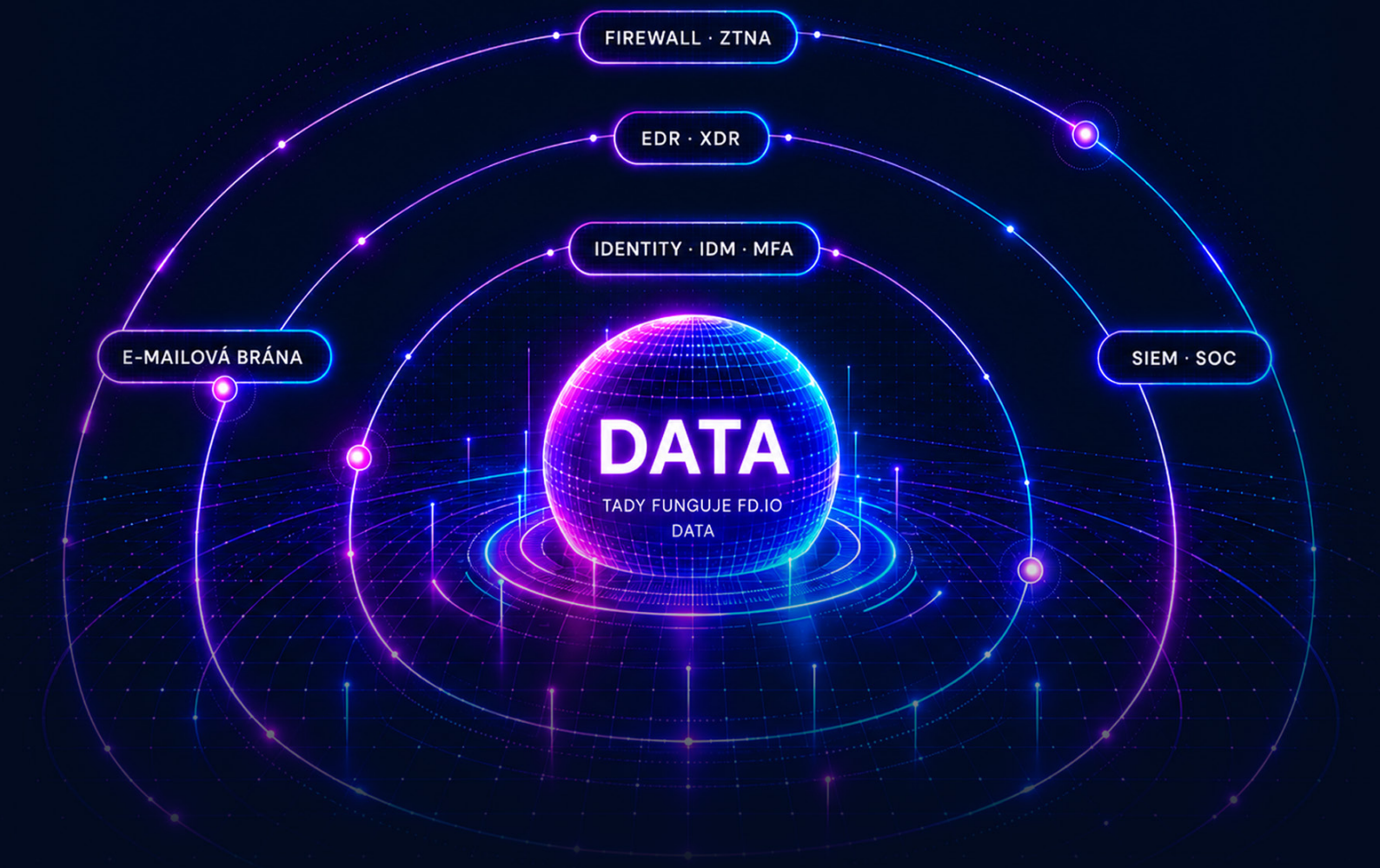
FREEDIVISION

SOLUTION GUIDE




# FreeDivision.io Data

## Data Security Platform

Ochrana citlivých dat přímo tam, kde leží – na souborových serverech, v Microsoft 365 a Copilotu, v e-mailu, v AI i v databázích.

# Proč nestačí hlídat jen cesty k datům

Firewally, EDR, správa identit i e-mailové brány jsou důležité – ale všechny stojí kolem dat. Hlídají síť, stanice, přihlášení a provoz na odchodu. Přitom neví, který dokument je citlivý, kdo k němu nemá mít přístup a kdo ho právě hromadně stahuje.

Jakmile se útočník přihlásí ukradeným heslem, pro firewall i EDR vypadá jako běžný zaměstnanec. Útočníkovi přitom nejde o firewall ani o stanici. Jde mu o data – a právě tam musí být i ochrana.

Situaci dále komplikuje Microsoft 365. Na souborovém serveru zakládali složky a nastavovali práva správci IT a přístupy měl někdo pod kontrolou. V Microsoft 365 vytvoří web, tým nebo odkaz „pro kohokoli" kdokoli. Firma s 500 lidmi má 5 administrátorů – v Microsoft 365 jich má 500. Sdílení nikdo neřídí a nikdo nemá přehled.

S nástupem Microsoft 365 Copilot a dalších AI nástrojů se z tohoto problému stává akutní riziko. Copilot vidí všechno, k čemu má uživatel přístup. Mzdy, smlouvy nebo personální dokumenty nasdílené příliš široce vytáhne během vteřin.

**FreeDivision.io Data** je postaven právě na tomto principu. Nehlídá cesty k datům, ale data samotná. Rozumí vašim datům a ví o nich všechno: co je citlivé, kde to leží, kdo k tomu má přístup a co s tím dělá.

# Executive Summary

Většina bezpečnostních nástrojů chrání cesty k datům. FreeDivision.io Data doplňuje chybějící vrstvu – ochranu přímo na datech, a to na souborových serverech, v Microsoft 365 a Copilotu, v e-mailu, v AI i v databázích.

Řešení stojí na principu Najít · Opravit · Hlídat. Vyhledá citlivá data a jejich expozici, automaticky odstraňuje rizika, jako jsou nadměrná oprávnění nebo rizikové odkazy, a behaviorální analytikou nepřetržitě hlídá, co se s daty děje. Nad všemi oblastmi stojí služba Managed Data Detection & Response (MDDR) s dohledem 24/7/365 a reakcí do 30 minut dle SLA.

Organizace tak získává přehled o skutečném stavu svých dat, snižuje riziko jejich úniku, bezpečně připravuje prostředí pro AI a má podklady pro NIS2, GDPR, DORA i AI Act. FreeDivision.io Data nenahrazuje stávající nástroje – doplňuje je.



**Propojte data. Získejte kontext.**
**Jednejte rychleji.**

# Jak řešení funguje

FreeDivision.io Data pracuje ve třech navazujících krocích: najde citlivá data, opraví rizika a nepřetržitě hlídá, co se s daty děje. Najít citlivá data je přitom ta snazší část – řešení nekončí u reportu, ale rizika automaticky odstraňuje.

Všechny oblasti ochrany sdílejí stejný kontext: citlivost dat, oprávnění, aktivitu a identity. O přístupech rozhodují ti, kdo datům rozumí, a nad celým prostředím drží nepřetržitý dohled tým MDDR.

## Najít

Řešení zjistí, kde leží citlivá data (osobní, finanční a regulovaná data i tajné klíče), kdo k nim má přístup a co se s nimi děje.

Při prvním průchodu skenujeme všechny relevantní typy souborů. FreeDivision.io Data následně přeskenuje jen to, co se změnilo. Výsledkem je mapa oprávnění, sdílení a expozice napříč úložišti.

## Opravit

Řešení odebírá nadměrná oprávnění a rizikové odkazy, doplňuje citlivostní štítky a archivuje zastaralá data. Vše probíhá průběžně a bez tiketů.

Odebírají se jen oprávnění, která nikdo nevyužívá, takže náprava nenarušuje práci uživatelů.

## Hlídat

Behaviorální analytika nad daty odhalí ransomware, kompromitované účty i insider threat.

Řešení vidí, že účet otevírá tisíce souborů, na které nikdy nesahal, nebo že na file serveru začalo hromadné šifrování – a zastavení útoku vynutí přes nástroje EDR dříve, než data odejdou.

## Rozhodují vlastníci dat

IT nemůže vědět, kdo má mít přístup ke složce „Obchod / Smlouvy“. To ví vedoucí obchodu. Samoobslužný portál proto přenáší rozhodování na vlastníky dat – stejně pro Windows file servery i Microsoft 365.

Uživatel požádá o přístup k datům sám a vlastník schválí jeho přístup s kontextem citlivosti dat. Přístupy na dobu určitou samy vyprší a pravidelné revize se potvrzují jedním klikem.

## Nepřetržitý dohled MDDR

Alerty ze všech oblastí sleduje, vyhodnocuje a řeší tým specialistů 24 hodin denně, 365 dní v roce, s reakcí do 30 minut dle SLA. Ozveme se, jen když je to opravdu potřeba. Služba hlídá mimo jiné pomalý ransomware, který postupně šifruje soubory, servisní účty, které poprvé sahají na citlivá data, nebo neaktivní účty dodavatelů, které začnou hromadně stahovat. Řešení se napojuje na SIEM, SOAR a ticketovací systémy.

# Klíčové schopnosti řešení

Jedna platforma, čtyři oblasti ochrany. Nad všemi stojí nepřetržitá služba MDDR.

## Souborové servery, Microsoft 365 a Copilot

Hlavní oblast: Windows file servery, NAS a Active Directory i SharePoint, OneDrive, Teams, Exchange a Entra ID. Mapa oprávnění NTFS a sdílení, úklid odkazů „kdokoli s odkazem“, audit každého přístupu a příprava prostředí před spuštěním Copilota. Doplňuje Microsoft Purview přesnými a automatickými štítky.

## Ochrana e-mailu

Phishing, BEC a podvody zastaví několik AI modelů – vizuální, jazykový a behaviorální – a AI sandbox, který denně prověří přes 100 milionů URL. Napojení přes API do Microsoft 365 za 5 minut, bez změny MX záznamů a bez zpoždění doručování.

## Ochrana AI

Inventář AI včetně shadow AI, AI Security Posture, penetrační testy AI, ochrana promptů a agentů za běhu a audity vůči EU AI Act. Řešení propojuje celý životní cyklus AI s kontextem dat.

## Databáze a další prostředí

Monitoring databází bez agentů a bez let implementace – jako cloudová služba s nasazením v řádu týdnů. Cloud AWS, Azure a GCP i SaaS jako Salesforce či Google Workspace.

# Varianty řešení

S FreeDivision.io Data lze začít analýzou rizik na vlastních datech a navázat plným provozem s nepřetržitým dohledem. Rozsah lze volit podle potřeb organizace – od souborových serverů a Microsoft 365 až po e-mail, AI a databáze.

[ANALÝZA]

## Analýza rizik dat na vašem prostředí

Nejlepší způsob, jak FreeDivision.io Data poznat, je vidět výsledky z vlastního prostředí. Řešení napojíme během pár hodin – bez infrastruktury a bez závazků.

Analýza ukáže, kde leží citlivá data a jaká je jejich expozice, co je přístupné celé firmě nebo komukoli s odkazem, kdo má nadměrná oprávnění, které identity a aplikace jsou rizikové a k čemu by se dostal útočník – nebo Copilot. Po celou dobu na prostředí dohlíží analytik MDDR.

Report vám zůstane, ať se rozhodnete jakkoli. Obdobně lze posoudit i e-mailová rizika nebo vyzkoušet ochranu AI.

[PROVOZ]

## Plně řízená ochrana dat s MDDR

Plné nasazení FreeDivision.io Data jako cloudové služby s nepřetržitou službou MDDR.

Organizace získává průběžné vyhledávání a klasifikaci citlivých dat, automatickou nápravu oprávnění a sdílení, samoobslužný portál pro vlastníky dat a behaviorální detekci hrozeb.

Alerty jsou 24/7 vyhodnoceny s reakcí do 30 minut dle SLA. Výsledky lze předávat do SIEM, SOAR a ticketovacích systémů i do prostředí FreeDivision.io Advanced.

# Typické scénáře využití

FreeDivision.io Data pomáhá organizaci identifikovat, kde leží její citlivá data, kdo k nim má přístup a co se s nimi děje.

## Bezpečné nasazení Microsoft 365 Copilot

Před nasazením řešení zjistí, co by Copilot mohl zpřístupnit všem, automaticky zúží nadměrná oprávnění a označí citlivé dokumenty štítky.

Po nasazení monitoruje prompty, odpovědi a data, na která AI sáhla, a pomáhá udržovat nejmenší možná oprávnění.

## Úklid oprávnění a sdílení

Složky přístupné „všem“ (Everyone, Domain Users), porušená dědičnost, odkazy „kdokoli s odkazem“, sdílení na celou firmu a s externisty, neaktivní účty i zastaralá data.

Řešení je najde a automaticky uklidí napříč file servery, weby, týmy i OneDrivy – bez narušení práce uživatelů.

## Detekce ransomwaru a zneužitých účtů

Příklad z praxe: přes 1 000 neúspěšných DNS odpovědí a dotazy na neobvyklé domény se znaky podvodu. Zbytek bezpečnostního stacku nic nezachytil.

Analytik MDDR alert eskaloval, na stanici byl nalezen ransomware a zákazník ji včas izoloval a infekci odstranil.

## Compliance a audit

Auditoři chtějí vědět, kde jsou osobní a regulovaná data, kdo k nim má přístup, co se s nimi dělo a jak rychle jste reagovali.

Řešení dává podklady pro NIS2, GDPR, DORA, AI Act i ISO 27001 bez ručního sběru dat – včetně auditní stopy přístupů a posouzení úniku do 72 hodin.

# Přínosy pro organizaci

Hodnotou FreeDivision.io Data není další report, ale data, která jsou průběžně pod kontrolou.



## Přehled o skutečném stavu dat

Organizace ví, kde leží citlivá data, kdo k nim má přístup a co se s nimi děje – na file serverech, v Microsoft 365, v AI i v databázích.



## Menší riziko úniku dat

Minimální oprávnění bez ruční práce, rychlejší reakce na incidenty a bezpečný základ pro AI. Útok se pomocí integrace s EDR zastaví dřív, než data odejdou.



## Snadnější compliance a nižší zátěž IT

Méně tiketů díky samoobslužnému portálu a automatizaci, doložitelné podklady pro audit a regulatorní požadavky.

# Data chráníme všude, kde leží

FreeDivision.io Data běží jako cloudová služba (SaaS) a pokrývá on-premise prostředí, Microsoft cloud, veřejný cloud i SaaS aplikace.

## On-premise

Windows file servery, NAS, UNIX/Linux, Active Directory

## Microsoft cloud

SharePoint Online, OneDrive, Teams, Exchange Online, Entra ID, Copilot, Azure

## Veřejný cloud

AWS, Azure a Google Cloud – úložiště, databáze, virtuální servery a AI služby

## SaaS týmová spolupráce

Salesforce, Google Workspace, Box, Slack, Zoom, Jira, GitHub, ChatGPT Enterprise

## Identity a síť

Active Directory, Entra ID, Okta, DNS, VPN, proxy, aplikace třetích stran

## Integrace

SIEM, SOAR, EDR/XDR, ticketovací systémy, Microsoft Purview, MCP server

### Podporované databáze

Microsoft SQL Server · Oracle · Exadata · PostgreSQL · MySQL · MariaDB · IBM DB2 · Amazon Aurora · Redshift · DynamoDB · Azure Cosmos DB · BigQuery · Snowflake · Databricks · MongoDB

### Podporované AI platformy

Azure OpenAI · AI Foundry · AWS Bedrock · SageMaker · Vertex AI · Snowflake Cortex · Databricks · OpenAI · Hugging Face

# Důkazy, které chtějí auditoři

Kde jsou osobní a regulovaná data, kdo k nim má přístup, co se s nimi dělo a jak rychle jste reagovali.

## NIS2

Zákon o kybernetické bezpečnosti

## GDPR

Ochrana osobních údajů

## DORA

Odolnost finančních institucí

## AI Act

Inventář a rizika AI

# Každá role v organizaci

FreeDivision.io Data není nástroj pro jednoho administrátora. Nad stejnými daty pracuje bezpečnost, compliance, DPO, audit, IT i samotní zaměstnanci.

## SOC

Alerty z behaviorální analytiky, rychlé vyšetření incidentů, MDDR jako rozšíření týmu.

## Security / CISO

Měřitelné snížení rizika, bezpečné nasazení Copilota, reporty pro vedení.

## IT administrátoři

Méně tiketů, automatický úklid oprávnění a skupin na Windows i v M365.

## Compliance

Podklady pro NIS2, DORA a ISO 27001 bez ručního sběru dat.

## DPO / GDPR

Kde leží osobní údaje a kdo k nim má přístup. Posouzení úniku do 72 hodin.

## Interní audit

Auditní stopa přístupů, doložené revize a schvalovací procesy.

## Vlastníci dat

Schvalují přístupy ke svým složkám a webům a provádějí revize.

## Všichni zaměstnanci

Samoobslužný portál: žádost o přístup na pár kliknutí, bez helpdesku.

# Proč FreeDivision

Úspěšná kybernetická bezpečnost nestojí pouze na moderních technologiích. Stejně důležití jsou lidé, správně nastavené procesy a schopnost dlouhodobě udržet data pod kontrolou.

Proto stavíme všechna řešení platformy FreeDivision.io na třech vzájemně propojených pilířích.

## Technologie

FreeDivision.io Data je cloudová platforma, která funguje přímo na datech. Jedna platforma pokrývá souborové servery, Microsoft 365 a Copilot, e-mail, AI i databáze a všechny oblasti sdílejí jeden kontext – citlivost dat, oprávnění, aktivitu a identity.

Databáze monitoruje bez agentů a s nasazením v řádu týdnů: tam, kde tradiční DAM potřebuje 226 komponent pro 200 DB serverů, stačí 2.

## Experti

Za ochranou dat nestojí jen technologie, ale především specialisté, kteří rozumí současným hrozbám i fungování organizací.

Alerty ze všech oblastí jsou pod dohledem týmu MDDR 24 hodin denně, 365 dní v roce a při potvrzené hrozbě se okamžitě řeší – s reakcí do 30 minut dle SLA. Organizace tak získává rozšíření vlastního bezpečnostního týmu, aniž by musela budovat vlastní SOC.

## Procesy

Ochrana dat přináší dlouhodobé výsledky pouze tehdy, pokud je součástí pravidelného a systematického procesu. FreeDivision.io Data propojuje vyhledávání citlivých dat, automatickou nápravu, rozhodování vlastníků dat, pravidelné revize přístupů a kompletní auditní stopu do jednoho opakovatelného modelu. Autorizační pravidla podle oddělení, lokality či role, etické zdi i delegace správy skupin s automatickou expirací zajišťují, že oprávnění zůstanou nejnižší možná i v čase.

# FreeDivision.io jako platforma pro komplexní kybernetickou bezpečnost

FreeDivision.io Data je součástí platformy FreeDivision.io, která propojuje technologie, odborné služby a řízení bezpečnosti do jednoho ekosystému.

Podle potřeb organizace jej lze rozšířit například o ochranu endpointů, řízení bezpečnostních operací, skenování a řízení zranitelností, správu identit a přístupů, bezpečnostní osvětu, řízení rizik nebo služby Threat Intelligence.

# Co nejlépe doplňuje FreeDivision.io Data

## Ochrana koncových zařízení

FreeDivision.io Essential zajišťuje ochranu pracovních stanic, notebooků, serverů a dalších endpointů prostřednictvím moderních technologií EDR/XDR. Společně s FreeDivision.io Data chrání jak zařízení, na kterých útok začíná, tak data, o která útočníkovi jde.

## Řízení bezpečnostních operací

FreeDivision.io Advanced poskytuje centralizované prostředí pro monitoring, korelaci bezpečnostních událostí, automatizaci reakcí a řízení bezpečnostních operací. Alerty z FreeDivision.io Data se v něm vyhodnocují společně s ostatními událostmi a vytvářejí jednotný pohled na bezpečnostní stav organizace.

## Bezpečnost identit

FreeDivision.io AuDit poskytuje rychlý přehled o rizicích identit, oprávnění a kvalitě hesel v Active Directory a Microsoft Entra ID. Doplňuje pohled na to, kdo má k datům přístup, o rizikovost samotných účtů.

## Lidský faktor

FreeDivision.io PhishingGym systematicky snižuje lidské riziko prostřednictvím phishingových simulací a vzdělávání. Phishing je přitom první krok útoku, který končí krádeží či zašifrováním dat.





# For Safety Reasons. Be Best. Not First.

## Závěr

Útočníkovi nejde o firewall ani o stanici. Jde mu o data. FreeDivision.io Data proto doplňuje stávající nástroje o chybějící vrstvu – ochranu přímo na datech.

Díky principu Najít · Opravit · Hlídat a nepřetržitému dohledu MDDR získává organizace přehled o skutečném stavu svých dat, automaticky snižuje jejich expozici a pomocí třetí strany zastaví útok dřív, než data odejdou.

Ve spojení s dalšími řešeními FreeDivision.io představuje FreeDivision.io Data přirozenou součást bezpečnostní architektury, která chrání to nejcennější, co organizace má – data.

## Připraveni zjistit, jak na tom vaše data opravdu jsou?

Začněte analýzou rizik dat – spuštění zabere jen pár hodin a uvidíte, co ve vašem prostředí skutečně je. FreeDivision.io Data napojíme na vaše prostředí a ukážeme výsledky z vašich vlastních dat. Bez infrastruktury, bez závazků – report vám zůstane.


ADRESA

FreeDivision s.r.o.
Rektorská 50/52
108 00 Praha 10 – Malešice
Česká republika

KONTAKT

sales@freedivision.com
+420 220 972 426

www.freedivision.io