File Security for Financial Services Sector

How Banking, Financial Services, and Insurance Organizations Can Prevent File-Borne Threats

Introduction

Cyberattacks on banking, financial services, and insurance organizations are growing in both frequency and sophistication — despite increased investment in cybersecurity and a stronger emphasis on risk management.

These attacks are largely driven by the high value of financial and personal data, which can be stolen, sold, or held for ransom. As financial institutions continue to digitize services and expand their digital footprint, they become even more attractive targets for threat actors.

This whitepaper covers the key cybersecurity threat vectors that affect financial institutions today and how they can secure their web applications, portals, and other infrastructure to protect critical data, as well as best practices for meeting regulatory compliance requirements.

In particular, we will explore one of the most overlooked, yet dangerous attack vectors on banking and financial services institutions: malicious file uploads. You will learn how to defend against these threats while maintaining operational continuity and productivity.

Your organization could be at risk if:

- You accept mortgage applications or loan payments online.
- You manage customers' banking details.
- You store or process sensitive data such as credit card numbers or social security numbers.
- You operate as a mortgage lender, insurance provider, international bank, or FinTech business.

Table of Contents

01

Why Financial Services Firms Are Prime Targets

With high stakes and high exposure, the financial services industry must treat file-based attack vectors as a critical threat surface.

Financial services organizations handle highly valuable data — from PII (personally identifiable information) and financial records to investment portfolios and transaction histories — making them a top target for cybercriminals. Users no longer need to install a rogue application to get infected. Something as routine as opening a seemingly harmless invoice, courier receipt, mortgage application, or account statement can deliver a malware payload that enables cybercriminals to compromise the organization's environment. File-borne threats embedded in everyday productivity documents are increasingly used as a covert delivery mechanism for ransomware, spyware, or data exfiltration tools.

Financial services firms are targeted for ransomware attacks as they possess critical data that they will go to any lengths to protect and retrieve, even to the extent of paying cybercriminals to keep quiet to minimize reputational damage.

Cybercriminals know that financial institutions have much to lose, both monetarily and reputationally. They aim to steal money from bank accounts, access sensitive, private, confidential data, or destabilize financial markets for political purposes. Attackers use new or recently discovered vulnerabilities (zero-day attacks) to target financial services organizations.

Simultaneously, to improve operational efficiency, enhance competitive advantages, and deliver better customer experiences, many financial services firms have adopted digital solutions and cloud services that can increase business, operational, and reputational risks if not appropriately secured.

Additionally, financial services companies store, transmit, and process an endless volume of sensitive information. They receive, distribute, and share numerous productivity files with employees, partners, and customers every day.

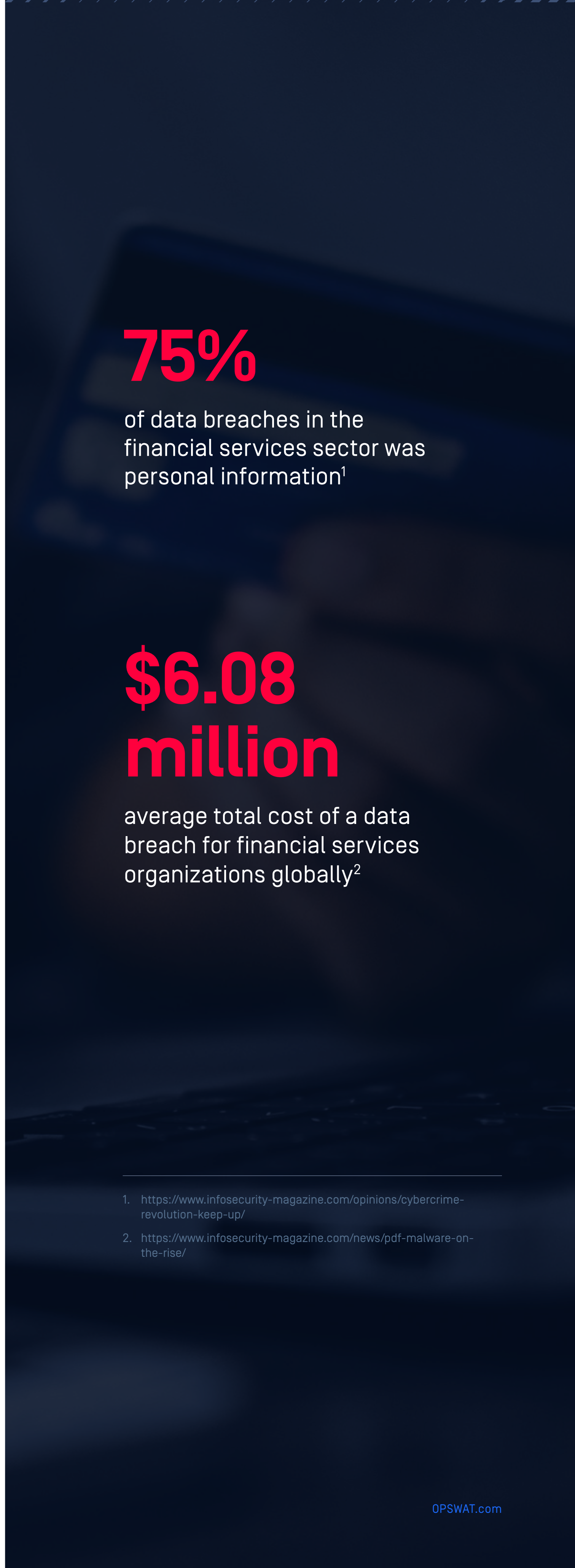
These sensitive and proprietary records are uploaded via web applications and portals or transferred within departments through attachments. They are often copied, distributed, and stored online for day-to-day access or as backups.

Due to the increasing digitalization of financial services and massive amounts of sensitive data, this sector has become an easy target for financially motivated criminals.

The combination of these facts and the growth in demand from customers, business partners, and investors for access to their financial information at any time has placed a significant burden on organizations. Regulatory, business, and technological changes in financial services environments today have increased the need for secure networks and infrastructure.

Governments and industry regulators are crafting new rules to respond to emerging cybersecurity challenges and the risks associated with digital innovation and transformation. There is a heightened focus on operational resilience, and the penalties for non-compliance are significant.

Organizations need to ensure compliance with existing and upcoming Financial Services regulations and cybersecurity standards like the due diligence expectations of the DTCC (Depository Trust & Clearing Corporation), the Safeguards and Privacy Rules of the GLBA (Gramm-Leach-Bliley Act), GDPR, PCI-DSS, FINRA KYC Rule 2090, region-specific requirements under the EU-US Privacy Shield Framework, and Korea's Good Software Certification requirements.



75%

of data breaches in the financial services sector was personal information[1]

$6.08 million

average total cost of a data breach for financial services organizations globally[2]

[1] https://www.infosecurity-magazine.com/opinions/cybercrime-revolution-keep-up/

[2] https://www.infosecurity-magazine.com/news/pdf-malware-on-the-rise/

02

Key File-Based Attack Vectors Impacting Financial Institutions

Organizations with valuable financial data to protect face complex challenges due to the high-value financial data they manage – with threats ranging from new hackers seeking quick gains to make a name for themselves, to sophisticated and organized targeted attacks from established groups with substantial funding and strategic malicious motivations.

Financial institutions face cybercriminals who increasingly exploit security blind spots within banking infrastructure, privacy loopholes in mobile banking applications, cloud-jacking of financial data repositories, and vulnerabilities in banking networks and software to gain unauthorized access to sensitive customer and transaction information. The financial sector experiences a continuous stream of unique malware variants specifically designed to target banking systems, payment gateways, and insurance databases.

Social engineering tactics are used by attackers on users who upload, download, receive, open, and edit many types of files every day. These tactics can target banking, financial services, and insurance employees who routinely handle sensitive financial documents, customer data, and transaction details. These manipulative strategies are used to convince users to open malicious email attachments disguised as loan applications or policy documents, or click deceptive links (phishing attacks), as well as convince them to give up personal information such as usernames, passwords, and financial information, which can then be used to breach the institutions they work for.

Insider threats represent a substantial risk to financial institutions, where a single compromised employee can access vast stores of financial and personal data.

Financial services organizations need to limit user access, detect, and redact (or block) sensitive data, audit and track role-based access, and encrypt stored data to protect assets from malicious insiders and unauthorized employee access, which could lead to accidental data breaches.

Sponsored attacks on financial firms can be funded by malicious organizations seeking to destabilize economic systems, compromise financial infrastructure, or gather intelligence on high-value targets. The financial sector has faced unprecedented challenges as cybercriminals develop sophisticated methods to infiltrate payment systems, manipulate transactions, and exfiltrate customer financial data, resulting in massive economic losses across the global financial ecosystem.

Web portals and applications are essential for the effective functioning of banking and financial firms, but also pose significant risks:

- Threat actors can conceal malicious code, macros, hyperlinks, and other harmful content within common files and upload them to an online portal to gain access to the organization's core banking systems and financial IT infrastructure.
- Inadvertent hosting and distribution of malicious files uploaded by a threat actor can lead to spreading malware to customers and significant service disruptions, resulting in expensive lawsuits and bad publicity. Users no longer need to install a rogue application to get infected – that can happen by opening what appears to be an invoice, a courier receipt, a mortgage application, or any other productivity file.
- If left unchecked, users can unknowingly submit sensitive information such as financial data, tax information, and other PII (personally identifiable information), putting financial institutions at risk of compliance violations with

Productivity Files and File Uploads

Document-borne malware is on the rise as productivity files offer an attack vector to cybercriminals. By concealing advanced threats that exploit vulnerabilities within common file types, attackers can compromise an end user or an entire system. Any file coming inside an organization should be audited and analyzed, even when the sender seems to be a trusted, reliable source.

The most uploaded and shared files in office settings are:

- Microsoft Office – DOC(X), XLS(X), PPT(X), etc.
- Images – JPEG, PNG, TIFF, etc.
- PDFs

Harmful code can be embedded in these file formats by attackers. Most people are aware of malicious macros, but Microsoft Office documents can contain many other kinds of advanced threats as well.
For example, OLE objects disguised as embedded multimedia or script-enabled ActiveX controls can be configured by attackers to download malicious payloads.[3] PDFs may contain JavaScript that performs malicious actions.[4]

Additionally, malicious files can be disguised as false file extensions. These are called “spoofed” files. There are several methods of concealing the true type of a file from users and even from anti-malware security measures.

Obfuscation is becoming an important tactic for threat actors, and PDF malware disguises malicious URLs by encrypting them, hiding them in compressed streams or using hexadecimal representations which can also hinder automated analysis of email security solutions.[5]

[3] https://www.infosecurity-magazine.com/news/pdf-malware-on-the-rise/

[4] https://www.forbes.com/sites/zakdoffman/2019/04/29/new-cyber-report-25-of-all-malware-hits-financial-services-card-fraud-up-200/?sh=1f2286e27a47

[5] IBM X-Force Threat Intelligence Index 2025

High-Risk Documents in Banking, Financial Services, and Insurance Environments

1

Customer-Facing Documents

Frequently exchanged over web portals, email, and mobile apps, these documents are a top target for cyberattacks due to their high data sensitivity and exposure.

- Loan and mortgage applications
- Bank statements and account summaries
- Insurance claim forms and policy documents
- Credit reports
- ID documents (passports, driver’s licenses, national IDs)

2

Financial and Strategic Documents

Often used in planning and decision-making, these documents contain sensitive financial data that could be exploited if leaked or tampered with.

- Budget forecasts and P&L statements
- M&A documents and investment strategies
- Audit reports and financial disclosures
- Board meeting notes and strategic plans

3

Employee and HR Documents

Containing personally identifiable information (PII) and confidential internal data, these files must be secured against unauthorized access and exfiltration.

- Employee onboarding forms
- Payroll records and tax forms
- Performance reviews
- Medical and benefits documentation
- Internal training materials

4

Regulatory and Compliance Documents

These are subject to strict controls, and any compromise can result in regulatory penalties or reputational damage.

- Regulatory filings (e.g., GLBA, GDPR, PCI-DSS)
- Compliance checklists and audit trails
- KYC/AML documentation
- Consent forms and privacy notices
- Internal control and due diligence reports

5

Regulatory and Compliance Documents

Files received from suppliers, partners, or consultants may contain embedded threats or violate data handling policies.

- Vendor contracts and agreements
- Invoices and purchase orders
- Risk assessments from external auditors
- Partner onboarding files
- Shared project documentation

6

Technical and Operational Documents

These files support infrastructure and application functions but are often overlooked as attack surfaces for malware or exploitation.

- Software installers and executables
- Archive files (.zip, .rar)
- Macro-enabled documents (.docm, .xlsm)
- Configuration and log files
- Scripts and code snippets

03

Assessing Unique Security Needs

Each financial services business has different workflows and unique security needs. When designing a strategy to keep productivity file uploads secure, it's important to assess and address your specific situation.

Start by Asking Questions

- How many security restrictions can you add without impacting critical financial operation?
- How reliant can your organization be on user and employee training? How confident are you that users will apply everything they learn in security training?
- How are you validating incoming files? Are you doing any pre-processing before you are making the files available? If so, how do you ensure they won't try to exploit the processing service?
- Which specialized security technologies have you deployed for protecting financial documents and data?
- How does your security stack address the unique document security challenges of the banking, financial services, and insurance sector?

Consider Your Use Case

- When and why do users need to upload files to your portal? For example, client onboarding forms, load applications, insurance claims, investment portfolios, or regulatory reporting documents.
- What filetypes are necessary or commonly used? For example, PDFs of financial statements, Word documents for contracts, Excel files for data analysis.
- What risks do those file types pose when entering your organizations? For example, PDFs may contain embedded JavaScript or malicious URLs, Excel files might carry macros or formulas that could execute harmful script, and images might be used to conceal malware or sensitive data.
- What processes do you have in place to validate files post-storage? Do you consistently scan documents to make sure they remain free from threats over time? If you are simply receiving scanned documents, collaborating with partners on draft agreements, or sharing invoices or POS.

If You Are Receiving or Sharing Documents

- Do you ever need to allow PDFs with embedded JavaScript?
- Can you trust documents that contain hyperlinks, macros, OLE objects, or ActiveX controls?
- How do you verify that an image is legitimate and hasn't been manipulated by a malicious actor?

It's one thing to decide that any file containing scripts or macros should not enter an organization; it's another thing to enforce that policy. Determining what is contained in a file without opening it is difficult. Therefore, further steps are necessary to defend against malicious files disguised as common productivity files.

04

File Security Best Practices for Financial Institutions

1

Only Allow Specific File Types

By limiting the list of allowed file types, you can avoid executables, scripts, and other potentially malicious content from being uploaded to your system.

2

Verify File Types

In addition to restricting the file types, it is important to ensure that no files are 'masking' as allowed file types. For instance, if an attacker were to rename an .exe to .docx, and your solution relies entirely on the file extension, it would bypass your check as a Word document which in fact it is not. Therefore, it is important to verify file types before allowing them to be uploaded.

3

Scan for Malware

To minimize risk, all files should be scanned for malware. We recommend multiscanning files with multiple anti-malware engines (using a combination of signatures, heuristics, and machine learning detection methods) to get the highest detection rate and the shortest window of exposure to malware outbreaks.

4

Remove Possible Embedded Threats

Files such as Microsoft Office documents, PDFs, and image files can have embedded threats in hidden scripts and macros that are not always detected by anti-malware engines. To remove risk and make sure that files contain no hidden threats, it is best practice to remove any possible embedded objects by using Deep CDR (Content Disarm and Reconstruction).

5

Authenticate Users

To increase security, it is good practice to require users to authenticate themselves before uploading a file. However, user authentication does not guarantee the user's machine itself isn't compromised.

6

Set a Maximum Name Length and Maximum File Size

Make sure to set a maximum name length (ideally restricted to a specific set of characters) and file size in order to prevent unauthorized file types.

7

Randomize Uploaded File Names

Randomly alter the uploaded file names so that attackers cannot try to access the file with the file name they uploaded. When using Deep CDR, you can configure the sanitized file names to contain random identifiers (e.g. the analysis data_id).

8

Store Uploaded Files Outside of the Web Root Folder

The directory to which files are uploaded should be separate from the website's public directory so that attackers cannot execute the file via the assigned path URL.

9

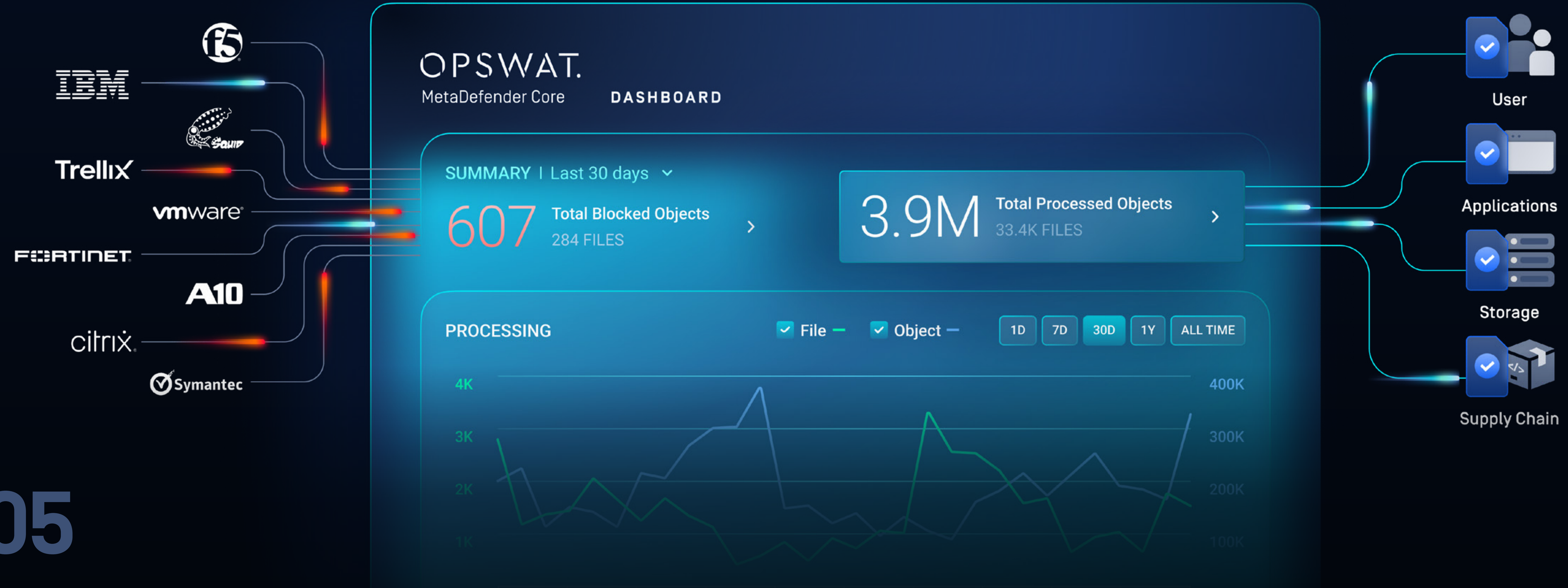
Check for Vulnerabilities in Files

Make sure that you check for vulnerabilities in software and firmware files before they are uploaded.

10

Use Simple Error Messages

When displaying file upload errors, do not include directory paths, server configuration settings, or other information that attackers could potentially use to gain further entry into your systems.



05

How OPSWAT Helps

MetaDefender for File Security

MetaDefender for File Security protects organizations from file-borne threats and zero-day attacks for secure file transfers across networks, applications, and customer operations.

MetaDefender technologies integrate advanced malware protection and detection with your existing IT solutions and applications for file upload security, as well as secure storage, email security, cross-domain solutions, and malware analysis.

Our solutions are used by financial institutions that require the highest level of security.

7 out of 10

Top US Banks

#1 Market Leader

MetaScan Multiscanning & Deep CDR Technology

30+ Engines

Powered by More Than 30 Top Tier AV Vendors

100% Protection

Verified by SE Labs Deep CDR Test

Deploy in as Little as One Hour

We Stop Attackers From Leveraging Your Own Files Against You

The MetaDefender™ Platform

Multiscanning

30+ AV Engines

AhnLab, Avira, Bitdefender, ClamAV, ESET, Quick Heal, K7 SECURITY, Vir.IT explorer PRO, IKARUS security software, EMSISOFT, TACHYON, NANO antivirus, COMODO, Xvirus, Zillya Laboratory, SOPHOS, Bkav, LIONIC Security Solution Provider, nG, varist, McAfee, ANTIY, CROWDSTRIKE, Filseclab, CMC CYBER SECURITY, WEBROOT, SYSTWEAK, BlackBerry | CYLANCE, GRIDINSOFT, RocketCyber, 火绒安全 HUORONG SECURITY, Microsoft Defender

- MetaScan
- Adaptive Sandbox — Real-Time, Emulation-Based Sandbox
- Vulnerability Assessment — Detect Application Vulnerabilities Before Install
- SBOM — Prevent Zero-Day Vulnerabilities In Applications
- Deep CDR — Content Disarm and Reconstruction
- Proactive DLP — Block Private and Personal Identifiable Information
- Threat Intelligence — Real-Time Threat Data and Insights
- Country of Origin — Country and Vendor of Origin Identification

Content Disarm and Reconstruction

180+ Supported File Types

DOC DOCX XLS XLSX PPT RFT PDF

HTML XML JPG PNG GIF SVG SVG

Deployments Options

On-Premises | Cloud | Air-Gapped

- MetaDefender Core
- MetaDefender ICAP Server
- MetaDefender Cloud
- MetaDefender Software Supply Chain
- MetaDefender Storage Security
- Cloud Security for Salesforce

MetaDefender for File Security delivers multi-layered security designed to protect your organization from malicious files.

Verify File Types

OPSWAT File Type Analysis technology combats spoofed file attacks by determining the actual file type based on the content of the file rather than just checking the extension. You can also configure security processes based on true file type.

Scan Files

OPSWAT Multiscanning technology leverages 30+ leading anti-malware engines and proactively detects over 99% of malware by using signatures, heuristics, and machine learning.

Detonate and Analyze Malware in a Controlled Environment

OPSWAT Adaptive Sandbox is a complete set of malware analysis technologies including threat-agnostic analysis of files and URLs, emulation of all targeted applications, a focus on Indicator-of-Compromise (IOC) extraction, and a Rapid Dynamic Analysis engine for targeted attack detection.

Extract Archive Files

OPSWAT currently supports archive scanning for over 30 types of compressed files. Archive handling options are configurable, and multi-level and encrypted archives are supported.

Protect Sensitive Data

OPSWAT Proactive DLP helps companies prevent sensitive and confidential information in files from leaving or entering the company's systems. Supports 110+ file types, including Microsoft Office documents, PDFs, CSVs, HTML, and image files.

Generate SBOM

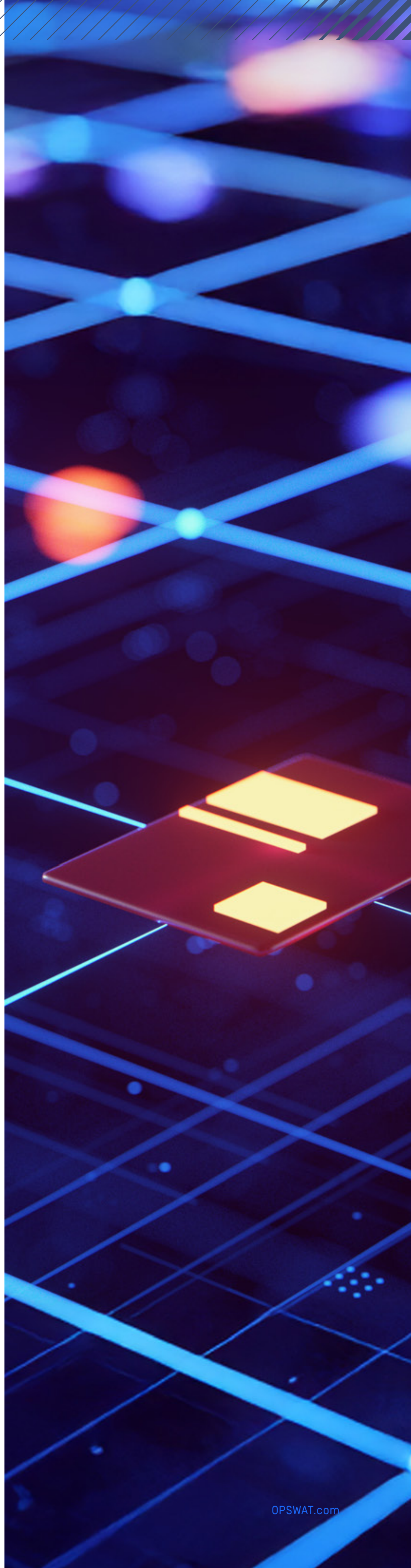
OPSWAT SBOM secures the software supply chain by providing a comprehensive component inventory for source code and containers. Supports 10+ programming languages and 5M+ third-party open-source components.

Detect Application and File-based Vulnerabilities

OPSWAT File-Based Vulnerability Assessment technology scans and analyzes binaries and installers to detect known application vulnerabilities before they are executed on endpoint devices, including IoT devices.

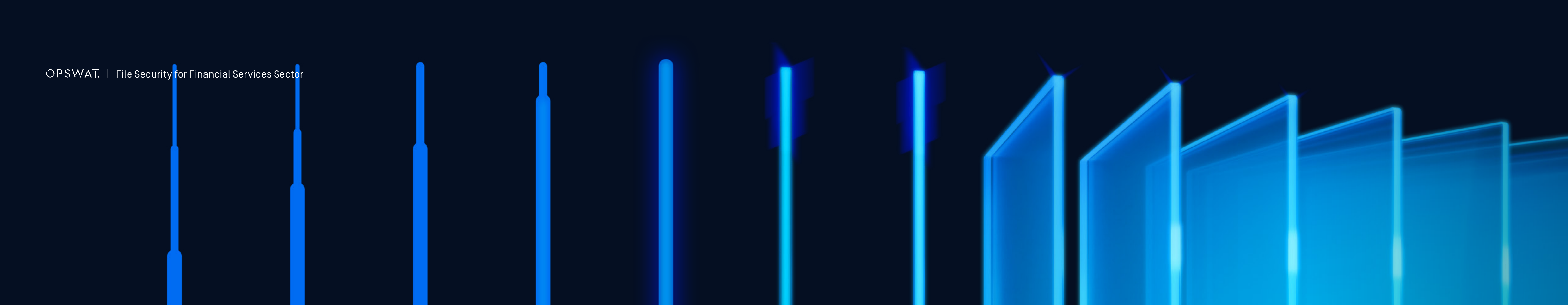
Sanitize Files

OPSWAT Deep CDR technology prevents potentially undetected file-borne threats by sanitizing and reconstructing files. With support for over 180 common file types, hundreds of file reconstruction options are available.



Use Cases and Integrations

	File Uploads	File Downloads	File Transfers	File Sharing	File Storage
Challenges	During file uploads, users may unknowingly submit infected content via web portals, emails, or customer-facing apps.	Download workflows are also high risk, especially when employees retrieve files from untrusted sources.	Files transferred internally and externally across MFT (managed file transfer) solutions must be inspected to prevent interception, alteration, or proprietary data theft.	Internally shared files between departments, systems, or partners can propagate threats if not properly scanned, heightening the risk of data leaks and compliance violations.	File storage carries risk; dormant files in S3 buckets or shared drives can harbor threats waiting to be activated.
Integrations	f5 NGINX vmware by Broadcom netscaler A10 FORTINET Trellix IBM Squid Symantec by Broadcom	Trellix cradlepoint Forcepoint BROADCOM MENLO SECURITY	FORTRA GoAnywhere netscaler NUTANIX Progress MOVEit IBM AIRLOCK axway globalscape xona SEEBURGER Cyolo	DELL EMC ISILON HUAWEI FILECLOUD	aws | S3 Google Cloud Microsoft Azure NetApp Alibaba Cloud MINIO CLOUDIAN box wasabi SharePoint Online | On-Prem DELL EMC OPSWAT MetaDefender Managed File Transfer ORACLE Cloud Infrastructure OneDrive



Key Differentiators

Advanced Threat Detection and Prevention Technologies

OPSWAT's industry-leading cybersecurity technologies include MetaScan Multiscanning, Proactive DLP, and Deep CDR, which prevents known and unknown threats and achieved a 100% protection score from SE Labs.

Custom Security Policies and Workflow

Enables administrators to create multiple workflows to handle different security policies based on users, file sources, and file types.

Low Total Cost of Ownership (TCO)

Flexible offerings provide beneficial TCO. Powerful control over cybersecurity through a single platform results in higher ROI, higher adoption, lower overhead, and fewer trained professionals needed to oversee complex systems.

Simple and Flexible Deployment

Fast and scalable implementation on-premises and in the cloud using REST API or any ICAP enabled product.

High Performance and Scalability

Processes and secures files in milliseconds without affecting performance. Scales to any volume with our built-in high-performance architecture and load-balancing features.

Aid Compliance

Meeting regulatory compliance requirements is time-consuming, and oversights can be costly. OPSWAT technologies help your organization with compliant processes, comprehensive visibility, and detailed reporting capabilities that strengthen your ability to meet OWASP guidelines and due-diligence expectations of DTCC (Depository Trust & Clearing Corporation), GLBA (Gramm-Leach-Bliley Act), GDPR, PCI-DSS, FINRA, and many other regulatory requirements.

GET STARTED

Are you ready to put MetaDefender on the front lines of your cybersecurity strategy?

Talk to one of our experts today.

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

OPSWAT.

Protecting the World's Critical Infrastructure

For the last 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 1,700 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.