OPSWAT.

EBOOK

Proven Deployments in Banking and Financial Services

Table of Contents

01 Introduction

02 Common Cybersecurity Challenges

03 Myths vs. Reality

04 Multi-Layered File Protection Strategy: Secure Your Infrastructure and Your Customers' Data

05 Use Cases and Proven Deployments

06 Building Resilient File Security for the Future

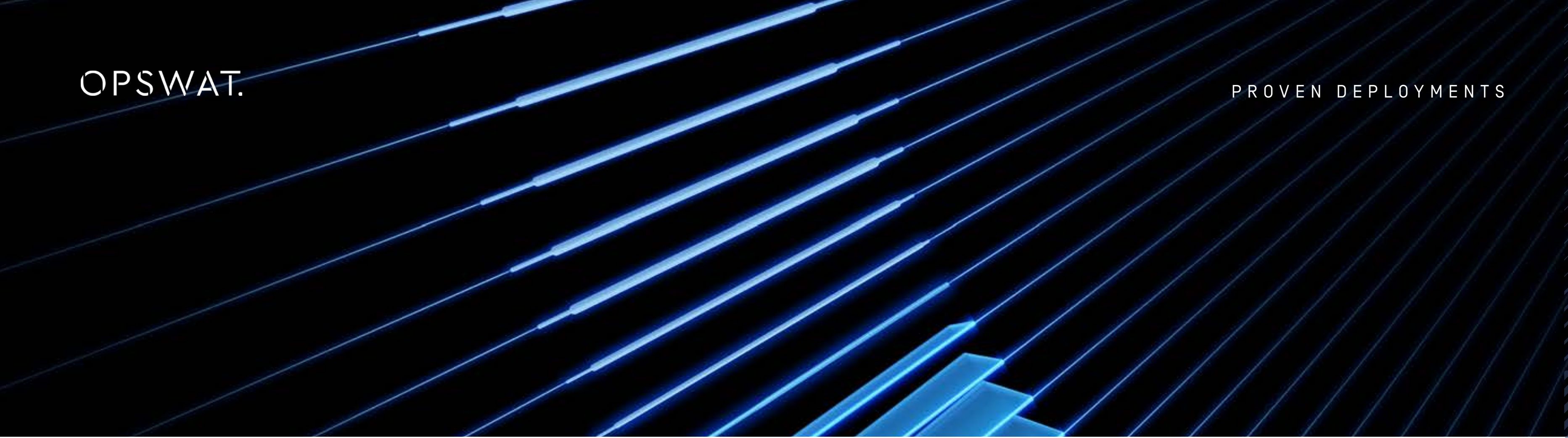
01

Introduction

Banking, financial services, and insurance organizations process thousands of files daily from loan applications and insurance claims to regulatory reports and customer correspondence. Each file represents both an opportunity to serve your customers better and a potential gateway for sophisticated cyberthreats targeting the financial sector.

Due to their critical role in the global economy and the high volume of sensitive financial data they manage, these organizations face unique and unprecedented cybersecurity challenges. The stakes have never been higher; a single compromised file can trigger cascading effects across your entire network, resulting in regulatory penalties, operational disruption, and irreparable damage to your institution's reputation.

This e-book cuts through the complexity and delivers actionable insights on building comprehensive file security defenses. Together, we'll identify the common challenges, demystify misunderstandings, and discover how leading financial institutions are successfully protecting their most sensitive assets while maintaining the operational efficiency that modern banking demands.



02

Common Cybersecurity Challenges

The financial services sector faces a unique constellation of cybersecurity challenges that extend far beyond traditional perimeter defense. Whether you're managing mortgage documents, insurance forms, or customer applications, financial files are one of the most direct pathways to valuable data and system access.

From state-sponsored APTs (advanced persistent threats) to sophisticated malware and zero-day exploits, attackers are increasingly embedding malicious content within seemingly legitimate business documents. Understanding these evolving threats is the first step toward building reliable defenses that can adapt and respond to tomorrow's unknown challenges along with today's known risks.

File-Borne Malware

Threat actors embed malware in PDFs, Excel spreadsheets, and Word documents to bypass traditional antivirus tools and target sensitive financial data.

Data Privacy and Compliance Requirements

Financial institutions are required to maintain strict compliance with regulations such as GDPR, PCI-DSS, SOX, FFIEC, KYC, and AML, while protecting customers' sensitive data.

Advanced Persistent Threats

APTs are sophisticated threats that remain undetected for extended periods, allowing attackers to move laterally through systems and cause substantial financial losses.

Phishing & Social Engineering Attacks

Malicious actors embed threats within legitimate documents to trick users into opening compromised files, leading to credential theft and network infiltration.

Insider Threats

Employees with privileged access to financial records and transaction systems may unintentionally leak data or expose systems through poor security practices.

High Volume and Variety of Files

Financial institutions handle large volumes of diverse files: loan applications, claims, trading documents across channels. An effective security solution must scale efficiently without compromising threat detection or performance.

Third-Party & Supply Chain Risks

Weak security controls in vendor ecosystems create cascading breaches as attackers exploit trusted third-party connections to infiltrate financial networks.

Complex Security Infrastructure

With a mix of legacy systems, cloud platforms, and third-party tools, deploying consistent security enforcement is challenging, which potentially leads to policy gaps and security blind spots.

Threat Detection and Response Delays

Outdated tools and limited SOC resources can hinder timely detection. Attackers exploit this gap to stay hidden while exfiltrating sensitive data or executing fraudulent transactions.

Recovery Time Objectives

Legacy systems and inadequate disaster recovery plans often prolong downtime after cyber incidents, resulting in financial losses and regulatory penalties.

03

Myths vs. Reality

Despite the critical importance of comprehensive file security, persistent misconceptions continue to create dangerous blind spots in financial institution defense strategies. These myths don't just represent outdated thinking—they actively undermine security effectiveness and create compliance vulnerabilities.

The gap between perception and reality in file security can be the difference between in-depth defense and a catastrophic breach. By examining these widespread misconceptions through the lens of actual threat intelligence and real-world attack patterns, we can build a foundation for security strategies that address genuine risks rather than perceived ones.

Myth	Reality
1. We already have a single antivirus engine with 100% protection.	Even the best antivirus solutions have limitations. New threats emerge constantly and relying solely on one (antivirus) leaves you vulnerable to threats that it hasn't been updated to detect. Conversely, layering multiple AV engines improves threat coverage and resilience.
2. Scanning endpoints, emails and web downloads with desktop AVs is enough.	Endpoint and email scanning are necessary, but far from sufficient. By the time a malicious file reaches the endpoint, it's likely too late. To truly reduce risk, files need to be secured at all transfer points, including web upload portals, cloud apps, and internal transfers.
3. Only high-risk uploads need to be scanned.	Trusted users, partners, and customers can still unknowingly upload malicious files. Attackers can exploit legitimate channels, including compromised accounts or partner systems. Assuming a file is safe based on its source creates blind spots. Every upload should be scanned to ensure consistent protection across all entry points.
4. Blocking risky file types is enough. Formats like JPEG or PDF are safe, and only unknown users pose a threat.	Malicious content can be embedded in PDFs, Office files, or images using obfuscation, exploits, or steganography. In banking, financial services or the insurance sector, most uploaded files are non-portable executable formats – and they're far from harmless. PDFs may contain JavaScript or phishing links; images can hide payloads in metadata. Threat actors often target trusted sources—compromised employees, partners, or supply chain vendors. Selective scanning creates blind spots and increases regulatory exposure.
5. We already use network security solutions like WAF, IPS, and proxies to protect our systems.	While these tools are essential for blocking malicious traffic and application-layer attacks like DDoS or CSRF, they aren't designed to inspect the contents of files. Threats hidden inside documents, images, or archives can easily slip through. To stop file-based attacks, you need deep content inspection beyond what traditional network security devices provide.

Myth	Reality
6. Integration is too time-consuming, complex, and unnecessary.	A strong security solution should enhance, not hinder, your operations. The right platform will integrate smoothly with existing IT environments without heavy reconfiguration and overhead. It will also support flexible deployment models from on-premises, cloud, to hybrid, and offers broad compatibility with existing infrastructure, making implementation fast and efficient.
7. Meeting regulatory compliance means we're secure.	Meeting regulatory requirements is essential, but it's not enough. Simply aiming to pass audits can leave critical gaps unaddressed. Compliance provides a baseline, but true cybersecurity maturity requires a proactive, risk-based approach tailored to your institution's unique vulnerabilities.
8. Traditional sandboxing is enough.	While useful, traditional sandboxes can be slow, expensive, and easily bypassed by advanced threats. Relying on them alone leaves gaps. A layered approach that combines Adaptive Sandbox, DLP (data loss prevention), and CDR (Content Disarm and Reconstruction), offers stronger, more reliable protection against both known and unknown threats.
9. Third-party security is the vendor's concern, not ours.	Third-party security is an extension of your organization's own security perimeter. A vulnerability in a partner's system can serve as a direct entry point for attackers to make their path to your infrastructure. Continuously monitor third-party access, enforce strict access controls, and apply zero-trust principles to minimize exposure.
10. We've never had a problem before, so we're safe.	Many breaches go undetected for weeks or even months. Just because an incident hasn't surfaced yet doesn't mean systems are secure. Proactive protection is essential. There's always a first time for everything and relying on luck alone leaves room for exposure.

04

Multi-Layered File Protection Strategy

Secure Your Infrastructure and Your Customers' Data

Effective file security in financial services requires a defense-in-depth approach that covers a wide range of attack surfaces. Your security solution must also protect sensitive data throughout its entire lifecycle: from the first time the file is uploaded to a banking web portal, for example, to when it is transferred, stored, and shared with other entities.

No single security control, regardless of how advanced, can address the full spectrum of file-based threats targeting financial institutions.

Organizations with the most mature cybersecurity strategies implement zero-trust models and a comprehensive security architecture that combines advanced threat prevention, adaptive threat analysis, data loss prevention, and vulnerability detection capabilities. This section outlines components for building resilient file security frameworks that scale with your business while maintaining the performance and reliability that financial operations demand.

The MetaDefender™

Core Technologies

Multiscanning

30+ AV Engines

AhnLab Avira Bitdefender ESET Quick Heal
K7 SECURITY VirIT IKARUS EMSISOFT
TACHYON NANO xcitium Zillya SOPHOS
Bkav LIONIC varist Trellix ANTIY
CROWDSTRIKE Filseclab opentext
SYSTWEAK ARCTIC WOLF SentinelOne GRIDINSOFT
RocketCyber 火绒安全 Microsoft Defender

Content Disarm and Reconstruction

200+ Supported File Types

DOC DOCX XLS XLSX PPT RFT PDF
HTML XML JPG PNG GIF SVG SVG

MetaScan

Deep CDR

Real-Time, Emulation-Based Sandbox

Adaptive Sandbox

Proactive DLP

Block Private and Personal Identifiable Information

Detect Application Vulnerabilities Before Install

Vulnerability Assessment

Threat Intelligence

Detect and Contextualize Emerging Threats

Prevent Zero-Day Vulnerabilities In Applications

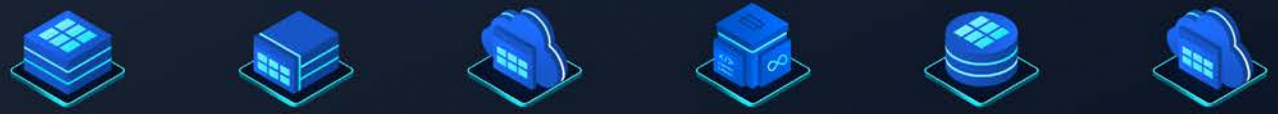
SBOM

Country of Origin

Country and Vendor of Origin Identification

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

MetaScan™ Multiscanning

Fast and Accurate Threat Detection

Many organizations rely on a single anti-malware engine, which can miss advanced or emerging threats. MetaScan Multiscanning addresses this by leveraging 30+ leading anti-malware engines to improve detection accuracy and speed. It combines signature, heuristic, and machine learning-based scanning with global threat intelligence to detect known and unknown threats. This multi-engine approach achieves over 99.2% malware detection while reducing false positives.

Deep CDR™

Prevent Zero-Day Attacks and Evasive Malware

Most cybersecurity solutions rely upon threat detection as their core protective function. Deep CDR does not rely on detection. It assumes all files are threats and rebuilds their content using a secure and efficient reconstruction process. Deep CDR supports over 200 file types and outputs safe and usable files. Deep CDR is extremely effective at preventing targeted attacks, emerging threats, ransomware, known threats, and unknown malware.

Proactive DLP™

Detect and Block Sensitive Data

Prevent potential data breaches and regulatory compliance violations by detecting and blocking sensitive data in files and emails. Proactive DLP handles various data, including credit card and social security numbers. Proactive DLP supports multiple file types, including Microsoft Office and PDF. AI-powered Document Classification detects adult content in images and offensive language in text.

File-Based Vulnerability Assessment

Detect Vulnerable Software Before Installation

All applications contain exploitable vulnerabilities of varying severity. Our File -Based Vulnerability Assessment improves endpoint security. It detects binaries and installers with known vulnerabilities in files, applications, and software before they are installed on endpoint devices, including IoT devices. It supports vulnerability detection for over 1 million files and over 20,000 applications.

Adaptive Sandbox

Advanced Threat Analysis

Adaptive Sandbox's unique threat analysis technology enables zero-day malware detection and extracts valuable IOCs with its advanced, emulation-based approach that operates 10x faster and 100x more efficiently than traditional sandboxes. Adaptive Sandbox is an indispensable tool for detailed threat and malware analysis, enabling organizations to stay ahead of emerging threats and shape their cybersecurity strategies accordingly.

Threat Intelligence

AI-Driven Malware Analysis for Evasive Threats

MetaDefender Threat Intelligence is an AI-driven malware analysis engine that helps security teams detect and respond to evasive file based threats including zero day attacks with 99.6% accuracy. By combining adaptive sandboxing with a real time reputation service, it empowers organizations to stay ahead of modern malware and reduce response times significantly.

SBOM (Software Bill of Materials)

Automated SBOM generation for code & containers

Stay compliant and secure in the software supply chain. With OPSWAT SBOM, developers can identify known vulnerabilities, validate licenses, and generate component inventory for open-source software (OSS), third-party dependencies, and containers.

Country of Origin

Country and Vendor of Origin Identification

The OPSWAT Country of Origin engine empowers organizations to instantly detect the geographic source of uploaded files including PE, MSI, and Self-extract.

By analyzing digital fingerprints and metadata, it can identify restricted locations and vendors. This enables automated filtering that blocks unauthorized access to sensitive data while ensuring compliance with data regulations across regions.

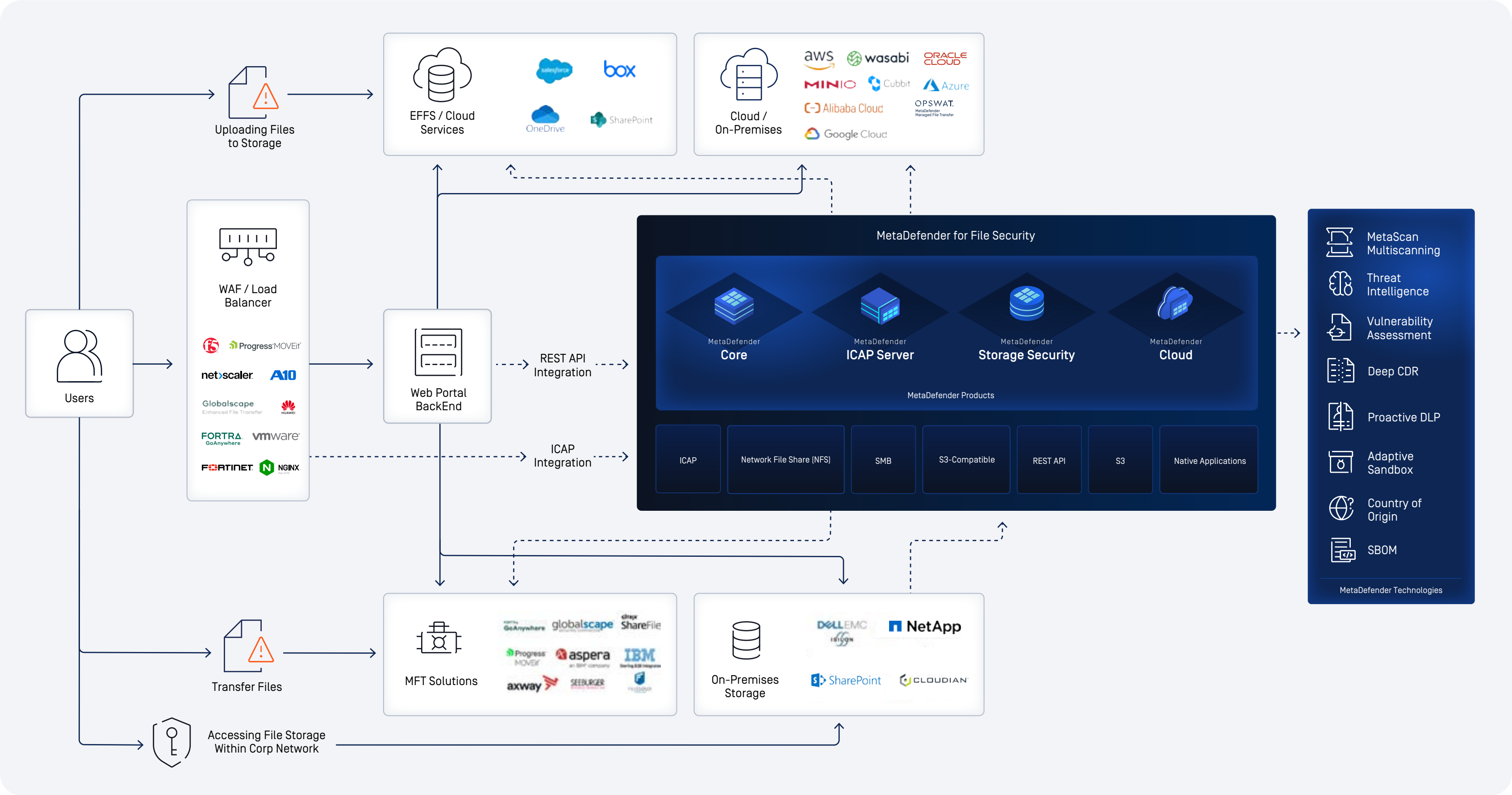
SOLUTION

MetaDefender for File Security

Integrate Advanced Security Tools with Your Existing Infrastructure

OPSWAT MetaDefender for File Security enables global financial institutions to exceed their security objectives, empowering them to better safeguard their critical infrastructure and sensitive financial data against evolving threats.

Through comprehensive, multi-layered protection, these institutions leverage advanced threat prevention capabilities while preserving operational efficiency and meeting stringent regulatory requirements. The integrated MetaDefender portfolio delivers seamless security wherever files reside across diverse technological ecosystems:



Users

Uploading Files to Storage

EFFS / Cloud Services

Cloud / On-Premises

WAF / Load Balancer

Web Portal BackEnd

REST API Integration

ICAP Integration

MetaDefender for File Security

MetaDefender Core

MetaDefender ICAP Server

MetaDefender Storage Security

MetaDefender Cloud

MetaDefender Products

ICAP

Network File Share (NFS)

SMB

S3-Compatible

REST API

S3

Native Applications

MetaScan Multiscanning

Threat Intelligence

Vulnerability Assessment

Deep CDR

Proactive DLP

Adaptive Sandbox

Country of Origin

SBOM

MetaDefender Technologies

Transfer Files

MFT Solutions

On-Premises Storage

Accessing File Storage Within Corp Network

MetaDefender Core integrates advanced malware prevention and detection capabilities into your existing IT solutions and infrastructure to handle common attack vectors by securing web portals from malicious file attacks, augmenting cybersecurity products, and developing malware analysis systems that adhere to company-specific policies.

MetaDefender ICAP Server integrates into your existing network devices to provide an additional layer of security for network traffic. Through the lightweight ICAP (internet content adaptation protocol), MetaDefender ICAP Server can analyze files for potentially malicious content and sensitive data before they reach end users, helping organizations meet security and compliance requirements.

MetaDefender Storage Security secures your files and data at rest across any storage environment—on-premises, hybrid, or cloud—preventing breaches, downtime, and compliance violations with comprehensive, multi-layered protection.

MetaDefender Cloud - A comprehensive cybersecurity platform providing detection, prevention, and threat intelligence technologies to secure organizations against file-borne malware. Easy to use and integrate, the MetaDefender Cloud API leverages advanced threat detection and prevention technologies.

05

Use Cases and Proven Deployments

Theory becomes practice when financial institutions successfully implement comprehensive file security solutions that protect their operations without disrupting business continuity. The following use cases demonstrate how leading organizations have addressed their unique challenges with MetaDefender for File Security solutions while achieving measurable improvements in security posture and regulatory compliance.

USE CASE #1

Overcoming the Challenge of Processing Thousands of Files Daily

Customer: Liechtensteinische Landesbank AG (LLB)

Region: Vaduz, Liechtenstein

Employees: 1,200+ employees

The client needed a solution that could support both the REST interface and ICAP, as well as ingest vast quantities of files, sanitize them thoroughly, then send them through quickly and seamlessly with the assurance that files were malware-free.

Challenges

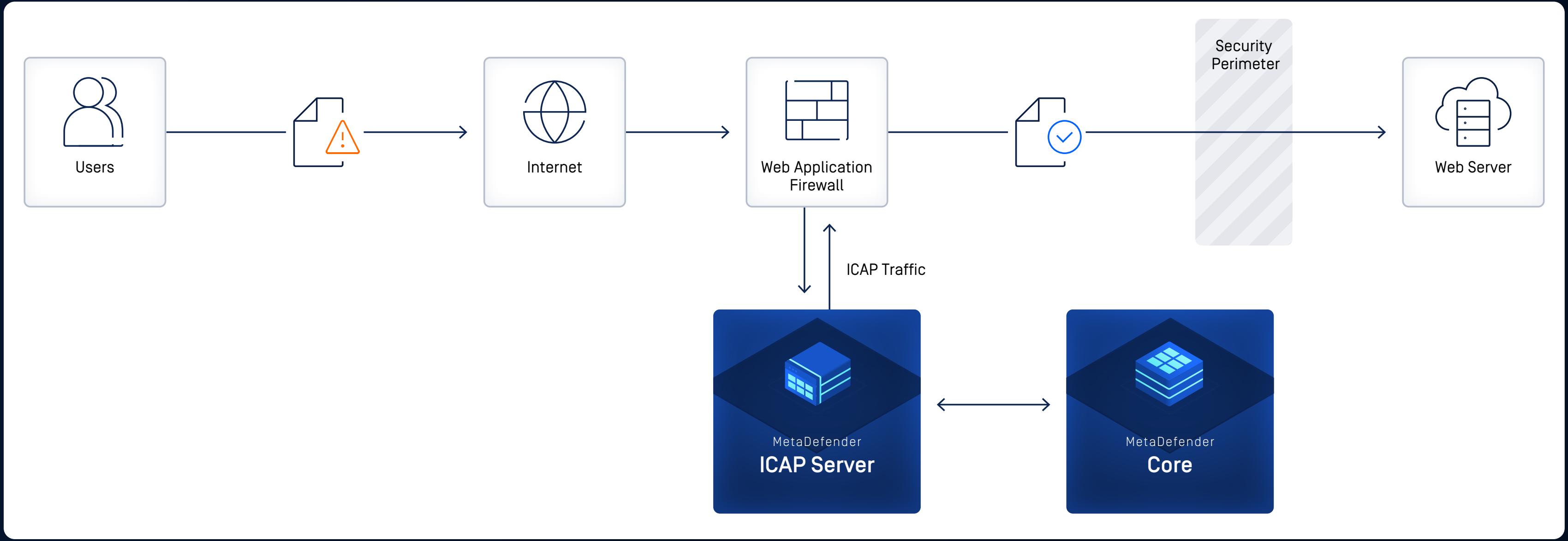
- Designing new channels for customer and prospect interactions in 2023 required a reimagined file-upload security solution
- Processing thousands of daily queries from customers and corporate clients created significant concerns about managing email load and mitigating malware risks hidden in attachments
- Accommodating the rising complexity of the client's infrastructure became a priority for the bank's system development
- Finding scalable solutions was essential for supporting the bank's growth as the organization expands and compliance regulations continue to evolve

Outcomes

- OPSWAT technologies completely streamlined the bank's file-uploading process while ensuring the security of LLB's network by totally sanitizing inbound files
- OPSWAT was the only provider that supported both the REST interface and ICAP
- MetaDefender Core and MetaDefender ICAP Server are integrated easily with the client's existing system and with MetaDefender ICAP Server, the workflow is much more streamlined with OPSWAT providing a single interface for all file sanitation
- After initial testing, multiple antivirus engines were deployed to ensure the safe delivery of files
- Compliance issues have been mitigated with a higher level of security confidence

USE CASE #1

Overcoming the Challenge of Processing Thousands of Files Daily



USE CASE #2

Securing Unverified Uploads and Protecting Client File Transfers

Customer: One of the largest financial institutions in Taiwan

Region: Global (Taiwan Headquarters)

Employees: 6,000+ employees

The bank faced multiple cybersecurity challenges, particularly in managing file transfers and handling incoming files from clients. OPSWAT's solutions offered a unique combination of secure, automated file handling with advanced threat detection, enabling the bank to tackle both internal and external data risks. The native integration of MetaDefender Core and MetaDefender Managed File Transfer (MFT) provided a seamless way to scan files at every point of transfer, ensuring end-to-end security.

Challenges

- Increased risk from unverified client uploads and reliance on USB devices for internal transfers exposed the bank to malware threats and data leakage
- Lack of automated file handling processes created inefficiencies and increased the risk of manual handling errors
- Needed centralized file management to maintain security and compliance during high-volume file submissions, especially for regulatory audits and relief programs

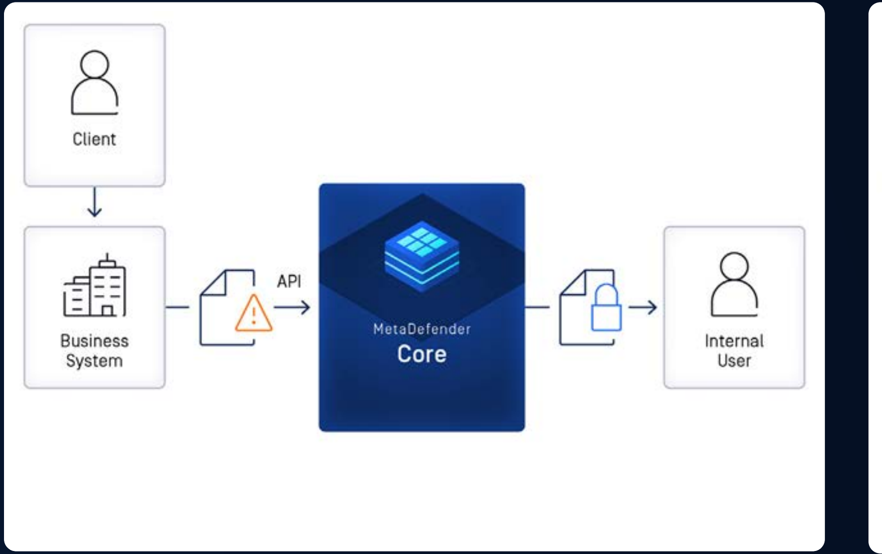
Solutions

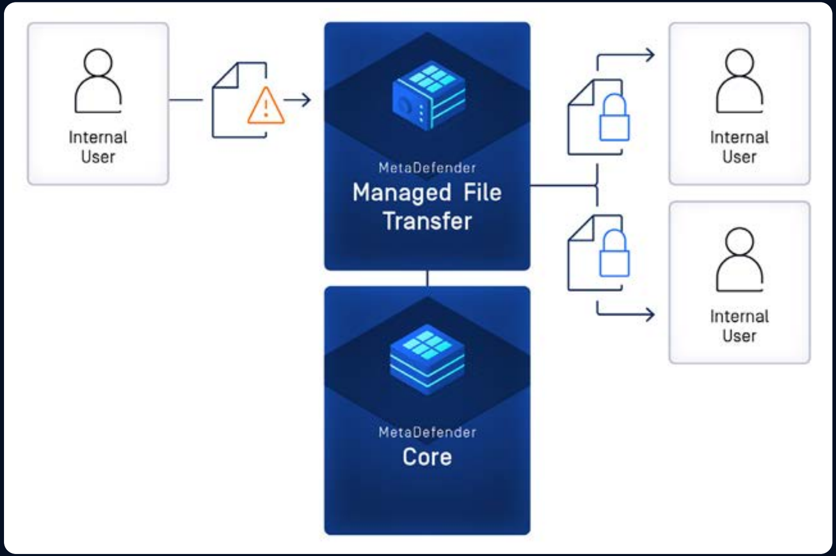
The bank implemented OPSWAT's MetaDefender Managed File Transfer and MetaDefender Core, which enabled them to:

- Securely scan and sanitize all incoming files through MetaScan Multiscanning and Deep CDR technologies, protecting against malware threats
- Replace USB-based file transfers with an automated MFT platform, improving efficiency and reducing data leakage risks
- Streamline compliance with detailed audit logs, encryption, and role-based access controls, enhancing data protection and audit readiness

USE CASE #2

Securing Unverified Uploads and Protecting Client File Transfers





USE CASE #3

Transcend Single-Engine Approach with OPSWAT's Advancing Threat Detection and Threat Analysis

Customer: Large financial institution in Europe

Region: Global (Europe Headquarters)

Employees: Thousands of employees

This European financial institution faced increasing targeted attacks and growing regulatory scrutiny. Its traditional single-engine antivirus approach was no longer sufficient against modern threats. The bank also needed to optimize the handling of flagged files to enhance efficiency and security. To address these challenges, OPSWAT deployed a robust combination of multi-scanning and behavioral analytics to enable fast, accurate triage of potentially malicious files.

Challenges

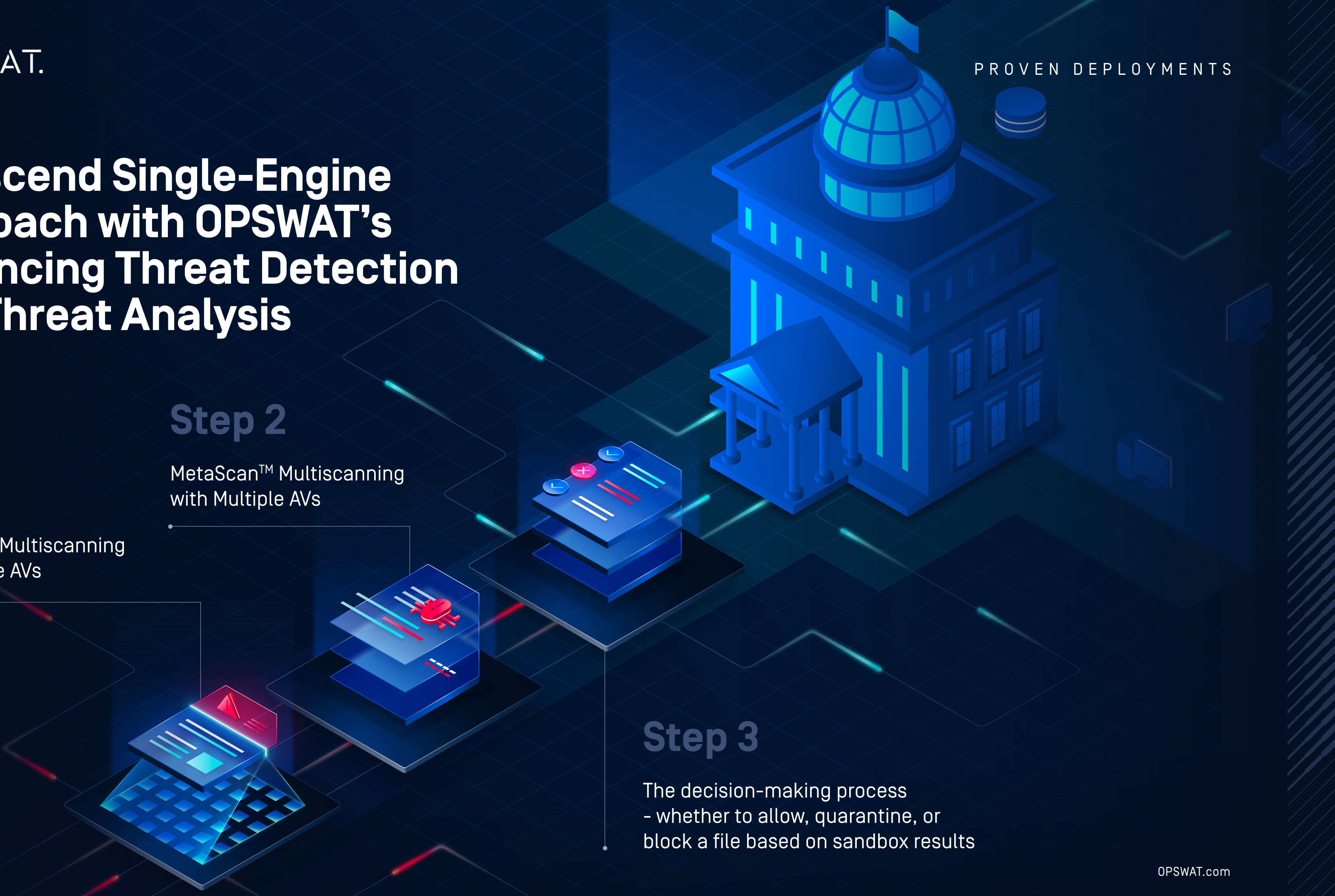
- Rising volume of targeted cyberattacks and increased regulatory pressure
- Limited detection capabilities of single-engine antivirus
- Operational inefficiencies caused by poor visibility into flagged files

Solutions

- Deployed MetaScan™ Multiscanning with multiple antivirus engines for improved detection accuracy
- Integrated Adaptive Sandbox for dynamic and static analysis within an air-gapped environment
- Streamlined File Triage through behavioral analysis and efficient threat investigation

USE CASE #3

Transcend Single-Engine Approach with OPSWAT's Advancing Threat Detection and Threat Analysis



Step 1

MetaScan™ Multiscanning
with Multiple AVs

Step 2

MetaScan™ Multiscanning
with Multiple AVs

Step 3

The decision-making process
- whether to allow, quarantine, or
block a file based on sandbox results

USE CASE #4

Securing AWS S3 with Minimal Workflow Disruption

Customer: A Major Financial Institution in The Middle East

Region: Global (The Middle East Headquarters)

Employees: 10K+ Employees

As a major player in the global financial market, the institution needed to ensure their files were untouchable. Any successful malware infiltration could have devastating consequences – for both the organization and its clients. OPSWAT's MetaDefender Storage Security™ solution combined with the MetaDefender ICAP Server™, provides comprehensive solution by continuously checking uploaded files to AWS S3 storage for malware in every 5 seconds with MetaScan™ Multiscanning and Deep CDR™ technology.

By providing continuous, automated file sanitization, OPSWAT empowered the institution to confidently manage their critical data in the cloud.

Challenges

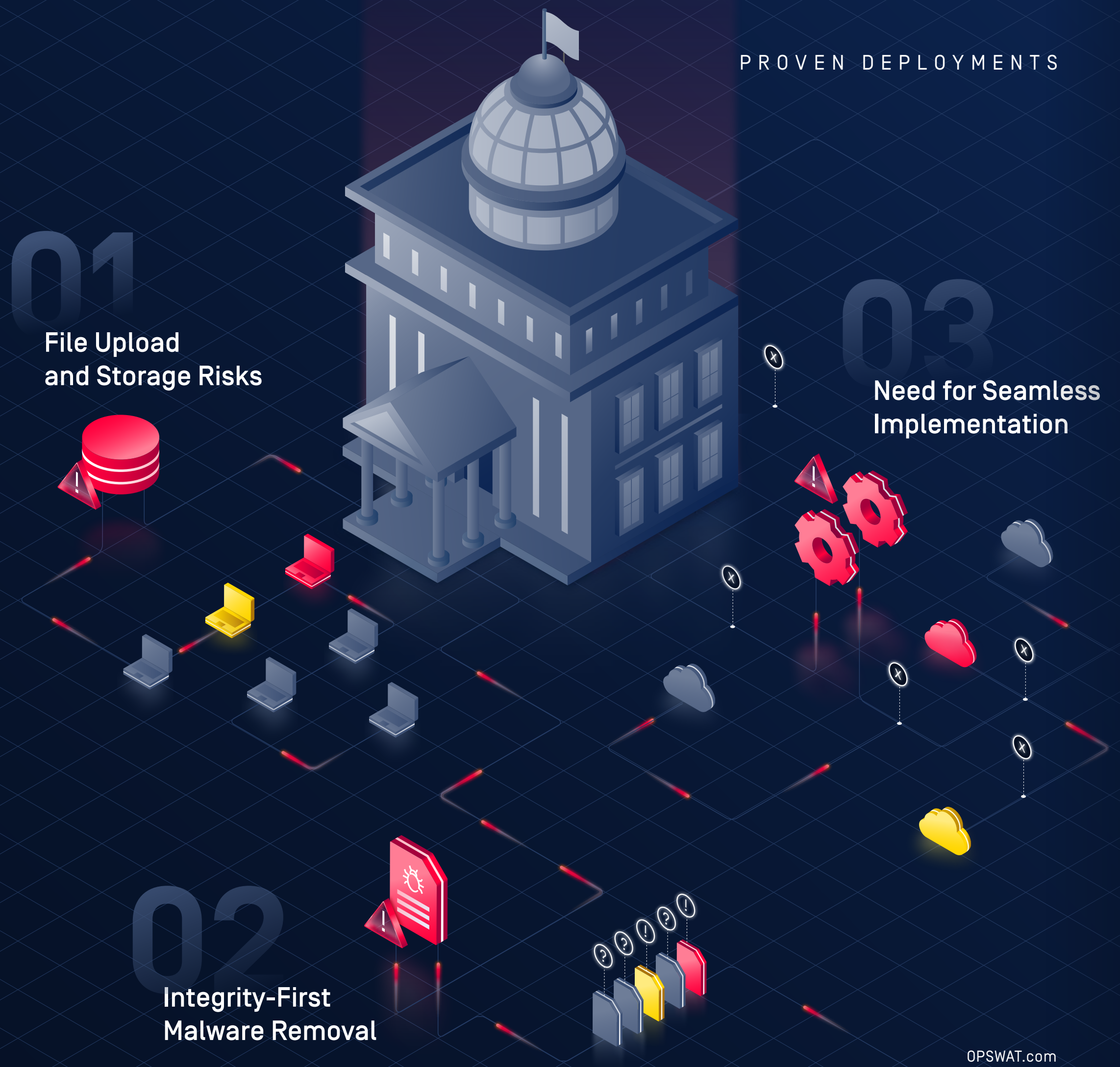
- File Upload and Storage Risks: Their file upload and object storage processes were vulnerable to malware threats, risking the exposure of financial data, client information, and transaction records
- Integrity-First Malware Removal: Malware removal was crucial, but any alteration or corruption of files could lead to data loss, operational disruptions, and reputational damage, especially in a highly regulated environment where fines and regulatory issues were a concern
- Need for Seamless Implementation: Security measures had to be implemented without disrupting their AWS S3 setup, as any interruptions could delay operations and impact on business-critical functions

Solutions

- MetaDefender Storage Security solution provides real-time, on-demand threat detection for AWS S3 storage, securing sensitive data without disrupting the existing setup
- MetaDefender ICAP Server applies a zero-trust approach to file handling, significantly reducing malware risks and ensuring data integrity through advanced threat prevention
- Deep CDR technology automatically sanitizes files, quarantining risky ones and ensuring compliance with regulatory standards while maintaining operational efficiency

USE CASE #4

Securing AWS S3 with Minimal Workflow Disruption



01 File Upload and Storage Risks

02 Integrity-First Malware Removal

03 Need for Seamless Implementation

USE CASE #5

Regulatory-Compliant File Security for Azure Digital Transformation

Customer: Swiss Re

Region: Global (Switzerland Headquarters)

Employees: 14,000+ Employees

Facing security challenges stemming from evolving financial regulations and the looming risk of malware compromising their web applications, Swiss Re teamed up with OPSWAT. The deployment of OPSWAT MetaDefender enabled Swiss Re to effectively combat these issues. OPSWAT technology is used to scan and validate incoming files using Meta Multiscanning technology, ensuring that the files are free from malware.

This collaboration not only trimmed response times and bolstered advanced malware detection but also provided scalable web application security, directly addressing Swiss Re's unique challenges and fortifying its path in the digital transformation journey.

Challenges

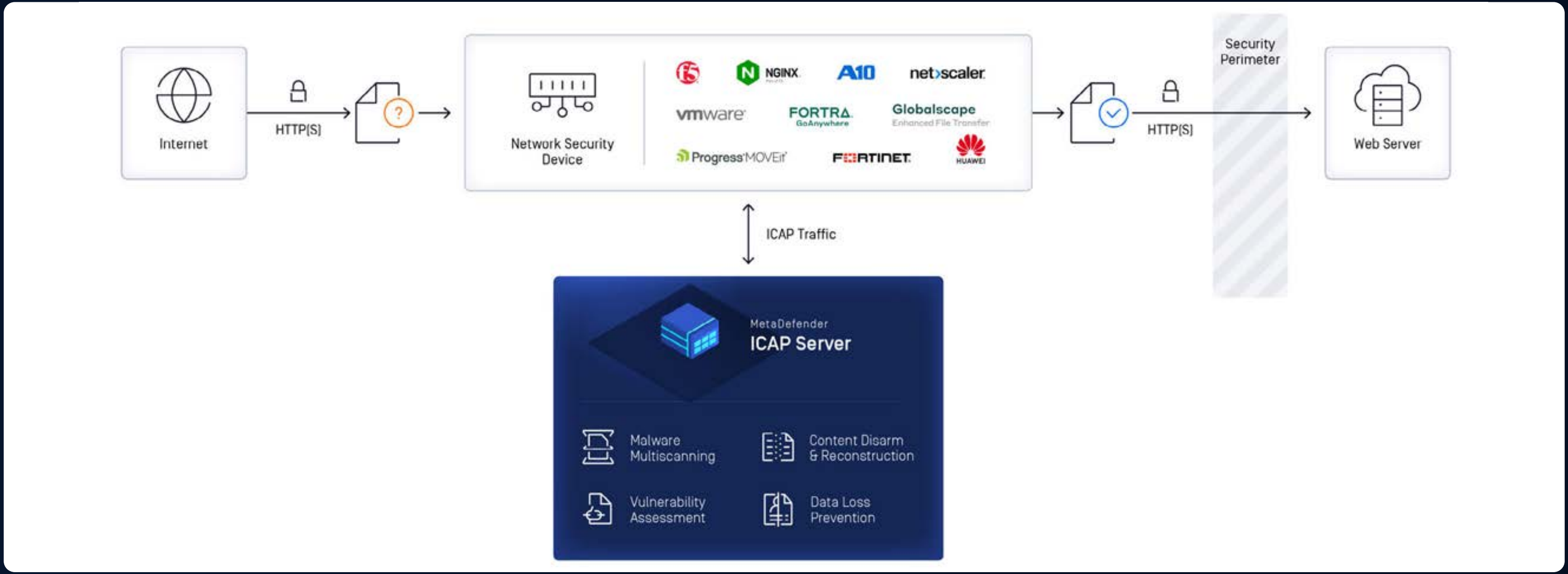
- Risk of infected file uploads to their web portals, risking the security and compliance of their network
- Compliance with FINMA and GDPR requires the utmost security for client personal data
- Difficulty in finding a solution that seamlessly integrates with their micro-services architecture
- Compatibility with their micro-services architecture, seeking a solution adaptable with their Azure/Kubernetes environment

Solutions

- Enabling scanning files at the network edge, ensuring security without compromising workflow or availability
- OPSWAT MetaDefender technologies help the client meet regulatory requirements, protecting web applications from malicious uploads
- MetaDefender ICAP Server easily integrates with and secures containerized deployments, aligning with Swiss Re's current and future roadmap
- MetaDefender ICAP Server provided flexibility for future integration points, offering a unified and user-friendly security experience

USE CASE #5

Regulatory-Compliant File Security for Azure Digital Transformation



06

Building Resilient File Security for the Future

The financial services landscape continues to evolve at an unprecedented pace, driven by digital transformation, regulatory changes, and increasingly sophisticated threat actors. In this environment, robust file security isn't just a technical requirement - it's a strategic imperative that enables trust, ensures compliance, and protects the foundation of your institution's operations.

The organizations that will thrive in tomorrow's financial ecosystem are those that recognize file security as a critical enabler of business success, not merely a compliance checkbox. By implementing comprehensive, multi-layered file protection strategies today, you're not just defending against current threats - you're building the resilient foundation necessary to adapt to whatever challenges emerge next.

The question isn't whether your institution can afford to invest in advanced file security. The question is whether you can afford not to. Your customers' trust, your regulatory standing, and your competitive advantage all depend on the decisions you make today about protecting the files that power your business.

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

Talk to one of our experts today.

Visit us at:
opswat.com/get-started
sales@opswat.com

Since 2002, 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 1,800 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