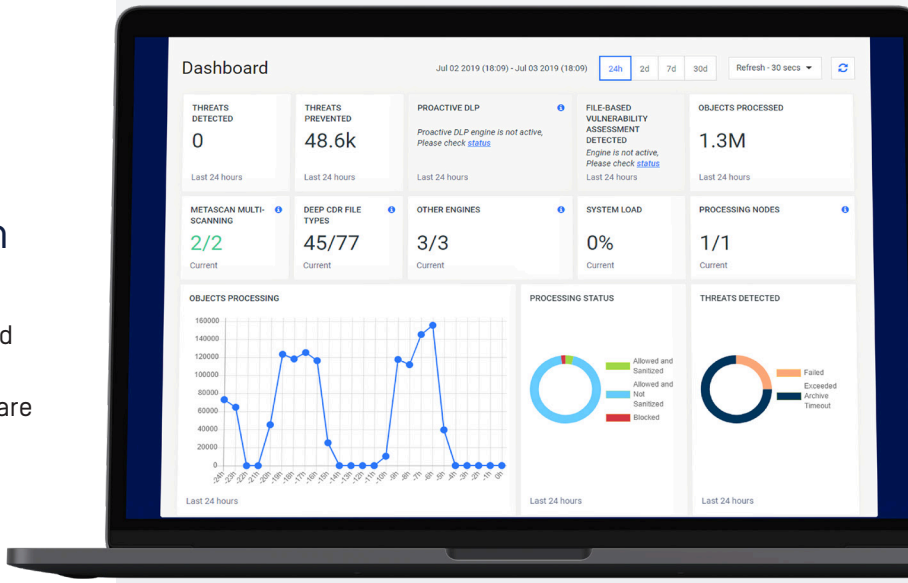
OPSWAT.

DATASHEET

MetaDefender® Core

Advanced threat prevention platform



No longer can your business rely solely on detection-based cybersecurity systems to provide adequate protection for your most valuable business assets, since zero-day malware learns how to bypass these defenses. Enterprises need to take more preventive approaches to combat advanced targeted attacks.

MetaDefender Core enables you to integrate advanced malware prevention and detection capabilities into your existing IT solutions and infrastructure for better handling common attack vectors: securing web portals from malicious file upload attacks, augmenting cybersecurity products, and developing your own malware analysis systems.

Benefits

- Mitigating risks for your critical systems and preventing threats that may have bypassed defenses
- Protection for sensitive personally identifiable information from entering or leaving your organization
- Easy deployment on Windows or Linux servers in your environment, even if air-gapped, or using our software-as-a-service offering via MetaDefender Cloud
- Support for many programming languages, for integration into your environment via REST API
- Low total cost of ownership with ongoing maintenance using centralized management

"We evaluated sandboxes, AV vendors and cloud multiscanning vendors for our zero-day malware file upload challenge and chose Deep Content Disarm and Reconstruction from OPSWAT."

Teza Mukkavilli

Head of Security, Upwork

OPSWAT.

MetaDefender Core

Key Features

Deep Content Disarm and Reconstruction (Deep CDR)

Rebuild over 80 common file types, ensuring maximum usability with safe content. Hundreds of file reconstruction options are available.

Multiscanning

Choose from over 30 leading antimalware engines in flexible package options. Proactively detects 99%+ of malware threats by using signatures, heuristics, and machine learning.

File-Based Vulnerability Assessment

Scan and analyze binaries and installers to detect known application vulnerabilities before they are executed on endpoint devices, including IoT devices

Proactive Data Loss Prevention (Proactive DLP)

Content-check 30+ common file types for personally identifiable information (PII) and redact or add watermark to this sensitive data before they are transferred.

100+ File Conversion Options

Keep files usable and intact through true "reconstruction" of file types or flatten files to less complex formats.

Custom Workflows

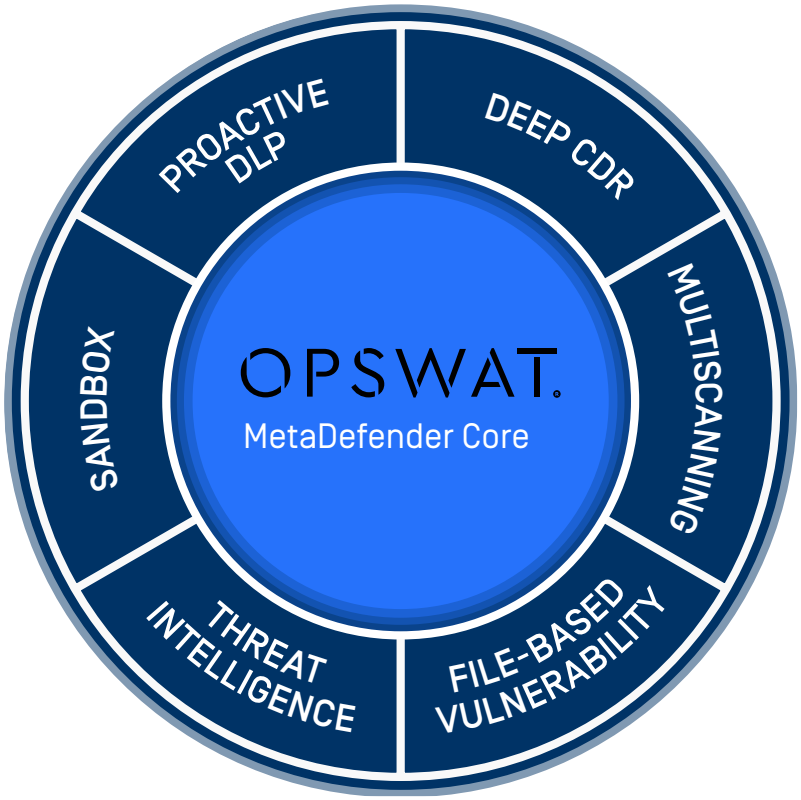
Create your own workflow for multiscanning and Deep CDR and customize the order and process in which files are handled.

Archive Extraction

Multiscanning and Deep CDR for more than 30 types of compressed files. Archive handling options are configurable, and encrypted archives are supported.

File Type Verification

Verify over 4,500 file types to determine the actual file type based on the content of the file, not the unreliable extension to combat spoofed file attacks.



OPSWAT protects critical infrastructure. Our goal is to eliminate malware and zero-day attacks. We believe that every file and every device pose a threat. Threats must be addressed at all locations at all times—at entries, at exits, and at rest. Our products focus on threat prevention and process creation for secure data transfer and safe device access.

The result is productive systems that minimize risks of compromise. That's why 98% of U.S. nuclear power facilities trust OPSWAT for cybersecurity and compliance.

For further information about MetaDefender Core visit opswat.com/products/metadefender/api

To contact a technical sales representative, please visit opswat.com/contact

OPSWAT.

Trust no file. Trust no device.