OPSWAT.

DATASHEET

Filescan Sandbox

Rapid. In-depth.

Why Filescan Sandbox?

The OPSWAT Filescan Sandbox integrates a wide range of state-of-the-art tools, services, and proprietary engines to identify Indicators of Compromise (IOCs) and quickly extract threats from files, documents, scripts, and URLs at scale. Using proprietary engines, it goes deeper than traditional static analysis tools providing actionable intelligence in a wide range of scenarios. With exceptional speed, it effectively minimizes the number of artifacts to sandbox, thus streamlining the otherwise time-consuming and resource-intensive process.

Filescan Sandbox employs a cutting-edge emulation engine capable of quickly deobfuscating and analyzing state-of-the-art, environment-aware malware in under 15 seconds. Additionally, it automatically cross-references any relevant Indicators of Compromise (IOCs), such as second stage, downloaded files or URLs, with comprehensive threat intelligence databases for accurate identification.

It integrates into diverse platforms and corporate systems through its straightforward RESTful HTTP-based API and open, agile architecture. The on-premises instance only requires a single server to enable the immediate processing of thousands of files and URLs per day. The web interface provides user-centric reports that are easy to understand and contain in-depth data.

Verified Technology

We are confident about our technology and actively seek feedback from users. As part of this effort, we operate a free community service at www.filescan.io, which undergoes rigorous scrutiny through thousands of daily scans. Our commitment to field testing against emerging malware and phishing threats creates a relevant and robust solution.

As passionate researchers, we frequently experiment with cutting-edge technology on the community platform, enabling us to adapt to the latest cybersecurity trends quickly— after thorough testing and validation, our technology transitions into our enterprise-grade commercial product.

Visit the OPSWAT Filescan documentation to learn more about integration and customization options.

Key Features

- Extract Indicators of Compromise (IOCs) from a wide range of executables, documents, scripts, and URLs.
- Emulates 90%+ of highly obfuscated state-of-the-art macro malware (VBA), VBS, PowerShell, Jscript, MSHTA, XSL, WSF.
- Improve detection of unknown malware with ML-powered Threat Intelligence Similarity Search.
- Simple and cost-effective, on-premises standalone deployment or private cloud.
- Rapid & deep analysis at a large scale (25K+ scans per day/ machine).
- REST API for automated integration and Single source of truth reputation endpoint.
- Single source of truth reputation endpoint
- Integrates with MetaDefender Core, MetaDefender Cloud, Palo Alto Cortex XSOAR, Splunk SOAR, VirusTotal, YARA, MITRE ATT&CK framework and more
- Clean and intuitive reports with in-depth data on demand and able to export in HTML, PDF, MISP, STIX.
- Designed, engineered, and maintained by experienced experts.

Example Hardware Setup

- Intel Xeon-E 2136 (12M Cache, 3.30 GHz)
- RAM 32GB DDR4 ECC 2666 MHz
- 2x SSD NVMe 256GB RAID

Note: this is an example system that would allow processing 25K files/ day with a retention period of 10 days.

Minimal Technical Requirements

- Ubuntu Server 20.04 LTS ("Focal Fossa")
- 8 vCPUs (Preferably 16 vCPUs)
- 16GB RAM (Preferably 32GB)
- 32 GB SSD Disk Space

Throughput / Hardware Requirements

The following table lists explanatory system specs with a retention period of 10 days:

Scans Per Day	Required System CPUs	Required System RAM	Required Storage per Retention Period
1000	4	4GB	256GB
2500	4	4GB	256GB
5000	4	4GB	256GB
10000	8	8GB	256GB
25000	16	16GB	256GB

Get in Touch

Start your free trial of Filescan at our community platform today. Need more privacy and want to learn about our on-premises offering? Please get in touch at sales@filescan.com.

OPSWAT.

Filescan Sandbox

Sandbox Engine Features	Filescan	Vendor A	Vendor B	Vendor C	Vendor D
Render URLs and Detect Phishing Sites	✓	✓			
Extract and Decode Nearly All Malicious VBA Macros	✓		✓		
Analyze VBA Stomped Files Targeted for Any System	✓				
Shellcode Emulation (x86, 32/64)	✓				
Export MISP (JSON) and STIX Report Formats	✓		✓		
Extract and Analyze Embedded PE Files	✓				
Deobfuscate Javascript/VBS	✓		Limited		
Deobfuscate Powershell Scripts	✓		Limited		
Deobfuscate MSHTA Scripts	✓				
Parse METF Embed Equation Exploit Structure	✓				
Parse Malformed RTF Files	✓				
Parse Office Binary File Formats (BIFF5/BIFF8)	✓				
Parse Strict OOXML File Format	✓				
Automatically Decode Embedded Base64 Strings	✓				
Extract Annotated Disassembly	✓				
Decrypt Password Protected Office Documents	✓		✓		
Decompile Java	✓		✓		
Decompile .NET	✓		✓		
Calculate .NET GUIDs (Module Version/TypeLib Id)	✓	✓			
Classify Imported APIs	✓			✓	
MITRE ATT&CK Support (In-report and Search)	✓		✓	✓	
Render PDF Pages	✓	✓	✓		
Extract Embedded Files (eg: OLE2 from Word)	✓	✓	✓		
Automatically Tag Samples Based on Signatures	✓	✓	✓		
YARA Support	✓	✓	✓		✓
Generate Text Metrics (Average Word Size, etc.)	✓				
Detect Cryptographic Constants	✓				✓
Text Analysis (Guessed Language)	✓	✓			

OPSWAT.

Filescan Sandbox

DATASHEET

Sandbox Engine Features	Filescan	Vendor A	Vendor B	Vendor C	Vendor D
Map UUIDs to Known Associated Files / Metadata	✓		Limited		
Filter Strings and Detect Interesting Ones	✓		✓	✓	
Extract and Detect Overlay	✓			✓	✓
Integrated Allowlist	✓	✓	✓		
Detect Alternative IOCs (Emails, Bitcoin Address, etc.)	✓		✓		✓
Calculate Authentihash	✓	✓	✓		
Verify Authenticode Signatures	✓	✓	✓	✓	
Parse RICH Header	✓	✓	Limited	✓	✓
Calculate Entropy of Resources	✓	✓		✓	✓
Detect URLs, Domains and IP Addresses	✓	Limited	✓	✓	✓
Calculate Hashes of Resources	✓	✓		✓	✓
Calculate Imphash	✓	✓	✓		✓
Calculate SSDEEP	✓	✓	✓		✓
Extract PDB Information	✓	✓	✓	✓	
Detect TLS Callbacks	✓		✓	✓	✓
Resolve Known Import Ordinals to Names	✓		✓	✓	✓
Detect Anomalies (eg: Header Checksum Validation)	✓	Limited	✓	✓	✓
Query VirusTotal and MetaDefender Cloud for Reputation Checks	✓	✓	✓	✓	✓
Detect Packers (PEiD)	✓	✓	✓	✓	✓
Detect File Types	✓	✓	✓	✓	✓
Calculate Hashes of Sections	✓	✓	✓	✓	✓
Calculate Entropy of Sections	✓	✓	✓	✓	✓
Extract Strings from Executable	✓	✓	✓	✓	✓
Extract/Detect Resources	✓	✓	✓	✓	✓
Extract/Detect PKCS7 Certificate	✓	✓	✓	✓	✓