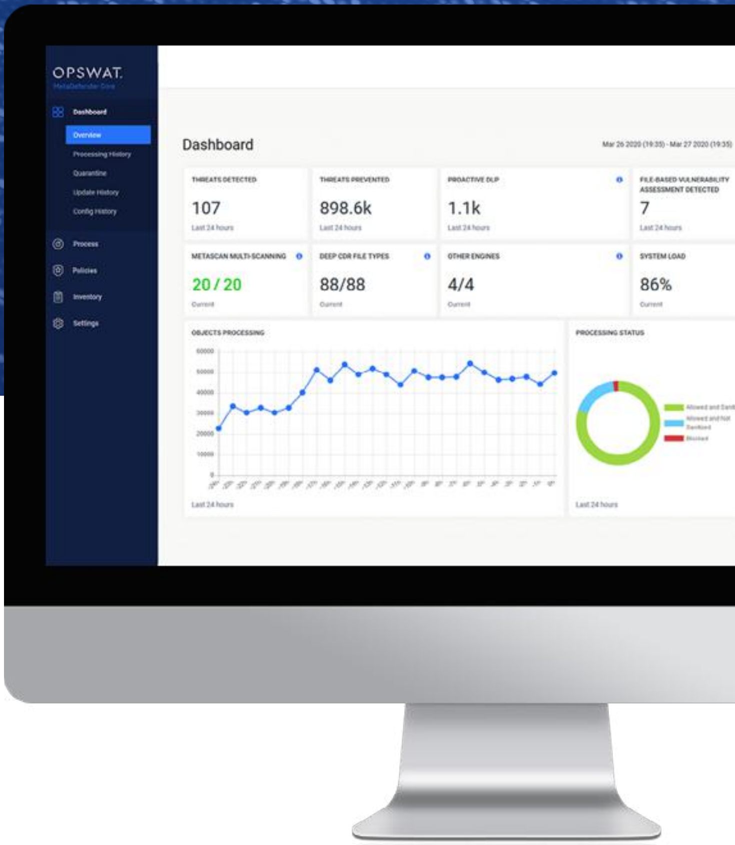
Solution Guide

File Upload Security

Protect Against Malicious File Uploads



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

METASCAN MULTI-SCANNING 20 / 20 Current

DEEP CDR FILE TYPES 88/88 Current

OTHER ENGINES 4/4 Current

SYSTEM LOAD 86% Current

Last 24 hours

Last 24 hours

File uploads are essential for user productivity, group collaboration, and application services. However, leaving file uploads unrestricted creates an attack vector for cybercriminals and causes data breaches.

Enterprises need a single robust layer of protection between uploaded files and their network.

Business and Technical Challenges

With malicious file uploads, attackers can compromise your servers or your entire system. Also, sensitive data can be leaked from your organization due to file transfer between internal and external users.

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 system with a disparate set of security products. However, this is not only costly and time-consuming but also problematic for consistent prevention and management.

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.

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.

6 Best Practices To Prevent File Upload Vulnerabilities

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

Key Differentiators

Advanced threat detection and prevention technologies

Providing industry-leading cybersecurity technologies including Multiscanning and Deep Content Disarm and Reconstruction (Deep CDR), which are the best ways to detect and prevent known and unknown threats.

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.

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.

Customizable policies

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

How We Can Help

File upload security assessment

Have the experts of OPSWAT's Professional Services quickly assess your File Upload security readiness. We tailor the evaluation to your organization's specific needs based on our proven methodology, then provide a detailed analysis report with follow up discussion and recommendations.

Prevent zero-day or advanced threats by passing your defenses

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.

Protect sensitive information in files

With OPSWAT Proactive Data Loss Prevention (Proactive DLP) technology you can content-check files for sensitive data when they are uploaded or downloaded from web applications. Also, you can check files transferred through web proxies, secure gateways, web application firewalls, storage systems, and block or redact it before it reaches the end user or exits the environment.

Provide nearly 100% known threat detection

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

Maximize vulnerability detection

Numerous organizations are exposed to attacks leveraging vulnerabilities. Uploaded files can trigger vulnerabilities in broken libraries/ applications. OPSWAT File-Based Vulnerability Assessment technology detects vulnerabilities in installers, binary files and Internet of Things (IoT) firmware before they are installed on your devices.

Meet compliance requirements

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

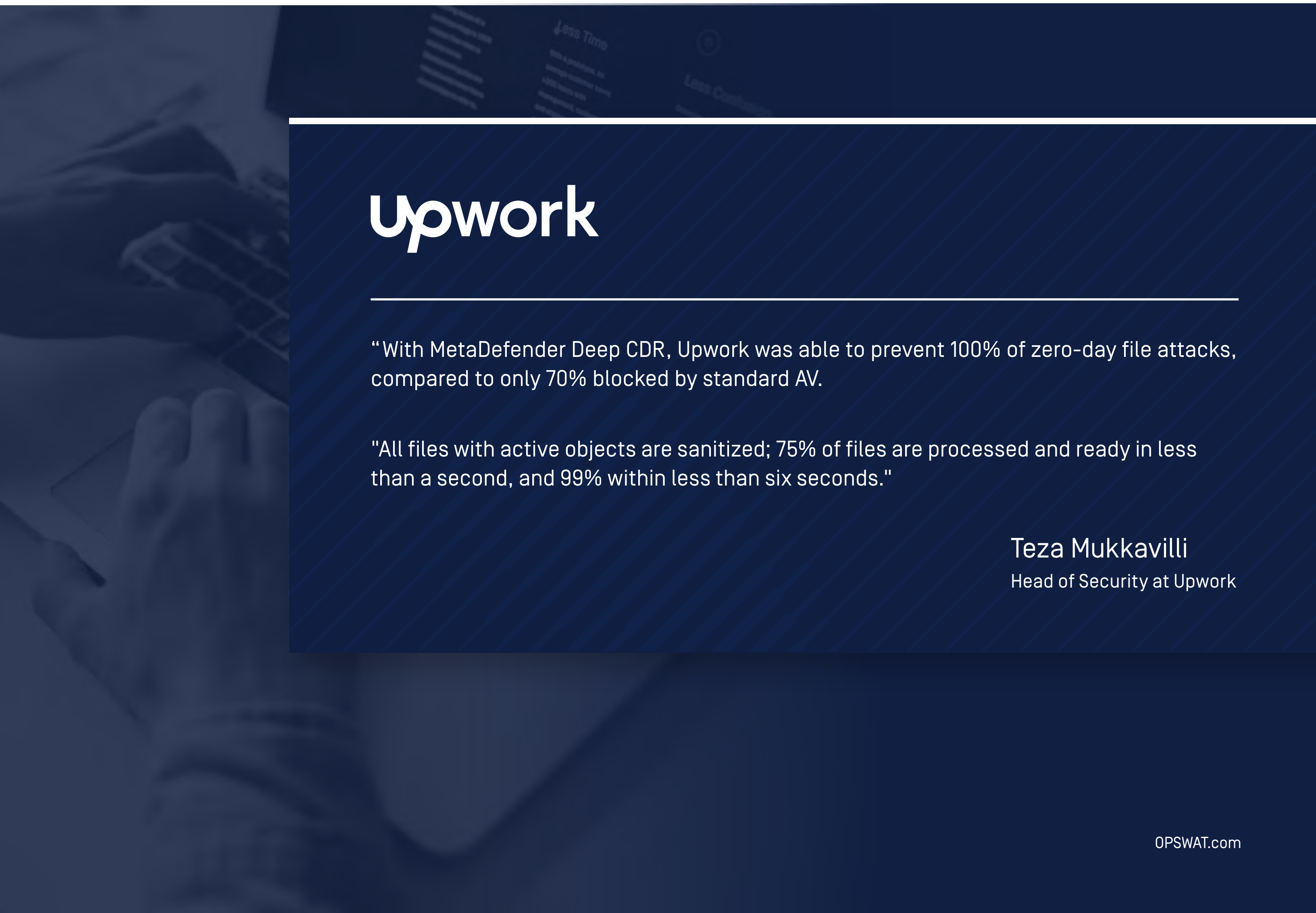
Customer Benefits

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.

Custom security policies and workflows
Enabling 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 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.



upwork

“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

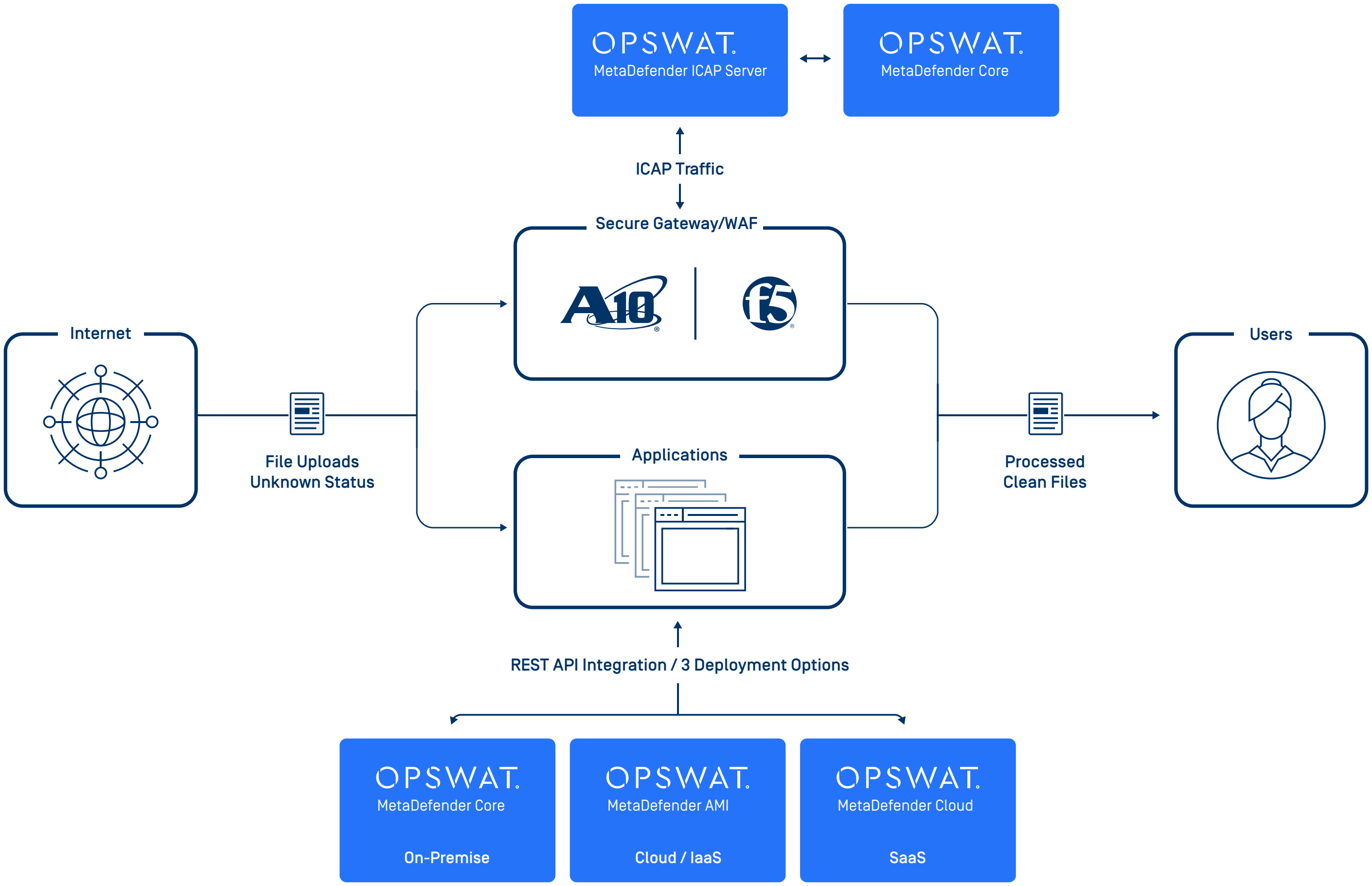
MetaDefender Deployments and Integrations

MetaDefender can be deployed within your premises, 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.

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®

Flexible Deployment Options



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

OPSWAT.

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.

Modified 20200805