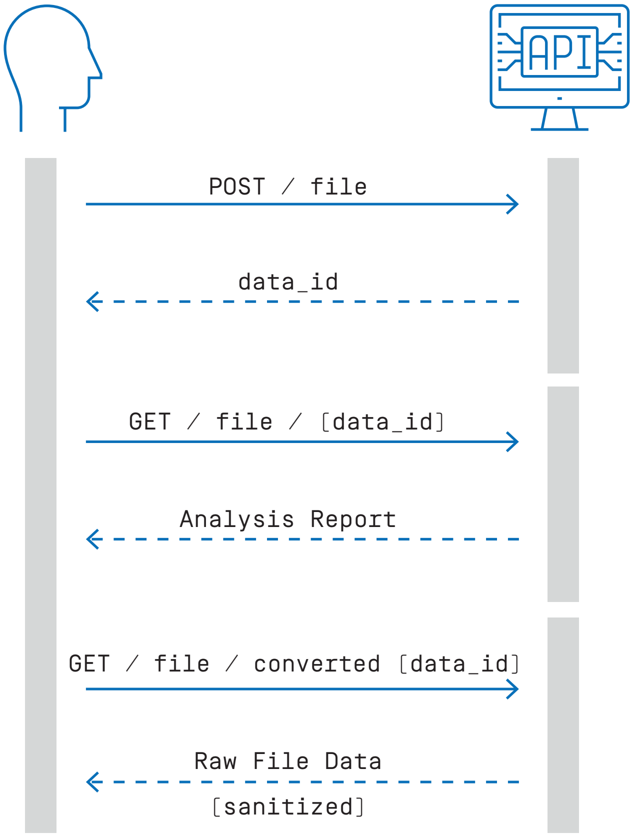
OPSWAT.

MetaDefender® API

Advanced Threat Prevention Development Platform

MetaDefender API allows you to integrate advanced malware protection and detection into your IT solutions and applications. MetaDefender provides industry leading multi-scanning, data sanitization, and vulnerability scanning to prevent known and unknown threats including, ransomware and zero-day attacks. Using our REST API, you can easily add detection and prevention of cyber security threats using data sanitization and more than 30 anti-malware engines. In addition, our large and growing vulnerability database allows you to find vulnerabilities in installers, binary files and Internet of Things (IoT) firmware.

MetaDefender API is used by Independent Software Vendors (ISVs) and malware researchers to enhance their existing solutions, and by IT Administrators to add advanced threat prevention to their systems to include malicious file upload protection.



Benefits

Multi-Scanning - Scan with over 30 anti-malware engines using signatures, heuristics, and machine learning technology for the highest and earliest detection of known and unknown threats.

Data Sanitization (CDR) – Disarm over 30 common file types, and reconstruct each file ensuring full usability with safe content.

Vulnerability Scanning – Detect known vulnerabilities in over 15,000 software applications using over 1 billion hashes.

> *“We evaluated sandboxes, AV vendors and cloud multi-scanning vendors for our zero-day malware file upload challenge and chose Data Sanitization from OPSWAT.”*
>
> Teza Mukkavilli
> Head of Security, Upwork

MetaDefender API Features

Data Sanitization (CDR) - Disarm over 30 common file types, and reconstruct each file ensuring full usability with safe content.

Multi-scanning - Choose from over 30 leading anti-malware engines in flexible package options. Third party anti-malware licenses are included.

Vulnerability Scanning - Scan binaries and installers to detect known application vulnerabilities before they are executed on endpoint devices, including IoT devices.

Archive Handling - Leverage improved, high performance detection of malware in compressed files and prevent archive bombs by extracting files and scanning them individually.

File Type Verification - Verify over 4500 File types to combat spoofed file attacks.

REST API - Use almost any programming language to leverage MetaDefender technology.

100+ File Conversion Options - Keep files usable and intact through true "reconstruction" of file types or flatten files to less complex formats.

Workflow Engine - Create your own workflow for multi-scanning and data sanitization (CDR) and customize the order and process in which files are handled.

Deployment Platforms - Deploy on Windows or Linux servers in your environment, even if it is air-gapped, or in our cloud using metadefender.com.

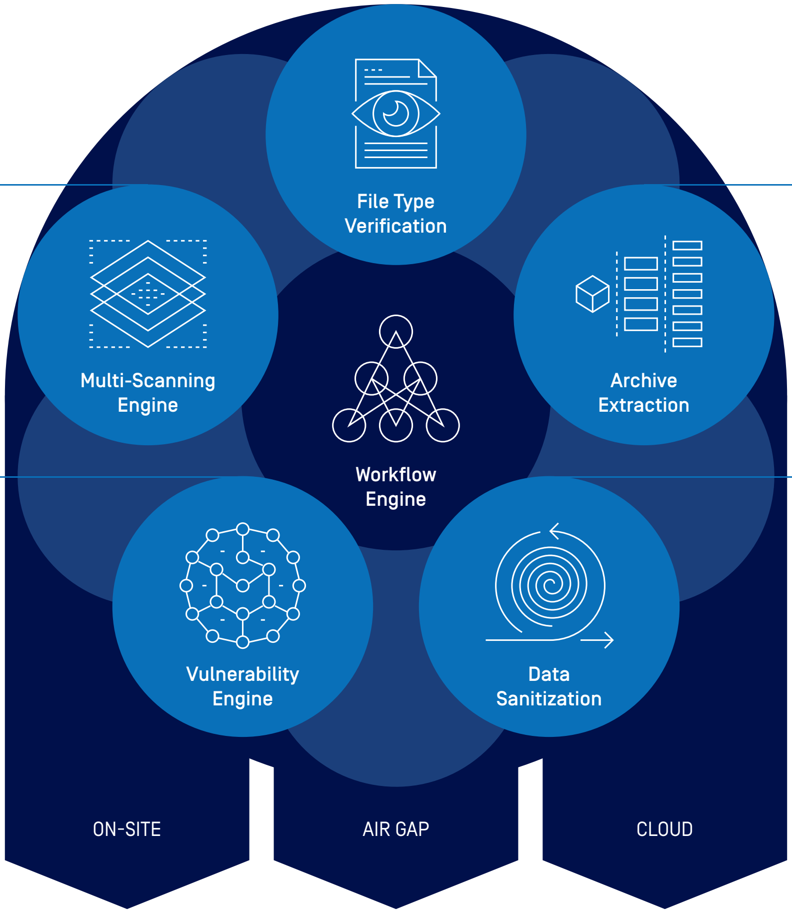
MetaDefender Architecture

30+
ANTI-MALWARE ENGINES

AhnLab
Symantec
nProtect
Kaspersky
McAfee
F-Prot
ESET
Bitdefender
AVG
LavaSoft
Zillya
Total Defense
Sophos
Quick Heal
Cyren
Trend Micro
Ikarus
Avira

15,000+
APPLICATIONS SUPPORTED

Adobe
Excel
Java
Powerpoint
Skype
Word



30+
SUPPORTED ARCHIVES

AR
ARJ
CAB
CHM
CPIO
CRAMPS
DMC
EXT
FAT
CPT
HFS
IHEX
ISO
LZH
LZMA
MBR
MSI
NSIS
NTFS
QCOW2
RAR
RPM
UDF
UEFI
VDI
VHD
and more...

30+
SUPPORTED FILE TYPES

DOC
DOCX
HTML
JPG
PDF
PPT
PPTX
XLS

OPSWAT.
Trust no file. Trust no device.

www.opswat.com