

# OPSWAT.

## MetaDefender<sup>®</sup> Core

Advanced threat prevention platform

Để bảo vệ cơ sở hạ tầng công nghệ thông tin (CNTT) – tài sản giá trị nhất của mỗi doanh nghiệp, bạn không thể chỉ phụ thuộc vào các công cụ phòng chống mã độc bằng phương pháp nhận diện các mẫu đã biết (Signatures) hay những hành vi đặc trưng của virus, bởi các mã độc zero-day và các loại mã độc khác hẳn nhiên được thiết kế để lẩn tránh các bộ lọc bảo mật truyền thống này. Các doanh nghiệp cần một giải pháp an ninh tiên tiến gồm đa phương thức phòng chống các cuộc tấn công mạng.

MetaDefender Core giúp bạn tích hợp nền tảng phát hiện và ngăn chặn mã độc tiên tiến hàng đầu thế giới vào các giải pháp và cơ sở hạ tầng CNTT hiện có của doanh nghiệp, để xử lý hầu hết các vấn đề an ninh mạng phổ biến như: bảo vệ website khỏi các cuộc tấn công bằng tập tin độc hại, tăng cường hiệu quả của các sản phẩm an ninh mạng và hệ thống phân tích mã độc hiện có của bạn.

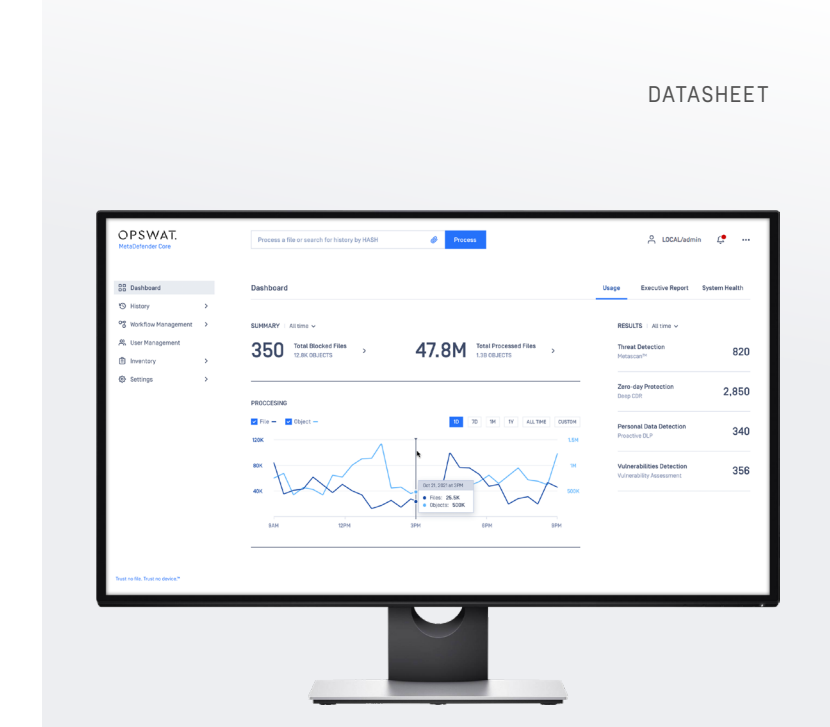
### Tính Năng và Lợi Ích Chính

**Công Nghệ Làm Sạch và Tái Lập Nội Dung Chuyên Sâu (Deep CDR)**  
Giúp làm sạch và tái cấu trúc hơn 130 loại tập tin phổ biến, trong khi đảm bảo tối đa tính khả dụng và nội dung an toàn. Cung cấp hàng trăm lựa chọn tái lập tập tin để chuyển đổi các tập tin thành các định dạng phổ biến và tiện lợi hơn khi sử dụng.

**Công Nghệ Nâng Cao Nhận Dạng Mã Độc Với Đa Ứng Dụng Xử Lý (Multiscanning)**  
Bạn có thể lựa chọn sử dụng hơn 30 chương trình nhận dạng mã độc hàng đầu hiện nay với nhiều gói sản phẩm linh hoạt. Nhanh chóng phát hiện hơn 99% mã độc bằng các phương pháp nhận diện mẫu mã độc, phân tích hành vi đặc trưng của virus và máy học.

**Hơn 100 Tùy Chọn Chuyển Đổi Tập Tin**  
Giữ nguyên tính khả dụng của tập tin thông qua quá trình tái cấu trúc tập tin hoặc chuyển đổi tập tin thành các định dạng dễ sử dụng hơn.

**Công Nghệ Chủ Động Ngăn Chặn Rò Rỉ Dữ Liệu (Proactive DLP)**  
Rà soát và ngăn chặn nội dung nhạy cảm trong hơn 70 loại tập tin phổ biến trước khi chúng được chuyển đi.



“Chúng tôi đã đánh giá kỹ lưỡng nhiều nhà cung cấp giải pháp bảo mật, bao gồm sandbox hay các chương trình nhận dạng mã độc ngay cả với môi trường đám mây, để giúp công ty chúng tôi đối mặt với các cuộc tấn công zero-day bởi các tập tin độc hại. Cuối cùng, chúng tôi tin chọn công nghệ làm sạch và tái lập nội dung chuyên sâu (Deep CDR) từ OPSWAT”

Giám đốc an ninh, Upwork

**Công Nghệ Đánh Giá Lỗ Hổng Bảo Mật Của Tập Tin (Vulnerability Assessment)**  
Quét các tập tin nhị phân và trình cài đặt để phát hiện các lỗ hổng bảo mật của ứng dụng trước khi chúng được thực thi trên các thiết bị đầu cuối, bao gồm cả các thiết bị trong môi trường vạn vật kết nối Internet (IoT).

**Tùy Chỉnh Quy Trình**  
Bạn có thể tự thiết kế quy trình hoạt động cho Multiscanning và Deep CDR để phù hợp với nhu cầu của doanh nghiệp, cũng như có thể tùy chỉnh thứ tự và quy tắc xử lý tập tin đối với từng đối tượng sử dụng, nguồn tập tin và loại tập tin.

**Giải Nén Tập Tin**  
Công nghệ Multiscanning và công nghệ Deep CDR khả dụng với hơn 50 loại tập tin nén phổ biến. Bạn có thể cấu hình các cách xử lý tập tin nén, và tập tin nén với mật khẩu cũng được hỗ trợ xử lý.

**Xác Minh Loại Tập Tin**  
Xác minh hơn 4500 loại tập tin nhằm chống lại các cuộc tấn công bằng tập tin giả mạo.

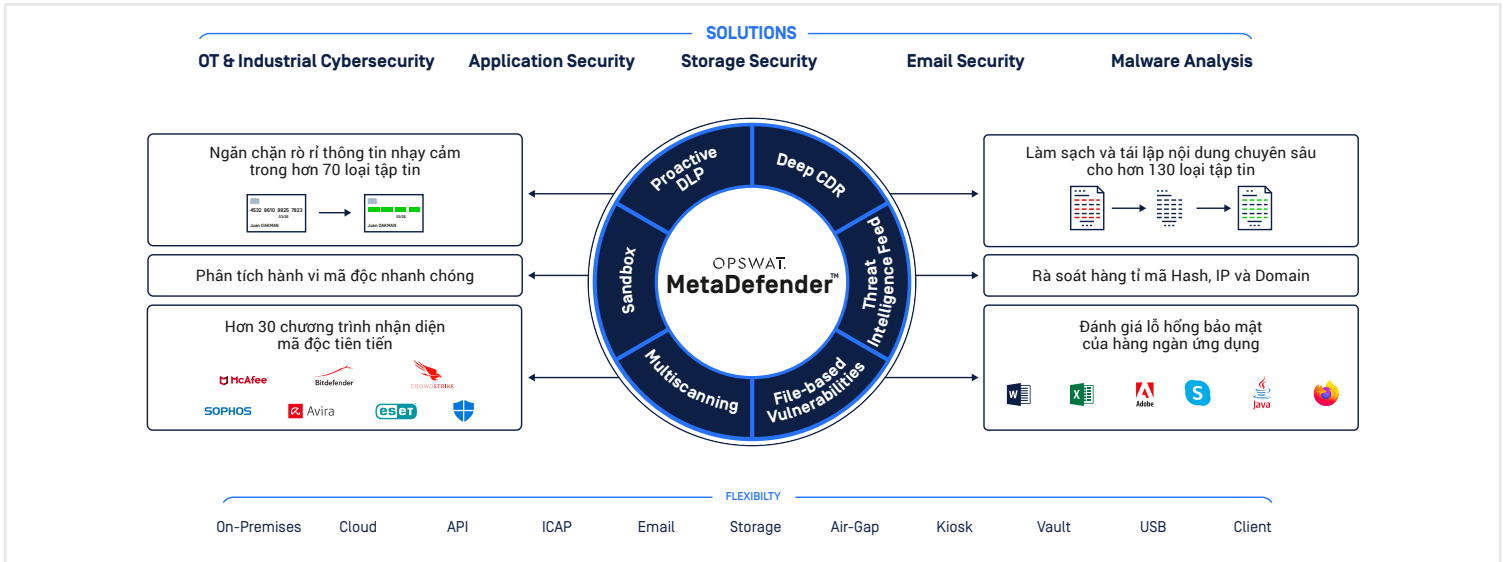
OPSWAT.

Trust no file. Trust no device.

OPSWAT.com

# OPSWAT.

## MetaDefender Core



## Tại Sao Nên Sử Dụng MetaDefender® Core

- Giảm thiểu rủi ro cho các cơ sở trọng yếu của bạn.
- Ngăn chặn các mã độc tinh vi có thể vượt qua các lớp phòng thủ an ninh của doanh nghiệp.
- Ngăn chặn các dữ liệu nhạy cảm ra vào hệ thống của doanh nghiệp.
- Dễ dàng triển khai trên các máy chủ Windows hoặc Linux trong môi trường của bạn, bao gồm khi chúng nằm trong mạng air-gapped (không kết nối trực tiếp với mạng Internet); hoặc bạn có thể sử dụng phần mềm dạng dịch vụ (SaaS) của chúng tôi thông qua MetaDefender Cloud.
- Hỗ trợ nhiều ngôn ngữ lập trình để tích hợp vào môi trường của bạn bằng tập lệnh giao tiếp qua chuẩn phổ biến REST (REST API).
- Tổng chi phí thấp với khả năng quản lý tập trung, mang lại hiệu suất vượt trội.

## Giới Thiệu về OPSWAT

OPSWAT bảo vệ các cơ sở hạ tầng trọng yếu. Mục tiêu của chúng tôi là loại các bộ phần mềm độc hại và các cuộc tấn công Zero-day. Chúng tôi tin rằng mọi tập tin và mọi thiết bị đều tiềm ẩn mỗi đe dọa. Các mối đe dọa phải được xử lý mọi lúc, mọi nơi, tại các đầu vào, đầu ra và toàn bộ hệ thống. Sản phẩm của chúng tôi tập trung vào việc ngăn chặn mỗi đe dọa và tạo quy trình nhằm bảo đảm an toàn quá trình truyền tải dữ liệu và truy cập thiết bị. Kết quả là các hệ thống sẽ được đảm bảo hiệu năng và giảm thiểu rủi ro phải thỏa hiệp với tội phạm mạng. Đó là lý do tại sao 98% các Cơ sở Năng lượng Hạt nhân của Hoa Kỳ tin tưởng lựa chọn các giải pháp bảo đảm an ninh mạng và tiêu chuẩn tuân thủ an ninh mạng của OPSWAT.

**Để biết thêm về MetaDefender Core, vui lòng truy cập:**

[opswat.com/products/metadefender/core](https://opswat.com/products/metadefender/core)

**Hoặc liên hệ với chuyên gia kỹ thuật của OPSWAT để được tư vấn chi tiết và hiểu cách MetaDefender Core bảo vệ doanh nghiệp của bạn khỏi các cuộc tấn công mạng:**

[opswat.com/contact](https://opswat.com/contact)

OPSWAT.

Trust no file. Trust no device.