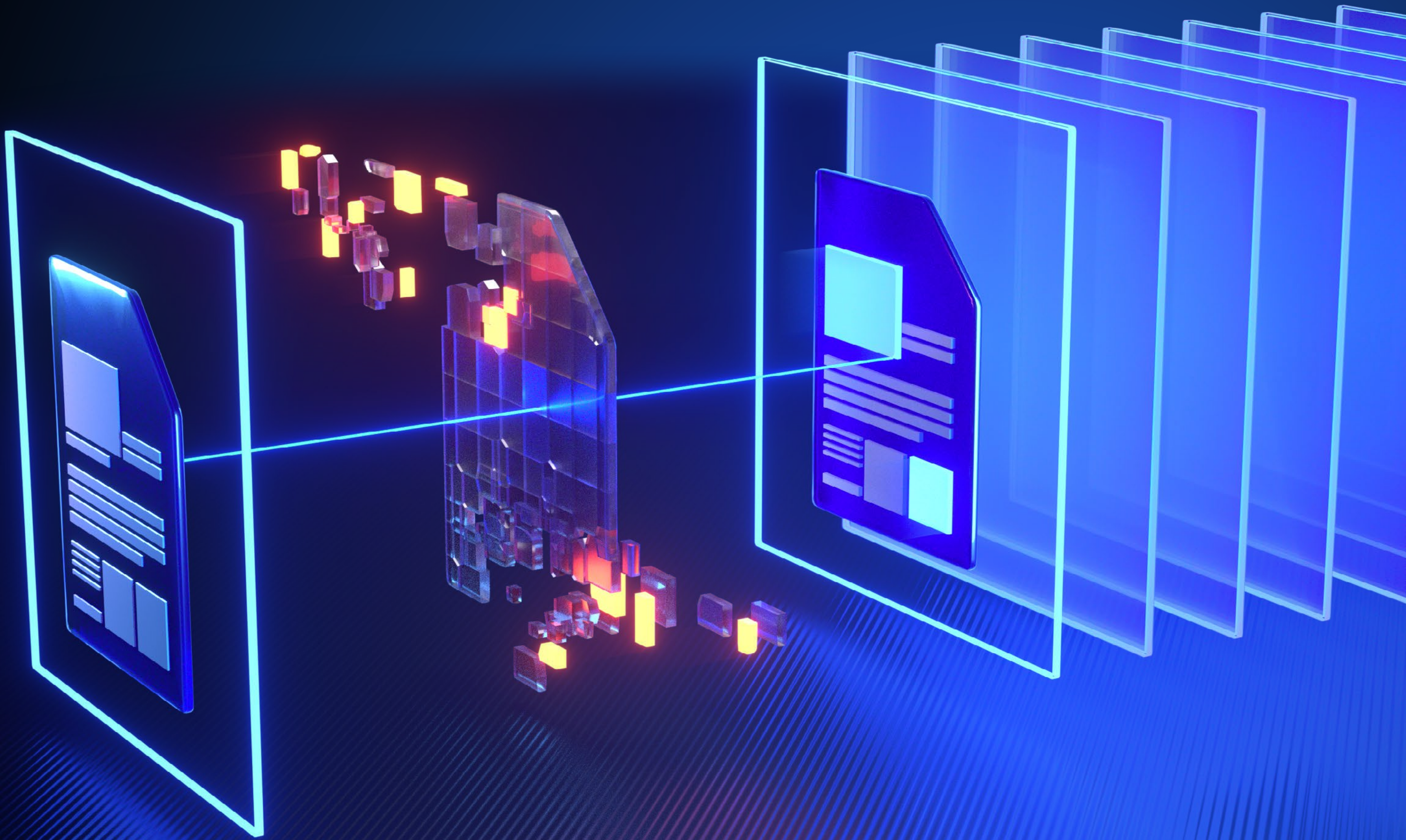
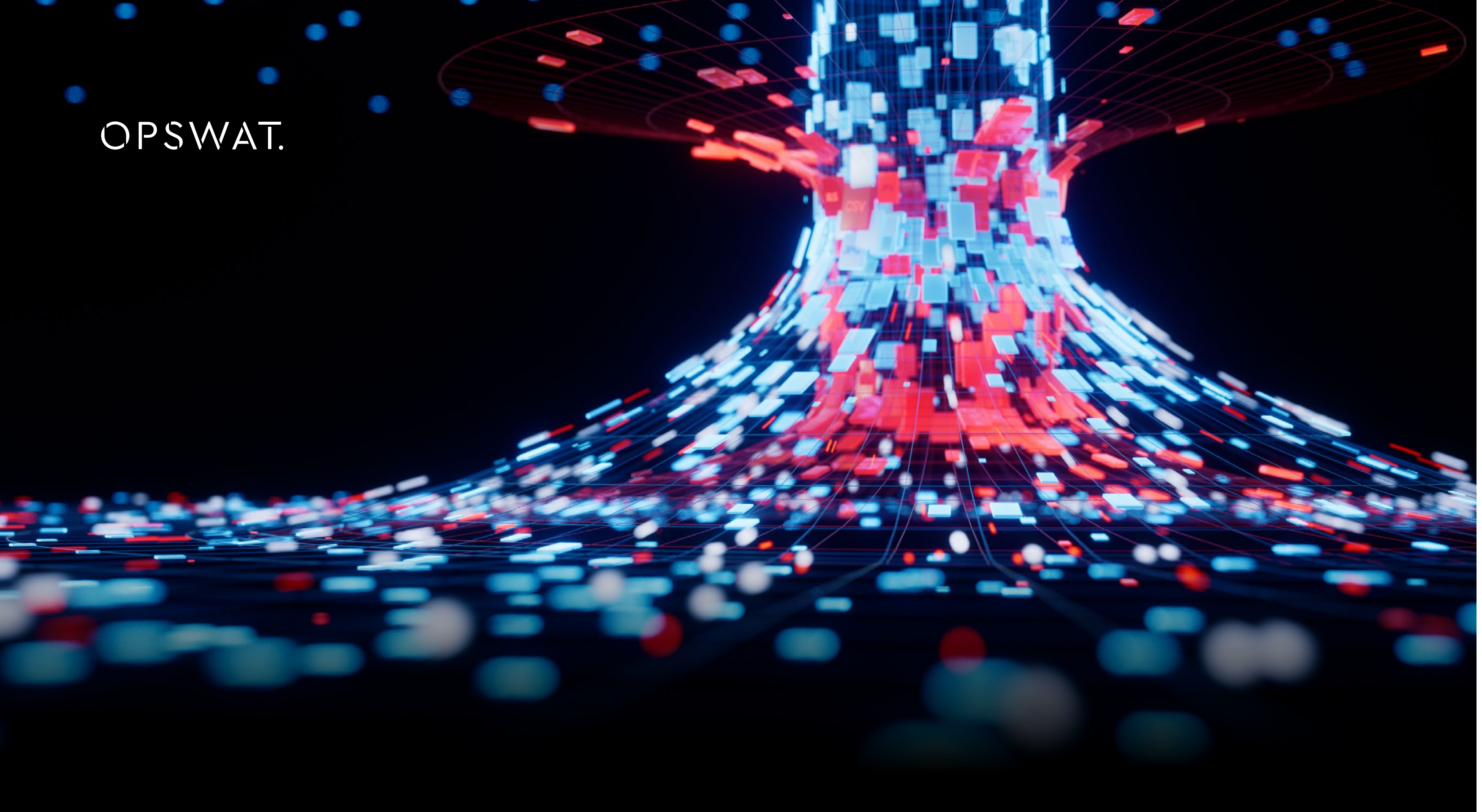
OPSWAT.

# Deep CDR™

File Regeneration that Protects from Evasive Malware and Zero-Day Exploits



Protecting the World's Critical Infrastructure



Detection-based technologies, including anti-malware engines and sandboxing, collectively provide important layers of protection. CDR strengthens this approach removing potentially harmful elements from files, supporting and enhancing these detection capabilities.

Deep CDR™ proactively disarms file-based threats and regenerates clean, usable files in milliseconds, extracting embedded scripts, macros, and out-of-policy content from 200+ file types and integrating seamlessly across your existing security stack.

## Key Challenges

**Undetected Threats**
Zero-day threats, targeted attacks, and evasive malware could bypass detection engines.

**Insufficient Protection**
AI, heuristic-based anti-malware, and traditional sandboxing detect anomalies but don't disarm malicious content.

**Productivity vs. Security Trade-offs**
Outright bans on macros and JavaScript may disrupt legitimate workflows.

**Incomplete Archive Scanning**
Traditional Security tools struggle to sanitize deeply nested archives and embedded file layers.

**Reactive Security Gaps**
Most tools act after compromise or block suspicious files without proactively regenerating clean, usable versions.

# Transforming File Security with Deep CDR

**Zero-Trust Security**
Enforces zero-trust at the file level, treating every file as potentially malicious, sanitizing and reconstructing it into a safe, usable version before it enters your environment.

**Proactive Threat Prevention**
Proactively removes threats before they can execute, neutralizing potentially malicious code, embedded threats, and zero-day exploits at the file level without relying on detection.

**High-Performance Security & Seamless Experience**
Delivers high-performance file sanitization in milliseconds, preserving file usability, integrating seamlessly into workflows, and offering tailored policies and flexible file conversion for efficiency without compromise.

- **200+** supported file types
- **200+** file conversion options
- **100%** Protection and Accuracy in SE Labs's Standalone CDR Test
- **100%** Rating in SecureIQ Lab's Content Disarm & Reconstruction Test
- Milliseconds to disarm and regenerate new, usable files **30x faster** than traditional sandboxing
- Recursively Scan Archives
- Tailored Security Policies

OPSWAT.

# How Deep CDR Works

1

## Identify & Scan

Verify file structure and identify all active embedded content in file

2

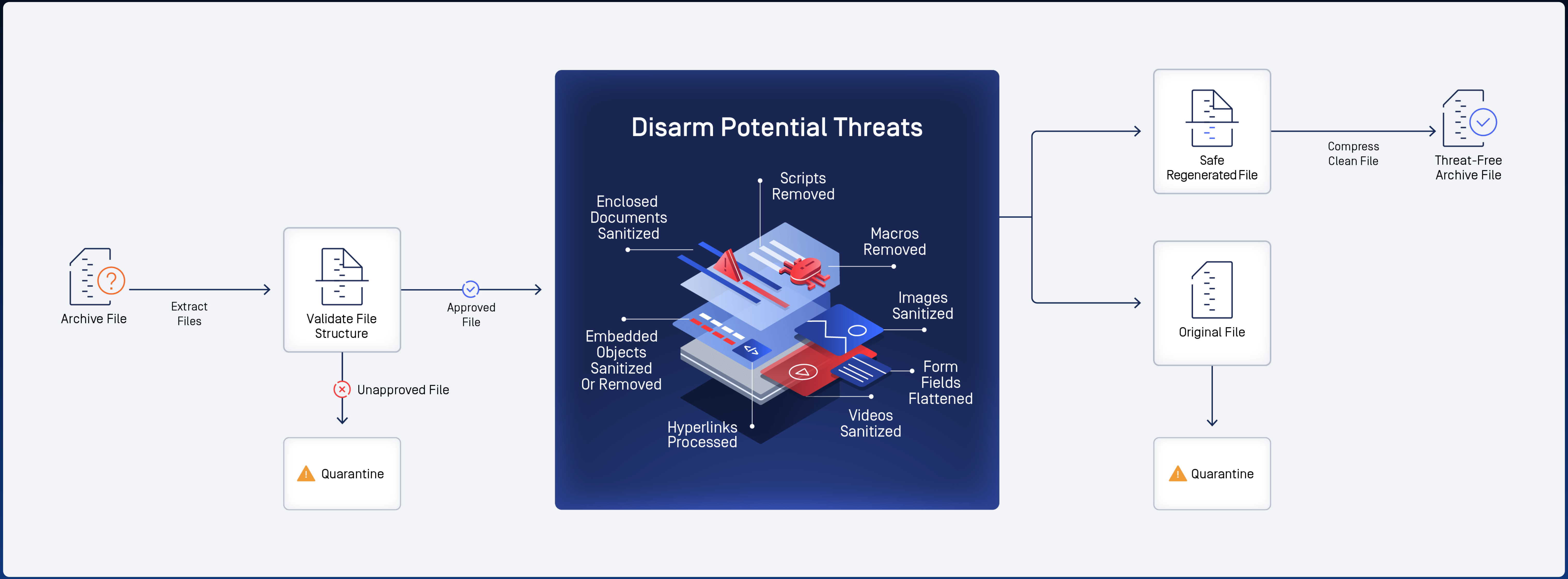
## Regenerate & Convert

Disarm all the potentially malicious content & regenerate file with safe components

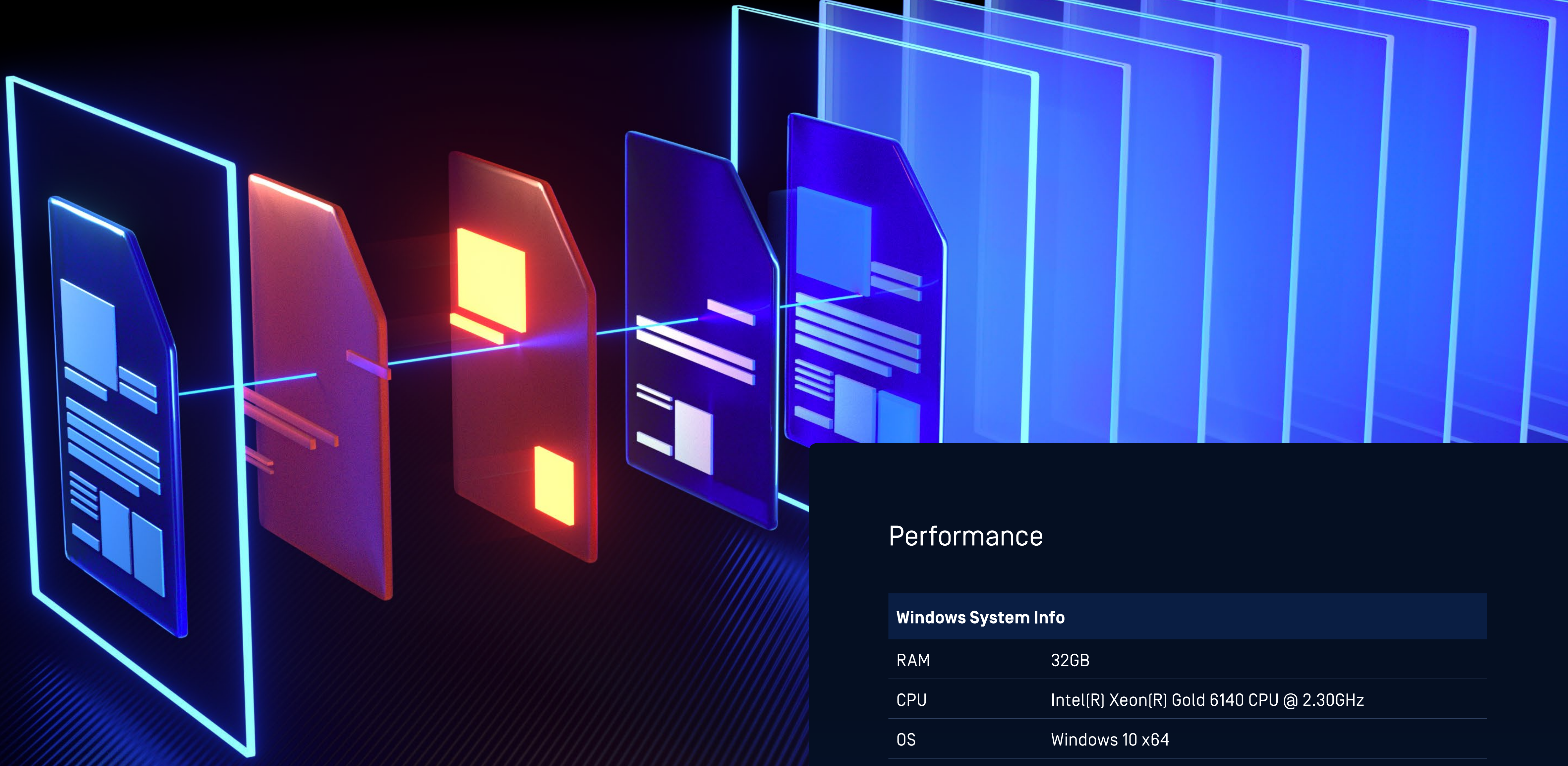
3

## Rebuild & Use

Generate threat-free file with full functionality & quarantine original file



OPSWAT.



## Key Features

**Threat Disarm**
Strips off all potentially harmful content - macros, scripts, embedded objects, and out-of-policy elements - from over 200 file types without relying on detection.

**File Regeneration**
Regenerates sanitized, safe files in milliseconds while preserving its structure and usability.

**File Structure Verification**
Performs deep inspection of objects inside the file to ensure they comply with official file specifications.

**Recursive Sanitization**
Recursively sanitizes deeply nested archive formats like ZIPs, PDFs and Office documents.

**Security Policy Tailoring**
Provides comprehensive configuration options that can be adjusted to meet different organizational requirements.

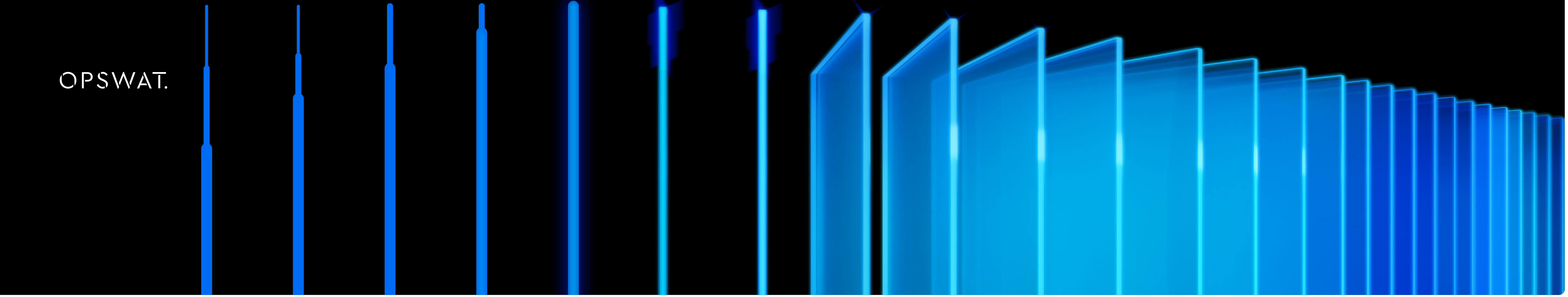
**Sanitization Details Report**
Provides forensic information about sanitized components, including the reason for action on risky objects.

**Seamless Integration**
Integrates effortlessly into existing workflows across email, web, file transfer, and endpoints.

**Customizable File Conversion**
Offers flexible file conversion options tailored to customer needs.

## Performance

| **Windows System Info** | |
|---|---|
| RAM | 32GB |
| CPU | Intel(R) Xeon(R) Gold 6140 CPU @ 2.30GHz |
| OS | Windows 10 x64 |
| Storage | 100 GB SSD |
| **Linux System Info** | |
| RAM | 32GB |
| CPU | 16 |
| OS | CentOS Linux release 7.6.1810 |
| Storage | 100 GB SSD |
| **Resources** | |
| MetaDefender Core™ version | v5.x Windows: MetaDefender Core v5.0.0 with 8 engines<br>v5.x Linux: MetaDefender Core v5.0.0 with 10 engines |
| Default Deep CDR configuration | Window version : 6.0.0.10522 |



## Benefits

| | |
|---|---|
| **Powerful** | Stops zero-day exploits, evasive malware, and targeted threats that traditional detection-based tools miss |
| **Efficient** | Provides safe, fully usable files instantly, maintaining productivity without delays |
| **Reliable** | Ensures file integrity and prevents embedded exploits through deep file structure verification |
| **Comprehensive** | Neutralizes threats embedded in multi-layered archives and complex file structures |
| **Tailored** | Adapts security enforcement to business policies |
| **File Structure Verification** | Performs deep inspection of objects inside the file to ensure they comply with official file specifications |
| **In-depth** | Enhances SOC visibility and auditability by delivering detailed sanitization reports |
| **Effortless** | Integrates seamlessly into existing workflows, minimizing operational overhead |
| **Flexible** | Offers customizable file conversions to match user needs and business processes |

## Test Results

| Conversion Type | Total File | Average File Size (KB) | Total Size (KB) | Average Time(s) Windows | Average Time(s) Linux |
|---|---|---|---|---|---|
| pdf2pdf | 700 | 840.608 | 428.672 | 0.612 | 0.371 |
| ai2ai | 500 | 1218.385 | 159.609 | 0.319 | 0.249 |
| docx2docx | 700 | 423.394 | 246.172 | 0.352 | 0.299 |
| dotx2dotx | 600 | 595.435 | 222.891 | 0.371 | 0.312 |
| docm2docm | 600 | 159.145 | 270.672 | 0.451 | 0.246 |
| dotm2dotm | 450 | 891.869 | 189.75 | 0.422 | 0.384 |
| xlsx2xlsx | 750 | 188.021 | 244.969 | 0.327 | 0.208 |
| xlsm2xlsm | 300 | 255.125 | 137.703 | 0.459 | 0.359 |

Get Started

# Are you ready to put Deep CDR on the front lines of your removable media security 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.