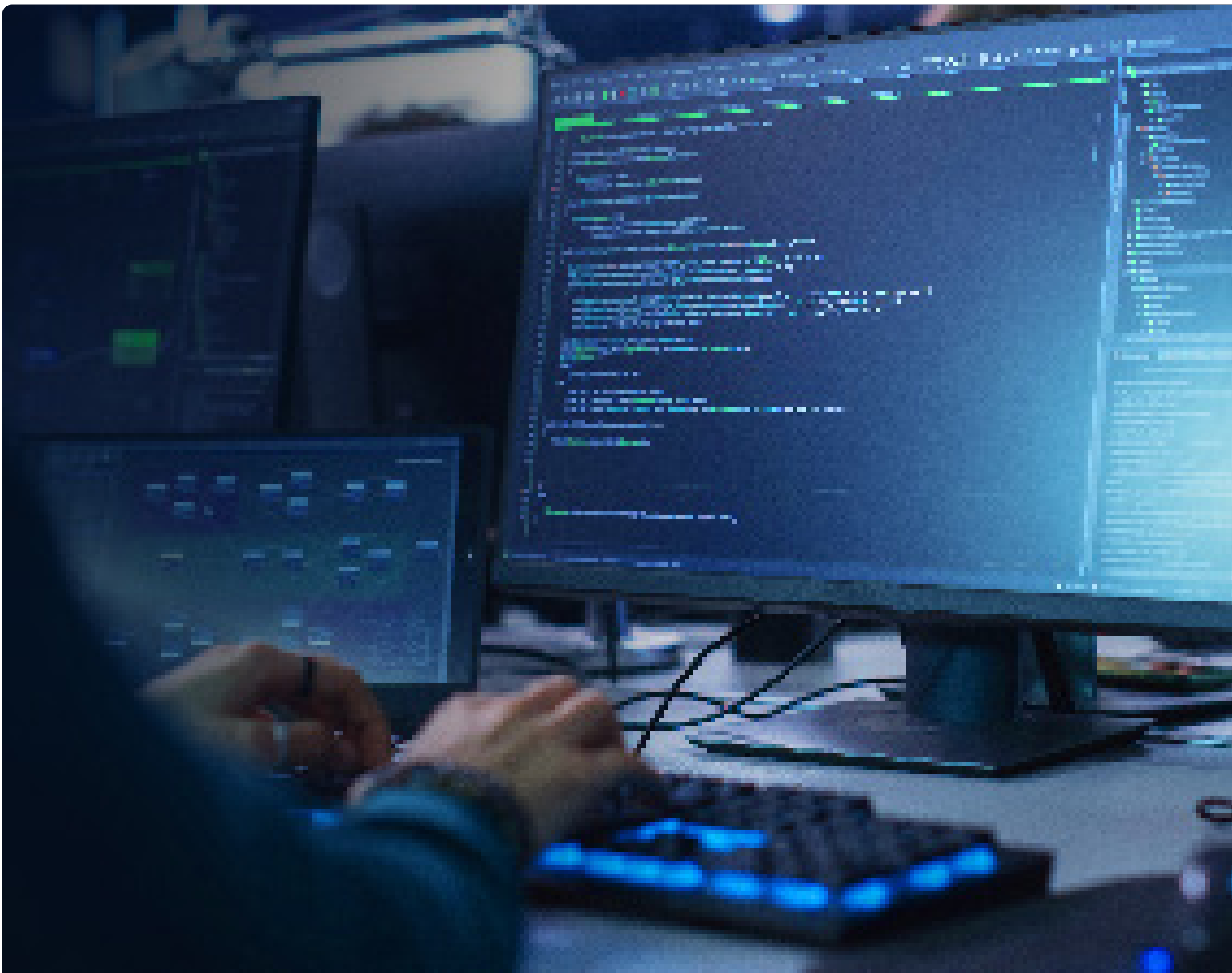
OPSWAT.

WHITEPAPER

How to Block Malicious File Uploads



Introduction

File uploads are necessary for employee productivity and for some websites and web applications to function, but they can provide an attack vector for cybercriminals. By concealing advanced threats that exploit vulnerabilities within common file types, attackers can compromise an end user's device or an entire system.

This whitepaper will outline the best methods for preventing malicious file uploads while still allowing legitimate users to upload files to organizations' systems.

Table of Contents

01 Challenges in File Upload Security

02 How Can Organizations Protect Themselves?

03 OPSWAT Can Help

01

Challenges in File Upload Security

To keep their businesses functioning, organizations must share files with their employees, partners, and consumers. File uploads are essential for user productivity, collaboration, and business services. As various departments handle sensitive data, it becomes increasingly critical to implement measures to ensure the security of file uploads. Unrestricted uploaded files can create an attack vector for malicious actors.

Nowadays, users no longer need to install a rogue application to get infected – that can happen by opening what appears to be a resume, an invoice, a courier receipt, or any other type of productivity file. Attackers can exploit poor input validation or even vulnerabilities in server-side processing solutions. They can easily gain control of the environment by either retrieving access keys (e.g., server-side request forgery (SSRF) attack using AWS EC2 metadata endpoint) or remote code execution (RCE) based on a vulnerability.

File-Borne Malware is on the Rise

Companies are becoming more concerned about file-borne malware. In our Web Application Security report[1], **76% of our survey participants expressed an increase in concern about file-borne malware** as companies shift away from on-premises and private clouds over the past year. In fact, 2024 alone saw over **48 million new instances of malware, adding to a growing total malware count surpassing 1.39 billion,** with Windows as the leading targeted operating system[2]. Based on this observation, it is essential for organizations to audit and analyze any incoming files, even if they appear to be from trusted and reliable sources.

The file types most frequently uploaded and shared in office settings are:

- Documents such as Microsoft Word (DOCX), PDF files, and spreadsheets (XLSX).
- Presentations such as PPTX.
- Images such as JPEG, PNG, TIFF, etc.
- Text files such as plain text (TXT) and rich text format (RTF) documents.
- Compressed files like ZIP and RAR archives.

Many everyday activities rely on file types that may seem harmless at first glance. However, attackers can exploit advanced features within these file formats, like macros in documents.. Clicking these macros can execute malicious payloads and compromise a system's security, leading to financial loss, reputational damage, and other unwanted consequences.

For instance, **in a DarkGate malware campaign detected in mid-January 2024, attackers exploited a recently fixed security vulnerability in Windows by utilizing deceptive software installers**[3]. Throughout the campaign, individuals were lured with PDFs containing Google DDM (DoubleClick Digital Marketing) open redirects, redirecting unsuspecting users to compromised websites hosting the Microsoft Windows SmartScreen bypass CVE-2024-21412, which ultimately led to malicious Microsoft (.MSI) installers.

These types of attacks do not activate on their own; attackers rely on social engineering tactics to lure users into triggering them by accident. Some PDFs may even contain keyloggers that perform malicious actions[4]. Images can carry hidden files using a still-widely used tactic called steganography — embedding malicious payloads within seemingly benign files like office documents[5]. Attackers can also use "spoofed" files, using false file extensions to evade anti-malware security measures.

To ban file uploads altogether would be impractical. It is therefore necessary to make file uploading and importing more secure for businesses to function efficiently.





02

How Can Organizations Protect Themselves?

Every organization has various procedures and security requirements. When developing a strategy to keep productivity file uploads secure, it's critical to evaluate your specific situation and use case.

1 **Start by Asking the Right Questions**

- How many restrictions can you add without impacting productivity?
- How much can you rely on user training? How confident are you that users will use everything they learn during security training?
- How are you validating incoming files? Are you doing any pre-processing before making these files available? If so, how do you ensure malicious actors won't try to exploit the processing service?
- How confident are you that a simulated sandbox environment can accurately mimic your live environment?

---

2 **Consider Your Use Case**

- When and why do users need to upload files on your portal?
- What file types will your organization mostly use or receive?
- What are the risks of allowing those files to enter your organization?

---

3 **If You Are Receiving or Sharing Documents**

- Is it absolutely necessary to allow PDFs with embedded JavaScript?
- Can you trust a document that contains hyperlinks, macros, OLE objects, or ActiveX controls?
- How do you know if an image is authentic and not produced by an attacker?

Choosing to limit any file containing scripts or macros from entering an organization is one thing; enforcing the policy is another, as it is difficult to determine exactly what a file contains without opening it.

Therefore, further steps are necessary to defend against malicious files disguised as common productivity files.

Best Practices

Here are our recommended approaches and best practices to ensure that no infected, malicious, or otherwise compromised files are uploaded into your system.

Limit 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.

Check Files for Vulnerabilities

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

Verify Actual File Types

Malicious files are often disguised as other file types. For instance, malicious actors have embedded malware into unassuming. CHM files, commonly found in help documents saved in HTML[6]. To prevent malicious executables or other spoofed files from entering a system, it is essential to identify and block files with incorrect extensions.

Scan All Files for Malware

To minimize risks, all files should be scanned for malware. The workflow should be clear and simple: any uploaded file should be analyzed for known malware, and the file shouldn't be made available to end users until the analysis is complete. It's best to scan 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.

Authenticate Users

Implementing user authentication is essential for enhancing security during file uploads. However, user authentication alone does not guarantee the security integrity of a user's device.

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 to prevent unauthorized file types.

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 make sure that files contain no hidden threats, it is best practice to sanitize files by removing any potentially malicious embedded objects.

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.

Randomize File Names

Randomly alter uploaded file names to prevent attackers from accessing those files by name after they are uploaded. This can be accomplished by making sure the sanitized file names contain random identifiers (e.g. the analysis data_id).

Use Simple Error Messages

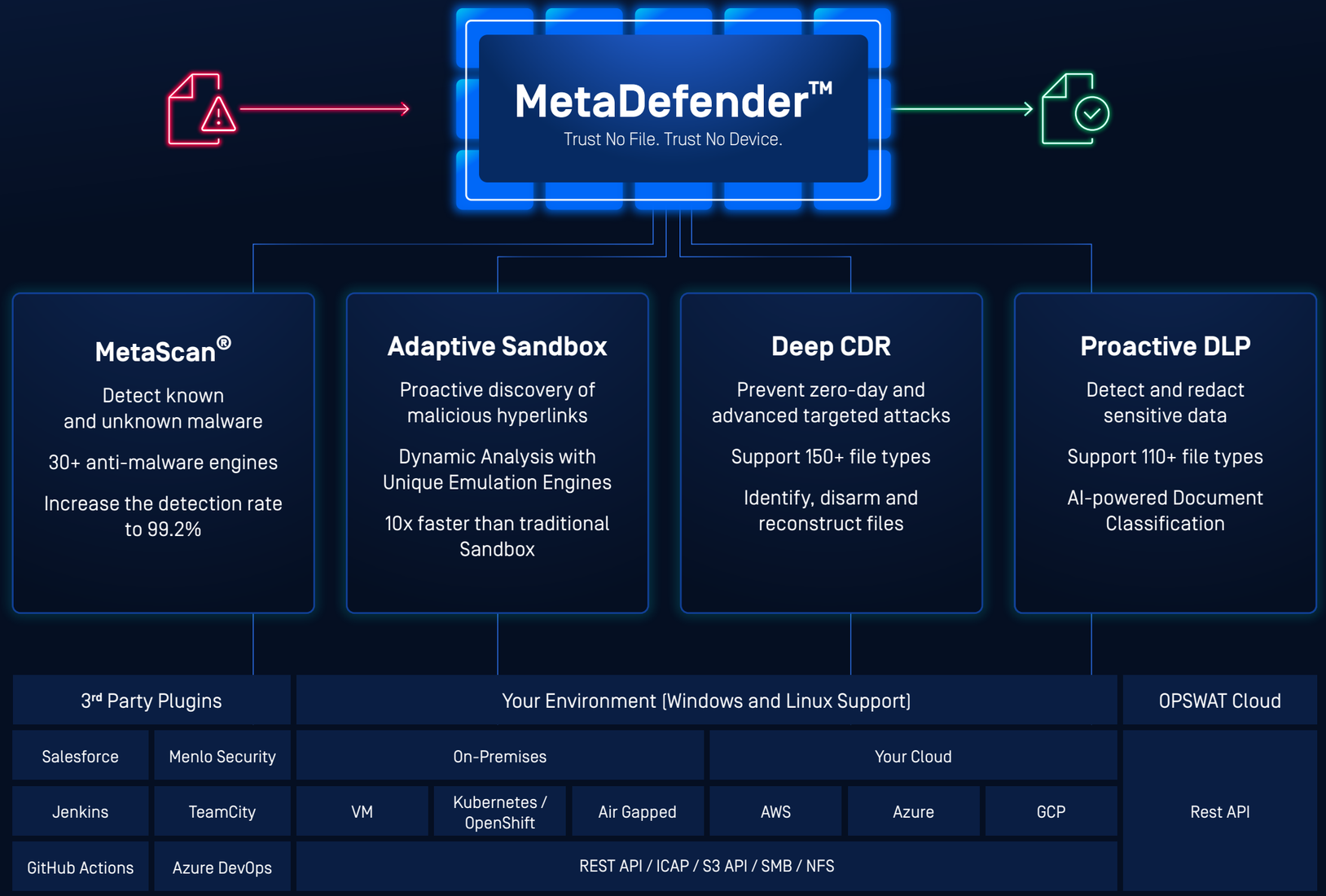
When displaying file upload errors, do not include directory paths, server configuration settings, or other information that attackers could potentially use to gain further entry into your systems.

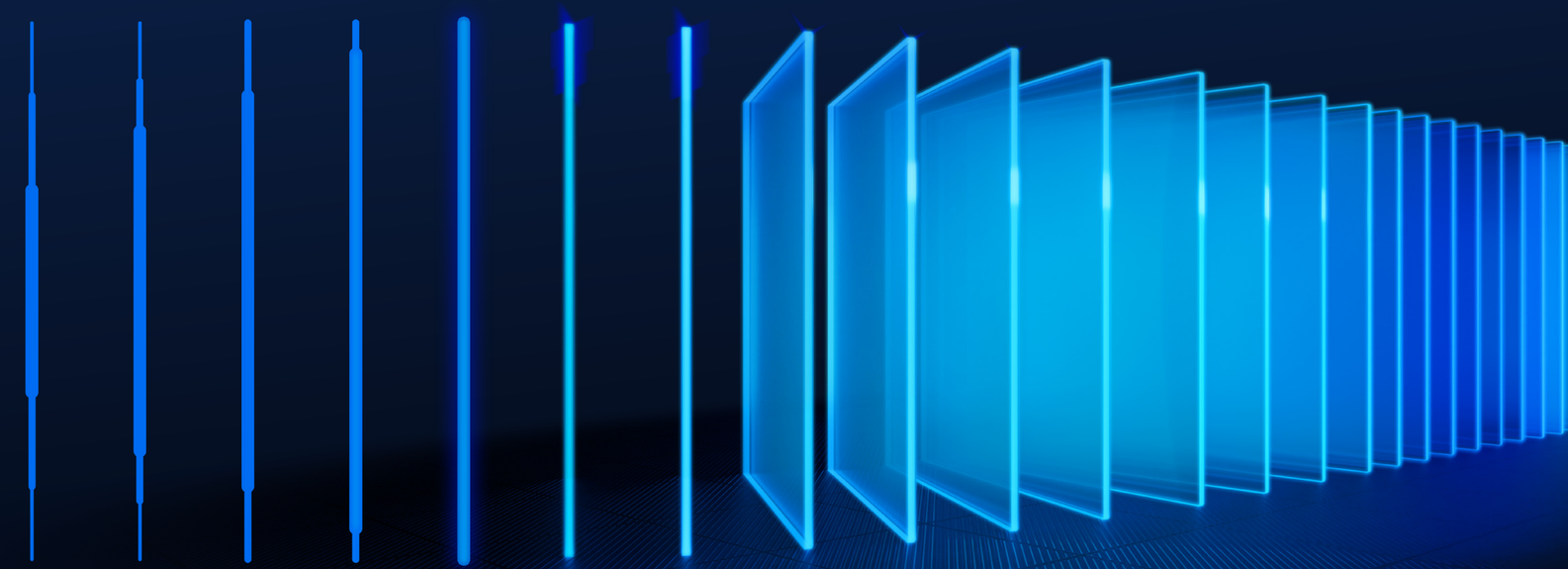
03

OPSWAT Can Help

MetaDefender for File Security protects organizations from file-borne malware and zero-day attacks, securing file uploads, downloads, transfers, sharing, and storage. OPSWAT MetaDefender technologies integrate multiple layers of defense, including advanced threat detection and prevention into your existing IT solutions and web applications. We help protect your files wherever they are—in transit or at rest—to help you meet your security and compliance requirements.

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





The MetaDefender Platform utilizes eight powerful technologies to provide comprehensive protection from malicious file uploads.

Verify File Types

OPSWAT File Type Verification 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.

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.

Sanitize Files

OPSWAT Deep CDR (Content Disarm and Reconstruction) prevents potentially undetected file-borne threats by sanitizing and regenerating safe-to-use files. With support for over 150 common file types, hundreds of file reconstruction options are available.

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.

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

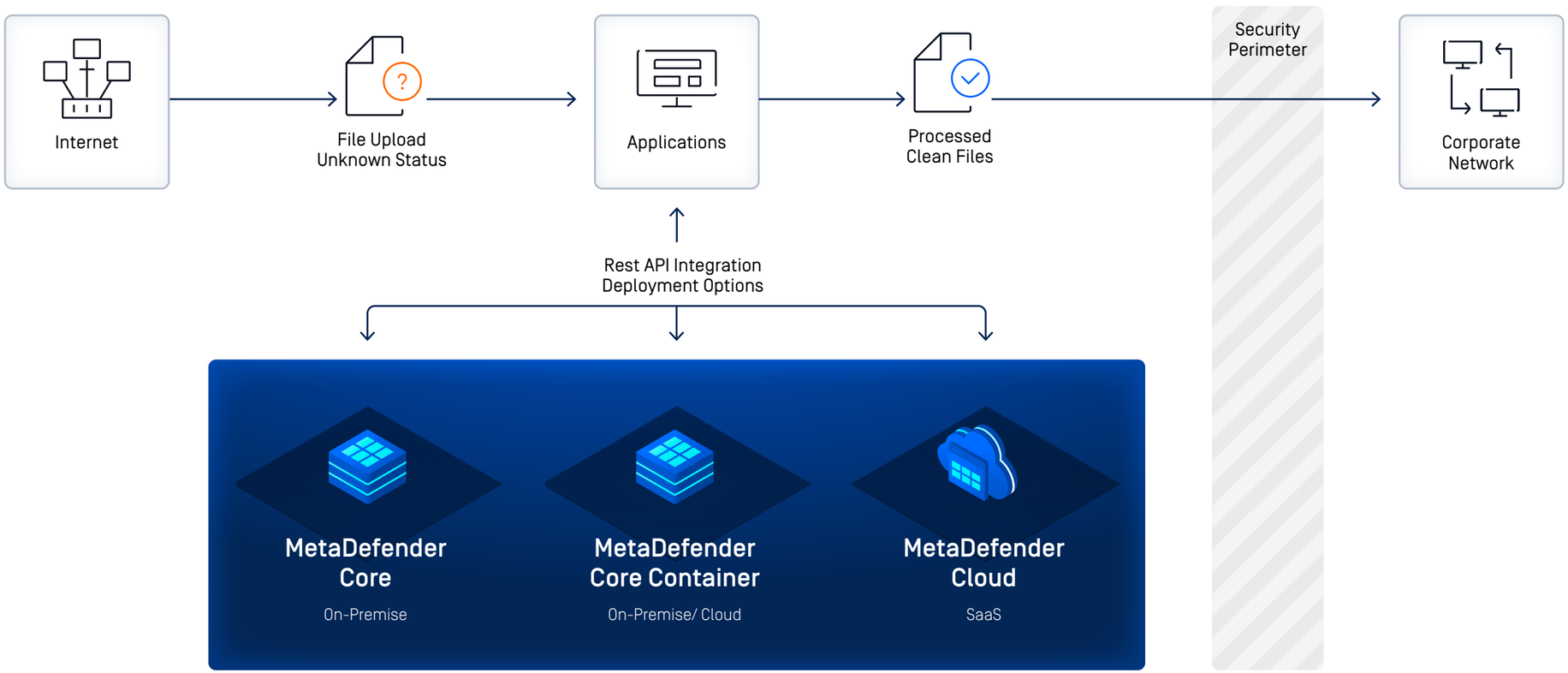
OPSWAT Adaptive Sandbox is a complete set of malware analysis technologies including, threat agnostic analysis of files and URLs, emulation of all targeted applications, a focus on Indicator-of-Compromise (IOC) extraction, and Rapid Dynamic Analysis engine for targeted attack detection.

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.

Integration and Deployment

OPSWAT offers a rich set of REST APIs that system administrators and developers can use to integrate dynamic security features into their security architecture. These APIs can integrate with existing security features on file upload servers to completely block malicious file upload attacks.



MetaDefender Platform offers a REST API integration for:

Multiscanning with Metascan

Leverage 30+ anti-malware engines to detect nearly 100% of known threats.

Deep CDR

Disarm active embedded threats and reconstruct every file to prevent zero-day and advanced evasive malware.

Proactive DLP

Detect and block sensitive and confidential file content to prevent data leakage in files and emails.

Adaptive Sandbox

Detonate and analyze malware in a controlled environment.

File-based Vulnerability Assessment

Scan and analyze binaries and installers to detect vulnerabilities before exposure.

Software Bill of Materials [SBOM]

Identify known vulnerabilities, validate licenses, and generate component inventory for container images, open-source software (OSS), and third-party dependencies.

Reputation

Matches file hashes against a database of known good and bad files and leverages advanced analyses to remediate false positives faster.

Threat Intelligence (cloud)

Provide enriched intelligence on threats on billions of hashes, IPs and domains.

Country of Origin

Identify file origins and manage access to restricted locations and vendors instantly for regulatory compliance and data protection.

MetaDefender Features

Environment

- Support for:
  - A. Windows 10, 11 IoT (22H2) only for End-User systems (e.g. Kiosk deployments)
  - B. Windows Server 2016, 2019, 2022
  - C. Linux
    - a.CentOS 7
    - b.RedHat Enterprise 7, 8, 9
    - c.Debian 9, 11
    - d.Ubuntu 18.04, 20.04
- Cloud deployments: AWS, Azure, Google Cloud Platform, OpenShift
- Container Support: Docker, Kubernetes
- Cloud integration available via MetaDefender.com

Integration

- REST APIs for automated integration into your workflow (HTTP/S)
- Internet content adaptation protocol (ICAP) for plug-and-play integration to any network security device
- AWS: Prevent malicious file uploads to web applications deployed on AWS
- Containers: Automated deployment and operability for advanced threat prevention

Special Features

- Sanitize specialized productivity documents (JTD, HWP, XML)
- Notification of vulnerabilities within applications before installing them
- Protection from spoofing attacks and archive bombs
- Optimized archive scanning and sanitization

More Information

Sample reports are available:

- Weekly multi-scanning efficiency for top threats statistics: https://www.MetaDefender.com/reports/statistics
- Data sanitization reports: https://www.MetaDefender.com/reports/sanitization
- 2023 Threat Intelligence Trends: Malware Analysis Survey Insights: https://www.opswat.com/resources/reports/2023-threat-intelligence-trends

Conclusion

File uploads are a major potential threat vector for any organization. However, there are concrete steps that organizations can take to protect themselves.

Key Takeaways

The everyday use of file types like documents, PDFs, and images can pose security risks due to exploitable features such as macros, keyloggers, and embedded archives. Attackers leverage these vulnerabilities to compromise systems, leading to financial loss and reputational damage.

Despite these risks, banning file uploads entirely would be impractical. Instead, businesses must prioritize secure file uploading and importing practices to maintain operational efficiency while minimizing security threats.

Organizations can protect themselves by tailoring their security strategies to their unique workflows and needs. This starts with asking pertinent questions while considering their specific file upload use cases.

MetaDefender for File Security protects organizations from file-borne threats and zero-day attacks that occur in file uploads, as well as 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 uploads, downloads, transfers, sharing, and storage security.



1. https://www.opswat.com/resources/reports/2023-state-of-web-application-security
2. https://portal.av-atlas.org/malware
3. https://thehackernews.com/2024/03/darkgate-malware-exploits-recently.html
4. https://threatresearch.ext.hp.com/pdf-malware-is-not-yet-dead/
5. https://cybersecuritynews.com/hackers-steganography-png-malware/
6. https://cybersecuritynews.com/kimsuky-apt-hackers-dropping-malware-via-cms-files/

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.

©2024 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.