OPSWAT.

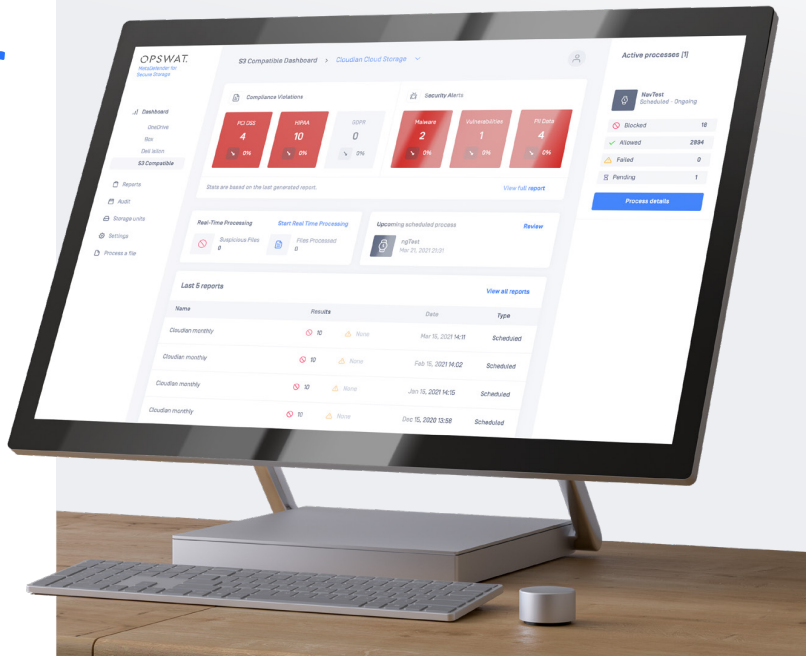
DATASHEET

MetaDefender® for Secure Storage

Zabezpečte svá úložiště

Řešení pro ukládání dat usnadňují přístup, sdílení a spolupráci. Pokud jde o malware a ztrátu citlivých dat, znamenají pro oddělení IT bezpečnosti velký problém. Jedná se totiž o kritickou bezpečnostní mezeru. Podle zprávy z roku 2020, 80 % společností zaznamenalo únik dat z cloudových úložišť.

Produkt MetaDefender for Secure Storage nabízí robustní vrstvu ochrany pro zabezpečení uložených podnikových dat. Pomáhá v prevenci narušení bezpečnosti dat, výpadků systému a případů porušení compliance v cloudových i podnikových úložištích.



Analýza. Náprava. Report.

Soubory od uživatelů v organizaci se skenují za účelem vyhledání malwaru a analyzují se u nich potenciální ztráty dat nebo zpřístupnění nevyžádaných soukromých dat. Podezřelé soubory je možné sanitizovat (odstranit nežádoucí prvky), citlivá data v souborech lze také automaticky upravit a nahlásit.

Díky nativní integraci s řadou cloudových i podnikových úložných služeb lze toto řešení snadno implementovat. Na základě automatizovaných reportů mají pracovníci IT dokonalý přehled o potenciálních rizicích spojených s uživateli a službami a mohou rychle přijmout nápravná opatření (remediace).

S řešením MetaDefender for Secure Storage můžete důvěřovat datům sdílených ve vaší organizaci.

Přínosy

Prevence zero-day hrozeb

Odzbrojení neznámého obsahu a výstup bezpečných použitelných souborů. Technologie OPSWAT Deep Content Disarm and Reconstruction (Deep CDR) se zaměřuje na prevenci útoků před jejich rozvinutím. Dokáže odstranit skrytý nebo neznámý malware z více než sta typů souborů.

Pokročilá detekce hrozeb

Multiskenování pěti až třiceti pěti předními antimalwarovými produkty (McAfee, ESET, Avira, K7, Crowdstrike, TrendMicro, Sophos a další) kombinuje veškeré detekční mechanismy (signatury, heuristiky, umělou inteligenci, NGAV) a ponechává minimální prostor chybám.

Zmírnění rizik souvisejících s dodržováním předpisů

Detekce, odstranění, maskování nebo blokování citlivých dat. Proaktivní technologie OPSWAT pro prevenci ztráty dat (DLP) poskytuje automatické reporty a remediaci v případě ztráty citlivých dat. Tak lze zajistit shodu s požadavky zákonů typu HIPAA, PCI-DSS nebo GDPR.

Široké integrační pokrytí

Integrace s Microsoft OneDrive, Sharepoint Online a Azure, Amazon S3, Box, Cloudian S3, Dell Isillon a veškerými SMB nebo S3 kompatibilními úložišti. Díky hladké integraci můžete jejich stav začít vyhodnocovat v řádu minut.

OPSWAT.

MetaDefender for Secure Storage

Funkce a vlastnosti

Nastavitelný rozsah zpracování

Na jedno kliknutí zpracujete celé úložiště, nebo pouze nové soubory, nebo proces přizpůsobíte pro konkrétní soubory.

Automatické výkazy

Okamžitý přehled o stavu řešení cloudového i podnikového úložiště prostřednictvím automatizovaných reportů zaslaných e-mailem přímo vám a dalším určeným pracovníkům v organizaci. Vše lze zobrazit i v reálném čase prostřednictvím komplexního ovládacího panelu.

Flexibilní plánování

Můžete zvolit kombinaci zpracování v reálném čase nebo možnost naplánování zpracování, které budou vyhovovat potřebám vaší organizace, a tak neustále vaše úložiště chránit před zero-day útoky a pokročilými perzistentními hrozbami (APT).

Plná auditovatelnost

Monitorování a logování historie uživatelských aktivit, které lze snadno exportovat za účelem plné transparentnosti a realizace podnikových auditů.

Automatizované pracovní úlohy

Kromě voleb pro manuální a automatizované plánování zpracování lze řešení integrovat do interních systémů prostřednictvím REST API.

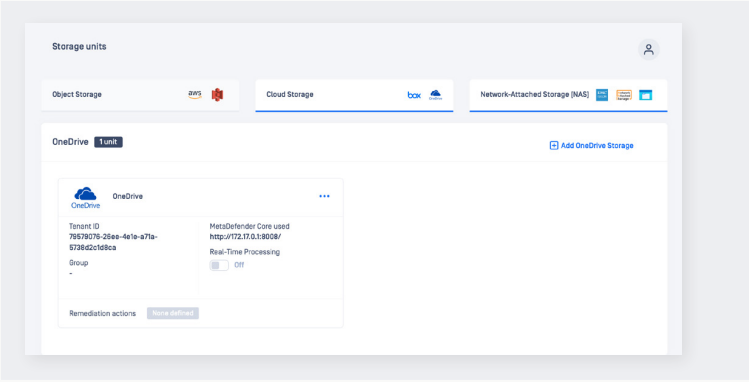
Správa uživatelů

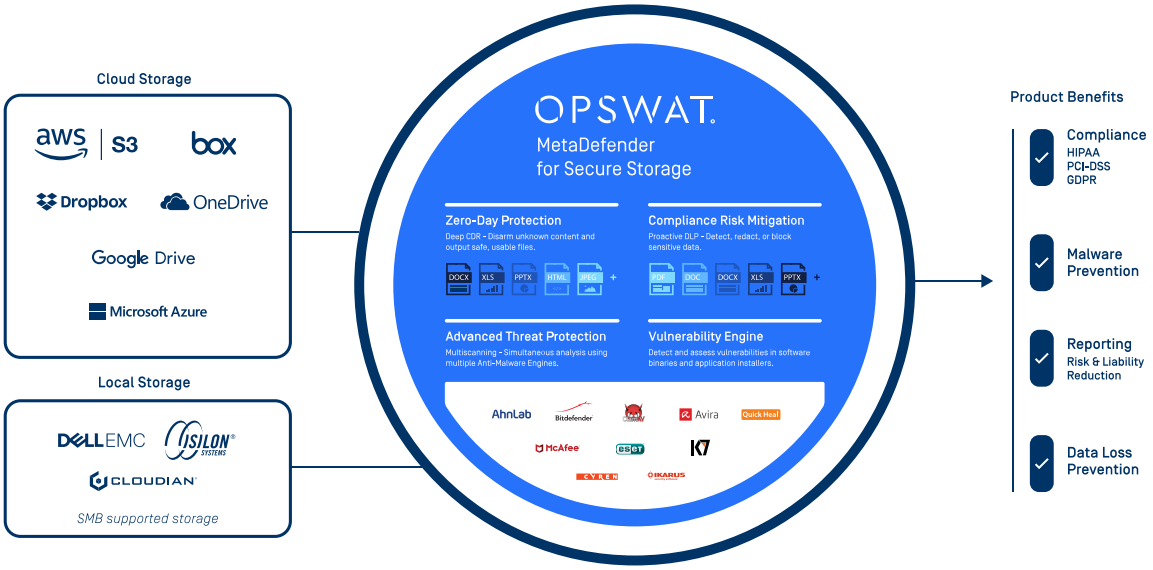
Řešení umožňuje IT oddělení efektivně spravovat rizika související se shodou s předpisy a narušením datové integrity, neboť lze poskytnout přístup více administrátorům na bázi rolí (včetně „read only“).

Integrace (Amazon S3, Dell a další)

V řádu minut lze nastavit a nakonfigurovat více jednotek úložišť od různých výrobců (ať v cloudu nebo v podnikovém systému), a tak spravovat a zabezpečovat veškerá vaše data v jednom zobrazení. Poskytujeme nativní API integrace s cílem minimalizovat režijní náklady.

- Integrace s veškerými instancemi Amazon S3 nebo jakýmkoliv S3 kompatibilním úložištěm.
- Zabezpečení všech vašich dat uložených v Microsoft OneDrive, SharePoint online, Azure File a Azur Blob úložišti.
- Hladká integrace všech vašich Dell Isilon nebo SMB kompatibilních podnikových úložišť.
- Snadná konfigurace všech jednotek vašich úložišť z řešení Box a jiných aplikací pro spolupráci.





OPSWAT.

MetaDefender for
Secure Storage

Jak OPSWAT minimalizuje rizika související se shodou s předpisy

Zákonné požadavky nařizují organizacím zajistit soukromí a bezpečnost citlivých zákaznických dat.

- OPSWAT kontroluje jakákoli citlivá data, která by mohla být neúmyslně vystavena škodlivým útokům. Přístup na bázi rolí (s možností „read-only“) minimalizuje porušení zákonů o soukromí dat. Naše produkty vás upozorní na případy zneužití a poskytnou vám přehled o podezřelých nebo neopatrných aktivitách uživatelů. Pokud by taková aktivita nebyla vaší organizací detekována, vystavilo by to vaši organizaci riziku postihu finančními pokutami a ztrátě pověsti.
- Pokročilá sada technologií OPSWAT včetně technologie multiskenování z více než třiceti antivirových řešení, technologie Deep Content Disarm and Reconstruction pro sanitizaci všech souborů a technologie Proactive Data Loss Prevention pro detekci a blokování citlivých dat pomáhají organizaci dostát všem požadovaným zákonným požadavkům.

Typy dat, která OPSWAT chrání

- Shoda se **směrnicemi PCI-DSS (Payment Card Industry–Data Security Standards)**
  - čísla kreditních karet

Riziko vyplývající z nezajištění shody

Podle blogu PCI Compliance (pcicomplianceguide.org/faq/#15) jsou pokuty v případě nezajištění shody následující:
Platební společnosti mohou podle svého uvážení udělit dotyčné bance za porušení shody se směrnicemi PCI pokutu ve výši pět až sto tisíc dolarů měsíčně. Banky nejčastěji tuto pokutu přesunou dál, až dopadne na obchodníky. Banka také pravděpodobně buď ukončí váš obchodní vztah nebo zvýší transakční poplatky. O pokutách se otevřeně nemluví, ani nejsou široce zveřejňovány, ale pro malé podniky mohou mít katastrofální důsledky.

- Shoda s **předpisem GDPR (General Data Protection Regulation)**
  - Osobní identifikovatelné informace (PII) datových subjektů
    - e-mail
    - datum narození
    - telefonní číslo
    - číslo pasu

Riziko vyplývající z nezajištění shody

Existují dvě úrovně administrativní pokuty v případě nedodržení požadavků GDPR:
- až deset milionů dolarů nebo v případě podniku 2 % ročního obratu (podle toho, která částka je vyšší)
- až dvacet milionů dolarů nebo v případě podniku 4 % ročního obratu (podle toho, která částka je vyšší)

Pokuty za porušení GDPR mají spíš nezávazný než povinný charakter, ukládají se případ od případu a podle předpisu by měly být „efektivní, úměrné a odrazující“.
ec.europa.eu/info/law/law-topis/data-protection/data-protection-eu_en

- Prevence porušení **zákona HIPAA (Health Insurance Portability and Accountability Act)**
  - čísla sociálního pojištění
  - datum narození
  - telefonní číslo
  - adresa

Riziko vyplývající z nezajištění shody

Pokuty za nezajištění shody vycházejí z úrovně zanedbání povinnosti a mohou se pohybovat od sta dolarů do padesáti tisíc dolarů za porušení (nebo za záznam); maximální výše pokuty je 1,5 milionu dolarů za rok za porušení stejného ustanovení. Porušení zákona může obnášet i trestní postih, který může znamenat trest odnětí svobody.
hhs.gov/hipaa/for-professionals/compliance-enforcement/data/enforcement-highlights/index.html

OPSWAT.

Trust no file. Trust no device.

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