OPSWAT.

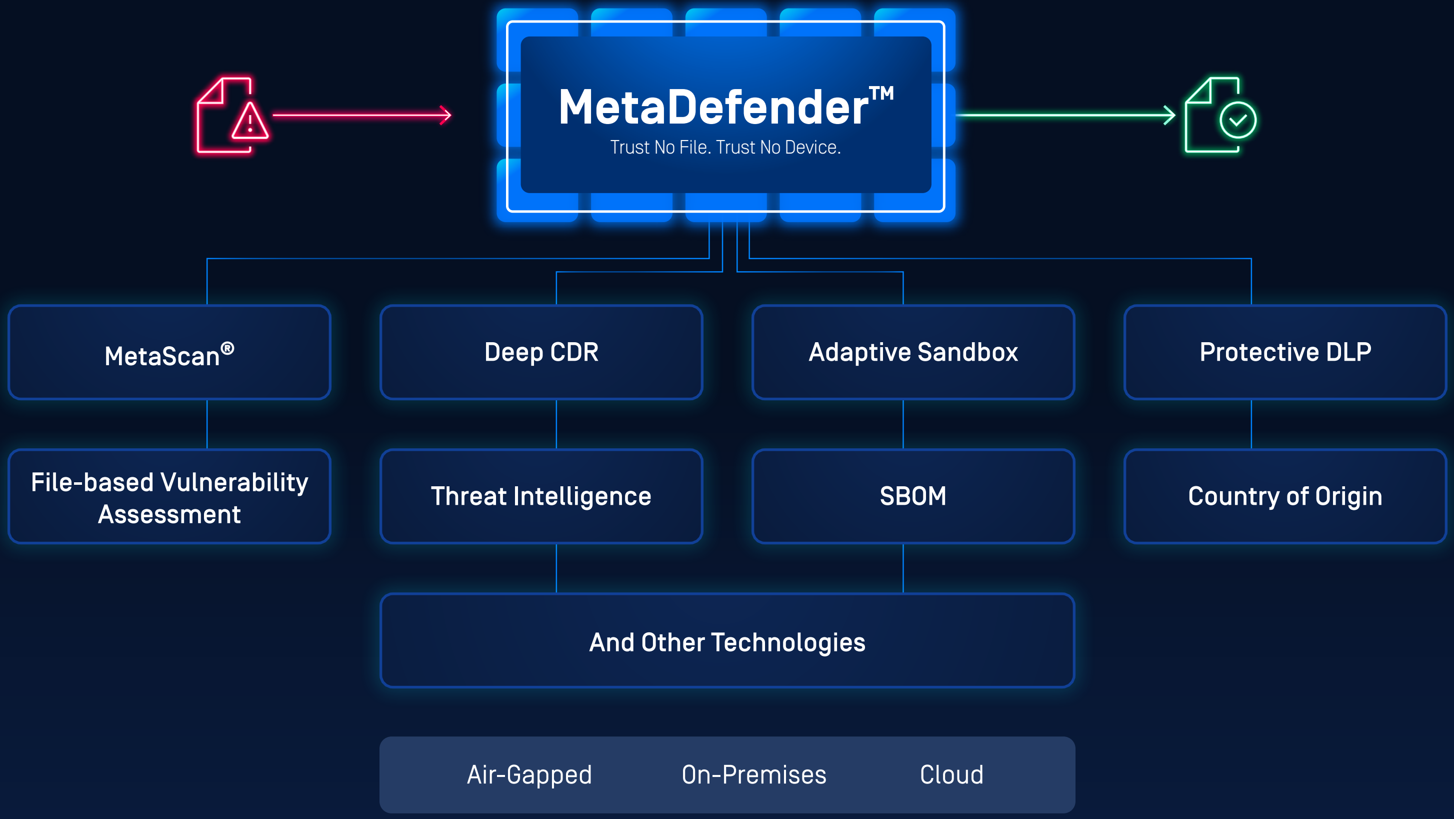
DATASHEET

MetaDefender™ Core

Advanced Threat Prevention Solution

With the growing threat of sophisticated, multi-layered, and zero-day attacks, business can no longer rely solely on detection-based cybersecurity systems to provide adequate protection for their most valuable business assets. Enterprises need to take more comprehensive and preventive approaches to combat advanced file-borne attacks.

MetaDefender Core integrates advanced malware prevention and detection capabilities into your existing IT solutions and infrastructure to handle common attack vectors by securing web portals from malicious file attacks, augmenting cybersecurity products, and developing malware analysis systems that adhere to company-specific policies.



MetaDefender™

Trust No File. Trust No Device.

MetaScan®

Deep CDR

Adaptive Sandbox

Protective DLP

File-based Vulnerability Assessment

Threat Intelligence

SBOM

Country of Origin

And Other Technologies

Air-Gapped

On-Premises

Cloud

Why MetaDefender™ Core

Risk Mitigation

Proactively safeguard critical infrastructure and prevent potential threats that may have slipped past conventional defenses.

Data Protection

Ensure the security of sensitive data and confidential information by securing files in transit or at rest from file-borne attacks.

Versatile Deployment

Easily deploy on Windows or Linux servers within your environment, including air-gapped networks, or opt for our SaaS solution through MetaDefender Cloud.

Seamless Integration

Seamlessly integrate into your existing environment with support for multiple programming languages via REST API.

Cost-Effective Maintenance

Achieve low total cost of ownership (TCO) with centralized management for ongoing maintenance, saving valuable resources.

Flexible Containerization

Simplify integration and maintenance with flexible deployment in containerization environments, reducing TCO, addressing potential conflicts from hidden dependencies, and enabling scalability across various platforms and operating systems.

Key Features

Prevent Zero-Day and Advanced Evasive Malware

Deep CDR (Content Disarm and Reconstruction) is a preventative technology that removes potentially malicious content from over 150+ file types. It validates, disarms, and regenerates safe-to-use files, eliminating advanced threats like APTs, zero-day attacks, and obfuscated malware before delivery.

Achieve Over 99% Threat Detection Accuracy

Multiscanning technology leverages 30+ leading anti-malware engines to proactively detect over 99% of malware threats. It combines signatures, heuristic analysis, and machine learning to identify file-borne threats.

Detect Application and File-Based Vulnerabilities

File-Based Vulnerability Assessment technology scans and analyzes binaries and installers to detect known application vulnerabilities before they are executed on endpoint devices, including IoT devices.

Adaptive Threat Analysis

Adaptive Sandbox is an emulation-based sandbox featuring threat agnostic analysis of files and URLs, identifying actionable indicators of compromise (IOCs) for incident response.

Prevent Regulatory Compliance Violations & Detect Adult Content

Proactive DLP (Data Lost Prevention) prevents sensitive and confidential information in 110+ file types from leaving or entering the company's systems by content-checking files before they are transferred. This helps enterprises meet regulatory requirements like HIPAA, PCI-DSS and GDPR. Proactive DLP also detects adult content in images and offensive language in text using OCR, machine learning and AI technologies.

100+ File Conversion Options

Use the file type conversion functionality to flatten files to fewer complex formats.

Generate SBOM (Software Bill of Materials)

Generating SBOMs secures software supply chains by providing comprehensive component inventories for source code and containers.

Workflow Engine

Create multiple workflows to handle different security policies based on users and file sources.

Archive Extraction

Scan over 30 types of compressed files. Archive handling options are configurable, and encrypted archives are supported.

File Type Verification

Determine the actual file type based on the content of the file, not unreliable extensions, which can easily be spoofed.

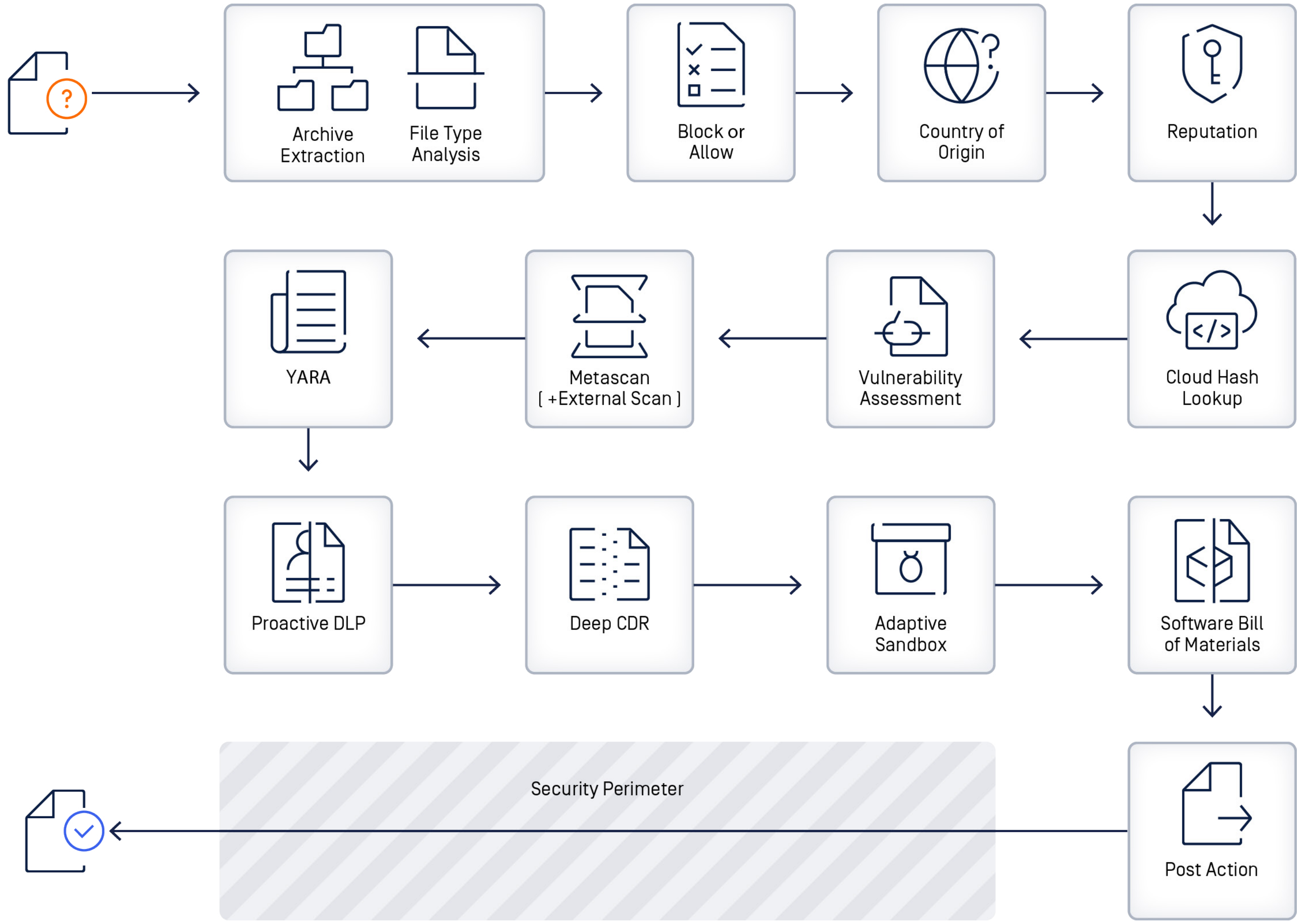
Faster False Positives Remediation

Reputation Engine matches file hashes against database of known good and bad files and leverages advanced analyses to remediate false positives faster.

Country of Origin

Detect the geographic source of uploaded files including PE, MSI, and self-extract file types. By analyzing digital fingerprints and metadata, it can identify restricted locations and vendors. This enables automated filtering that blocks unauthorized access to sensitive data while ensuring compliance with data regulations across regions.

MetaDefender™ Core Workflow



Ready to integrate MetaDefender Core with your cybersecurity strategy?

OPSWAT.

Protecting the World's Critical Infrastructure

Talk to one of our experts today.

Scan the QR code or visit us at:
opswat.com/get-started
sales@opswat.com