FREEDIVISION

SOLUTION GUIDE

FreeDivision.io Essential

Endpoint Security

Ochrana endpointů bez investic do vlastního SOC.

Kybernetická bezpečnost začíná na endpointu

Digitální prostředí organizací je stále složitější, počet koncových zařízení roste a způsob práce zaměstnanců se zásadně proměnil. Pracovní stanice, notebooky, servery i mobilní zařízení dnes zpracovávají citlivá data, komunikují s cloudovými službami a jsou nedílnou součástí každodenního provozu.

Stejnou změnou prošli i útočníci.

Současné útoky proto stále častěji kombinují technické postupy se zneužitím uživatelských účtů, legitimních procesů a běžných pracovních nástrojů. Incidenty tak mohou zůstat dlouhou dobu neodhalené a způsobit významné provozní, finanční i reputační škody.
Ochrana endpointů je proto jedním ze základních pilířů moderní kybernetické bezpečnosti.

FreeDivision.io Essential kombinuje pokročilé technologie EDR/XDR s odbornými službami FreeDivision a poskytuje organizacím způsob, jak tuto oblast zabezpečit bez nutnosti budovat vlastní Security Operations Center (SOC).

FreeDivision.io Essential zároveň respektuje rozdílné potřeby jednotlivých organizací. Některé organizace disponují vlastním bezpečnostním týmem a požadují především kvalitní technologickou platformu. Jiné hledají kompletně řízenou službu, která převezme každodenní dohled nad bezpečnostními událostmi. Řešení proto nabízí obě varianty a umožňuje zvolit model odpovídající dostupným kapacitám i úrovni vyspělosti bezpečnostních procesů.

Executive Summary

FreeDivision.io Essential je řešení pro řízenou ochranu koncových zařízení určené organizacím, které chtějí zvýšit úroveň kybernetické bezpečnosti bez zbytečné provozní složitosti.
Řešení propojuje pokročilé technologie Endpoint Detection and Response (EDR) a Extended Detection and Response (XDR) s implementačními, konzultačními a provozními službami společnosti FreeDivision. Výsledkem je jednotné prostředí pro ochranu pracovních stanic, notebooků, serverů a dalších endpointů, které umožňuje průběžně monitorovat bezpečnostní stav zařízení, odhalovat známé i dosud neznámé hrozby a podporovat rychlou reakci na incidenty.

Na rozdíl od tradičních antivirových řešení není ochrana založena pouze na detekci známých škodlivých souborů. Řešení průběžně analyzuje chování procesů, aplikací i uživatelů, vyhodnocuje vzájemné souvislosti jednotlivých událostí a poskytuje bezpečnostním týmům potřebný kontext pro správné rozhodování. Tímto způsobem lze odhalit i útoky, které využívají legitimní systémové nástroje nebo dosud neznámé techniky. Organizace získává nejen vyšší úroveň ochrany, ale také lepší přehled o vlastním prostředí. Centralizovaný management umožňuje sledovat stav všech chráněných zařízení z jednoho místa, spravovat bezpečnostní politiky, vyhodnocovat zranitelnosti a efektivně řídit bezpečnostní opatření napříč celou infrastrukturou. Řešení je dostupné ve dvou provozních modelech.

Varianta 1 je určena organizacím, které chtějí technologii provozovat vlastními specialisty.

Varianta 2 rozšiřuje implementaci o kontinuální dohled bezpečnostních specialistů FreeDivision, vyhodnocování alertů, podporu při řešení incidentů a pravidelný reporting.

FreeDivision.io Essential představuje přirozený vstupní bod do platformy FreeDivision.io. Organizace tak získává nejen okamžitou ochranu endpointů, ale také pevný základ pro další rozvoj bezpečnostní architektury a budoucí rozšíření o pokročilé bezpečnostní služby.

Proč začít právě u endpointů

Endpoint bývá místem, kde se setkává uživatel, firemní data i podnikové aplikace – a právě proto patří k nejčastějším cílům útočníků.

Notebook otevřený mimo firemní síť, pracovní stanice s neaktualizovanou aplikací, server se zranitelnou službou nebo kompromitovaný uživatelský účet mohou představovat vstupní bod pro další postup útočníka.

Tradiční antivirová ochrana již sama o sobě nedokáže pokrýt současné techniky útoků. Úspěšná obrana proto vyžaduje průběžné sledování chování zařízení, schopnost rozpoznat odchylky od běžného provozu a možnost rychle reagovat na vznikající incident.

Právě zde přináší FreeDivision.io Essential svou hodnotu: poskytuje potřebnou viditelnost, propojuje související události do kontextu a pomáhá týmům soustředit se na skutečně významné hrozby.

Ochrana endpointů tak není pouze reakcí na jednotlivé útoky. Je základem bezpečnostní architektury, na které lze dlouhodobě stavět další vrstvy kybernetické ochrany.

Jak řešení funguje

Účinná ochrana endpointů nespočívá v jedné technologii. Je výsledkem propojení několika navazujících činností, které společně vytvářejí schopnost útok včas odhalit, správně vyhodnotit a účinně zastavit.

FreeDivision.io Essential je postaveno právě na tomto principu. Jednotlivé bezpečnostní funkce nejsou izolované, ale tvoří jeden logický celek. Řešení průběžně sbírá telemetrii z chráněných zařízení, analyzuje jejich chování, vyhodnocuje vznikající události a podle jejich závažnosti podporuje automatizovanou nebo řízenou reakci.

Výsledkem není pouze seznam bezpečnostních upozornění, ale informace, které mají jasný kontext a umožňují rychlé rozhodování.

Každý incident prochází několika navazujícími kroky.

1/ Monitorování

Řešení nepřetržitě sleduje aktivitu pracovních stanic, notebooků a serverů. Zaznamenává změny v systému, spouštěné procesy, síťovou komunikaci, práci uživatelů i bezpečnostně významné události. Organizace tak získává průběžný přehled o dění na všech chráněných zařízeních bez ohledu na jejich umístění.

2/ Detekce

Namísto spoléhání na známé signatury využívá řešení kombinaci behaviorální analýzy, pravidel detekce a korelace událostí. Takto dokáže identifikovat nejen známý malware, ale také dosud neznámé útoky, zneužití legitimních systémových nástrojů nebo nestandardní chování uživatelů.

3/ Vyhodnocení

Samotná detekce nestačí. Každá bezpečnostní událost je doplněna o kontext, který pomáhá určit její skutečný význam. Bezpečnostní tým okamžitě vidí, kterého zařízení se incident týká, kdo je přihlášeným uživatelem, jaké procesy incidentu předcházely a jaké mohou být jeho dopady na organizaci.

Právě schopnost spojit jednotlivé informace do jednoho přehledného obrazu výrazně zkracuje čas potřebný pro analýzu a rozhodnutí o dalším postupu.

4/ Reakce

Pokud je incident potvrzen, umožňuje řešení okamžitě přijmout opatření k omezení jeho dopadu. Mezi nejčastější reakce patří izolace kompromitovaného zařízení od sítě, ukončení škodlivých procesů, blokace komunikace se známými škodlivými adresami nebo omezení dalších aktivit útočníka.
Cílem není pouze odstranit důsledky útoku, ale zabránit jeho dalšímu šíření.

5/ Náprava a průběžné zlepšování

Každý bezpečnostní incident představuje zároveň příležitost ke zlepšení. Informace získané během analýzy pomáhají upravovat bezpečnostní politiky, zpřesňovat detekční scénáře a posilovat odolnost organizace vůči podobným útokům v budoucnu.

Řešení se tak nestává pouze nástrojem pro reakci na incidenty, ale důležitou součástí dlouhodobého rozvoje bezpečnostní architektury.

Klíčové schopnosti řešení

FreeDivision.io Essential poskytuje soubor funkcí, které pokrývají celý životní cyklus ochrany endpointů. Jejich cílem není přidávat další bezpečnostní nástroje do prostředí organizace, ale vytvořit jednotný systém, který zvyšuje viditelnost, urychluje reakci a usnadňuje každodenní správu.

Detekce hrozeb v reálném čase

Řešení průběžně monitoruje bezpečnostní události na všech chráněných zařízeních a okamžitě upozorňuje na podezřelé aktivity. Pomocí behaviorální analýzy dokáže rozpoznat i útoky, které neodpovídají známým signaturám nebo využívají legitimní systémové procesy.

Přínosem není pouze rychlejší odhalení hrozby, ale především možnost zasáhnout ještě před tím, než dojde ke kompromitaci dalších systémů.

Pokročilá ochrana endpointů

Řešení chrání zařízení před malware (včetně ransomware), exploity i dalšími formami útoků. Ochrana je doplněna o správu firewallu, kontrolu síťové komunikace a možnost centrální správy Microsoft Defenderu, pokud je součástí prostředí organizace.

Jednotlivé bezpečnostní mechanismy spolupracují a vytvářejí vícevrstvou ochranu bez nutnosti provozovat několik samostatných nástrojů.

Přehled o zranitelnostech

Součástí řešení je také průběžné vyhodnocování známých zranitelností koncových zařízení. Organizace získává přehled o jejich aktuálním stavu a může lépe určovat priority při plánování bezpečnostních opatření a aktualizací.

Bezpečnost se tak neřeší jako nápravné opatření až ve chvíli, kdy dojde k incidentu, ale již při odstraňování potenciálních rizik jako prevence.

Centralizovaná správa

Všechny informace jsou dostupné v jednotném managementu. Bezpečnostní tým pracuje s jedním rozhraním, ve kterém sleduje stav zařízení, analyzuje incidenty, spravuje bezpečnostní politiky a vyhodnocuje celkovou úroveň ochrany. Umožňuje ucelený vhled do úrovně bezpečnosti infrastruktury organizace.

Centralizace zjednodušuje každodenní provoz a zkracuje dobu potřebnou k řešení bezpečnostních událostí.

Kontext uživatelů a zařízení

Integrace s Active Directory nebo Microsoft Entra ID propojuje bezpečnostní události s konkrétními uživateli, skupinami a zařízeními. Bezpečnostní tým tak nepracuje pouze s technickými informacemi, ale získává širší pohled na souvislosti jednotlivých incidentů.

Správný kontext významně usnadňuje rozhodování o prioritách i následných opatřeních.

Řízení bezpečnostních politik

Součástí řešení není pouze detekce hrozeb, ale také aktivní prosazování bezpečnostních pravidel v prostředí organizace. Správně nastavené politiky významně snižují pravděpodobnost úspěšného útoku a zároveň usnadňují dodržování interních bezpečnostních standardů.

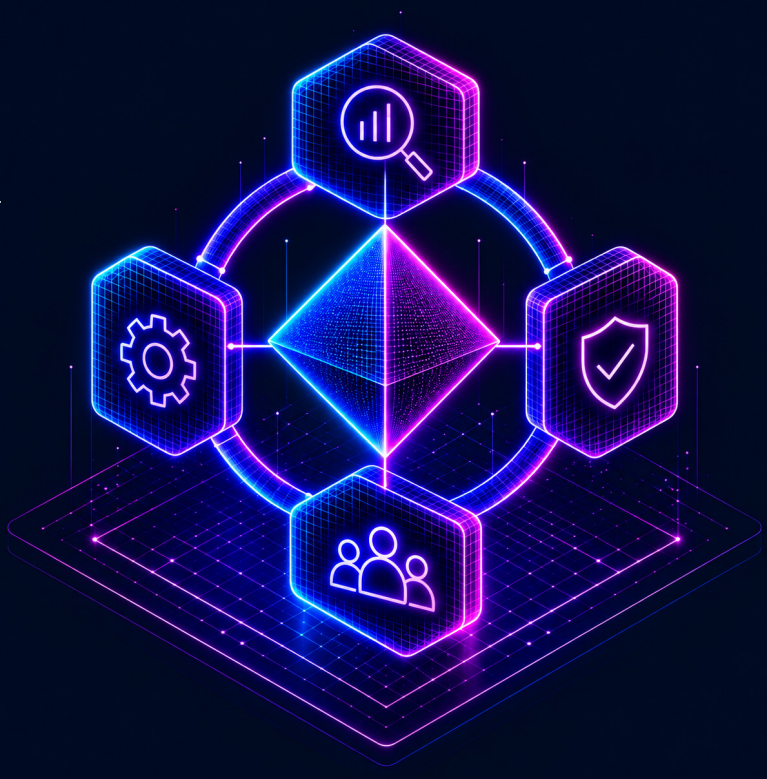
Řešení podporuje zejména:

- správu a řízení vyměnitelných médií,
- detekci a blokování neschválených USB zařízení,
- audit využívání USB portů,
- správu firewallových pravidel,
- vytváření různých bezpečnostních profilů podle typu zařízení nebo uživatele,
- podporu VPN a síťových politik,
- centrální správu bezpečnostních nastavení.

Na těchto zásadách centralizovaného řízení lze bezpečnostní opatření uplatňovat konzistentně napříč celou organizací a současně přizpůsobit jejich úroveň specifickým požadavkům jednotlivých oddělení nebo typů zařízení.

Dobře nastavené bezpečnostní politiky tak nepředstavují překážku pro uživatele, ale účinný nástroj pro dlouhodobé snižování bezpečnostních rizik.

Bezpečnostní politika se tímto způsobem stává aktivním nástrojem řízení rizik, nikoli pouze souborem statických pravidel.



Varianty řešení

Každá organizace má odlišnou úroveň interních bezpečnostních kapacit. Zatímco některé společnosti provozují vlastní bezpečnostní tým a chtějí mít plnou kontrolu nad každodenním vyhodnocováním bezpečnostních událostí, jiné preferují model, ve kterém se mohou soustředit na svůj hlavní předmět podnikání a provoz bezpečnostních technologií přenechat specialistům.

FreeDivision.io Essential proto nabízí dva jasně definované provozní modely. Oba využívají stejnou technologickou platformu i stejný způsob implementace. Liší se především tím, kdo zajišťuje každodenní dohled nad bezpečnostním prostředím a reakci na vznikající incidenty.

[VARIANTA 1]

Technologie + implementační služby

Tato varianta je určena organizacím, které disponují vlastním IT nebo bezpečnostním týmem a chtějí provozovat řešení samostatně.

Součástí dodávky je implementace technologie, návrh architektury, konfigurace prostředí, nastavení detekčních scénářů, integrace do stávající infrastruktury, projektové řízení i zaškolení administrátorů.

Po dokončení implementace přechází každodenní provoz do kompetence zákazníka. Jeho tým provádí průběžné sledování bezpečnostních událostí, vyhodnocuje vznikající alerty a rozhoduje o dalším postupu při řešení incidentů. Zákazník si tvoří vlastní scénáře a playbooky.

Tento model je vhodný zejména pro organizace, které již mají zavedené bezpečnostní procesy a potřebují moderní platformu pro ochranu endpointů.

[VARIANTA 2]

Technologie + implementace + Managed SOC

Druhá varianta rozšiřuje řešení o kontinuální dohled specialistů společnosti FreeDivision.

Vedle implementace technologie zahrnuje také průběžné monitorování endpointů, analýzu bezpečnostních událostí, vyhodnocování alertů, podporu při řešení incidentů a pravidelný reporting.

Organizace získává přístup ke zkušenostem bezpečnostních analytiků bez nutnosti budovat vlastní Security Operations Center. Interní IT tým se může soustředit na rozvoj informačních systémů a běžný provoz infrastruktury, zatímco každodenní bezpečnostní dohled zajišťují specialisté FreeDivision. Scénáře a playbooky jsou tvořeny ve vzájemné spolupráci zákazníka a specialistů SOC.

Tento model je vhodný pro organizace, které chtějí dosáhnout vysoké úrovně ochrany při zachování přehledných provozních nákladů, odpovídající kontroly a minimálních požadavků na vlastní personální kapacity.

Typické scénáře hrozeb

Současné kybernetické útoky využívají širokou škálu technik a jejich průběh je stále obtížnější rozpoznat pouze pomocí tradičních bezpečnostních nástrojů. FreeDivision.io Essential je navrženo tak, aby pomáhalo odhalovat nejčastější scénáře útoků na koncová zařízení a umožňovalo na ně rychle reagovat.

Ransomware

Ransomware patří mezi nejzávažnější hrozby současnosti. Útočníci se snaží zašifrovat firemní data, zastavit provoz organizace a následně požadovat výkupné.

Řešení průběžně sleduje chování procesů a dokáže rozpoznat aktivity typické pro šifrovací útoky ještě před jejich dokončením. V případě potvrzeného incidentu umožňuje izolovat kompromitované zařízení a zabránit dalšímu šíření útoku.

Malware a škodlivé skripty (škodlivý kód a exploitace)

Útočníci stále častěji využívají legitimní administrátorské nástroje, skriptovací jazyky nebo běžné systémové procesy. Takové útoky mohou obejít klasickou antivirovou kontrolu.

Behaviorální analýza pomáhá identifikovat nestandardní chování aplikací a odhalovat aktivity, které by jinak zůstaly skryté.

Kompromitace uživatelských účtů

Odcizené přihlašovací údaje představují jeden z nejčastějších způsobů průniku do podnikové infrastruktury.

Řešení propojuje bezpečnostní události s identitou uživatele a umožňuje rychle rozpoznat neobvyklé přihlášení, podezřelé aktivity nebo pokusy o eskalaci oprávnění.

Laterální pohyb útočníka

Bezpečnost identit se mění s každým novým uživatelem, změnou role nebo úpravou oprávnění.

Pravidelná kontrola pomáhá odhalovat zastaralé účty, nadměrná oprávnění, neaktivní identity i další rizikové změny dříve, než mohou být zneužity při skutečném útoku.

Přínosy pro organizaci

Nasazení řešení pro ochranu endpointů nepředstavuje pouze technologickou investici. Jeho skutečná hodnota spočívá v tom, že pomáhá organizaci snižovat bezpečnostní rizika, zvyšovat provozní stabilitu a efektivněji využívat vlastní odborné kapacity.

FreeDivision.io Essential bylo navrženo tak, aby přinášelo měřitelné přínosy jak managementu organizace, tak IT a bezpečnostním týmům, které zajišťují každodenní provoz.

Vyšší úroveň ochrany nejvíce exponované části infrastruktury

Koncová zařízení představují přirozený vstupní bod většiny současných kybernetických útoků. Jejich průběžná ochrana významně snižuje pravděpodobnost úspěšného průniku do podnikové infrastruktury a omezuje prostor pro šíření útočníka mezi jednotlivými systémy.

Řešení poskytuje nepřetržitý přehled o bezpečnostním stavu endpointů a umožňuje odhalovat rizika dříve, než se změní v bezpečnostní incident.

Rychlejší detekce a efektivnější reakce

Doba mezi vznikem bezpečnostního incidentu a jeho odhalením často rozhoduje o rozsahu vzniklých škod.

Bezpečnostní týmy mohou reagovat rychleji, přesněji a s lepším pochopením souvislostí jednotlivých incidentů pouze tehdy, pokud mají k dispozici průběžný monitoring, behaviorální analýzu a centralizovaný přehled o bezpečnostních událostech.

Výsledkem je kratší doba potřebná pro analýzu, rychlejší přijetí nápravných opatření a omezení dopadů útoku na provoz organizace.

Efektivnější využití interních kapacit

Nedostatek zkušených bezpečnostních specialistů představuje dlouhodobou výzvu většiny organizací.

FreeDivision.io Essential pomáhá tento problém řešit dvěma způsoby. Organizace může technologii provozovat vlastním týmem nebo využít variantu Managed SOC, ve které každodenní bezpečnostní dohled zajišťují specialisté FreeDivision.

Oba modely umožňují lépe plánovat využití interních kapacit a soustředit odborné pracovníky na činnosti s nejvyšší přidanou hodnotou.

Centralizovaný přehled o bezpečnostním prostředí

Řešení sjednocuje informace o bezpečnostních událostech, zranitelnostech, uživatelích i zařízeních do jednoho prostředí.

Bezpečnostní tým tak nemusí pracovat s několika samostatnými nástroji a může efektivněji vyhodnocovat stav celé infrastruktury.

Jednotný pohled na bezpečnostní prostředí zároveň usnadňuje plánování dalších investic a stanovování priorit při rozvoji kybernetické bezpečnosti.

Připravený na další rozvoj

Kybernetická bezpečnost není jednorázový projekt. Vyvíjí se společně s organizací, její infrastrukturou i měnícími se hrozbami. FreeDivision.io Essential proto není uzavřeným řešením. Je navrženo jako první vrstva bezpečnostní architektury, kterou lze postupně rozšiřovat o další technologie, služby i procesy podle potřeb organizace se zaměřením na hlubší ochranu dat, identit nebo exposure management a s použitím moderních prvků automatizace a pokročilé seniorní analýzy (SOAR).

Proč FreeDivision

Úspěšná ochrana endpointů není dána pouze kvalitou technologie. Stejně důležité jsou zkušenosti lidí, způsob implementace a schopnost dlouhodobě rozvíjet bezpečnostní prostředí organizace.
Proto stavíme naše řešení na třech vzájemně propojených pilířích.

Technologie

Využíváme moderní EDR/XDR platformy, které poskytují vysokou úroveň viditelnosti, pokročilé možnosti detekce a podporují rychlou reakci na bezpečnostní incidenty.

Technologie však pro nás není cílem. Je prostředkem, který umožňuje budovat dlouhodobě udržitelnou bezpečnostní architekturu.

Experti

Za každým úspěšným bezpečnostním řešením stojí lidé.

Naši specialisté navrhují architekturu řešení, zajišťují implementaci, pomáhají s optimalizací bezpečnostních politik a podle zvolené varianty poskytují také průběžný dohled nad bezpečnostním prostředím.

Organizace tak získává partnera, který rozumí technologii i praktickému provozu.

Procesy

Technologie i odborné znalosti mají největší hodnotu tehdy, pokud jsou součástí dobře nastavených procesů.

Řešení proto podporuje standardizovaný způsob detekce, analýzy a řešení bezpečnostních incidentů. Díky tomu lze dosahovat konzistentních výsledků, zkracovat dobu reakce a průběžně zvyšovat úroveň bezpečnosti.

Právě propojení technologií, expertů a procesů představuje přístup, na kterém je platforma FreeDivision.io dlouhodobě postavena.

Další rozvoj v rámci platformy FreeDivision.io

Ochrana endpointů je prvním krokem k moderní kybernetické bezpečnosti.

Jak organizace roste, rozšiřují se její informační systémy, přibývají uživatelé, aplikace i objem zpracovávaných dat. Stejně se mění také požadavky na bezpečnostní dohled, řízení rizik a automatizaci bezpečnostních procesů.

FreeDivision.io Essential je proto navrženo jako přirozený vstupní bod do platformy FreeDivision.io.

Organizace může postupně rozšiřovat své bezpečnostní schopnosti o další vrstvy ochrany:

- pokročilé řízení bezpečnostních operací
- skenování a řízení zranitelností
- správu privilegovaných přístupů
- ochranu dat
- řízení bezpečnostních rizik
- správu identit
- pokročilé služby Threat Intelligence
- phishingové kampaně
- akreditované vzdělávání v oblasti kyberbezpečnosti
- další specializované komponenty ekosystému FreeDivision.io

Jednotlivá rozšíření tak mohou navazovat na existující architekturu bez nutnosti budovat samostatná prostředí.

Výsledkem je architektura, která může růst společně s organizací.

Vzhledem k jednotné architektuře není nutné budovat jednotlivé části bezpečnostního prostředí izolovaně. Každá další vrstva navazuje na již existující řešení a rozšiřuje jeho možnosti bez zbytečné provozní složitosti.

For Safety Reasons.
Be Best. Not First.

Závěr

FreeDivision.io Essential propojuje technologii EDR/XDR, odborné znalosti a bezpečnostní procesy do jednoho modelu ochrany koncových zařízení.

Organizace si může zvolit vlastní provoz nebo plně řízenou službu podle svých interních kapacit a potřeb. V obou případech získá-vá základ pro dlouhodobé zvyšování kybernetické odolnosti i další rozvoj bezpečnostní architektury.

FreeDivision.io Essential poskytuje organizacím moderní způsob ochrany koncových zařízení založený na kombinaci pokročilých technologií, odborných znalostí a ověřených bezpečnostních procesů.

Připraveni získat kontrolu nad bezpečností endpointů?

Společně navrhneme způsob nasazení, který bude odpovídat velikosti, architektuře i bezpečnostním požadavkům vaší organizace.

FreeDivision.io Essential je prvním krokem k bezpečnostní architektuře, která roste společně s vaším podnikáním.

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