OPSWAT.

OPSWAT for Finance Industry

Prevention-First File Security for Banking, Financial Services, and Insurance Organizations

Financial institutions process millions of files daily, including loan applications, KYC (Know Your Customer) documents, trading data, insurance claims, and wire instructions. Every file is a potential entry point for malware, data theft, or regulatory exposure. Files are operationally essential, and with no option to simply block them, institutions need a control layer that inspects and sanitizes content at every entry point. That's what OPSWAT delivers.

61%
of organizations experienced an average of eight breaches involving sensitive file data in the past two years

$2.7M
average file-based breach cost per organization

1 in 3
organizations are highly confident in file security during third-party transfers

Source: OPSWAT – Ponemon Institute State of File Security Report

The Challenge

Financial institutions face a converging set of threats at the file layer, where external content becomes internal risk.

- **Malware & Zero-Day Exposure:** Malicious files blend into everyday business workflows via loan applications, KYC submissions, and claims documents arriving through uploads, transfer, and storage portals
- **Sensitive Data Leakage:** PII (Personally Identifiable Information) and financial records require end-to-end control
- **Third-Party Trust Failure:** Every vendor, partner, and service provider that exchanges files with a financial institution is a potential entry point that bypasses perimeter controls
- **Operational Disruption:** A single infected upload can compromise core systems, stalling onboarding, freezing claims processing, and halting transactions across the business
- **AI Ingestion Risk:** Documents fed into LLM (Large Language Model) and RAG (Retrieval-Augmented Generation) pipelines introduce data poisoning and prompt injection exposure
- **SOC Alert Fatigue:** High-volume daily file events overwhelm analysts, and AI-generated content is accelerating file proliferation faster than traditional triage methods can keep pace
- **Regulatory Exposure:** A single uninspected file transfer can trigger simultaneous violations across PCI DSS, GDPR, SOX, FFIEC, DORA, NYDFS 500, SWIFT CSP, and KYC/AML
- **DevSecOps and Application Security:** Vulnerabilities in build artifacts, open-source dependencies, and CI/CD pipelines can introduce threats directly into production financial applications

OPSWAT.

SOLUTION BRIEF

Why OPSWAT

OPSWAT delivers a prevention-first control layer at every file entry point: inspecting, sanitizing, and verifying content before it reaches critical systems.

Benefits	OPSWAT Capability
Malware and Zero-Day Detection	Multi-layered threat detection and prevention with Metascan™ Multiscanning, Deep CDR™, and Adaptive Sandbox technology.
Sensitive Data Protection	Proactive DLP™ technology identifies, redacts, anonymizes, or blocks PII and financial data inside files.
Third-Party Trust	Policy-driven inspection validates and sanitizes vendor and partner files.
AI Ingestion Integrity	File inspection before RAG and LLM ingestion reduces data poisoning, prompt injection, and confidential data leakage.
DevSecOps & Application Security	Protect the applications powering digital banking, trading platforms, and insurance portals with software supply chain security.
Faster SOC Response	Predictive AIin AI's pre-execution malware detection has a 0.1% false positive rate, delivering verdicts in milliseconds, while MetaDefender Aether™ performs zero-day detection 20x faster than traditional tools—feeding structured, high-confidence threat context directly into SIEM workflows to cut analyst triage time.
Post-Quantum Readiness	Hardware-enforced unidirectional data flows address HNDL (Harvest Now, Decrypt Later) and prevent inbound attack vectors for sensitive keys and transaction data.

Key Use Cases

Customer Onboarding and KYC

Inspect and sanitize ID documents and forms before they reach downstream systems.

Claims & Document Processing

Reduce malware and confidentiality risk in high-volume third-party document exchange.

Email & Collaboration Security

Inspect attachments and shared files to reduce phishing and malware delivery.

Managed File Transfer

Validate vendor, partner, and correspondent files before ingestion.

Cloud & Hybrid Workflows

Extend file trust-boundary controls into API-driven and cloud-native architectures.

AI & LLM Pipeline Security

Block PII and malicious content from entering RAG pipelines and AI ingestion workflows.

MetaDefender™ Solutions for Financial Services

MetaDefender Core	MetaDefender ICAP Server	MetaDefender Storage Security	MetaDefender Cloud	MetaDefender Managed File Transfer	MetaDefender Email Security	MetaDefender Software Supply Chain	MetaDefender Aether™	Peripheral Media Protection
REST API integration for web application	ICAP integration with proxies for network traffic security	Protect financial data at rest	Secure uploaded and shared files in cloud environments	Protect data across IT, OT, cloud, and partner environments	Prevent email-borne attacks	Secure financial, banking and insurance applications	Rapid zero-day detection at the perimeter	Prevent peripheral and removable media attacks

MetaDefender Technologies

Metascan™ Multiscanning · Deep CDR™ · Proactive DLP™ · Adaptive Sandbox · Threat Intelligence · File-Based Vulnerability Assessment · SBOM · Country of Origin · Predictive AIin AI

Business Outcomes

BANKING	FINANCIAL SERVICES	INSURANCE
File-Based Malware and Fraud Prevention Reduce file-borne malware, ransomware, and fraud risk at onboarding, transaction, and correspondent banking channels.	**Client and Investment Data Protection** Protect investment data, client portfolios, trading records, and transaction files from file-borne threats, insider risk, and data leakage across brokerage and wealth management workflows.	**Claims and Workflow Integrity** Prevent malware and fraud risk in claims and broker workflows without disrupting SLAs.
Digital Transformation Secure digital transformation and AI adoption without introducing uninspected file intake channels.	**Regulatory Compliance** Strengthen compliance posture across SEC, FINRA, and DORA with threat prevention and file inspection evidence.	**Data Protection** Protect policyholder PII across broker, agent, and reinsurance networks with auditable DLP controls.
Security at Scale Inspect large volumes of inbound files at speed without disrupting customer onboarding, transaction processing, or business-critical workflows	**Third-Party Risk Management** Reduce vendor and partner file risk across data providers, custodians, and fintech partners.	**Security at Scale** Support compliance with state insurance regulators, GDPR, PCI DSS, and third-party risk requirements.

Get Started

OPSWAT MetaDefender solutions deploy across your existing on-premises, cloud, hybrid, and air-gapped environments and are trusted by global banks, regional financial institutions, insurers, and market infrastructure providers worldwide.

Talk to an Expert
opswat.com/get-started
sales@opswat.com

OPSWAT.
Protecting the World's Critical Infrastructure