File Upload Security

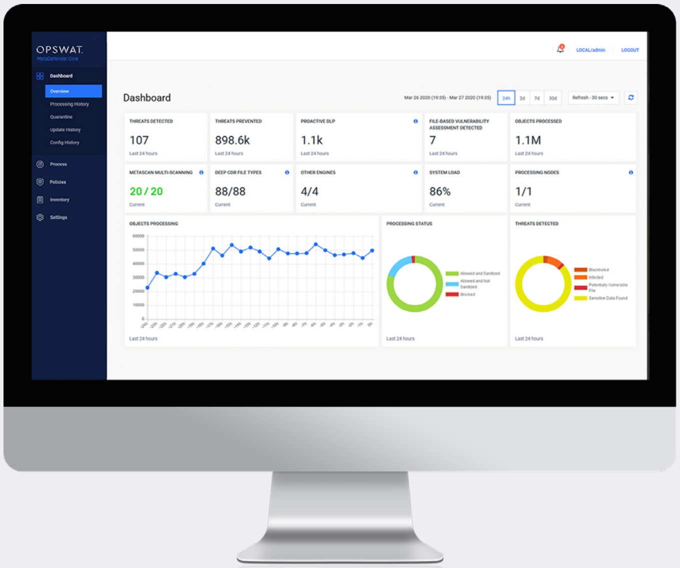
Protect Against Malicious File Uploads

Business and Technical Challenges

With malicious file uploads, attackers can compromise your servers or your entire system. This can result in leaked sensitive data from your organization or high ransom pay outs to cybercriminals. Since limiting file transfers from internal or external parties is not an option, protective measures need to be taken in order to accept incoming files. When traditional signature-based and behavior-based detection mechanisms are insufficient to prevent advanced threats and zero-day attacks, many organizations attempt to protect their systems with an inhouse manufactured set of security products. However, this is costly, time-consuming and adds a lot of overhead for maintenance and upgrades.

6 Best Practices To Prevent File Upload Vulnerabilities

- Remove possible embedded threats
- Verify file types
- Scan files with multiple anti-malware engines
- Restrict specific file extensions
- Check for vulnerabilities in files
- Authenticate users



Dashboard

Mar 26 2020 (19:35) - Mar 27 2020 (19:35)

THREATS DETECTED
107
Last 24 hours

THREATS PREVENTED
898.6k
Last 24 hours

PROACTIVE DLP
1.1k
Last 24 hours

FILE-BASED VULNERABILITY ASSESSMENT DETECTED
7
Last 24 hours

OBJECTS PROCESSED
1.1M
Last 24 hours

METASCAN MULTI-SCANNING
20 / 20
Current

DEEP CDR FILE TYPES
88/88
Current

OTHER ENGINES
4/4
Current

SYSTEM LOAD
86%
Current

PROCESSING NODES
1/1
Current

Last 24 hours

Last 24 hours

Last 24 hours

The OPSWAT™ Solutions

OPSWAT is committed to preventing threats and zero-day attacks for secure data transfer across your network, applications, and customer operations. With almost two decades of experience in securing critical infrastructure systems, OPSWAT technologies integrate advanced malware protection and detection into your IT solutions and applications. MetaDefender - our advanced threat prevention solution for file uploads is used by organizations that require the highest level of security, including critical infrastructure, government agencies, and financial institutions.

Key Differentiators

1. Advanced Threat Detection and Prevention Technologies

Industry-leading cybersecurity technologies include Multiscanning and Deep Content Disarm and Reconstruction (Deep CDR) that detect and prevent both known and unknown threats.

2. Simple and flexible deployment

Fast and scalable implementation on-premises and in the cloud using REST API or any Internet Content Adaptation Protocol (ICAP) enabled product.

3. High performance and scalability

Fast scanning and reconstruction of files in milliseconds without affecting performance. Scalability to any volume with our built-in high-performance architecture and load balancing features.

4. Customizable policies

Configurable workflow and analysis rules based on user, file source, and file type.

How We Can Help

Almost 100% Known Threat Detection

OPSWAT Multiscanning technology leverages 30+ anti-malware engines, significantly improves detection of known and unknown threats, and provides the earliest protection against malware outbreaks.

Prevent Zero-Day Attacks and Advanced Malware Threats

OPSWAT Deep Content Disarm and Reconstruction (Deep CDR) technology prevents potentially undetected file-borne threats by sanitizing and reconstructing files ensuring that any possible embedded threats are neutralized while maintaining full usability with safe content.

Maximize Vulnerability Detection

Numerous organizations are exposed to attacks leveraging file vulnerabilities. Uploaded files can trigger vulnerabilities in libraries/applications. OPSWAT File-based Vulnerability Assessment technology detects vulnerabilities in installers, binary files and Internet of Things (IoT) firmware at the gateway of your network, before the file enters your organization.

Protect Sensitive and Important Information in Files

With OPSWAT Proactive Data Loss Prevention (Proactive DLP) technology you can content-check files for PII (personally identifiable information) when they are uploaded, and block or redact specific content before it reaches the end user or exits the environment.

Meet Compliance Requirements

Regulatory compliance requirements are enforced to minimize breaches and privacy violations. Meeting compliance is time consuming and can be costly—when requirements are not met. OPSWAT technologies provide compliant processes, comprehensive visibility, detailed reporting capabilities, and help meet requirements in the OWASP guidelines.

Customer Benefits

Custom security policies and workflows

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

Comprehensive protection

Mitigating risks on your critical systems and preventing threats that may have bypassed defenses.

Continuous visibility and control

A centralized UI with a real-time visual security status dashboard, providing complete visibility to your assets and immediately alerting you of potential threats.

Low total cost of ownership (TCO)

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

What We Offer

File Upload Security Assessment Service

OPSWAT Professional Services team runs a series of tests designed to uncover security holes and vulnerabilities in your organization's file upload service. We tailor the evaluation to your organization’s specific needs based on our proven methodology, then an OPSWAT technical expert will discuss various recommendations and next steps with you.

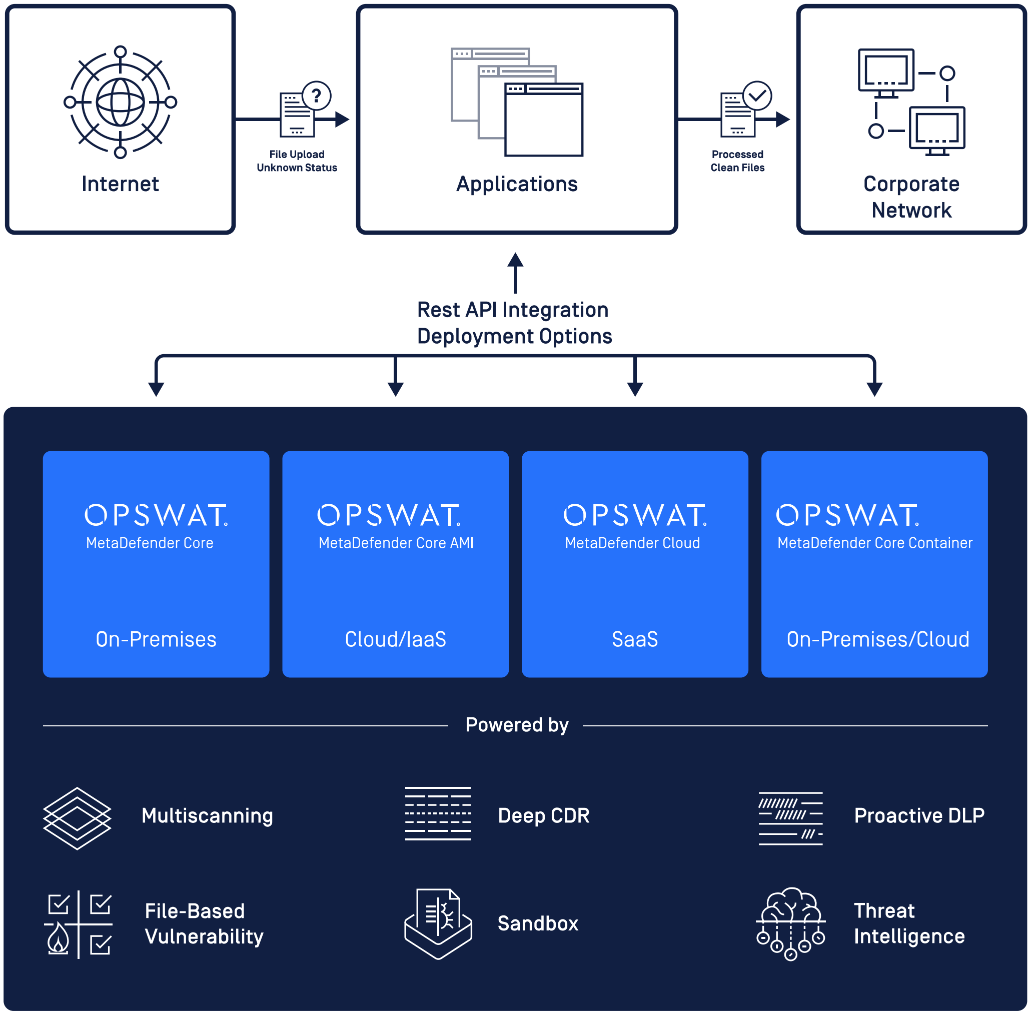
Custom Applications and Integrations Service

Have our engineers build the applications and integrations that you need to interface with your OPSWAT products. Whether it is building applications that augment our security products or integrating your existing automated workflows with our security products, we have you covered.

MetaDefender Suites for Your Organization

MetaDefender can be deployed on-premises, within your cloud infrastructure or by integration with MetaDefender Cloud. Depending on where the data lives, we offer native connectors or ability to integrate via REST API that supports a variety of deployment scenarios.

- On-Prem - For on-premises deployments with strict constraints, MetaDefender Core is often the best solution.
- SaaS - If you need MetaDefender to integrate with SaaS products, consider MetaDefender Cloud for easy scalability, 24/7 availability, and minimal overhead.
- Cloud/IaaS - If you'd like to deploy in an IaaS environment, still consider MetaDefender Cloud, but if you're sending files outside your organization, MetaDefender Core can be deployed in a cloud environment. For AWS deployments, consider MetaDefender AMI for seamless scalability that is easy to implement.



Internet

File Upload
Unknown Status

Applications

Processed
Clean Files

Corporate
Network

Rest API Integration
Deployment Options

OPSWAT.
MetaDefender Core
On-Premises

OPSWAT.
MetaDefender Core AMI
Cloud/IaaS

OPSWAT.
MetaDefender Cloud
SaaS

OPSWAT.
MetaDefender Core Container
On-Premises/Cloud

Powered by

Multiscanning

Deep CDR

Proactive DLP

File-Based
Vulnerability

Sandbox

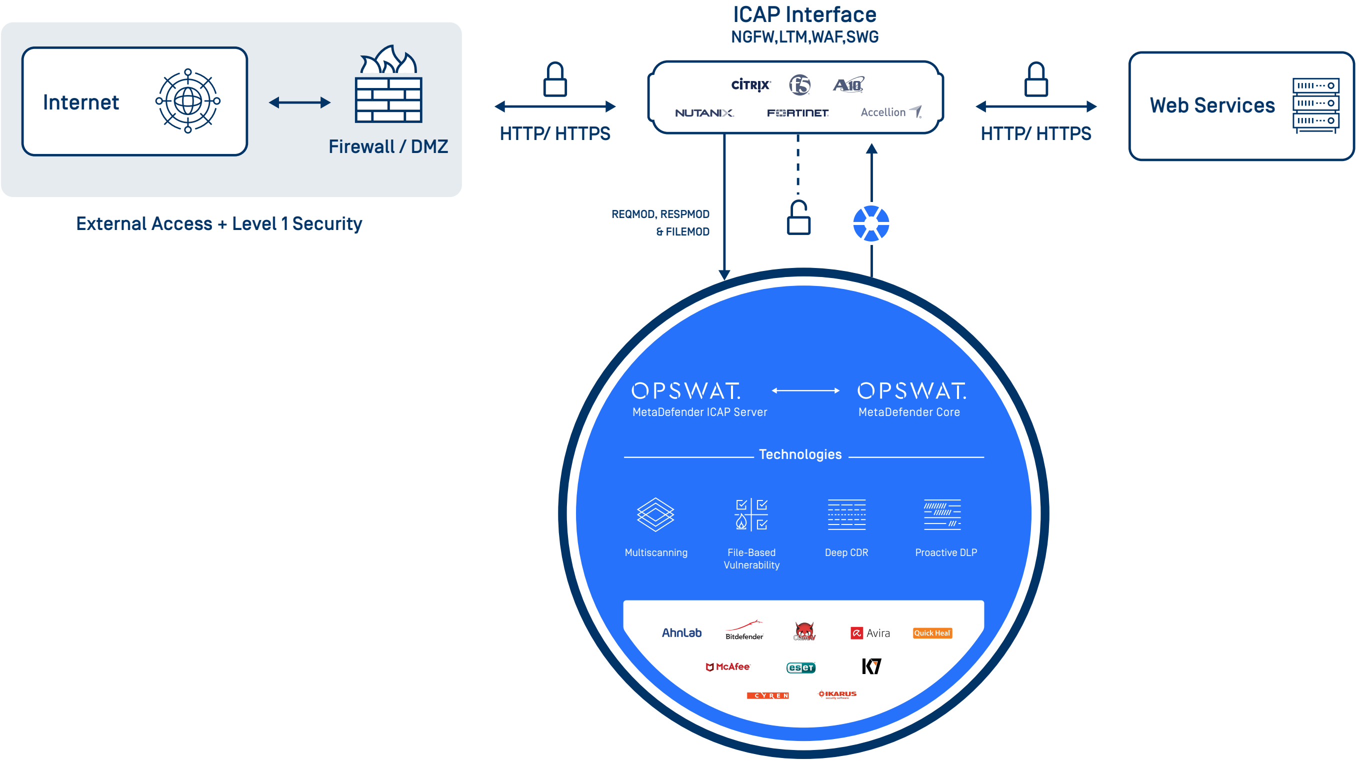
Threat
Intelligence

Internet Content Adaptation Protocol (ICAP)

One of the most popular native connector solutions is MetaDefender ICAP Server, which offers native integration to most Web Application Firewalls (WAFs) and Load Balancers (LBs), including:

- F5 Advanced WAF™
- F5 Big-IP® ASM™
- F5 Big-IP LTM™
- F5 SSL Orchestrator™
- A10 Networks Thunder® SSLi®

> "With MetaDefender Deep CDR, Upwork was able to prevent 100% of zero-day file attacks, compared to only 70% blocked by standard AV.
>
> "All files with active objects are sanitized; 75% of files are processed and ready in less than a second, and 99% within less than six seconds."
>
> Teza Mukkavilli
> Head of Security at Upwork



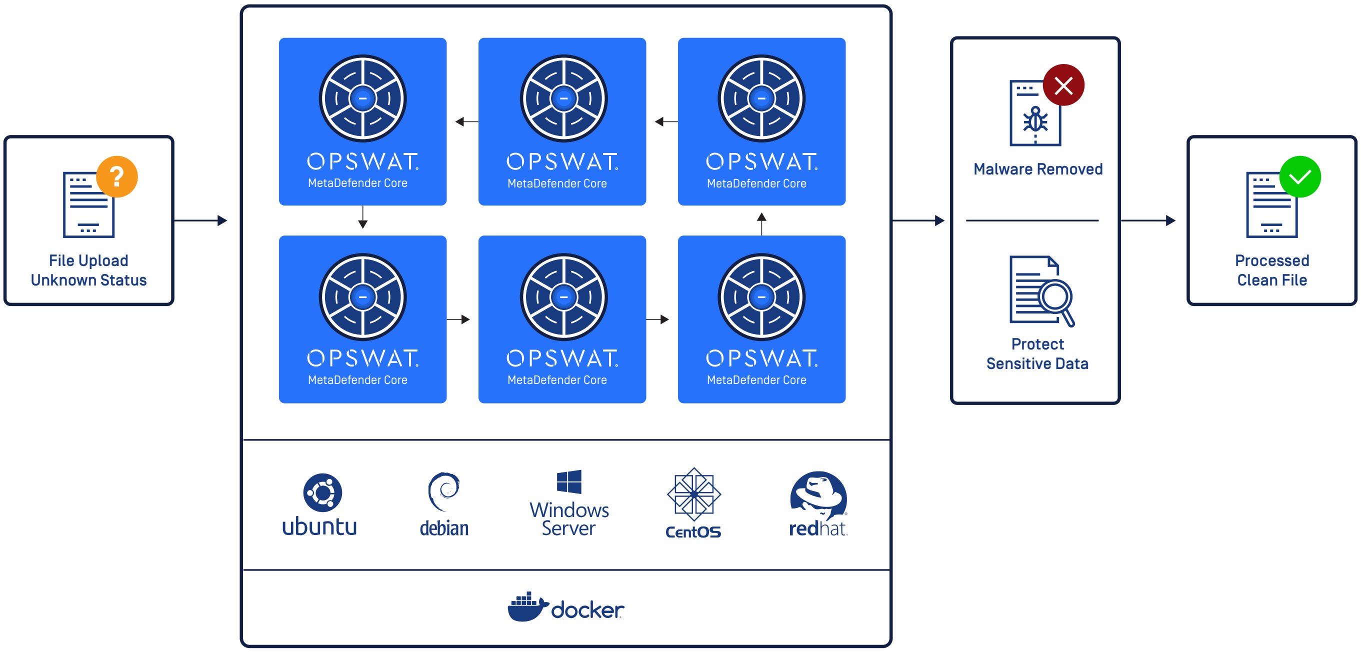
MetaDefender Core Container

Our new solution enables the deployment of MetaDefender Core in a containerized ecosystem. With MetaDefender Core Container, enterprises can scale the advanced multi-layered cybersecurity platform across different environments and operating systems, while ensuring application uniformity, removing any environment-specific dependencies, lowering resource consumption, and focus on preventing malware attacks.

Containerization is the step that will propel enterprises from single-tiered monolithic applications toward the modern, multi-tiered microservices architecture.

- Automated deployment and operability simplify integration and maintenance
- Significantly lower TCO (Total Cost of Ownership)
- Remove the complexity and ambiguity caused by the external factors such as conflict application dependencies
- Easy and flexible horizontal scaling
- Respond to load spikes by scaling only the required services

How MetaDefender Core Works in a Containerization Environment



Case Study

OPSWAT customer	Upwork - A freelancing website that connects businesses with freelance talents for highly skilled knowledge work such as web, mobile and software development and design.
Security challenge	▪ Upwork receives millions of files a day from clients and freelancers and needs to ensure that those files are free from threats to protect both their own systems and the systems of Upwork users. ▪ Upwork suffered 3-4 malware attacks per week.
OPSWAT's solution	Upwork added Deep CDR to their existing security architecture. MetaDefender Deep CDR breaks down a file (such as Microsoft Office, PDF and image files) into its component parts, and removes any potentially malicious elements, including macros, scripts, or embedded files. The file is then reconstructed with the remaining safe content. Even if a document contains an undetected threat, it is made harmless in the process.
Results	✓ Deep CDR effectively nullifies the remaining attacks. ✓ Upwork witnessed a 70% drop in malware attacks. ✓ Upwork is now able to prevent 100% of zero-day file attacks. ✓ No further maintenance or overhead, and with little to no impact on user experience.

Use Cybersecurity That Works

Schedule a meeting with an OPSWAT technical expert to explore how OPSWAT helps you protect your infrastructure from advanced sophisticated threats, please visit **opswat.com/contact**

For further information about File Upload Security, visit **opswat.com/solutions/file-upload-security**

SCHEDULE A MEETING

Trust no file. Trust no device.

Trusted by over 1,000 large enterprises and government organizations worldwide

OPSWAT protects critical infrastructure. Our goal is to eliminate malware and zero-day attacks. We believe that every file and every device pose a threat. Threats must be addressed at all locations at all times—at entries, at exits, and at rest. Our products focus on threat prevention and process creation for secure data transfer and safe device access. The result is productive systems that minimize risks of compromise. That's why 98% of U.S. nuclear power facilities trust OPSWAT for cybersecurity and compliance.

OPSWAT.com/contact