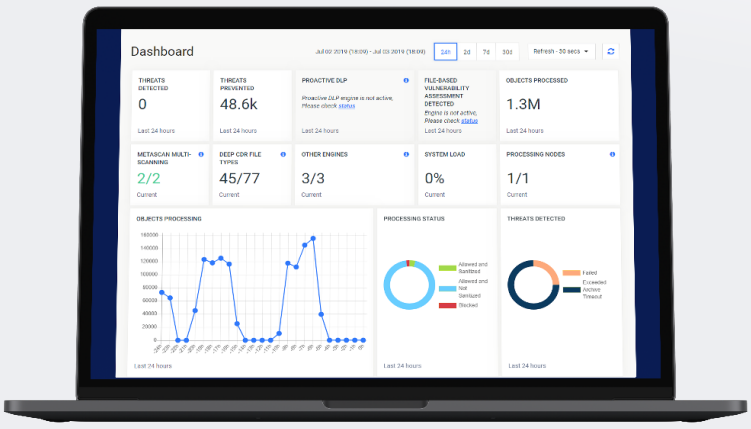
OPSWAT.

DATASHEET

MetaDefender® Core

Piattaforma evoluta di prevenzione delle minacce



La tua azienda non può più affidarsi esclusivamente a sistemi di sicurezza informatica basati sul rilevamento per fornire una protezione adeguata per le risorse aziendali più preziose, poiché i malware zero-day imparano ad aggirare queste difese. È necessario adottare approcci più preventivi per combattere attacchi mirati evoluti.

MetaDefender Core consente di integrare funzionalità evolute di prevenzione e rilevamento dei malware nelle soluzioni e nell'infrastruttura IT esistenti, per gestire al meglio i vettori di attacco comuni e migliorare gli strumenti di sicurezza informatica sviluppando sistemi di analisi del malware dedicati.

> "Per affrontare le problematiche dell'upload di file contenenti malware zero-day, abbiamo valutato sandbox, AV e sistemi multiscanning in cloud e abbiamo scelto Deep Content Disarm and Reconstruction di OPSWAT".
>
> Teza Mukkavilli
> Head of Security, Upwork

Caratteristiche e vantaggi principali

Deep Content Disarm and Reconstruction (Deep CDR)

Ricostruisce oltre 100 dei più comuni tipi di file, garantendo la massima usabilità e contenuti sicuri. Sono disponibili centinaia di opzioni di ricostruzione dei file.

Multiscanning

È possibile scegliere tra oltre 30 motori anti malware leader, nei vari package disponibili. Rileva in modo proattivo oltre il 99% delle minacce malware utilizzando firme, analisi e machine learning.

File-Based Vulnerability Assessment

Scansiona e analizza file binari e programmi di installazione per rilevare le vulnerabilità note delle applicazioni prima che vengano eseguite sugli endpoint, inclusi i dispositivi IoT.

Proactive Data Loss Prevention (Proactive DLP)

Controlla il contenuto di oltre 30 tra i più comuni tipi di file, per rilevare informazioni personali o sensibili, censurandole o aggiungendo una filigrana per offuscarle, prima che vengano trasferiti.

Oltre 100 opzioni di conversione file

Mantiene i file utilizzabili e intatti attraverso una vera "ricostruzione" dei vari tipi di file o la conversione in formati meno complessi.

Custom Workflows

Crea i tuoi workflows personalizzando i parametri di multiscaning e Deep CDR o l'ordine dei processi che gestiscono file.

Estrazione archivi

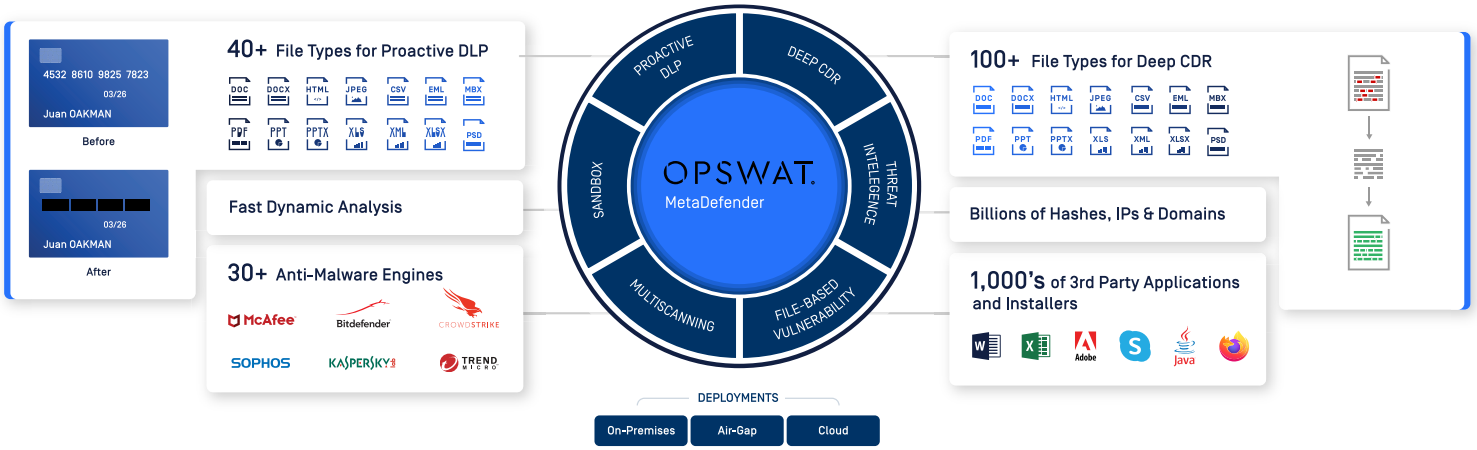
Multiscansione e Deep CDR per più di 30 tipi di file compressi. Le opzioni di gestione degli archivi sono configurabili e sono supportati gli archivi crittografati.

Verifica del tipo di file

Verifica oltre 4.500 tipi di file per determinare se il tipo di file corrisponde effettivamente al suo contenuto e non affidandosi semplicemente all'estensione.

OPSWAT.

MetaDefender Core



Perché MetaDefender Core

- Mitiga i rischi per i sistemi critici e previene le minacce che potrebbero aver aggirato le difese standard
- Protegge le informazioni sensibili e personali in ingresso o in uscita dalla tua organizzazione
- Facile implementazione su server Windows o Linux nell'infrastruttura esistente, anche se air-gapped, o utilizzando l'offerta software-as-a-service tramite MetaDefender Cloud
- Supporta molti linguaggi di programmazione, tramite l'integrazione nell'ambiente tramite API REST
- Ridotto total cost of ownership (TCO) con manutenzione flessibile grazie alla gestione centralizzata
- Implementazione flessibile in ambienti a comparti, per semplificare l'integrazione e la manutenzione, riducendo il TCO e i potenziali conflitti causati da dipendenze nascoste; facilmente scalabile tra ambienti e sistemi operativi diversi.

Informazioni su OPSWAT

OPSWAT protegge le infrastrutture critiche. Il nostro obiettivo è quello di eliminare attacchi malware e zero-day. Crediamo che ogni file e ogni dispositivo rappresenti una minaccia. Le minacce devono essere affrontate in tutte le condizioni e in ogni momento — in entrata, in uscita e archiviate. I nostri prodotti si concentrano sulla prevenzione delle minacce e sulla creazione di processi per il trasferimento sicuro dei dati e l'accesso sicuro ai dispositivi. Il risultato sono sistemi produttivi che riducono al minimo i rischi di compromissione. Ecco perché il 98% degli impianti nucleari statunitensi si affida a OPSWAT per la sicurezza informatica e la conformità.

Per ulteriori informazioni su MetaDefender Core
opswat.com/products/metadefender/api

Per contattare un rappresentante tecnico commerciale
opswat.com/contact

OPSWAT.
Trust no file. Trust no device.

MLS we care about IT
OPSWAT. AUTHORIZED DISTRIBUTOR

OPSWAT.com/contact