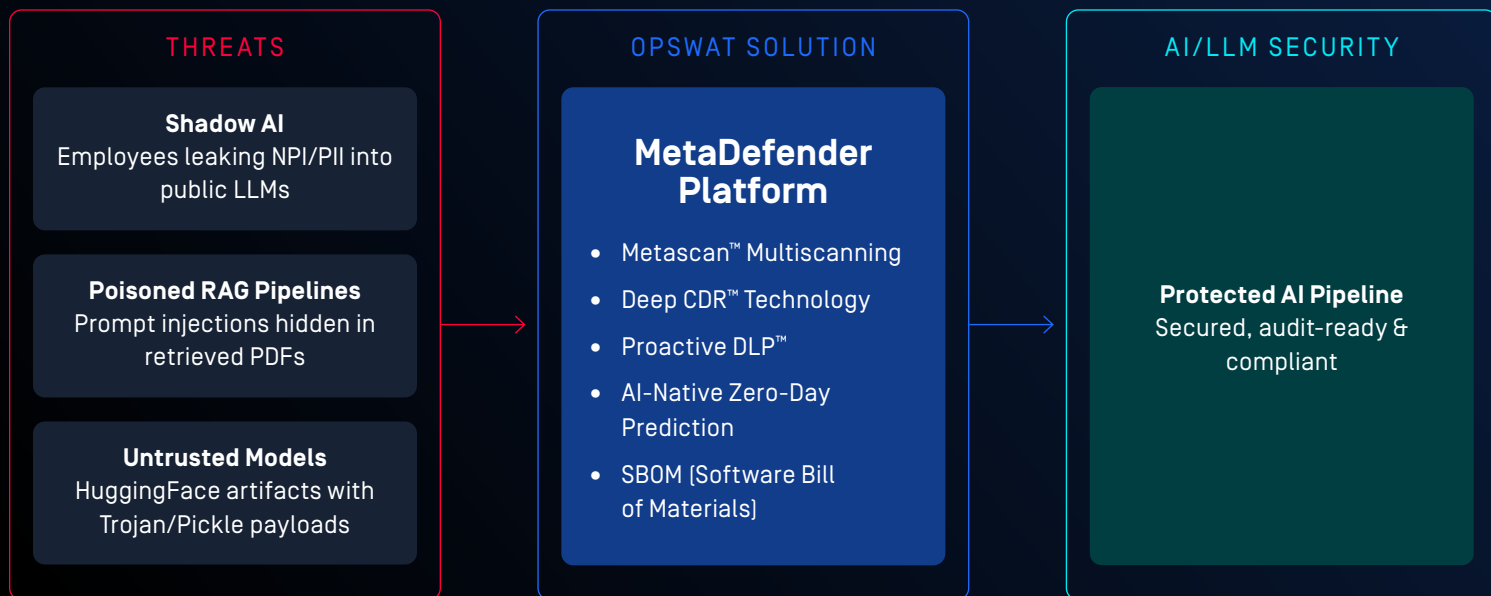
OPSWAT.

OPSWAT FOR FINANCIAL SERVICES

Secure AI Innovations for the Finance Industry

Protect every stage of your AI and LLM pipeline while aligning with EU AI Act, GDPR, DORA requirements, and more.

AI delivers real value in financial services, but rapid adoption creates compounding risks including shadow AI, pipeline integrity threats, and unvetted model repositories. OPSWAT secures all three entry points.



The OPSWAT Value

01

Real-Time Data Protection

Monitors network egress in real time to detect and block NPI/PII and trade secrets before they reach any third-party AI service.

Prevents irreversible data exposure and regulatory fines.

02

Deep CDR™ Technology

Sanitizes RAG PDFs and Office files by stripping out-of-policy objects before the model reads them.

Ensures the AI follows institutional logic, not attacker instructions.

03

Model Vetting

Detonates and scans model artifacts (Pickle, PyTorch, TensorFlow, Safetensors) in an Adaptive Sandbox to catch supply-chain threats.

Protects infrastructure from poisoned third-party supply chains.

04

Immutable Auditing

Proactive DLP + SBOM scans and redacts the full training and inference pipeline.

Audit-ready proof of sanitization for risk committees and regulators.

OPSWAT.

Protecting the World's Critical Infrastructure

Ready to secure your AI pipeline without compromising compliance? Connect with one of our experts: opswat.com/get-started

