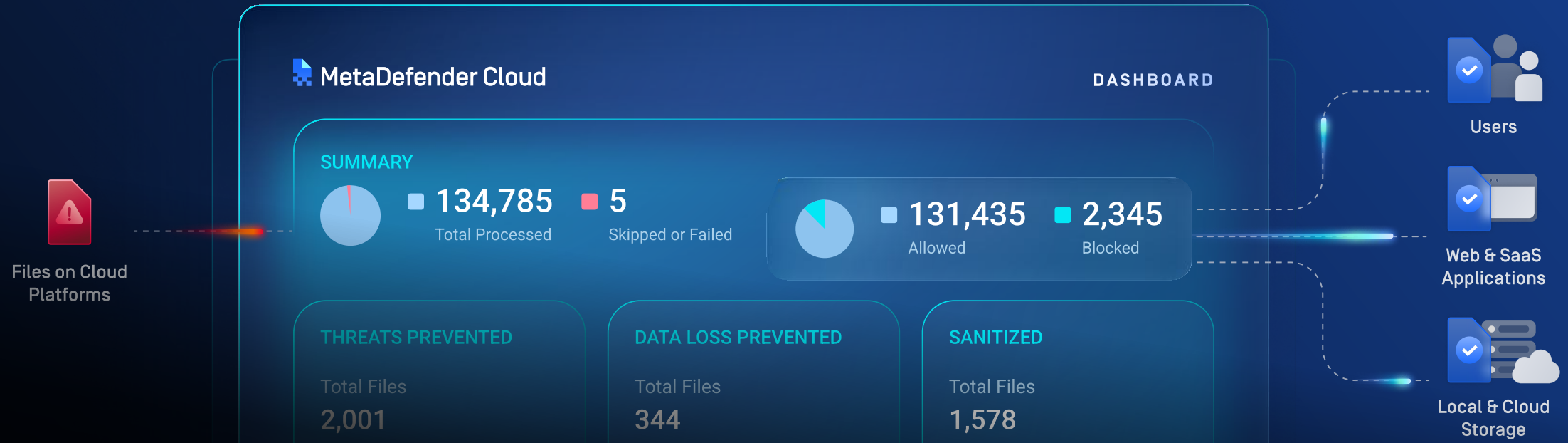
OPSWAT.



FINANCIAL SERVICES & INSURANCE

MetaDefender™ Cloud

Secure every file. Protect every exchange.

AI-powered, cloud-native file security for financial services and insurance.

OPSWAT.

Contents

01 There's a Threat Inside Every File 03

02 The Challenge 04

03 Consistent Controls at Every Entry Point 05

04 How MetaDefender Cloud Protects Your Business 06

05 Key Use Cases 08

06 Customer Story 09

07 Modules and Deployment 10

08 Business Outcomes 11

OPSWAT.

There's a Threat Inside Every File

Financial institutions run on files from customers and partners, yet Kaspersky now detects an average of 500,000 malicious ones every day. One that slips through can become an attack, and an attack a breach that erodes customer trust and invites regulatory investigations.

Even a trusted sender can now deliver malware straight into your file workflows. MetaDefender Cloud inspects every file, detecting and neutralizing threats at enterprise scale without slowing anyone down. As a managed service, it gives compliance audit evidence and security control; no need for an infrastructure of your own.

$6.3M

average cost of a data breach in financial services

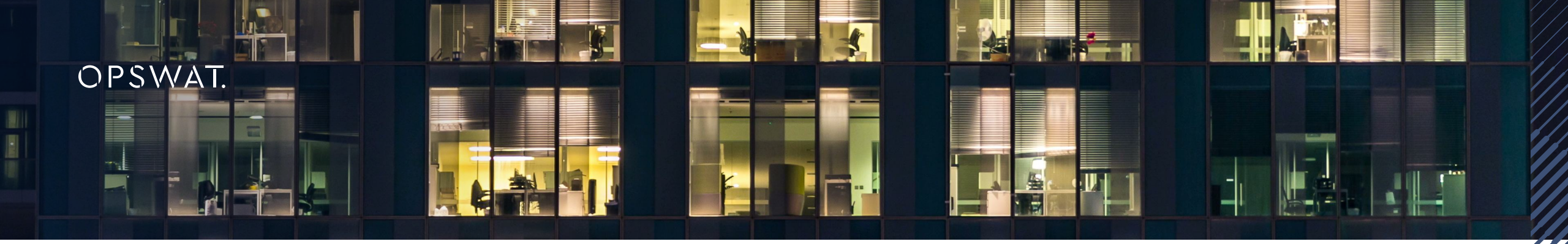
1 in 4

malicious breaches were AI-enabled, up 56% year over year

48%

of breaches involved a third party, a 60% increase year over year

Sources: IBM Cost of a Data Breach Report 2026 · Verizon 2026 Data Breach Investigations Report



The Challenge

For banks and insurers, files can introduce risk through the very workflows that keep the business running. Yet zero-trust strategies do not always extend to the file itself: a trusted sender, authenticated user, or approved platform does not guarantee safe content.

Closing this gap means inspecting files consistently, regardless of their source, before they enter business workflows.

Onboarding runs on outside documents:
IDs, proof of income, and forms from applicants must be checked without delaying time-sensitive workflows.

Claims multiply entry points:
Photos, PDFs, and forms arrive via portals, email, brokers, and SaaS. Inconsistent checks leave gaps.

Antivirus alone isn't enough:
Signature-based scanning misses new and evasive malware. An undetected threat is not a safe file.

Trusted partners still send unsafe files:
Files from brokers, suppliers, and partners need the same scrutiny as any external content.

File checks must be traceable:
Without records of inspection results and decisions, teams struggle to prove control effectiveness in audits.

Volume strains on-prem capacity:
In-house scanning means infrastructure, maintenance, and capacity planning that can't keep pace.

OPSWAT.

Consistent Controls at Every Entry Point

Customer Portals and Web Apps

Onboarding, loan, and claims uploads inspected inline before they reach application logic.

REST API · ICAP Cloud

Cloud and Hybrid Storage

Documents at rest in AWS, Azure, Wasabi, and SharePoint scanned, sanitized, and policy-protected.

Storage Security Cloud



MetaDefender
Cloud

- Metascan Multiscanning
- Deep CDR
- Proactive DLP
- Adaptive Sandbox

SaaS Business Applications

Files attached to cases, accounts, and policies in Salesforce scanned in the background.

MetaDefender for Salesforce

Employee Browsers

Downloads checked for Chrome and Edge users before they land on endpoints.

Browser Extensions

OPSWAT.

How MetaDefender Cloud Protects Your Business

99%

of known malware detected Metascan™ Multiscanning, 20+ engines

200+

file types sanitized and rebuilt Deep CDR technology

99.9%

zero-day detection efficacy MetaDefender™ Aether

125+

file types for data redaction Proactive DLP™



OPSWAT.

1/ Stop known and unknown threats

Layered multiscanning, sanitization, and sandboxing, plus Predictive AI verdicts before a file ever executes.

2/ Compliance and audit ready

Supports Compliance & Alignment With: PCI DSS · HIPAA · GDPR · NIST frameworks
Certifications: ISO/IEC 27001 · SOC 2

3/ Control customer data in files

Detect and redact sensitive customer and financial data before it's exposed.

5/ Apply Policy by Channel and Risk

Rule-based orchestration by file type, size, and scan result.

Blocks disguised files (type mismatch) and malformed or corrupted file structures.

Automatically routes suspicious files from multiscanning to Sandbox for dynamic analysis, so you detonate only what policy requires.

6/ No Customer Data Retained

Zero file retention: when enabled, files are deleted immediately after analysis.

Scan results scoped to the user or organization that submitted the file.

7/ One Platform Across Business Units

Sub-organizations per business unit or application, with per-organization API limits and scoped visibility.

Centralized dashboards, drill-down reporting, and usage trends across all organizations.

Enterprise tier adds mTLS (mutual Transport Layer Security), IP range restrictions, customer-provided identity provider, and custom domain.

OPSWAT.

Key Use Cases

One Unified Approach To File Security Across The Organization

Financial institutions can use MetaDefender Cloud to scale consistent file inspection and sanitization across applications, checking inbound files at the application layer before they enter business workflows. This approach brings common protection to entry points and use cases such as:

01 Customer Onboarding And KYC

Inspect and sanitize ID documents and forms from web and mobile portals before they reach downstream systems.

02 Claims And Policy Documents

Reduce malware and confidentiality risk in high-volume exchange with brokers, agents, and policy holders.

03 Cloud Storage Protection

Scan and sanitize files at rest in AWS, Azure, Wasabi, and SharePoint with MetaDefender Storage Security Cloud.

04 Salesforce File Uploads

Scan files and check URLs, IPs, and domains inside Salesforce in the background, without disrupting workflows.

05 Web Applications and Portals

Route uploads from proxies, WAFs, load balancers, and managed file transfer gateways to ICAP (Internet Content Adaptation Protocol) Cloud for consistent inspection.

06 Third-Party File Intake

Validate and sanitize files from vendors, custodians, and fintech partners at the point of ingestion.

OPSWAT.

CUSTOMER STORY · INSURANCE

Visana Scales File Upload Security For Clients Without Operational Overhead

One of Switzerland's largest health and accident insurers moved client upload scanning from on-premises MetaDefender™ Core to MetaDefender™ Cloud, routing traffic through MetaDefender ICAP Cloud from its existing Airlock Gateway.

Industry
Insurance

Location
Switzerland

Size
1K–5K employees

Products
MetaDefender Cloud, ICAP Cloud

The solution

Visana directs upload traffic from Airlock Gateway to MetaDefender ICAP Cloud. MetaDefender Cloud scans every file, including JSON (JavaScript Object Notation) payloads and complex documents, with Metascan Multiscanning. Files are held in OPSWAT-managed temporary storage only for the duration of processing, with private processing enabled to meet Visana's requirements, and are hosted in the

Results

Before	After
Client uploads insufficiently secured	Files scanned with 20+ anti-malware engines
High operational overhead	Overhead absorbed by OPSWAT
Slow and costly scaling	Virtually unlimited scaling capability
Processes bottlenecked behind privacy	Higher, compliance-ready threat coverage

"MetaDefender Cloud gave us the flexibility to scale, stay compliant, and keep file security strong..."

Stefan Brotschi
IAM (Identity & Access Management) Engineer, Visana

OPSWAT.

Modules and Deployment

MetaDefender Cloud Modules

MetaDefender Cloud (API): REST API for web applications, portals, and custom workflows

MetaDefender ICAP Cloud: proxies, WAFs, load balancers, and managed file transfer gateways

MetaDefender Storage Security Cloud: AWS, Azure, Wasabi, and SharePoint

MetaDefender for Salesforce: secure uploads and reputation checks inside Salesforce

Browser Extensions: file security for Chrome and Edge

Cloud Delivery Without Compromise

- Same Deep CDR, Proactive DLP, and Workflows UI as MetaDefender Core, with MetaDefender Aether zero-day detection available on both.
- Maintenance, engine updates, and upgrades handled by OPSWAT.
- Inherently scalable, managed on OPSWAT's cloud infrastructure.
- Multi-region deployment with a dedicated pre-production environment.
- Standard, Professional, and Enterprise license tiers.

OPSWAT.

Business Outcomes

Banking

Keep onboarding and payments moving: Inspect documents from digital onboarding, lending, and correspondent channels inline, with verdicts fast enough that customers do not notice.

Absorb peaks without procurement: Quarter-end and campaign volumes are handled on OPSWAT-managed capacity; there is no scanning hardware to size or refresh.

Financial Services

Protect client and market data in transit: Detect and redact PII and account data in brokerage, custody, and wealth documents before they leave or enter the firm.

Produce evidence for SEC, FINRA, and DORA reviews: Centralized reporting and SIEM integration show what was inspected, when, and with what result.

Insurance

Shorten the claims cycle safely: Sanitize claim photos, forms, and broker documents in the background so adjusters open clean files without added steps.

Keep health and personal data private: Enable zero-retention processing and choose regional hosting to support GDPR compliance and national insurance regulatory requirements.



GET STARTED

Every file inspected across all entry points. Prevention, detection, and AI, working together to keep threats out. No infrastructure to run.

Explore MetaDefender Cloud today

Request a demo

Scan the QR code or visit us at:
opswat.com/get-started
sales@opswat.com

For over 20 years OPSWAT, a global leader in IT, OT, and ICS critical infrastructure cybersecurity, has continuously evolved an end-to-end solutions platform that gives public and private sector organizations and enterprises spanning Financial Services, Defense, Manufacturing, Energy, Aerospace, and Transportation Systems the critical advantage needed to protect their complex networks from cyberthreats.
Built on a "Trust no file. Trust no device.™" philosophy, OPSWAT solves customers' challenges like hardware scanning to secure the transfer of data, files, and device access with zero-trust solutions and patented technologies across every level of their infrastructure.

OPSWAT is trusted globally by more than 1,900 organizations, governments, and institutions across critical infrastructure to help secure their devices, files, and networks from known and unknown threats, zero-day attacks, and malware, while ensuring compliance with industry and government-driven policies and regulations.

Discover how OPSWAT is protecting the world's critical infrastructure and securing our way of life; visit www.opswat.com

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. Rev. 2026-9