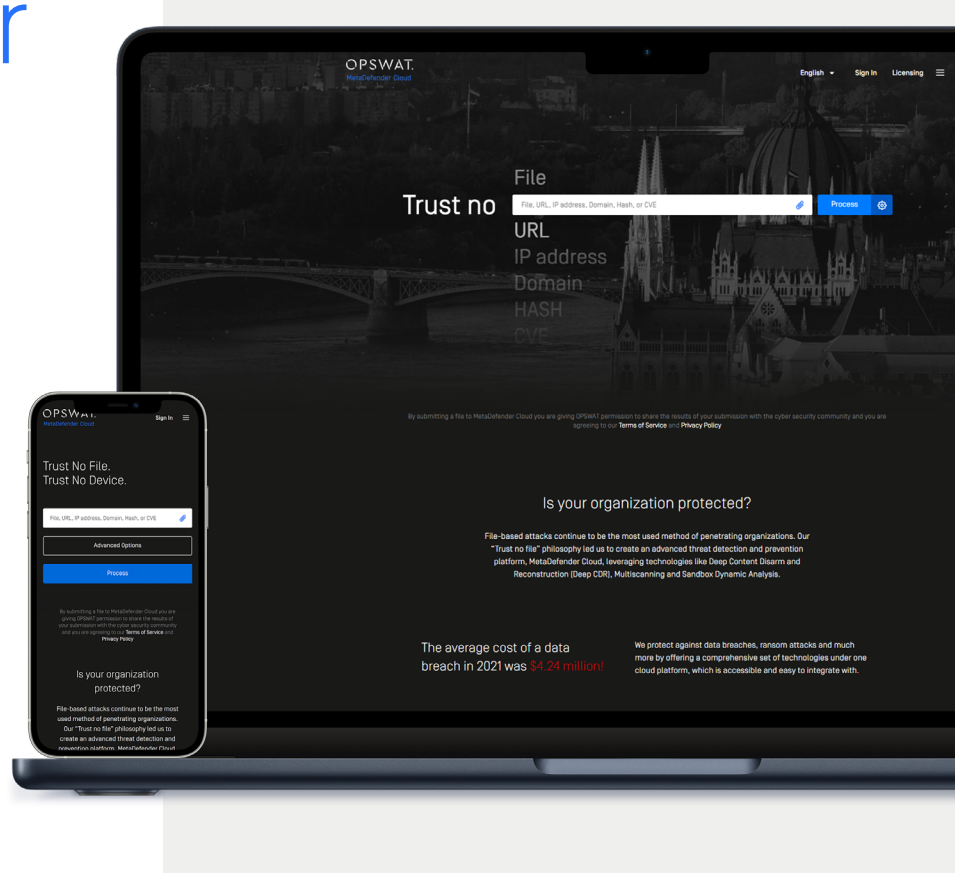
MetaDefender Cloud™

Cloud-Based Advanced Threat Prevention



Attackers increasingly use trusted channels to upload harmful files. More than 90% of malicious attacks originate via trusted channels such as email, web applications, cloud storage, and B2B file transfers. Organizations must protect their operations against these sophisticated attacks.

OPSWAT's "Trust no file" philosophy secures against file-based attacks by offering a comprehensive set of malware detection tools under one easy-to-implement cloud platform.

Detect, Analyze and Eliminate Malware and Zero-day Attacks

Benefits

Advanced Threat Prevention
Detect and prevent threats in real-time with our comprehensive Multiscanning and Deep Content Disarm & Reconstruction (Deep CDR) technologies.

Performance & Scalability
Scale to any volume of scans with our high-performance architecture and load balancing feature. Fast scanning and reconstruction without affecting performance.

Data Security with Private Scanning
Analyze user-submitted files with MetaDefender Cloud without exposing the file's content. After the analysis finishes, files are deleted from OPSWAT servers.

Reduced Complexity and Effort
Eliminate worry with our cloud solution and remove the burden of managing software infrastructure in your organization. We continually update our infrastructure, so your organization does not have to worry about engine definitions, software updates, or unpatched vulnerabilities.

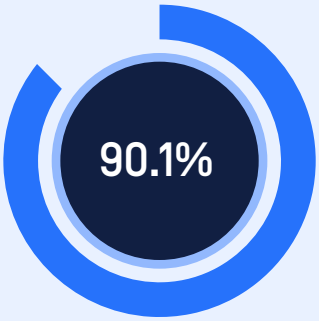
OPSWAT.

MetaDefender Cloud

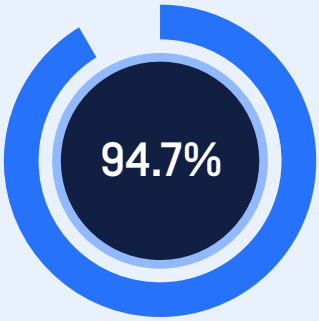
DATASHEET

Antivirus Detection Rates

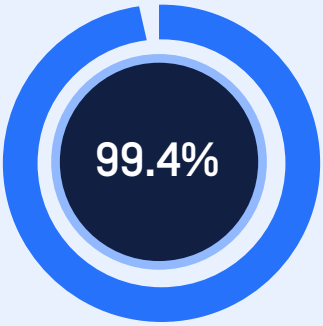
Three Available Packages



Standard Tier
10 Engines

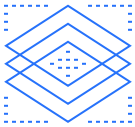


Professional Tier
15 Engines



Enterprise Tier
23 Engines

Key Features



Multiscanning
Multiscanning increase detection rates and decrease outbreak detection times with multiscanning. Simultaneously analyze file uploads using 20+ industry-leading antimalware engines such as McAfee, Kaspersky, or Bitdefender, using signatures, heuristics, and machine learning.

Deep CDR
Prevent Zero-Day and targeted attacks using OPSWAT's Deep CDR technology (ranked # 1 in the industry). We assume all files are malicious and sanitize and rebuild each file preserving the same visual data with safe content.

Sandbox Dynamic Analysis
Detect and destroy malware by exposing and recording malicious behavior. Not all malware is detectable by static methods such as multiscanning, especially new malware which use zero-day attacks. OPSWAT Sandbox expands the malware detection capabilities of MetaDefender Cloud, giving organizations a complete toolset of security technologies.

Threat Intelligence
We provide live feeds for both blocklisting and allowlisting hashes which can also be used in offline environments. The feeds are updated instantly with the latest file hashes analyzed by our platform from malware sharing programs, customer files, and more. Also, we gather data from multiple real-time online sources specializing in IP addresses, domain, and URL reputation to provide a lookup service that returns aggregated results to our users.

OPSWAT.

MetaDefender Cloud

DATASHEET

Use Cases

Web UI

The desktop and mobile friendly UI offers users full access to all the features offered by MetaDefender Cloud including malware analysis and IP domain verification.

Cloud Security for Salesforce

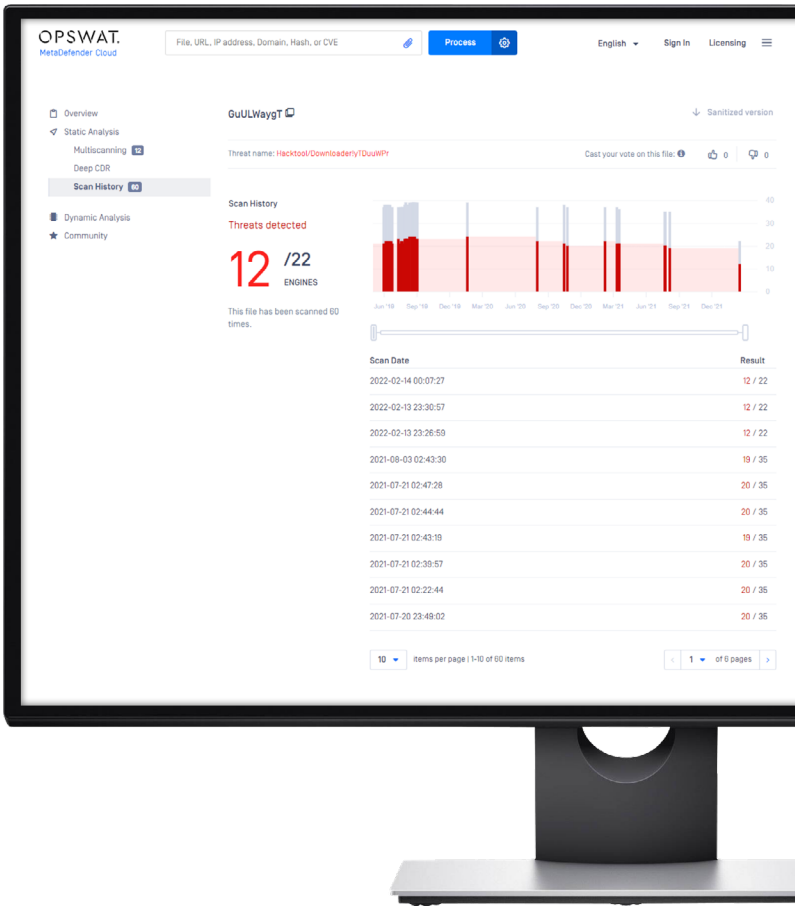
OPSWAT Cloud Security for Salesforce scans and sanitizes every file uploaded to Salesforce removing malicious content hiding inside files.

REST API

All features are exposed as a REST API. With straightforward API key authentication, it's simple to integrate into any application and perfect for automating file and IP-domain analysis.

Remote Browser Isolation (RBI) Integration

Integrates with your remote browser isolation (RBI) solution to scan and sanitize content that your users download to protect their local machines and network. Currently we have a native integration with Menlo Security's RBI solution.



Product Licensing

We offer 3 different MetaDefender Cloud APIs that each enable different security flows.

Analysis API	Prevention API	Reputation API
Analysis API includes access to our Sandbox dynamic analysis technology: ▪ Execute files on multiple operating systems ▪ Automated interpretation of the behavior ▪ Configurable analysis settings	The MetaDefender Cloud Prevention API includes: ▪ Scanning files with 23 traditional and next-gen anti-malware engines ▪ Preventing 0-day attacks by productivity documents using Deep CDR	The MetaDefender Cloud Reputation API includes: ▪ Access to billions of malware and hashes via REST API ▪ Scanning IP addresses, URLs and domains using up to 30 different engines ▪ Correlating hashes to millions of known applications and providing specific application data from vendors like Microsoft, Adobe, and others

OPSWAT.

Protecting the World's Critical Infrastructure