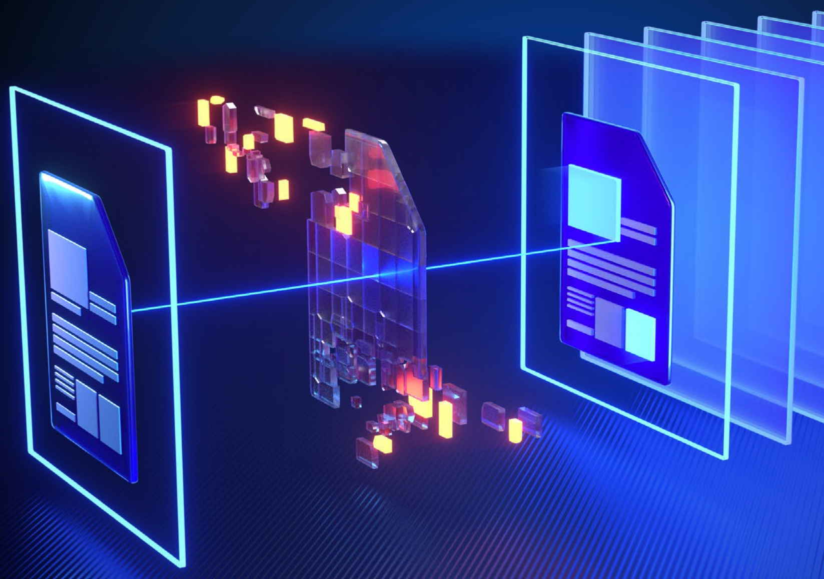
OPSWAT.

DATASHEET

Deep CDR™

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



Deep CDR is a file regeneration technology that proactively disarms file-based threats by reconstructing clean, usable files. It removes potentially harmful elements before files enter the environment, strengthening detection-based security against evasive malware and zero-day exploits.

Simple detection-based tools fail to disarm zero-day and evasive threats, disrupt productivity by blocking active content, and lack deep archive sanitization, leaving critical gaps in file security.

Key Features

Threat Disarm
Strips off all potentially harmful content (macros, scripts, embedded objects, and out-of-policy elements) from over 200 file types.

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

File Structure Verification
Performs deep inspection of objects 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.

Benefits

Powerful
Stops zero-day exploits, defeats advanced obfuscation techniques, including steganography, by removing potential threats at the file level.

Efficient
Disarms and regenerates clean, fully usable files in milliseconds.

Reliable
Removes threats from complex files while preserving structure, content integrity, and usability.

Comprehensive
Protects against out-of-policy and potentially malicious content, supporting a wide range of embedded objects beyond macros.

In-depth
Enhances SOC visibility and auditability by delivering detailed sanitization reports.

Operational Flexibility & Control
Aligns security enforcement with business policies, integrates seamlessly into existing workflows, and supports customizable file conversion to meet user and business requirements.

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 v5.x Linux: MetaDefender Core v5.0.0 with 10 engines
Default Deep CDR configuration	Window version : 6.0.0.10522

- **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 and Reconstruction Test
- Recursively Scan Archives
- Tailored Security Policies
- Milliseconds to disarm and regenerate new, usable files **30x faster** than traditional sandboxing

OPSWAT.
Protecting the World's Critical Infrastructure

opswat.com/get-started