FREEDIVISION

SOLUTION GUIDE



FreeDivision.io Endpoint

Automatizovaná správa endpointů a zranitelností

Najde zranitelnosti, seřadí je podle rizika a sám je opraví – na Windows, macOS i Linuxu, na serverech, pracovních stanicích i IoT zařízeních.

Proč nestačí zranitelnosti jen najít

Skenery zranitelností, nástroje pro patchování, správa pracovních stanic i vzdálená podpora obvykle běží odděleně. Každý vidí kus pravdy – a mezi reportem a skutečnou opravou leží týdny ruční práce.

Útočníci přitom zneužívají známé zranitelnosti během dnů od zveřejnění. Ruční patchování znamená stáhnout, otestovat, naplánovat, nasadit a ověřit – zařízení po zařízení a každý měsíc znovu. Notebooky mimo firemní síť vypadnou z evidence, aplikace třetích stran zůstanou neaktualizované a ověření proběhne až při auditu.

Řada rizik navíc nevzniká chybějícím patchem, ale špatnou konfigurací. Ta v běžném reportu skeneru zapadne mezi stovky dalších nálezů a čeká ve frontě tiketů. Téměř 60 % organizací, které v posledních dvou letech zažily únik dat, uvedlo jako příčinu neopravenou známou zranitelnost.

FreeDivision.io Endpoint tuto mezeru zavírá. Zranitelnosti nejen najde, ale seřadí podle rizika a sám je opraví – patchem, změnou konfigurace nebo automatizovaným workflow – a doloží, že oprava proběhla.

Executive Summary

FreeDivision.io Endpoint nahrazuje několik oddělených nástrojů jedním. Z jedné cloudové konzole a s jedním lehkým agentem pokrývá Patch Management operačních systémů i aplikací třetích stran, vyhledání a nápravu zranitelností a chybných konfigurací, automatizaci bez programování a správu zařízení včetně vzdálené podpory.

Řešení stojí na principu Najít · Opravit · Ověřit. Automaticky vyhledá zařízení v síti i mimo ni, nasadí opravy v servisních oknech přes pilotní skupinu až do produkce a průběžně hodnotí stav každého zařízení. Rizikové zařízení umí izolovat do karantény.

Organizace tak získává přehled o všech zařízeních, rychlejší opravu zranitelností, menší útočnou plochu a méně ruční práce pro IT. Reporty slouží jako podklady pro NIS2, ISO 27001, CIS Benchmarks i PCI DSS.



Ostatní problém nahlásí.
FreeDivision.io Endpoint ho opraví.

Jak řešení funguje

FreeDivision.io Endpoint pracuje ve třech navazujících krocích: najde zranitelnosti, opraví je a ověří, že oprava zabrala. Najít zranitelnost je přitom ta snazší část – řešení nekončí u reportu, ale opravy samo nasadí.

Všechny oblasti sdílejí stejný inventář zařízení, stejné reporty a stejnou automatizaci. Na zařízení stačí jeden lehký agent, konzole běží v cloudu a není potřeba vlastní infrastruktura.

Najít

Řešení automaticky vyhledá zařízení v síti i mimo ni, včetně neřízených a IoT zařízení, a vytvoří přehled hardwaru a softwaru v reálném čase.

Průběžně skenuje chybějící patche, zranitelnosti operačního systému, bezpečnostní slabiny a chybné konfigurace a řadí je podle závažnosti a ohrožení konkrétních zařízení.

Opravit

Patche operačních systémů i aplikací, připravené opravy konfigurací a automatizovaná workflow nasadí bez tiketů a bez nočních směn.

K dispozici je knihovna více než 2 000 oprav konfigurací a 200 bezpečnostních workflow. Riziko tak lze snížit i dřív, než výrobce vydá opravu.

Ověřit

Opakovaný sken potvrdí, že riziko zmizelo. Stav zařízení se hodnotí průběžně a výsledek je v reportu pro vedení i auditory.

Organizace má doklad, že oprava proběhla – ne až při příštím auditu, ale po každé změně.

Nejdřív test, pak produkce

Patche se nejdřív nasadí na pilotní skupinu. Workflow zkontroluje prerekvizity a stabilitu zařízení a teprve potom pokračuje do produkce – bez ručního hlídání.

Nasazení probíhá v servisních oknech, která určují, kdy a kde se smí patchovat. Po dokončení přijde plánovaný report o výsledku.

Monitoring a hodnocení každého zařízení

Stav zařízení se ověřuje průběžně. Bezpečnostní profily zařízení se sestavují jednoduchým přetažením a přístup k chráněným zdrojům dostanou jen zařízení, která profil splňují. Nevyhovující zařízení se automaticky opraví, nebo izoluje do karantény, a po nápravě se průběžně vrací do shody. Výsledky lze předávat do SIEM, ticketovacích systémů a dalších nástrojů přes otevřené API.

Klíčové schopnosti řešení

Jedna konzole, čtyři oblasti. Nad všemi stojí průběžný monitoring a hodnocení každého zařízení.

Patch Management

Hlavní oblast: Windows, macOS a Linux na stanicích, noteboocích i serverech a stovky aplikací třetích stran, například Adobe, Java nebo Chrome. Automatické nasazení oprav z každého Patch Tuesday, feature updaty a upgrade Windows na místě i z vlastního ISO, servisní okna a nové patche v konzoli během hodin od vydání.

Zranitelnosti a náprava

Skener najde zranitelnosti operačního systému, bezpečnostní slabiny a chybné konfigurace a seřadí je podle rizika. Připravené a otestované opravy je odstraní automaticky – jako plánovaná úloha nebo jako reakce na změnu stavu zařízení.

Automatizace bez kódu

Workflow se skládá intuitivně přetažením, k dispozici je knihovna hotových playbooků. Sekvence pilot → ověření → produkce, PowerShell skripty jako součást workflow a self-healing, díky kterému se zařízení samo vrátí do požadovaného stavu.

Správa zařízení a podpora

Inventář, distribuce softwaru a konfigurací, vzdálený monitoring a diagnostika (Event & Process Viewer, WMI dotazy, PowerShell, CMD) a vzdálená podpora z prohlížeče se sdílením relace a přenosem souborů. Přehled a správa BitLockeru včetně úschovy klíčů.

Varianty řešení

S FreeDivision.io Endpoint lze začít bezplatným auditem zranitelností na vlastních zařízeních a navázat pilotním a plným provozem – od vybrané skupiny zařízení až po celou organizaci.

[ANALÝZA]

Audit zranitelností endpointů zdarma

Na vybraná zařízení nasadíme lehkého agenta a ukážeme výsledky z vašeho vlastního prostředí – bez vlastní infrastruktury a bez závazků.

Audit ukáže chybějící patche operačních systémů i aplikací třetích stran, zranitelnosti a chybné konfigurace seřazené podle rizika, zařízení mimo kontrolu – neaktuální, neznámá nebo bez šifrování – a shodu s CIS Benchmarks a dalšími standardy.

Součástí je doporučený plán nápravy s prioritami. Report vám zůstane, ať se rozhodnete jakkoli.

[PROVOZ]

Automatizovaná správa endpointů v provozu

Pilotní provoz na vybrané skupině zařízení s nastavením servisních oken a prvních automatických workflow, vyhodnocený s naším týmem.

Plné nasazení přináší automatický Patch Management, průběžné skenování a nápravu zranitelností, automatizaci, správu zařízení i vzdálenou podporu – pro zařízení v kanceláři, doma i na cestách.

Výsledky lze předávat do SIEM, ticketovacích systémů i do prostředí FreeDivision.io Advanced.

Typické scénáře využití

FreeDivision.io Endpoint pomáhá organizaci udržet všechna zařízení aktuální, zabezpečená a pod kontrolou – bez ruční práce.

Patch Tuesday bez přesčasů

Microsoft vydá v jednom měsíci i přes 150 oprav a některé chyby jsou už aktivně zneužívané.

Patche se automaticky nasadí na pilotní skupinu, workflow zkontroluje stav zařízení a po ověření pokračuje do produkce. Kritické zranitelnosti jsou opravené bez ručního zásahu a report je připravený pro vedení.

Oprava bez dostupného patche

Řada rizik vzniká špatnou konfigurací nebo chybou, na kterou výrobce ještě nevydal opravu.

Řešení použije připravenou opravu konfigurace z knihovny a riziko sníží ještě před vydáním patche. Opakovaný sken potvrdí, že zmizelo.

Zařízení mimo firemní síť

Notebooky doma a na cestách, včetně BYOD zařízení, často vypadnou z evidence a zůstávají neaktualizované.

Agent komunikuje s cloudovou konzolí přes internet, takže zařízení dostávají patche, opravy i vzdálenou podporu, ať jsou kdekoli.

Compliance a audit

Auditoři chtějí vědět, které patche chybí, která zařízení nevyhovují a kdy byla zranitelnost opravena.

Řešení dává podklady pro NIS2, ISO 27001, CIS Benchmarks i PCI DSS bez ručního sběru dat – včetně doloženého nasazení oprav a historie změn.

Přínosy pro organizaci

Hodnotou FreeDivision.io Endpoint není další report, ale zranitelnosti, které jsou opravené.



Přehled o všech zařízeních

Organizace ví, jaká zařízení má, co na nich chybí a v jakém jsou stavu – v kanceláři, doma, v datovém centru i v cloudu.



Rychlejší oprava a menší útočná plocha

Zranitelnosti se opravují automaticky a průběžně, rizikové zařízení lze izolovat do karantény a riziko snížit i před vydáním patche.



Méně nástrojů a ruční práce pro IT

Jedna konzole a jeden agent místo několika nástrojů, automatizace místo skriptů a doložitelné podklady pro audit.

Spravujeme zařízení všude, kde pracují

FreeDivision.io Endpoint běží jako cloudová služba a pokrývá pracovní stanice, servery i IoT zařízení – v síti i mimo ni.

Windows

Stanice, notebooky a Windows Server včetně feature updatů a upgradů

macOS

Notebooky a pracovní stanice Mac – aktualizace systému i aplikací

Linux

Servery a stanice s Linuxem – patche, skenování a vzdálené příkazy

IoT zařízení

Kamerové a vstupní systémy, HVAC i chytré měření

Virtuální a cloudové servery

Virtuální stroje a servery v cloudu, zařízení v síti i mimo ni

Integrace

Otevřené API pro integrace se SIEM, ticketovacími systémy a nástroji pro vzdálenou správu

Nástroje pro vzdálený monitoring a diagnostiku

Event Viewer | Process Viewer | WMI dotazy | PowerShell | CMD | Prohlížeč souborů | Registry | Sdílení relace | Přenos souborů | BitLocker

Důkazy, které chtějí auditoři

Které patche chybí, která zařízení nevyhovují a kdy byla zranitelnost opravena – v reportech pro vedení, auditory i regulátory.

NIS2

Zákon o kybernetické bezpečnosti

CIS

Benchmarks a kontrola konfigurací

ISO 27001

Řízení zranitelností a změn

PCI DSS

Ochrana platebních dat

Pro každého v organizaci

FreeDivision.io Endpoint není jen nástroj pro správce. Nad stejnými daty o zařízeních pracuje IT, bezpečnost, helpdesk, compliance i vedení.

IT administrátoři

Patchování, distribuce softwaru a konfigurace bez nočních směn a ručních skriptů.

Security / CISO

Měřitelné snížení útočné plochy a přehled zranitelností podle rizika.

SOC

Okamžitá izolace rizikového zařízení a rychlá náprava po incidentu.

Helpdesk

Vzdálená podpora z prohlížeče a diagnostika bez fyzického přístupu.

Compliance

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

Interní audit

Doložené nasazení oprav, stav zařízení a historie změn.

Vedení

Srozumitelné dashboardy o stavu zabezpečení zařízení a jeho vývoji.

Zaměstnanci

Aktuální a funkční zařízení, aktualizace v servisních oknech, rychlá pomoc na dálku.

Proč FreeDivision

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

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

Technologie

FreeDivision.io Endpoint je cloudová platforma s jedním lehkým agentem. Jedna konzole pokrývá Patch Management, vyhledání a nápravu zranitelností, automatizaci i správu zařízení a všechny oblasti sdílejí stejný inventář, reporty a workflow.

Knihovna více než 2 000 oprav konfigurací a 200 bezpečnostních workflow umožňuje opravovat automaticky – bez programování a i tam, kde patch ještě neexistuje.

Experti

Za správou endpointů nestojí jen technologie, ale především specialisté, kteří rozumí současným hrozbám i provozu IT v organizacích.

Náš tým pomůže s auditem zranitelností, nasazením agenta, nastavením servisních oken, skupin a workflow i s vyhodnocením výsledků. Organizace tak získává podporu zkušených techniků, aniž by musela budovat vlastní know-how od nuly.

Procesy

Správa zranitelností přináší dlouhodobé výsledky pouze tehdy, pokud je součástí pravidelného a systematického procesu. FreeDivision.io Endpoint propojuje vyhledání zařízení, skenování, prioritizaci, automatickou nápravu, nasazení přes pilotní skupinu do produkce a ověření opakovaným skenem do jednoho opakovatelného modelu. Servisní okna, bezpečnostní profily a průběžné hodnocení zařízení zajišťují, že zařízení zůstanou v požadovaném stavu i v čase.

FreeDivision.io jako platforma pro komplexní kybernetickou bezpečnost

FreeDivision.io Endpoint 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 technologiemi EDR/XDR, řízení bezpečnostních operací, ochranu dat, správu identit a přístupů, bezpečnostní osvětu, řízení rizik nebo služby Threat Intelligence.

Co nejlépe doplňuje FreeDivision.io Endpoint

Detekce a reakce na endpointech

FreeDivision.io Essential chrání pracovní stanice, notebooky a servery prostřednictvím moderních technologií EDR/XDR. Společně s FreeDivision.io Endpoint zavírá zranitelnosti dřív, než je útočník zneužije, a zároveň odhalí a zastaví útok, který přesto začne např. z důvodu nesprávného použití infikovaných periférií.

Řízení bezpečnostních operací

FreeDivision.io Advanced poskytuje centralizované prostředí pro monitoring, korelaci bezpečnostních událostí, automatizaci reakcí a řízení bezpečnostních operací. Stav zařízení a zranitelností z FreeDivision.io Endpoint se v něm vyhodnocuje společně s ostatními událostmi.

Ochrana dat

FreeDivision.io Data chrání citlivá data přímo tam, kde leží – na souborových serverech, v Microsoft 365 a Copilotu, v e-mailu i v databázích. Doplňuje zabezpečená zařízení o kontrolu nad daty, o která útočníkovi jde.

Řízení rizik

FreeDivision.io Risk propojuje aktiva, hrozby, zranitelnosti a opatření do jednoho systému řízení rizik. Výsledky správy zranitelností z FreeDivision.io Endpoint tak lze doložit v rizikové analýze i při auditu.





For Safety Reasons. Be Best. Not First.

Závěr

Zranitelnost najde každý skener. Rozhoduje ale, kdo a jak rychle ji opraví. FreeDivision.io Endpoint proto nekončí u reportu – zranitelnosti seřadí podle rizika, sám je opraví a doloží, že oprava zabrala.

Díky principu Najít · Opravit · Ověřit, automatizaci bez programování a jedné cloudové konzoli získává organizace přehled o všech zařízeních, menší útočnou plochu a méně ruční práce pro IT.

Ve spojení s dalšími řešeními FreeDivision.io představuje FreeDivision.io Endpoint přirozenou součást bezpečnostní architektury, která zavírá cesty útočníkům dřív, než jimi projdou.

Připraveni zjistit, jak na tom vaše zařízení opravdu jsou?

Začněte bezplatným auditem zranitelností endpointů. Na vybraná zařízení nasadíme lehkého agenta a ukážeme výsledky z vašeho vlastního prostředí. Bez vlastní 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