OPSWAT.

OPSWAT Government Cloud 15 Pack

Important Notice

In addition to the OPSWAT cloud products listed in this pricing pack, OPSWAT also offers a range of on-premises and hybrid solutions that are not delivered via the cloud. These include solutions for Cross Domain, Sheep Dip, and IMPEX use cases, designed for environments with strict security, air-gap, or regulatory requirements.

These solutions are licensed and priced separately based on deployment architecture, scale, and customer requirements, and are not included in cloud product pricing. Customers interested in these non-cloud offerings should contact OPSWAT for detailed information, technical discussions, and customised pricing.

Table of Contents

01

OPSWAT MetaDefender Cloud Products - Pricing

SKU	Product Description	Item Sale Price (12 Months)	Item Sale Price (36 Months)	Item Sale Price (60 Months)
MD-CLOUD-PREVENT-STD	OPSWAT MetaDefender Cloud Prevention API prevents file-borne threats by detecting known threats via multi-scanning and by removing potentially malicious active content in documents via data sanitization (Content Disarm and Reconstruction). The standard version of MD Cloud Prevention API comes with 10 Anti-Virus/Anti-Malware Engines. Price is for 1,000 API requests/day (annual price). Deep CDR and multi-scanning are counting as separate requests (will consume 2 API calls out of the daily limit)	£5186.14	£13,224.66	£19,188.72
MD-CLOUD-PREVENT-PRO	OPSWAT MetaDefender Cloud Prevention API prevents file-borne threats by detecting known threats via multi-scanning and by removing potentially malicious active content in documents via data sanitization (Content Disarm and Reconstruction). The professional version of MD Cloud Prevention API comes with 15 Anti-Virus/Anti-Malware Engines. Price is for 1,000 API requests/day (annual price). Deep CDR and multi-scanning are counting as separate requests (will consume 2 API calls out of the daily limit).	£10,373.46	£26,452.32	£38,381.80
MD-CLOUD-PREVENT-ENT	OPSWAT MetaDefender Cloud Prevention API prevents file-borne threats by detecting known threats via multi-scanning and by removing potentially malicious active content in documents via data sanitization (Content Disarm and Reconstruction). The enterprise version of MD Cloud Prevention API comes with 24 Anti-Virus/Anti-Malware Engines. Price is for 1,000 API requests/day (annual price). Deep CDR and multi-scanning are counting as separate requests (will consume 2 API calls out of the daily limit).	£20,745.73	£52,901.61	£76,759.20

SKU	Product Description	Item Sale Price (12 Months)	Item Sale Price (36 Months)	Item Sale Price (60 Months)
MD-CLOUD-ANALYSIS-1K (Sandbox)	OPSWAT MetaDefender Next-gen emulation cloud sandbox: Adaptive Threat Analysis with superior anti-evasion tech, 100x resource efficiency, and 10x speed. Specializes in detecting zero-day malware and targeted attacks in Documents (Office) and Scripts via MetaDefender Cloud UI or API (1,000 files/day).	£9,365.38	£23,881.72	£34,651.91
MD-CLOUD-ANALYSIS-5K (Sandbox)	OPSWAT MetaDefender Next-gen emulation cloud sandbox: Adaptive Threat Analysis with superior anti-evasion tech, 100x resource efficiency, and 10x speed. Specializes in detecting zero-day malware and targeted attacks in Documents (Office) and Scripts via MetaDefender Cloud UI or API (5,000 files/day).	£34,964.09	£89,158.44	£129,367.15
MD-CLOUD-ANALYSIS-10K (Sandbox)	OPSWAT MetaDefender Next-gen emulation cloud sandbox: Adaptive Threat Analysis with superior anti-evasion tech, 100x resource efficiency, and 10x speed. Specializes in detecting zero-day malware and targeted attacks in Documents (Office) and Scripts via MetaDefender Cloud UI or API (10,000 files/day).	£53,694.86	£136,921.89	£198,670.97
MD-CLOUD-REPUTATION-25K	OPSWAT MetaDefender Reputation Service (Layer 1): Provides real-time file, IP, URL, and domain reputation to ensure file safety before access. (25,000 queries/day)	£13,600.59	£34,681.50	£50,322.18
MD-CLOUD-REPUTATION-50K	OPSWAT MetaDefender Reputation Service (Layer 1): Provides real-time file, IP, URL, and domain reputation to ensure file safety before access. (50,000 queries/day)	£20,696.55	£52,776.20	£76,577.24
MD-CLOUD-REPUTATION-100K	OPSWAT MetaDefender Reputation Service (Layer 1): Provides real-time file, IP, URL, and domain reputation to ensure file safety before access. (100,000 queries/day)	£28,383.84	£72,378.79	£105,020.21
MD-CLOUD-REPUTATION-200K	OPSWAT MetaDefender Reputation Service (Layer 1): Provides real-time file, IP, URL, and domain reputation to ensure file safety before access. (200,000 queries/day)	£44,941.08	£114,599.75	£166,282.00
MD-CLOUD-REPUTATION-1M	OPSWAT MetaDefender Reputation Service (Layer 1): Provides real-time file, IP, URL, and domain reputation to ensure file safety before access. (1,000,000 queries/day)	£165,868.07	£422,963.57	£613,711.84

SKU	Product Description	Item Sale Price (12 Months)	Item Sale Price (36 Months)	Item Sale Price (60 Months)
MD-CLOUD-SANDBOX-SEARCH-1K	OPSWAT MetaDefender Advanced Reputation Search allows searching for threat patterns and expression, as well as detection of unknown zero-day malware using a next-gen ML based similarity search. (1,000 queries/day)	£4,936.32	£12,587.62	£18,264.38
MD-CLOUD-SANDBOX-SEARCH-5K	OPSWAT MetaDefender Advanced Reputation Search allows searching for threat patterns and expression, as well as detection of unknown zero-day malware using a next-gen ML based similarity search. (5,000 queries /day)	£17,277.12	£44,056.66	£63,925.34
MD-CLOUD-SANDBOX-SEARCH-25K	OPSWAT MetaDefender Advanced Reputation Search allows searching for threat patterns and expression, as well as detection of unknown zero-day malware using a next-gen ML based similarity search. (25,000 queries/day)	£27,149.76	£69,231.89	£100,454.11
MD-CLOUD-SANDBOX-SEARCH-100K	OPSWAT MetaDefender Advanced Reputation Search allows searching for threat patterns and expression, as well as detection of unknown zero-day malware using a next-gen ML based similarity search. (100,000 queries/day)	£83,146.14	£212,022.66	£307,640.72
MD-CLOUD-ICAP-SERVER	OPSWAT MetaDefender ICAP Server, now available as a SaaS, hosted alongside MetaDefender Cloud. MetaDefender ICAP Server inspects and sanitizes network traffic passing through network security devices; protecting the environment from advanced cybersecurity threats such as zero-day attacks, phishing, ransomware, and other advanced threats which can bypass legacy anti-malware prevention solutions. MetaDefender ICAP Server integrates with ICAP-enabled devices such as firewalls, ADCs, load balancers, reverse and forward proxies, MFTs, and compatible NAS (network-attached storage) devices. This product leverages MetaDefender technologies such as multi-scanning, Proactive DLP, Deep CDR, threat intelligence, and vulnerability checks of IoT firmware and application installers. Price is for 1,000 API requests/day (annual price). Deep CDR and multi-scanning are counting as separate requests (will consume 2 API calls out of the daily limit).	POA	POA	POA

SKU	Product Description	Item Sale Price (12 Months)	Item Sale Price (36 Months)	Item Sale Price (60 Months)
MD-CLOUD-STORAGE	OPSWAT MetaDefender Storage Security Cloud offers comprehensive protection for cloud storage by allowing customers to choose between MetaDefender Cloud Prevention, MetaDefender Cloud Analysis, or both. This flexible solution ensures cloud-stored files are safeguarded against both known and unknown threats. With seamless API integration, MetaDefender Storage Security Cloud provides scalable, real-time file scanning, sanitization, and analysis to keep your cloud storage secure. Price is for 1,000 API requests/day (annual price). Deep CDR and multi-scanning are counting as separate requests (will consume 2 API calls out of the daily limit).	POA	POA	POA
MD-CLOUD-SFDC-U-FSIO	OPSWAT MetaDefender for Salesforce leverages multiple AV engines using MetaDefender Cloud as well as OPSWAT's industry-leading Deep Content Disarm and Reconstruction (CDR) technology for prevention of known, unknown and zero-day attacks in documents and files. The product is licensed by number of units 1 unit = 5 API calls per day. Limit is applied at account level based on total number of units licensed (additional custom limit is available for extra cost).	£80.79	£206.01	£298.92
MYOPSWAT-CM-CLOUD	OPSWAT Central Management - A Cloud Platform - to manage IT Access Solutions, Endpoint Security, Peripheral Media Protection Solutions, Hardware Supply Change Solutions, and File Security Solutions	£0.00	£0.00	£0.00
MD-EMAIL-CLOUD-STANDARD	OPSWAT MetaDefender Cloud Email Security is a 100% cloud email security service that protects against email-borne threats - including malware, ransomware and zero-day attacks. Included in the price is Deep CDR and scanning with 5 engines. Price is per mailbox per year.	£18.19	£46.38	£67.30
MD-EMAIL-CLOUD-MAX	OPSWAT MetaDefender Cloud Email Security is a 100% cloud email security service that protects against email-borne threats - including malware, ransomware and zero-day attacks. Included in the price is Deep CDR and scanning with 17 engines. Price is per mailbox per year.	£54.58	£139.18	£201.95

OPSWAT.

02

METADEFENDER

Cloud™

Secure Your Enterprise Data Storage

OPSWAT's cloud security solutions enable fearless collaboration for today's distributed workforce. We deliver flexible, scalable protection for data stored both on-premises and across cloud-based platforms like SharePoint, Box, and other SaaS services.

Our product suite includes MetaDefender Cloud API, Cloud Security for Salesforce (CSFS), ICAP Cloud, and Storage Security Cloud, providing advanced threat prevention, data security, and compliance capabilities.

Core Technologies for Advanced Threat Prevention, Data Security, and Compliance Capabilities

Metascan™ Multiscanning

No single engine detects all possible malware. Strengthen resiliency by analyzing files with 20+ industry-leading anti-malware engines.

Deep CDR™

Deconstruct each file and rebuild it with only safe to consume components to prevent Zero-Day and targeted attacks.

Proactive DLP™

Prevent potential data breaches and regulatory compliance violations by detecting and blocking sensitive data in files in 110+ file types.

Adaptive Sandbox

Detonate malware in a controlled environment to expose malicious behavior by recording and classifying file behavior.

Seamless Integration with Cloud-Based Platforms Provides Flexible and Scalable Protection

As opposed to traditional security systems, MetaDefender Cloud adapts to your specific security needs with flexible deployment models (API-driven security, ICAP, native plugins).

Simplify security management with minimal IT effort required for deployment. All functions are hosted entirely in the cloud, eliminating the need for on-prem hardware and streamlining security operations.

MetaDefender Cloud in Action

Global Financial Services Provider Reinforces Defense with OPSWAT MetaDefender Cloud

Our client needed a comprehensive, multi-faced solution to deal with the unprecedented level of cybersecurity challenges faced by financial institutions.

With MetaDefender Cloud, they got a three-fold approach. It starts with static scanning, deploying 20+ AVs. Next, Deep CDR technology neutralizes any potential zero-day threats embedded in the files. Finally, Sandboxing technology applies dynamic behavioral analysis to identify evasive or previously unknown malware strains.

Financial institutions are a prime target for cybercriminals, as 65% of them reported a ransomware attack in 2024. In this high-stakes context, each file upload could become an entry point for file-borne threats. By choosing MetaDefender Cloud for active defense, they've demonstrated their commitment to protecting sensitive data.

Enterprise-Grade Protection, Legal Compliance, and Data Privacy

- SOC 2 Type II Certified
- GDPR-aligned Architecture
- Private Processing Options, Data Residency Flexibility, and Enhanced Privacy Features
- 20+ Antivirus Engines
- ISO 27001 & ISO 9001 Compliance
- P90 SLA 8 Seconds

Native Integrations

aws S3 | salesforce | Google Cloud | SharePoint | OneDrive | 10 01 | f5 | box

OPSWAT.

03

METADEFENDER

Sandbox™

AI-Powered Malware Analysis for Evasive Threats

MetaDefender Sandbox is a multi-layered, AI-powered malware analysis solution designed to detect and classify even the most evasive zero-day threats By combining dynamic analysis, threat scoring, and high-speed emulation, it delivers actionable insights to protect critical networks from zero-day attacks. The latest 2.5.0 release introduces enhanced UI, and a next-gen advanced PE Emulator for breakthrough detection of obfuscated malware.

Key Features

Dynamic Analysis

- 30+ AV engines, YARA rules, heuristic scanning
- YARA & Config extraction for the most prevalent malware families
- Detects evasive malware & sandbox-aware threats through our inhouse Threat Indicator Library
- Analyze broken Office files used in zero-day attacks
- Embedded file & script decoding (e.g., VBA, PowerShell, AutoIT, JavaScript)
- Detection of .NET loaders & suspicious binary anomalies
- HTML parser support improves detection of evasive or malformed threats
- Brand Detection Model with additional brands added, supports OCR Capabilities

Threat Hunting & Forensics

- MITRE ATT&CK mapping and machine learning similarity search
- AI-powered phishing and URL threat detection
- Web threat detection with ML-based multi-label classification, content/style analysis, and automated threat detection pipeline providing faster, consistent, and efficient workflows.

Advanced Emulation

- Powered by the next-gen advanced PE Emulator Beta—purpose-built to outpace traditional sandboxes +48% more high-confidence verdicts and +224% more IOCs/day (Source: Filescan.io)
- Defeats anti-VM, anti-debug, and time-based evasion—no manual tuning required
- Unpacks multi-stage payloads, decrypts runtime packers, and reveals hidden IOCs
- Detects fileless malware, custom loaders, and sandbox-aware threats missed by legacy tools
- Shellcode execution, memory dump integration, and event tracking for deeper behavioral insights

Threat Indicator Repository

- 50B+ hashes, IPs, domains for enhanced threat attribution
- MISP & STIX integration for automated extraction and sharing
- Custom generated YARA rules for in-depth threat profiling with tagging, naming and associated metadata

Flexible Deployment & API-First Design

- On-premises, hybrid, or cloud-native deployment
- REST API for seamless integration
- SIEM/SOAR support: Splunk, Cortex XSOAR, CEF Syslog
- Setup Wizard for Simplified Deployment

Speed & Accuracy Across the Entire Threat Detection Pipeline

Analysis Layers	Key Capabilities
Layer 1 Threat Reputation	Reputation analysis, OSINT lookups, hash/IP reputation
Layer 2 Dynamic Analysis	YARA scanning, unpacking, decompilation
Layer 3 Threat Scoring	Emulation-based detonation, evasive malware detection
Layer 4 Threat Hunting	Deep behavior analysis, IOC extraction, ML clustering

Technical Specifications

Deployment Options

- On-Premises: 32GB RAM, 256GB SSD
- Cloud: AWS m6a/c6a instances, up to 25K scans/day
- API & GUI-based integrations
- Support for Ubuntu 24.04
- Support Red Hat Offline Installation (RHEL 9)
- Support Rocky Linux

Integration and Reporting

- SIEM/SOAR: Splunk, Cortex XSOAR, Assemblyline 4
- Threat Intel Feeds: MISP, STIX 2.1
- Data Export: JSON, PDF, HTML

Why MetaDefender Sandbox?

Fastest Malware Analysis
Verdicts in seconds, not minutes

Seamless SOC Integration
REST API, SIEM & SOAR support

Low Resource Consumption
10x more efficient than traditional VM-based sandboxes

Unparalleled Threat Visibility
IOCs, malware family detection, MITRE ATT&CK mapping

04

METADEFENDER

ICAP Cloud

Advanced Cloud-Based Threat Protection

MetaDefender ICAP Cloud is OPSWAT's advanced cloud-based security solution that offers comprehensive threat detection and prevention for network traffic. Leveraging the powerful capabilities of OPSWAT's MetaDefender Platform, MetaDefender ICAP Cloud provides seamless integration with ICAP-enabled devices, offering organizations the flexibility of a cloud-based platform that ensures robust protection against malware, zero-day attacks, and data breaches.

Designed for scalability and ease of management, MetaDefender ICAP Cloud eliminates the need for on-premises infrastructure and significantly lowers operational costs. With global deployments, MetaDefender ICAP Cloud aids data sovereignty and compliance with regional regulations, providing businesses with a solution that secures network traffic from malicious file upload attacks and data leakage.

Key Benefits

Real-Time Threat Detection

MetaDefender ICAP Cloud protects against malicious file uploads, zero-day attacks, and sensitive data exposure in real time, ensuring your network is always secure.

Scalability and High Availability

Our cloud infrastructure supports high availability and scalability, with load balancing features that enable organizations to handle peak loads without performance degradation.

Effortless Integration

Our solution integrates effectively with existing ICAP-enabled devices such as load balancers, proxies, and web application firewalls (WAPs), simplifying deployment and adoption.

Data Sovereignty and Privacy

Regional deployments aid compliance with local data protection regulations, while private scanning and processing features maintain user confidentiality.

Cost Efficiency

MetaDefender ICAP Cloud eliminates the costs associated with maintaining on-premises hardware, offering a lower total cost of ownership (TCO) and predictable operational expenses.

Key Features

Key Feature	Related Benefit
Multiscanning Utilizes over 20 industry-leading anti-malware engines to provide comprehensive malware detection through signatures, heuristics, and machine learning.	Achieves over 99% malware detection rates, reducing infection risks and improving security posture.
Deep CDR Removes potentially malicious and out-of-policy content and regenerates new, safe-to-use files.	Prevents potential threats, including zero-day attacks, and supports files with nested archives.
Proactive DLP Inspects files for sensitive information such as PII, financial data, and confidential documents.	Prevents unauthorized data transfer and exposure of secrets, aiding compliance with data protection regulations.
File-Based Vulnerability Assessment Analyzes files for known vulnerabilities before execution, identifying and flagging risky files.	Reduces the risk of cyberattacks by preventing the exploitation of file and application vulnerabilities.
Private Scanning and Processing Ensures the files are scanned without being stored on OPSWAT storage systems, with results only being available to the owner.	Maintains data privacy and confidentiality, preventing unauthorized access or sharing of sensitive files.
Organizations Feature Allows the creation of multiple organizations within MetaDefender ICAP Cloud, with role-based access control (RBAC) and administrative management.	Enhances management and security by enabling structured access control and easy license management.

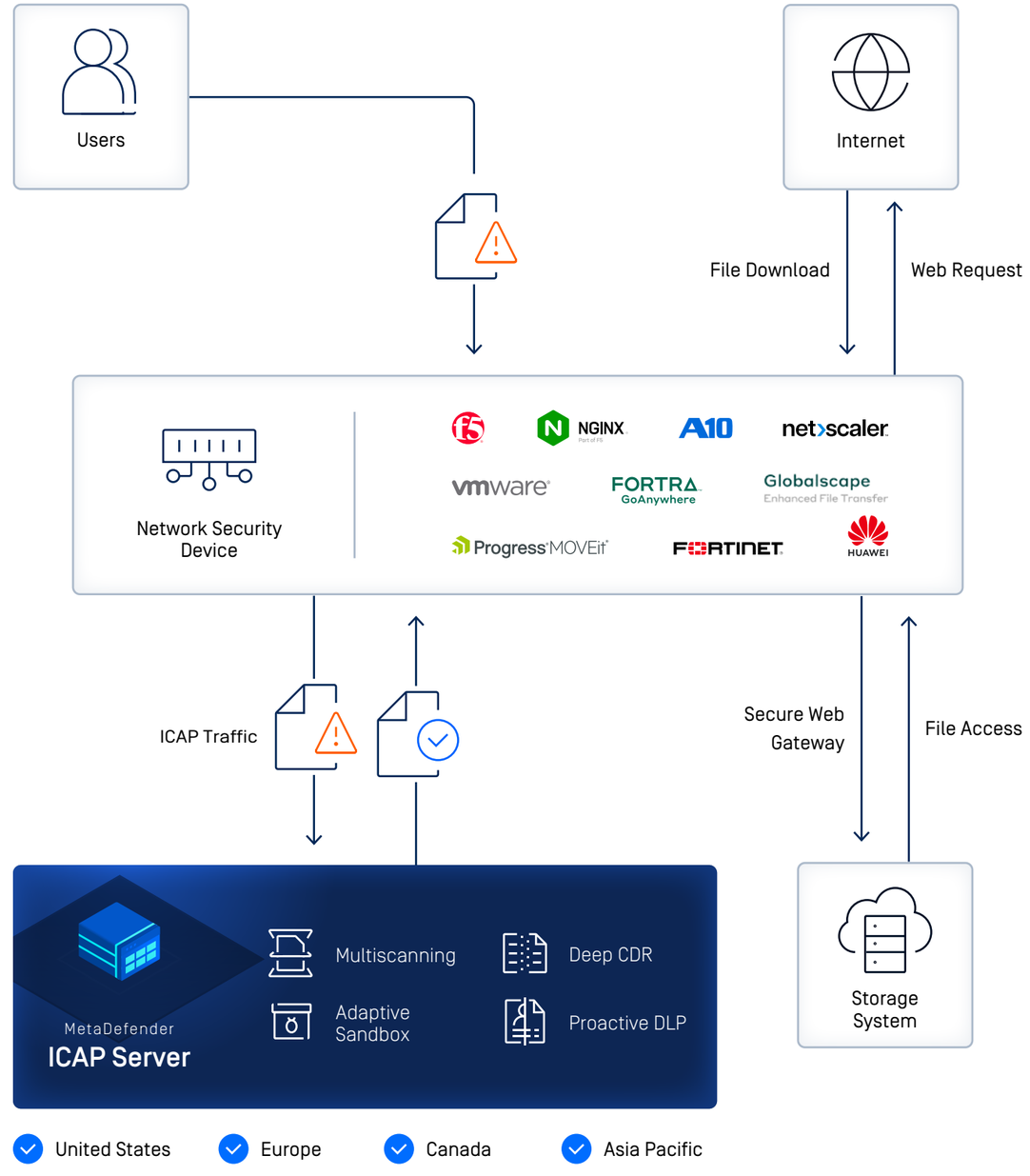
Part of OPSWAT's Cloud-based Cybersecurity Platform

MetaDefender ICAP Cloud is an integral component of OPSWAT's MetaDefender Cloud, a comprehensive cloud-based cybersecurity platform designed to protect organizations from emerging threats. MetaDefender Cloud offers a powerful suite of tools and services that deliver high-level protection against malware, zero-day attacks, and data breaches. With its effective integration capabilities, MetaDefender ICAP Cloud ensures that network traffic is thoroughly inspected and secured, providing organizations with a flexible, scalable, and efficient solution to meet their cybersecurity needs.

Specifications

- Regional Coverage: Deployments in EU, USA, Canada, Australia, APAC
- Service Level Agreements (SLAs) ensure high availability and reliability
- Support: 24/7 expert support and rapid troubleshooting

Enhanced Privacy and Security	Features such as private scanning and mutual TLS (mTLS) provide secure communication and data handling, building trust with users.
Disaster Recovery and Compliance	Benefits from OPSWAT-managed disaster recovery, ensuring business continuity and compliance with certifications such as ISO 9001, ISO 27001, and SOC2.
Unified Threat Detection Platform	Integrates with MetaDefender Cloud for enhanced security capabilities, offering a multi-layered security solution.
Custom Reporting and Analytics	Offers on-demand reporting and analytics, providing insights into security posture and helping organizations make informed decisions.
Flexible API Integration	Supports easy integration with existing systems and applications through MetaDefender Cloud APIs.



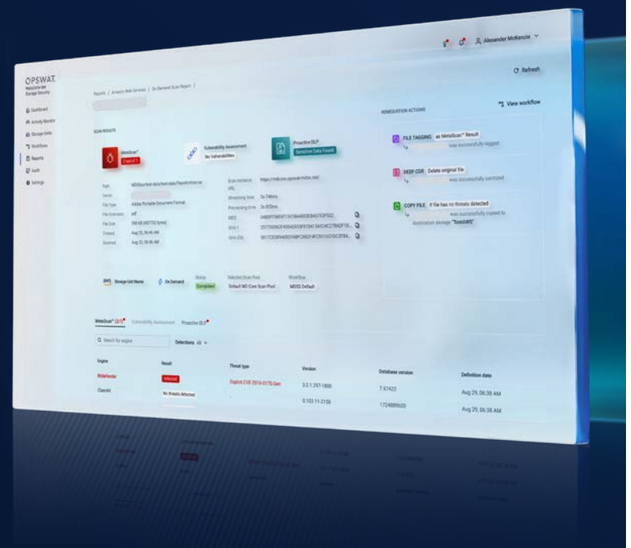
OPSWAT.

05

METADEFENDER

Storage Security Cloud

Cloud-Native Data Protection for Hybrid Workflows



MetaDefender Storage Security Cloud is a SaaS-native solution designed to provide comprehensive security for businesses transitioning to cloud environments. Built for hybrid workflows, it delivers flexible, scalable protection for data stored both on-premises and across cloud-based platforms like SharePoint, Box, and other SaaS services. By eliminating hardware dependencies and automating updates, MetaDefender Storage Security Cloud simplifies security management while ensuring that your files are always protected.

Seamless Integration

Hybrid Security for Cloud and SaaS

Built to meet the growing demand for hybrid storage security, MetaDefender Storage Security Cloud supports businesses moving to the cloud while securing their existing on-premises environments.

Simple and Flexible Protection

Protect critical workflows across popular SaaS platforms like SharePoint and Box with ease. MetaDefender Storage Security Cloud adapts to your business needs without the complexity of traditional security systems.

Scalable and Cost-Effective

Benefit from scalable protection that grows with your business. MetaDefender Storage Security Cloud offers pay-as-you-go pricing with no costly on-prem hardware investments, making it an efficient solution for businesses of all sizes.

Simplicity and Security

Cloud-Native Scanning and Sanitization

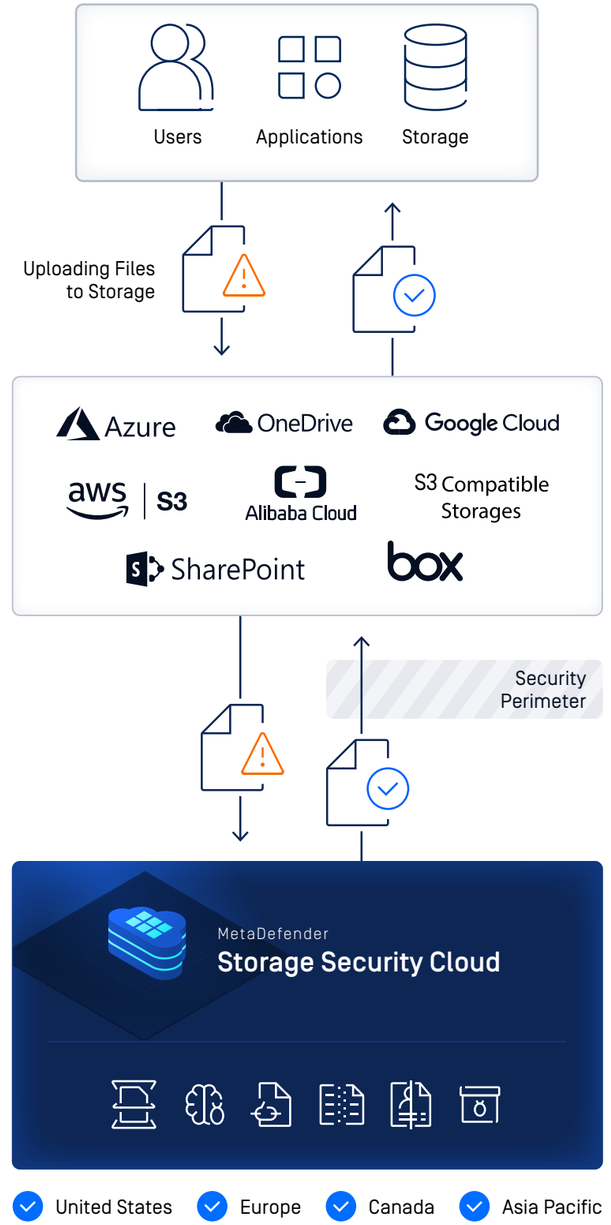
All scanning, threat detection, and management functions are hosted entirely in the cloud, eliminating the need for on-prem hardware and streamlining security operations.

Effortless Setup and Maintenance

With minimal IT effort required for deployment, MetaDefender Storage Security Cloud offers rapid setup. Automatic updates ensure that your system is always equipped with the latest security features and protections.

Centralized Real-Time Security

Protect your data no matter where it's stored—on-premises or in the cloud. With centralized management and real-time scanning, MetaDefender Storage Security Cloud ensures that files are safeguarded wherever they reside.



06

MetaDefender for Salesforce

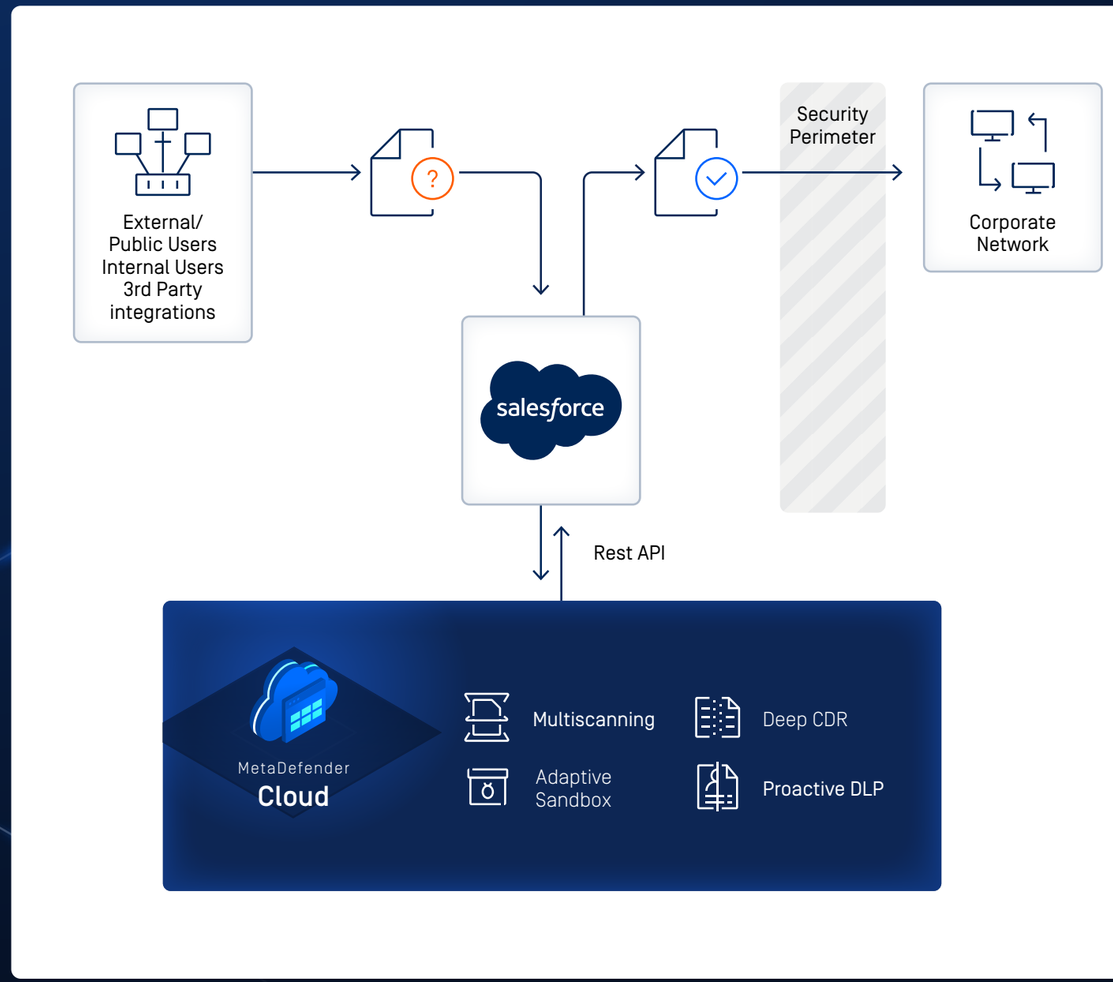
Secure File Uploads for Salesforce

Protect your Salesforce data with automatic file-scans at upload, without slowing down your workflows. OPSWAT's MetaDefender for Salesforce catches known and unknown threats, removes malicious content, and prevents infected files from reaching user or being shared across the system.

No extra steps. No user action required. Just automatic protection where it counts.

MetaDefender for Salesforce is now listed on:

The Salesforce App Exchange Platform



Salesforce Challenges

More than 150,000 businesses use Salesforce, due to undeniable advantages in terms of flexibility, ease-of-use, and accessibility. However, the lack of built-in malware scanning leaves organizations vulnerable to cyberattacks, introduced via file uploads. Here are some of the challenges faced by businesses using Salesforce:

Malware

Salesforce itself doesn't scan uploaded files for malware, nor does it assess URLs, links, IPs, or domains for malicious behavior, which creates an opening for threat actors to embed harmful content or reference dangerous sources before they are uploaded or shared.

Shared Security Responsibility

Salesforce is responsible for securing the core platform infrastructure, but the responsibility for configuring security settings, managing user access controls, and implementing data protection measures falls squarely on your organization.

Third-Party Application File Upload Vulnerabilities

Security protocols within third-party applications designed for file upload functionality may vary significantly. Unlike Salesforce, some third-party applications might possess weaker defenses against malware or malicious content embedded within uploaded files.

Data Breaches

Data stored in Salesforce usually includes customer information, financial data, and proprietary business processes. A breach can lead to severe consequences, such as financial loss, reputational damage, and regulatory fines.

Benefits

Native Salesforce Integration
Purpose-built for Salesforce, MetaDefender for Salesforce integrates with your system in a few minutes.

Advanced Threat Detection
All files are scanned with up to 15 commercial anti-malware engines, which employ a combination of heuristics, machine learning, and signature-based detection methods. Multiscanning improves detection rates, reduces outbreak exposure times, and achieves a near-zero exposure rate.

Zero-day Threat Prevention
Using our Deep CDR technology, each file is disarmed and regenerated, ensuring only safe, clean and usable content reaches your systems. Deep CDR supports 130+ file types, including PDFs, archives, and most common office documents.

Data Loss Prevention
Prevent potential data leaks and regulatory compliance violations by detecting and blocking sensitive, out-of-policy, and confidential data in files and emails.

Cloud Scalability
Whether your users upload one file or hundreds, our high-performance cloud architecture allows you to scale to any volume of usage as your requirements change.

Regulatory Compliance
A dynamic dashboard provides complete visibility, real-time reports, and management tools from one interface, which helps meet requirements for PCI DSS, HIPAA, NIST as well as standard audits.

Features

Metascan™	Uses 30+ leading anti-malware engines to proactively detect over 95% of file-based threats for the highest and earliest detection of malware.
Deep CDR™	Scans, sanitizes, and regenerates over 200 common file types uploaded to the Salesforce environment, ensuring maximum protection against file-based attacks.
Adaptive Sandbox	Detects and analyzes malware by exposing and recording malicious behavior in an emulated environment. The Adaptive Sandbox runs 10x faster and 100x more efficiently than a conventional sandbox.
Proactive DLP™	Detects and blocks sensitive, out-of-policy, and confidential data within files and emails. Supporting over 110+ file types, including Microsoft Office, PDF, CSV, HTML and image files.
Reputation Service	Automatically scans URLs, IPs, domains, and Salesforce record content to classify risk and provide immediate visibility into potential threats across your Salesforce environment.
Private Scanning	Analyzes user-submitted files without exposing their content. After the analysis, files are deleted from OPSWAT servers.
Large File Scanning	Scans and processes files larger than 10MB.
Rescan on Download	Provides an additional layer of security for users when downloading files.
Rescan on Demand	The option to rescan uploaded files on demand, based on a selected response, providing more control over flagged files or re-checks.
Skip Scanning	A configuration to define what file extensions (based on the file name) can be skipped. Available for certain file types.
Email Body Scanning	Ability to scan the incoming emails within Salesforce.
Advanced File Scan Capabilities	Cover file content, email body text, and attachments, further protecting against malicious content.
Profile-based Security Assessment	Allows administrators to classify profiles and designate files from untrusted profiles for security processing.
Flexible Administration Permissions	Ensure role-based access for additional security.
Infected File Notifications	Sent in-app and via email to ensure administrators are immediately informed of any infected files.
Centralized Control and Visualization Report	Provides a dynamic dashboard with complete visibility, real-time reports, and management tools in one interface.

07

OPSWAT Support and Pricing Notes

- Minimum term is twelve months.
- Prices are quoted per defined term and are exclusive of VAT.
- Support costs are charged at 15 percent for Silver, 20 percent for Gold, or 25 percent for Platinum, calculated on the Annual Software Price for the term.
- The supplier reserves the right to increase the service price if the GBP/USD exchange rate changes by five percent or more.
- Pricing is based on a USD/GBP exchange rate of 0.74
- All pricing is subject to an annual cost adjustment of up to fifteen percent when purchased on an annual basis.

	Silver	Gold	Platinum
Support Hours			
Support via OPSWAT Portal Case Management System	**7AM to 7PM** (business days)	**24 hours** (business days)	**24 x 7 x 365**
Support via Chat	**7AM to 7PM** (business days)	**24 hours** (business days)	**24 hours** (business days)
Support via Phone	Not included	**24 hours** (business days)	**24 x 7 x 365**
Incident Response Times			
First Response Times for Blocker Severity Issues	Within 4 hours*	Within 2 hours*	Within 1 hours
First Response Times for Blocker Lower Issues	Within 3 business days	Within 2 business days	Within 1 business day
Hardware and Appliance Warranty**			
Advanced Replacement Warranty	Warranty Sold Separately	Warranty Sold Separately	Warranty Sold Separately
Customer Success Management			
Assigned Customer Success Manager	✕	✕	✓
Quarterly Conference Call Reviews	✕	✕	✓
Yearly Roadmap Review with the Product Team	✕	✕	✓
Quarterly Summary Reports	✕	✕	✓

During the hours covered in that support plan (*)

See our Hardware and Appliance Warranty section below (**)

GET STARTED

Are you ready to put Cloud Security 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 1,900 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.