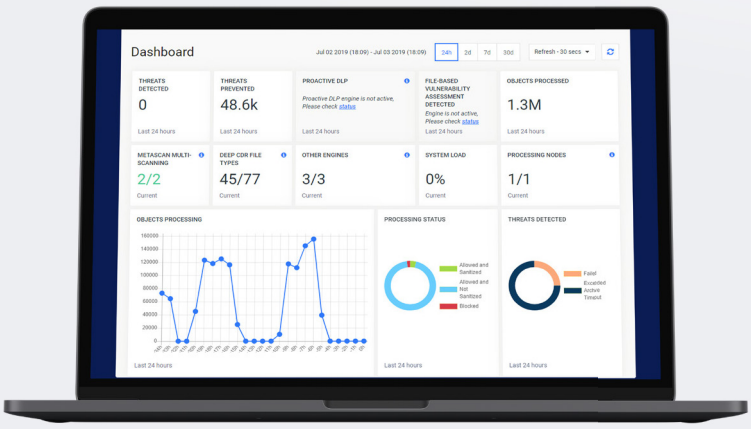
OPSWAT.

DATASHEET

MetaDefender® Core

Platforma pro pokročilou ochranu proti hrozbám



Při ochraně infrastruktury už vaše organizace nemůže spoléhat jen na tradiční bezpečnostní systémy na bázi detekce kybernetických hrozeb. Zero-day malwary se učí, jak tyto obranné prostředky překonat. Podniky potřebují systém prevence, který bude schopen čelit i pokročilým cíleným útokům.

Platforma MetaDefender Core vám umožní integrovat pokročilou malwarovou ochranu a její detekční schopnosti do stávajících IT řešení a infrastruktury. Tak budete schopni lépe zvládnout různé směry útoků: zabezpečíte webové portály před útoky na bázi uploadovaných škodlivých souborů, doplníte produkty pro kybernetickou bezpečnost a vytvoříte si vlastní systém analýzy malwaru.

> *„Vyhodnocovali jsme sandboxy, antivirové produkty a multiskenovací nástroje různých dodavatelů z hlediska efektivity odhalování malware při uploudu souborů a vybrali jsme Deep Content Disarm and Reconstruction od OPSWAT.“*
>
> **Teza Kukkavilli**
> Ředitel bezpečnosti, Upwork

Klíčové funkce a přínosy

Technologie Deep Content Disarm and Reconstruction (Deep CDR)

Provádí vnitřní kontrolu a rekonstrukci více než sta běžných typů souborů, a tak zajišťuje jejich maximální použitelnost i bezpečný obsah. K dispozici jsou stovky voleb rekonstrukce souborů.

Multiskenování

Můžete si vybrat z více než třiceti předních antimalwarových enginů ve flexibilních produktových balících. Proaktivně detekují přes 99 % malwarových hrozeb prostřednictvím signatur, heuristik a strojového učení.

Vyhodnocení zranitelnosti na bázi souboru

Skenování a analýza binárních souborů a instalačních kódů aplikací za účelem detekce známých zranitelností aplikací před jejich spuštěním na koncových zařízeních, včetně zařízení IoT.

Proaktivní prevence ztráty dat (Data Loss Prevention, DLP)

Kontrola obsahu ve více než třiceti běžných typů souborů s cílem vyhledat informace umožňující osobní identifikaci (PII); možnost upravit tyto citlivé informace nebo k nim před přenosem přidat digitální vodoznak.

Možnost konverze více jak 100 typů souborů

Zachování použitelnosti a neporušenosti souborů díky skutečné „rekonstrukci“ typů souborů nebo úpravy souboru na méně složitý formát.

Vlastní workflow

Můžete si určit vlastní workflow provádění multiskenování a Deep CDR a přizpůsobit proces a pořadí, v jakém se soubory budou zpracovávat.

Extrakce a kontrola komprimovaných souborů

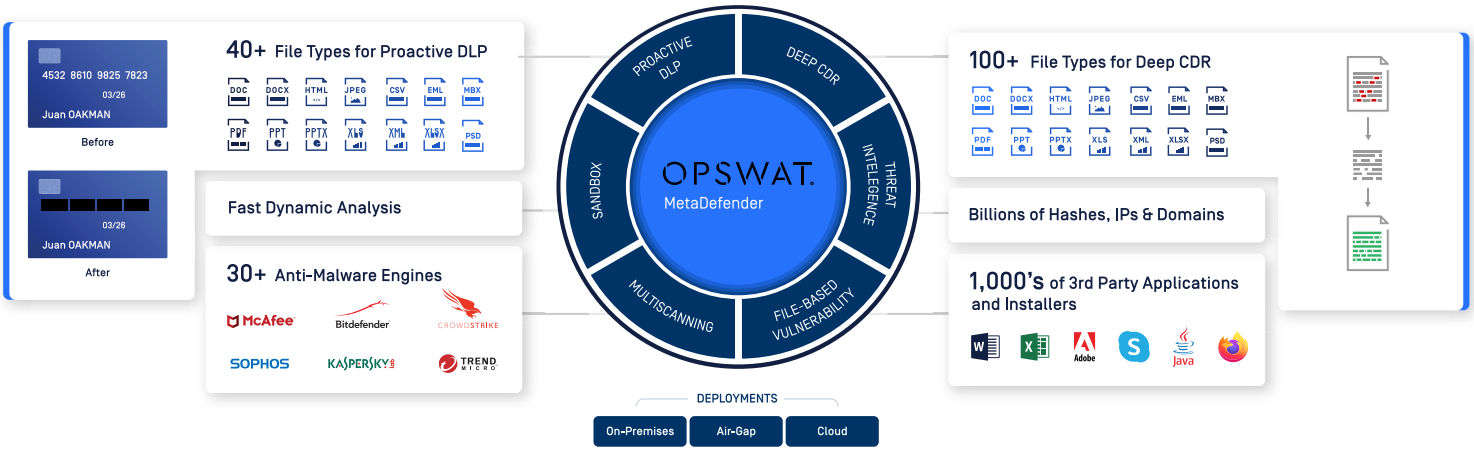
Technologii multiskenování a Deep CDR lze aplikovat na více než třicet typů komprimovaných souborů. Možnosti zpracování archivů jsou konfigurovatelné a jsou podporovány i kontroly šifrovaných archivů.

Ověření typu souboru

Lze ověřovat přes 4500 typů souborů a určovat jejich skutečný typ na základě obsahu souboru, nikoli pouze na základě podvrhnuté přípony. Účinná součást boje proti útokům na bázi falešných (maskovaných) souborů.

OPSWAT.

MetaDefender Core



Proč MetaDefender Core

- Zmírňuje rizika u vašich kritických systémů a chrání před hrozbami, které dokázaly obejít jiné bezpečnostní prvky.
- Chrání citlivé informace umožňující osobní identifikaci – zabraňuje jejich odchodu nebo vstupu do sítě organizace.
- Snadná instalace na servery Windows nebo Linux ve vašem prostředí, a to i v případě odpojených sítí (air-gapped) nebo v případě použití našeho softwaru formou SAAS prostřednictvím MetaDefender Cloud.
- Podpora mnoha programovacích jazyků umožňuje integraci do vašeho prostředí prostřednictvím REST API.
- Nízké celkové náklady vlastnictví (TCO) díky údržbě s využitím centralizované správy.
- Flexibilní implementace v prostředí kontejnerů zjednodušuje integraci a údržbu, snižuje TCO, zmírňuje potenciální konflikty v důsledku skrytých závislostí a umožňuje postupné rozšiřování do různých prostředí a operačních systémů.

O společnosti OPSWAT

OPSWAT zajišťuje ochranu kritických infrastruktur. Naším cílem je eliminovat malwarové a zero-day útoky. Věříme, že každý soubor a každé zařízení v sobě nese riziko. Hrozby je nutno řešit na všech místech a neustále – na vstupech, na výstupech i v ostatních částech sítí. Naše produkty se zaměřují na prevenci hrozeb a tvorbu procesů pro bezpečný přenos dat a bezpečný přístup do zařízení. Výsledkem je produktivní systém, který minimalizuje riziko narušení bezpečnosti. Proto například 98 % jaderných elektráren v USA využívá pro kybernetickou bezpečnost a shodu OPSWAT.

Více informací o MetaDefender Core
opswat.com/products/metadefender/core

Kontakt na technické obchodní zástupce
opswat.com/contact

Arrow ECS, a.s.

distributor řešení OPSWAT pro Českou republiku a Slovenskou republiku

Kontakty
arrow.com/ecs/cz

+420 597 488 811
sale.ecs.cz@arrow.com

OPSWAT.
Trust no file. Trust no device.

ARROW