OPSWAT.

Průvodce řešením
File Upload Security

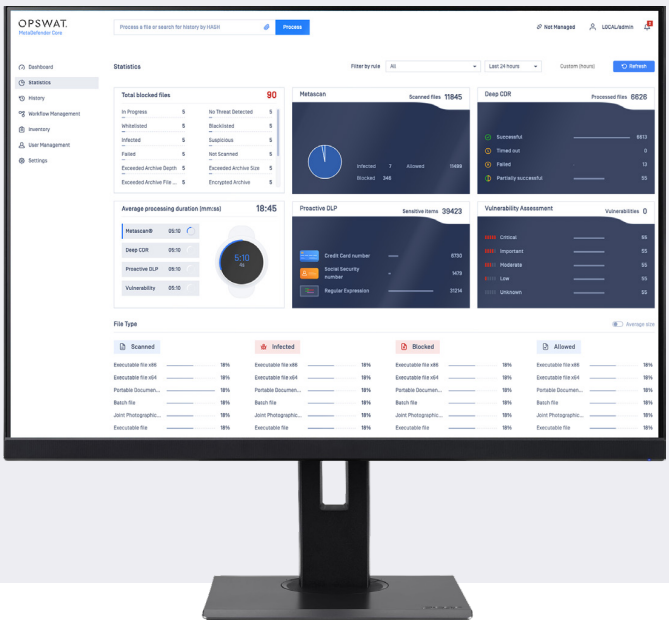
MetaDefender® ICAP Server – plug-and-play řešení pro ochranu sítě proti škodlivému internetovému obsahu

Obchodní a technické výzvy

Ochrana webových aplikací organizace před malwarem je náročnější než kdy dříve. Přispívá k tomu jednak komercializace kyberpodvodů a jednak nárůst sofistikovanosti jejich metod. Útočníci mohou využít možnosti nahrání souborů ve webových aplikacích a tak ohrozit zaměstnance, zákazníky, servery nebo celé organizace. Výsledkem mohou být úniky citlivých dat z vaší organizace nebo vysoké platby za výkupné kyberzločincům. Protože z praktických důvodů nelze omezovat přenosy souborů od interních či externích uživatelů, je potřeba přijmout ochranná opatření, aby bylo možno soubory bezpečně přijímat. Určitou míru ochrany nabízí skenování souborů pomocí tradičních antivirových produktů (AV), které hledají známé viry. Tím však není zajištěna komplexní ochrana před sofistikovaným malwarem a zero-day útoky. Tradiční AV řešení také poskytují jen omezenou ochranu před únikem citlivých dat.

6 osvědčených metod pro ochranu uploadů do webových aplikací

- Omezit povolené přípony souborů
- Ověřovat typ souborů a tak zabránit vstupu maskovaných souborů (spoofing)
- Autentizovat uživatele
- Skenovat soubory pomocí více antimalwarových produktů
- Odstraňovat ze souborů potenciální vložené hrozby
- Kontrolovat zranitelnosti v souborech



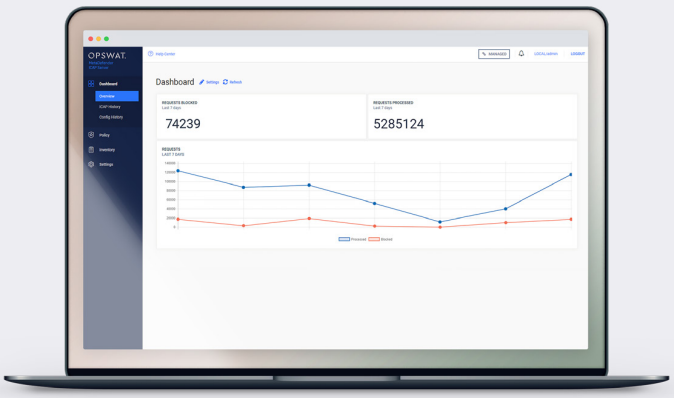
Řešení OPSWAT

OPSWAT se zaměřuje na ochranu proti pokročilým hrozbám a zero-day útokům a zajištění bezpečných přenosů dat v rámci sítě, webových aplikací a transakcí se zákazníky. Díky více než dvaceti letům zkušeností v oblasti bezpečnosti kritických infrastrukturních systémů poskytuje OPSWAT technologie, které hladce zaintegrují pokročilou malwarovou ochranu a detekci do vašich IT řešení a aplikací. MetaDefender ICAP Server na platformě MetaDefender Core představuje řešení pokročilé prevence hrozeb pro zjednodušenou bezpečnost uploadu souborů. Toto řešení využívají organizace na celém světě, které vyžadují vysokou úroveň bezpečnosti, včetně kritických infrastruktur, státních úřadů, finančních institucí a zdravotnických organizací.

OPSWAT.

Průvodce řešením
File Upload Security

MetaDefender ICAP Server



Tradiční detekční mechanismy na bázi signatur a chování souborů jsou při prevenci pokročilých cílených hrozeb a zero-day útoků nedostatečné. V mnoha organizacích se pokoušejí své systémy chránit pomocí souboru bezpečnostních produktů, které si vytvoří interně. Takový přístup je však nákladný, časově náročný a nese s sebou i další režijní náklady na údržbu a aktualizace.

Zapojit. Analyzovat. Zabezpečit.

OPSWAT nabízí řešení, která dokážou pokročilým útokům zabránit, a zároveň výrazně snižují břemeno údržby, konfigurací a aktualizací.

Když zákazník nahraje soubor do vaší webové aplikace nebo webové stránky, produkt MetaDefender ICAP Server jej ve spolupráci s MetaDefender Core zkontroluje. To zajišťuje vašim uživatelům a systémům komplexní ochranu před škodlivým internetovým obsahem. MetaDefender ICAP Server poskytuje rozhraní ICAP mezi pokročilými bezpečnostními funkcemi MetaDefender Core a libovolnou klientskou aplikací, která podporuje protokol ICAP. Jsou to například bezpečnostní brány, proxy, reverzní proxy, load balancery, webové aplikační firewally a podobně.

Každý soubor je zpracován pomocí špičkových technologií pro detekci a prevenci hrozeb. Veškeré podezřelé soubory jsou blokovány nebo sanitizovány, a teprve pak k nim mohou mít koncoví uživatelé přístup. Kromě toho lze identifikovat citlivá data a buď je upravit, odstranit nebo zablokovat v souladu s pravidly organizace. Tak mohou organizace lépe zajistit požadavky povinných zákonných předpisů.

> *„Používáme technologie OPSWAT již několik let v různých integracích a v různých produktech. Jejich pověst v odvětví je prostě skvělá. Pracuji v tomto odvětví již třicet let a OPSWAT je firma, které jsem vždy důvěřoval a se kterou se výborně spolupracuje.“*
>
> **Joe Peck**
> Ředitel produktového managementu, společnost F5

> *„Pomocí řešení MetaDefender Deep CDR jsme v Upwork byli schopni zabránit sto procentům zero-day souborových útoků v porovnání se sedmdesáti procenty blokovanými standardním antivirovým skenováním. Všechny soubory s aktivními objekty se sanitizují: 75 % souborů se zpracuje a je připraveno za kratší dobu než vteřinu a 99 % souborů během méně než šesti vteřin.“*
>
> **Teza Mukkavilli**
> Ředitel bezpečnosti, společnost Upwork

- Obsáhlá detekce a prevence hrozeb ve vaší síti v reálném čase.
- Ochrana proti zero-day a pokročilými cílenými útoky.
- Detekce zranitelností na bázi souborů před instalací.
- Citlivá data již nebudou vstupovat do vaší organizace ani ji opouštět.
- Přizpůsobitelná pravidla, pořadí pracovních úloh a analýzy pro splnění vašich jedinečných bezpečnostních potřeb.
- Jednoduchá integrace s libovolným zařízením podporujícím ICAP.

OPSWAT.

Průvodce řešením
MetaDefender ICAP Server

Komplexní ochrana

Vícevrstvé obranné prvky snižují rizika pro vaše kritické systémy a zabraňují hrozbám, které tradiční obranu dokážou překonat.

Nízké náklady na vlastnictví (TCO)

Flexibilní bezpečnostní řešení, která poskytují výbornou úroveň dlouhodobých TCO. Kyberbezpečnost lze spravovat z jedné platformy, což znamená vyšší návratnosti investice a nižší režijní náklady; na dohled nad složitými organizačními systémy stačí méně školených profesionálů.

Nepřetržitý přehled a kontrola

Centralizované uživatelské rozhraní se zobrazením stavu bezpečnosti v reálném čase poskytuje komplexní přehled o vašich systémech a okamžitě vás upozorní na potenciální hrozby.

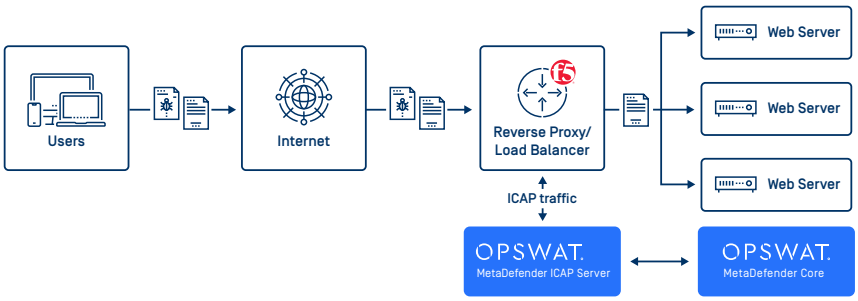
Nastavitelná bezpečnostní pravidla a pracovní úlohy

Administrátoři mohou vytvořit více pracovních úloh a různých bezpečnostních pravidel na bázi uživatelů, zdroje souborů a typu souborů.

Integrace produktu MetaDefender ICAP Server

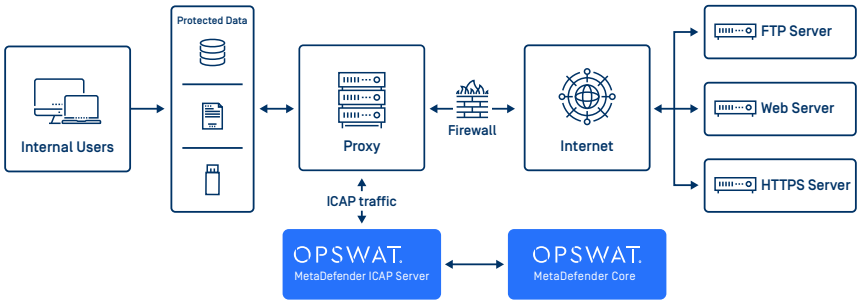
Reverzní proxy / webový aplikační firewall / load balancer
Chrání aplikační webové servery před uploadem škodlivých souborů.

Podporuje: F5 Advanced WAF, F5 Big-IP ASM, F5 Big-IP LTM, VMware Avi Vantage



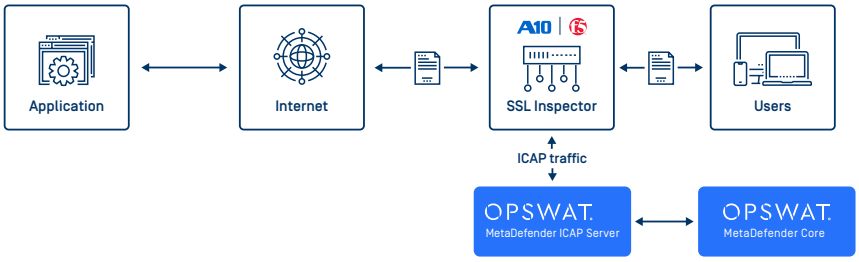
Forward proxy / webová gateway / firewall
Prověřuje webový provoz před jeho vstupem do zabezpečené sítě.

Podporuje: Squid, Citrix Netscaler, Axway SecureTransport, ARA Networks JAGUAR5000, McAfee Web Gateway, Fortinet FortiGate.



SSL inspekce
Integruje více funkcí MetaDefender v bodě dešifrování pro zjednodušení a agilitu.

Podporuje: F5 SSL Orchestrator, A10 Networks Thunder SSLi.

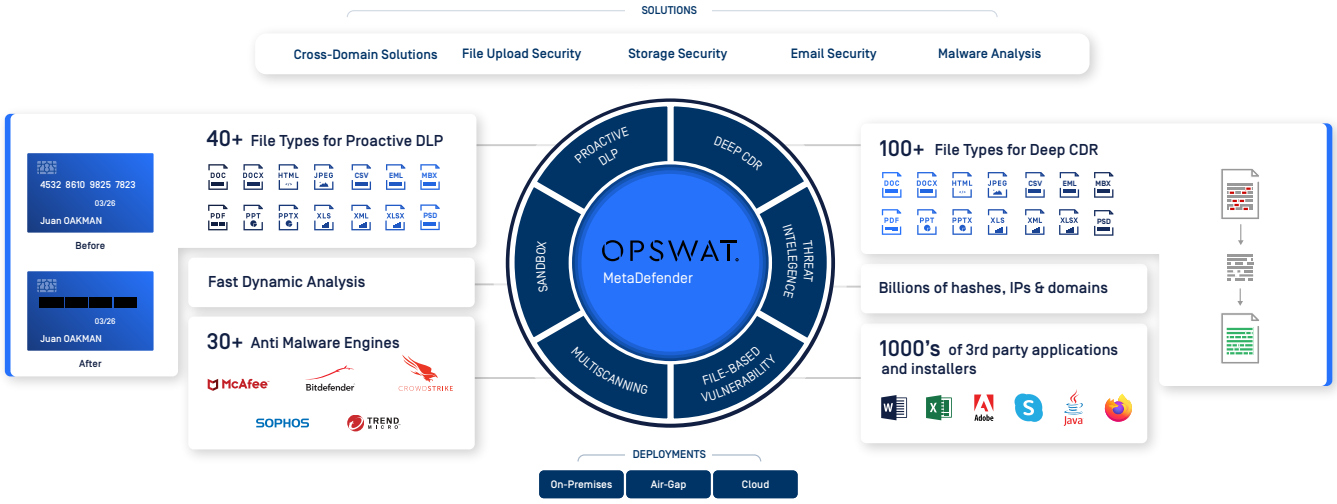


OPSWAT.

Průvodce řešením
MetaDefender ICAP Server

Technologie platformy MetaDefender

MetaDefender ICAP Server využívá technologie platformy MetaDefender Core pro špičkovou detekci a prevenci známého i neznámého malwaru.



Deep CDR
Odzbrojení vloženého obsahu a rekonstrukce souborů, účinná prevence neznámých zero-day a pokročilých hrozeb.

Proactive DLP
Prevence úniku citlivých dat.

Multiscanning
Detekce téměř sto procent známých hrozeb.

File-based Vulnerability
Detekce zranitelností před jejich zneužitím.

Threat Intelligence
Zkoumání nových hrozeb a určení reputace souboru.

Sandbox
Hloubková analýza pro detekci chování malwaru, prevence útoků.

Používejte kybernetickou bezpečnost, která funguje

Naplánujte si schůzku s technickým specialistou OPSWAT a zjistěte, jak vám může OPSWAT pomoci chránit vaši infrastrukturu před pokročilými sofistikovanými hrozbami. Navštivte opswat.com/contact.

Další informace o bezpečnosti uploadu souborů najdete na opswat.com/solutions/file-upload-security.

NAPLÁNUJTE SCHŮZKU

OPSWAT.
Trust no file. Trust no device.

Řešením OPSWAT důvěřuje více než 1 000 velkých podniků a státních organizací po celém světě

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 zajištění shody s předpisy OPSWAT.

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