OPSWAT.

# Technologie Content Disarm and Reconstruction (CDR) Průvodce výběrem řešení

Jak zvolit nejlepší řešení CDR, které ochrání kritickou infrastrukturu před pokročilými malwarovými a zero-day útoky

# Přehled

V tomto průvodci najdete základní informace o technologii Content Disarm and Reconstruction (CDR), která chrání organizaci a její kritickou infrastrukturu před nově se objevujícími kybernetickými hrozbami, a přehled kritérií, které je třeba brát v úvahu při výběru vhodného řešení CDR pro vaši organizaci.

Průvodce obsahuje tři části:

1. Jak technologie CDR a sanitizace dat zabraňuje známým i neznámým malwarům v proniknutí do systému organizace.
2. Klíčové otázky při výběru řešení CDR.
3. Proč technologie Deep CDR společnosti OPSWAT poskytuje pokročilou úroveň ochrany před hrozbami a předčí jiné produkty na trhu.

ČÁST 1

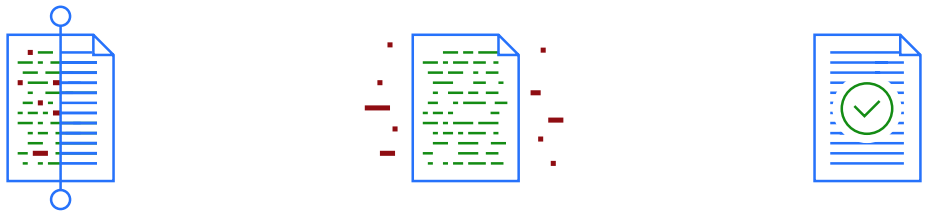
# Jak technologie CDR bojuje s nově se objevujícími hrozbami

## Co je CDR?

CDR je zkratka pro Content Disarm and Reconstruction (doslova odzbrojení a rekonstrukce obsahu). Technologie CDR, někdy také známá jako sanitizace dat, je pokročilou technologií pro prevenci hrozeb, která nespoléhá jen na detekci známých škodlivých prvků. V souladu s filozofií „nulové důvěry" vychází z předpokladu, že každý soubor může být škodlivý. Proto sanitizuje a rekonstruuje všechny soubory, přičemž zachová jejich plnou použitelnost s bezpečným obsahem. Znamená to, že soubory jsou rozebrány a vše, co by mohlo být potenciálně nebezpečné, odstraní – a pak soubor znovu sestaví. Technologie CDR je vysoce účinná při prevenci známých i neznámých hrozeb, včetně zero-day cílených útoků, které jsou vybaveny technologií maskování obsaženého malware.

## Jak CDR funguje?

Proces CDR probíhá ve třech krocích:



1. Ověření typu souboru a identifikace všeho aktivního vloženého obsahu v daném souboru.
2. Odstranění veškerého potenciálně škodlivého obsahu a rekonstrukce souboru pouze s bezpečným obsahem.
3. Použití plně funkčního očištěného souboru (bez jakýchkoli hrozeb) – a přesun původního souboru do karantény.

### 1. Identifikace a skenování souborů

Po vstupu do sanitizačního systému se soubory vyhodnocují a ověřují - zjišťuje se typ souboru a jeho konzistentnost. Lze identifikovat přes 4500 typů souborů. Každý soubor se skenuje s cílem identifikovat v souboru vložený aktivní obsah, například makra, linky (odkazy) a OLE objekty. Zkoumají se přípony souborů s cílem zjistit, zda zdánlivě jednoduché soubory nejsou ve skutečnosti soubory složitými. Soubory se škodlivým obsahem jsou označeny a organizace dostane upozornění, že se může jednat o útok. Řešení OPSWAT Deep CDR podporuje sanitizaci pro více než 100 běžných souborových typů, včetně PDF, Microsoft Office, HTML, řady formátů dat pro digitální fotografie, nebo také JTD a HWP.

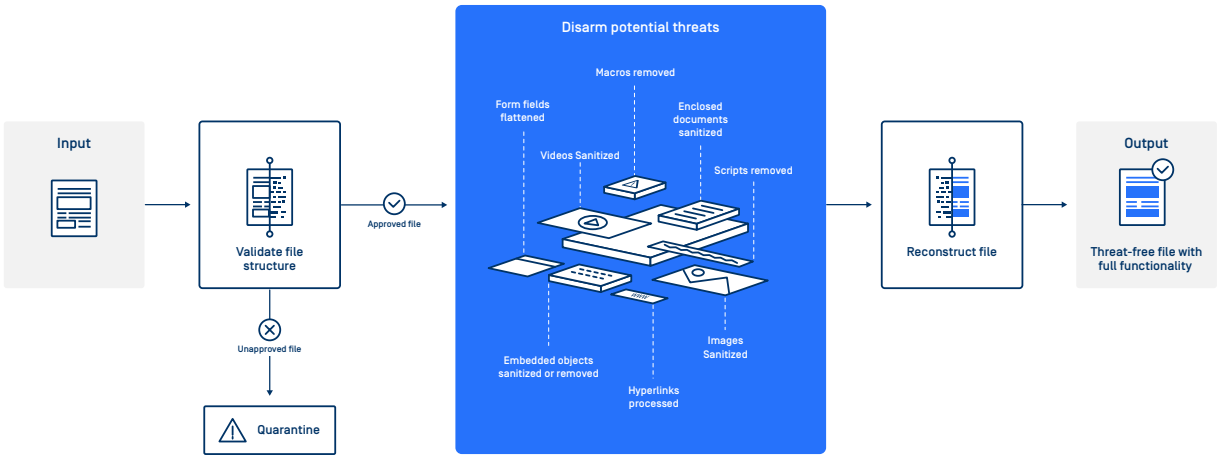
## 2. Sanitizace souborů

Soubory se rychlým a bezpečným procesem rekonstruují. Prvky souboru se rozdělí do jednotlivých komponent, škodlivé prvky se odstraní a metadata a veškeré souborové charakteristiky se zrekonstruují. Nové soubory se rekompilují, přejmenují a dodají, přičemž se zachová integrita struktury souboru. Uživatelé mohou se soubory bezpečně pracovat bez ztráty použitelnosti.

## 3. Použití souborů

Nově regenerované soubory nyní lze používat. I složité soubory si zachovají použitelnost – například animace vložené do souboru PowerPoint zůstávají po dokončení procesu CDR nedotčeny. Původní soubory se nakonec přesunou do karantény za účelem zálohování a případného dalšího prozkoumání. Vytvořením plně použitelných souborů s bezpečným obsahem chrání řešení CDR organizace před vysoce sofistikovanými hrozbami a přitom zachovává produktivitu uživatelů.

Na obrázku je přehled fungování řešení OPSWAT Deep CDR. Více informací k této technologii najdete v části 3.




**Identifikace, sanitizace, rekonstrukce: Přehled činnosti OPSWAT Deep CDR**

## Dva nejobvyklejší případy nasazení řešení CDR

**Může CDR zabránit hrozbám na bázi softwarových zranitelností?**

Softwarová zranitelnost se odkazuje na slabé místo nějakého softwarového produktu, které lze zneužít při kybernetických útocích. Klíčovou příčinou bezpečnostních incidentů bývají známé i neznámé zranitelnosti. Mnohé zranitelnosti využívají k narušení souboru kontejnery.

Hackeři například mohou využít zveřejněnou zranitelnost aplikací Adobe Acrobat a Adobe Reader, CVE-2019-16451, k tomu, aby distribuovali takzvaný backdoor malware schopný kontrolovat infikovaný systém – což pak útočníkům umožní instalovat programy, zobrazovat, modifikovat a vymazávat data nebo vytvářet nové účty s plnými uživatelskými oprávněními.

OPSWAT Deep CDR dokáže účinně řešit zranitelnosti na bázi souborů, neboť při rekonstrukci souboru se odstraní škodlivé příkazy a exploity skryté ve fotografiích, videích a dalších neškodných datových formátech.

**Může CDR ochránit před rizikem stále složitějších formátů souborů?**

Souborové formáty umožňují stále složitější funkce prostřednictvím vložených skriptů, maker a dalších programovacích prvků navržených tak, aby zefektivňovaly činnost programu a podpořily produktivitu uživatelů. Například soubory PDF mohou obsahovat aktivní linky (odkazy), media soubory, formy, Unicode znaky a šifrovaná data.

**60%**
útoků v roce 2019 bylo cílených

**1,045**
veřejně odhalených zranitelností v roce 2019

**59%**
společností zažilo útoky na bázi škodlivého kódu

Složitost souborů umožňuje uživatelům lepší produktivitu, ale zároveň poskytuje hackerům prostor do nich vkládat skripty a exploity, které využívají zranitelností v aplikacích. OPSWAT Deep CDR chrání proti těmto zranitelnostem na bázi souborů, neboť při rekonstrukci souborů veškeré škodlivé příkazy, skripty a jiné vložené objekty odstraní.

ČÁST 2

# Jak vybrat technologické řešení CDR

Na trhu je dnes k dispozici řada řešení CDR. Jak zjistit, které řešení bude pro vaši organizaci nejlepší? Sestavili jsme seznam patnácti otázek, které je vhodné při hodnocení různých řešení CDR posoudit.

1. **Jaké typy archivačních formátů řešení podporuje?**

   Archivy v posledních letech stále více převládají v integraci a ukládání více typů souborů do jednoho svazku. Požádejte o přezkoumání seznamu archivů, které CDR podporuje, a zkontrolujte, zda můžete ovládat související funkce, například úroveň rekurze. Pokud je například PDF vložen do souboru PowerPoint, může technologie analyzovat a rekonstruovat oba soubory?

2. **Kolik typů souboru řešení podporuje?**

   Existuje přes pět tisíc známých typů souborů. Ptejte se, kolik typů souboru řešení CDR podporuje, překontrolujte informace a porovnejte seznam typů souboru se soubory, které vaše organizace používá.

3. **Je zachována použitelnost souboru?**

   Pracujete-li se soubory typu PowerPoint, které obsahují animace, soubory Excel, kde chcete zachovat makra, atd., potřebujete mít jistotu, že rekonstruované soubory uvedené funkcionality neztratí. Můžete to zjistit jednoduše tak, že při hodnocení necháte řešení CDR zpracovat nějaký vzorový soubor s takovou funkcionalitou.

4. **Lze řešení konfigurovat tak, aby vyhovovalo podmínkám vašeho prostředí?**

   Zkontrolujte, zda můžete nakonfigurovat, které vložené objekty se mají u jednotlivých typů souborů odstraňovat/sanitizovat. Zjistěte, zda můžete podrobněji nastavit sanitizační proces a také kvalitu fotografií, zpracování linků a tak dále.

5. **Lze vytvořit auditní sledování?**

   Ptejte se například, zda řešení zaznamenává a protokoluje, které objekty byly odstraněny a které objekty byly sanitizovány. Zjistěte, zda můžete ověřovat neporušenost / integritu archivů.

6. **Lze zavést různá pravidla pro různé datové zdroje?**

   Například zjistěte, zda vám řešení umožní v externích e-mailech excelovská makra odstraňovat, ale v interních e-mailech zachovávat.

7. **Které operační systémy řešení podporuje?**

   Máte-li v organizaci systémy na bázi Windows a Linuxu, dokáže řešení podporovat obojí?

### 8. Jaký je výkon řešení u různých typů souboru?

Ke zpracování různých souborových typů je potřeba různý výkon řešení. Vyzkoušejte si řešení CDR na vzorových souborech, včetně velkých souborů a víceúrovňových archivů, a ověřte, že bude výkon řešení splňovat nároky vaší organizace.

### 9. Jak bezpečná je architektura řešení?

Jsou v řešení použity bezpečné designové vzory? Jak je CDR engine chráněný? Postupovalo se při vývoji řešení podle pravidel Secure SDLC (Software Development Lifecycle) a můžete provést statickou analýzu kódu? Byly použity knihovny jiných výrobců? Požádejte o předložení designu řešení a pokládejte otázky na potenciální bezpečnostní rizika jednotlivých komponent.

### 10. Je technologie dlouhodobě udržitelná?

Kolik inženýrů aktivně pracuje na dané technologii CDR? Požádejte o organizační schéma a ověřte počet osob a jejich kvalifikaci. Prověřte inženýrské procesy QA dodavatele řešení. Je proces kompilace (build) bezpečný? Používá dodavatel řešení, které zabrání, aby během buildu došlo k vložení malwaru? Jaké bezpečnostní certifikace dodavatel má?

### 11. Jakými testy technologie CDR prošla?

Existuje nějaké nezávislé ověření kvality řešení, například nějakou státní institucí nebo jinou nezávislou organizací? Požádejte o výsledky v penetračních testech. Jak velká je testovací datová sada? Požádejte o předložení vzorků skutečného malwaru a zero-day útoků. Požádejte o manuální ověření testovací datové sady. Testují se aktuální hrozby? Požádejte o datovou sadu.

### 12. Lze řešení CDR snadno integrovat s vašimi současnými produkty?

Požádejte o přehled dokumentace k REST API.

### 13. Je technologie průběžně aktualizovaná?

Vyžádejte si přehled produktových aktualizací za poslední dvě čtvrtletí. Vyžádejte si také plán budoucího produktového vývoje (roadmap).

### 14. Jak rychle je řešení schopno podporovat nový souborový typ?

Existuje pět tisíc souborových formátů – kolik nových formátů řešení integrovalo za poslední dvě čtvrtletí? Ptejte se na konkrétní souborové typy, které ve vaší organizaci používáte, včetně regionálních souborových typů, jako je HWP nebo JTD.

### 15. Je řádně chráněno duševní vlastnictví?

Využívá-li technologie knihovny třetích stran, jsou řádně licencované? Požádejte o předložení licenčních ujednání (EULA) nebo jiných podpůrných dokumentů. Ptejte se na technologické patenty.

ČÁST 3

# Jak může OPSWAT pomoci

Společnost OPSWAT vyvinula technologii CDR pro řešení zero-day kybernetických hrozeb, které tradiční antimalwarové řešení a dynamické analýzy jako sandboxy nedetekují.

Tradiční řešení antimalwaru a dynamických analýz, jako jsou sandboxy, některé hrozby nezachytí, protože byly vytvořeny tak, aby detekovaly anomálie v souboru nebo v chování souboru.

CDR technologie od OPSWAT – Deep CDR – je postavena na předpokladu, že každý soubor může být škodlivý. Všechny soubory proto nechá projít procesem důkladné analýzy, odstraní z nich potenciálně škodlivé prvky a pak je opět sestaví tak, aby byl soubor pro uživatele použitelný, ale neškodný. Naše technologie CDR tedy poskytuje ochranu, aniž by potřebovala vědět, zda je podezřelý soubor „špatný“ nebo „dobrý“.

OPSWAT uvedla technologii Deep CDR v roce 2012 a od té doby se naše řešení na bázi Deep CDR v široké míře implementují po celém světě, zejména mezi zákazníky v odvětvích s kritickou infrastrukturou.

Deep CDR zdokonaluje bezpečnostní efektivitu běžných řešení CDR v tom smyslu, že se při analýze souborů zanořuje „hlouběji“ do vrstev komprese a vložených objektů – představte si například excelovou tabulku uvnitř dokumentu Word, který je vložený do souboru PDF a tento PDF je doručen do vaší e-mailové schránky jako jeden zazipovaný soubor.

Zranitelnosti v aplikacích Adobe Acrobat a Reader umožňují speciálně vytvořenému souboru PDF spustit škodlivý kód, který antimalwarové produkty nedetekují.

Technologie Deep CDR takový škodlivý obsah odstraní, aniž by spoléhala na detekci. Jako kdybyste vzali zbraň a odstranili cokoli, co najdete v jejích komorách. Nezáleží, zda to bude kulka, slepý náboj nebo smítko prachu – důležité je, že když někdo náhodou zbraň použije, nikoho nezraní.

Proč se zanořovat hlouběji do souborů?

Podle analytické zprávy společnosti Verizon (Data Breach Investigations Report) slouží mnohé PDF soubory jako mechanismus pro dodání dokumentů Office umožňujících spouštět makra (dokumenty Office jsou vloženy do PDF).

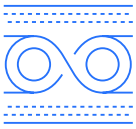
Podle analytické zprávy společnosti Symantec (Internet Security Threat Report) bylo v roce 2019 až 48 % škodlivých příloh tvořeno soubory Office. Oproti roku 2017, kdy to bylo pouze 5 %, to je velký skok.

Deep CDR rozloží PDF, odstraní vložený dokument, rozebere dokument, odstraní potenciálně škodlivý aktivní obsah a poté zrekonstruuje každý objekt v každé vnořené vrstvě. Dříve než Acrobat, Word nebo některá z desítek dalších podporovaných aplikací přistoupí k souborům nebo se jich jen dotkne.

## Vlastnosti a přínosy technologie Deep CDR od OPSWAT

### Podpora více než 100 typů souborů

Řešení dokáže sanitizovat a rekonstruovat více než sto běžných typů souborů, čímž zajistí, aby byl soubor plně použitelný a současně bezpečný. K podporovaným typům souborů patří PDF, Microsoft Office, HTML, mnohé formáty dat pro digitální fotografie, také JTD a HWP.



### Více než 200 možností souborových konverzí

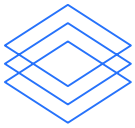
Nastavitelná konverze souborů vám umožní změnit soubor na jiné formáty (například konvertovat soubor .jpg na soubor .bmp, pak na soubor .pdf a pak zpátky na .jpg). Více konverzí zabrání hrozbám na bázi dokumentů ve vstupu do vysoce bezpečných sítí.

### Ověření více než 4500 typů souboru

Lze ověřovat více než 4500 typů souborů, a tak bojovat proti útokům na bázi falešných typů souborů, zejména detekovat složité soubory, které se tváří jako jednoduché.

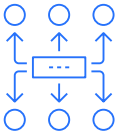
### 30x vyšší výkon

Deep CDR poskytuje rychlou a efektivní prevenci: je v průměru 30krát rychlejší než analýza v sandboxu a chrání proti malwaru (včetně zero-day) vytvořenému tak, aby se detekci v sandboxu vyhnul.



### Multiskenování – integrace více než 30 antivirových nástrojů

Integrace s technologií OPSWAT Multiscanning, která uživatele varuje, že se stal terčem útoku. Poskytuje přehled napříč různými datovými kanály a vstupními body pro soubory, včetně příloh e-mailů, souborů na přenosných médiích nebo souborů stažených v prohlížeči. Tak zvyšuje bezpečnost celé organizace.



### Nastavitelné pracovní úlohy

Pořadí kroků činnosti Multiscanning a Deep CDR lze pro různé vstupní body souborů nastavit. Podle datového kanálu, z něhož soubory přicházejí, můžete například nastavit, že se externí soubory nejprve sanitizují, sanitizované verze se dodají uživatelům a pak se na původních souborech provede multiskenování, které poskytne komplexní informace o matrixu případného útoku.

## Řešení OPSWAT pro ochranu kritické infrastruktury

OPSWAT nabízí pokročilá řešení pro prevenci hrozeb, které jsou určena pro odstranění mnoha problémů v kritických infrastrukturách:

- **Cross-Domain** – Řídí a zabezpečuje transfer dat nebo zařízení v rozsáhlých a segmentovaných síťových prostředích.
- **Email Security** – Chrání organizaci proti pokročilým e-mailovým útokům.
- **File Upload Security** – Zabraňuje uploadům škodlivých souborů, které mohou narušit bezpečnost sítě.
- **Malware Analysis** – Analyzuje podezřelé soubory nebo zařízení, jak v podnikové síti tak v cloudu.

- **Network Access Control** – Zabraňuje rizikovým zařízením včetně BYOD a IoT v přístupu do sítě a poskytuje plný přehled o koncových bodech.
- **Secure Access** – Poskytuje bezpečný lokální i vzdálený přístup do cloudových aplikací, interních sítí a k jiným zdrojům.
- **Storage Security** – Chrání služby úložiště v rámci podnikového systému i v cloudu a pomáhá dodržovat shodu s předpisy o soukromí dat.

Kromě technologie Deep CDR využívá OPSWAT několik dalších špičkových technologií, například Multiscanning, Proactive DLP nebo Threat Inteligence. Výsledkem je vynikající řešení na ochranu před kybernetickými hrozbami. Základ tvoří platforma MetaDefender, která tyto technologie integruje do komplexního modulárního řešení. Řešení se může rozšiřovat spolu s vaší organizací a lze jej implementovat pro širokou škálu případů použití.


**Přehled platformy OPSWAT MetaDefender**

## Další informace

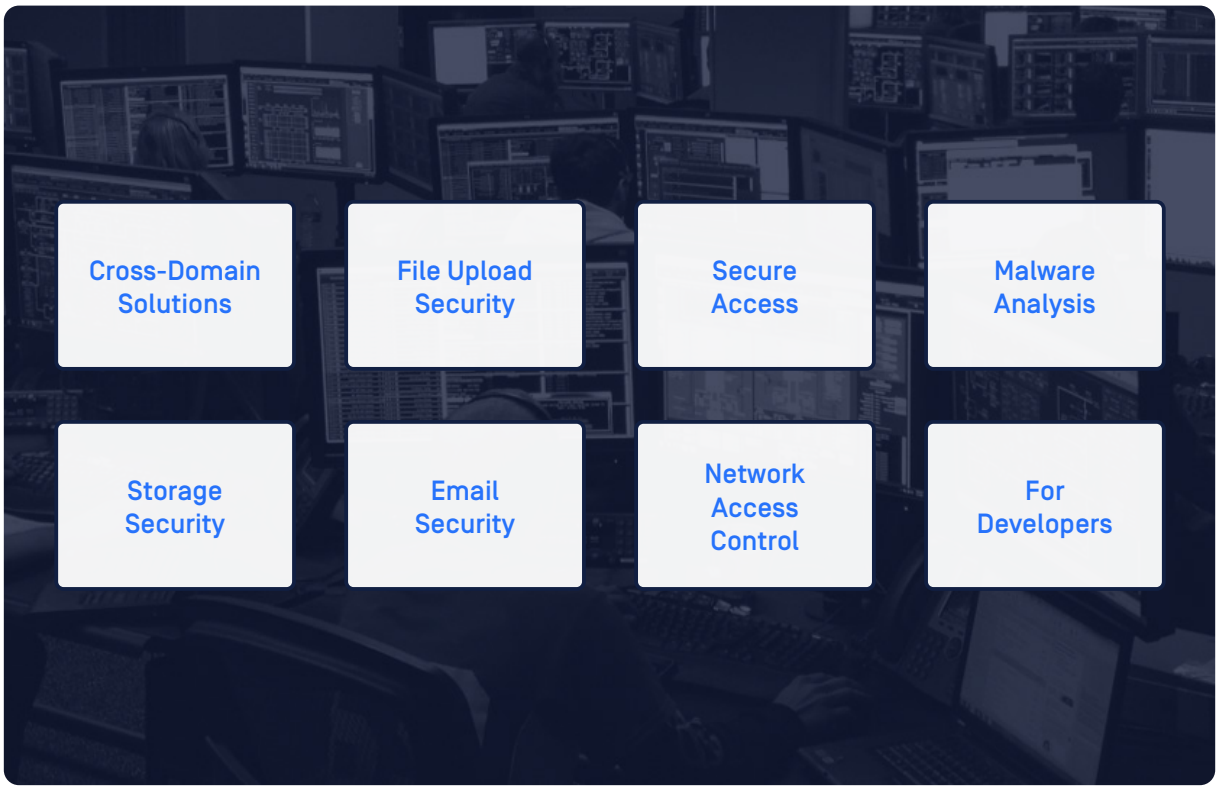
Chcete-li se dovědět o přínosech technologie CDR pro ochranu kybernetické bezpečnosti více, kontaktujte nás a promluvte si s některým z našich bezpečnostních expertů.

Můžete také využít dalších informačních zdrojů o technologii CDR na OPSWAT_CDR.

## O společnosti OPSWAT

Společnost OPSWAT je globálním lídrem v odvětví kybernetické bezpečnosti kritické infrastruktury a pomáhá ochránit přední světové organizace v této oblasti před malwarovými a zero-day útoky. Pro minimalizaci rizika narušení bezpečnosti nabízejí řešení OPSWAT Critical Infrastructure Protection (CIP) jak soukromým tak veřejným organizacích zavést procesy, které zajistí bezpečný přenos souborů a zařízení dovnitř i ven z kritických sítí.

Více než tisíc organizací po celém světě z odvětví finančních služeb, státní obrany, průmyslové výroby, energetiky, leteckého a kosmického průmyslu a dopravních systémů důvěřují OPSWAT při zabezpečení svých souborů a zařízení, zajištění shody se zákonnými a odvětvovými předpisy, ochraně své pověsti a také svých zaměstnanců, zákazníků i obchodních partnerů před narušením bezpečnosti jejich dat.




Navštivte nás na LinkedIn, Twittru, Facebooku nebo YouTube.

OPSWAT.
Trust no file. Trust no device.



ARROW

**Arrow ECS, a.s.**
distributor řešení OPSWAT pro Česku republiku a Slovenskou republiku

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