Společnost **Bitdefender je lídrem v oblasti kybernetické bezpečnosti**, který poskytuje nejlepší řešení prevence, detekce a reakce na hrozby ve své třídě po celém světě.
Celosvětově chrání více jak 500 000 000 strojů ve 150 zemích. Pomocí mnohavrstvé ochrany s využitím strojového učení a umělé inteligence umí odhalovat a zablokovat i ty nejsofistikovanější útoky (Ransomware, bez souborové, cílené atd.).

GLOBÁLNÍ VÝROBCE INOVATIVNÍ CYBER-SECURITY

s lokalizovanými produkty do češtiny s lokální podporou v ČR/SK

ZALOŽEN 2001

1,800+ ZAMĚSTNANCŮ
900+ z toho v R&D / ENGINEERING

150+ VELKÝCH CYBER-SECURITY FIREM VYUŽÍVÁ BITDEFENDER TECHNOLOGII

20K+ PARTNERŮ CELOSVĚTOVĚ
150+ OEM PARTNERŮ

CENTRÁLA BITDEFENDER JE V BUKUREŠTI V RUMUNSKU A POBOČKY MÁ V USA, VELKÉ BRITÁNII, V EVROPĚ, NA STŘEDNÍM VÝCHODĚ A V AUSTRÁLII.

UZNÁVANÝ INOVATIVNÍ LÍDR

PATENTOVÉ PORTFOLIO: 111+ SCHVÁLENÝCH, 200+ PŘED SCHVÁLENÍM. PRŮKOPNÍK V OBLASTI NASAZENÍ STROJOVÉHO UČENÍ JIŽ OD2008.

- **2008** – První detekce pomocí strojového učení
- **2011** – První algoritmus se snížením šumu vytvořený za účelem rozpoznání špatně klasifikovaných vzorců
- **2013** – První automatizovaná detekce datových toků postavená na strojovém učení
- **2014** – První použití hloubkového učení za účelem zvýšení účinnosti detekce
- **2015** – První řešení IoT bezpečnosti (Bitdefender Box)
- **2016** – Hypervisor-based memory introspection (HVI)
- **2017** – Nastavitelné strojové učení proti cíleným útokům (HyperDetect)
- **2018** – První výrobce který vytvořil nastavitelné strojové učení bezagentově
- **2019** – **První prointegrované řešení EPP s EDR obsahující Prevenci, Detekci, Odezvu a Bezpečnostní analýzuř**

PRAVIDELNĚ VÍTĚZÍ V TESTECH

AV-TEST, 4 ocenění v roce 2020

FORRESTER® WAVE LEADER 2019 Cloud Workload Security

Lídr v prvním hodnocení Forrester® WAVE™ pro zabezpečení cloudové pracovní zátěže

AV comparatives Product of the Year 2019

Nejvíce umístění na 1. místě v letech 2018 až 2021 ve srovnávacích testech AV Comparatives.

MITRE | ATT&CK®

Nejvyšší celkový počet detekcí a 100% detekce útočných technik pro Linux v hodnocení MITRE ATT&CK® 2021

FORRESTER®

"Největší dodavatel EDR, o kterém jste neuvažovali, ale měli byste", The Forrester® Wave™: 2020

THE RADICATI GROUP, INC.
A TECHNOLOGY MARKET RESEARCH FIRM

Největší hráč v oblasti Radicati Endpoint Security MQ 2020

GravityZone ULTRA

Dokonalé řešení pro ochranu koncových bodů: pokročilá prevence, rozšířená detekce, účinná reakce a analýza rizik.
GravityZone Ultra kombinuje nejúčinnější ochranu na světě s funkcemi eXtended Endpoint Detection and Response (XEDR), které vám pomohou chránit vaši infrastrukturu koncových bodů (pracovních stanic, serverů nebo kontejnerů) v celém životním cyklu hrozeb, a to s vysokou účinností a efektivitou.

Nová korelace událostí napříč koncovými body posouvá detekci a sledování hrozeb na novou úroveň tím, že kombinuje granularitu a bohatý bezpečnostní kontext EDR s analýzou celé infrastruktury XDR (eXtended Detection and Response).

Díky zabudované analýze rizik (pro rizika generovaná koncovým bodem a uživateli) a inovacím v oblasti hardeningu, nativně minimalizujeme útočný povrch koncového bodu, čímž útočníkům ztěžujeme průnik.

S řešením GravityZone Ultra zkrátíte dobu potřebnou k odhalení hrozeb a reakci na ně prostřednictvím integrovaného bezpečnostního systému, a zároveň snížíte potřebu řešení od více dodavatelů.

Jak GravityZone Ultra pomáhá?

Nejúčinnější ochrana koncových bodů na světě

GravityZone sjednocuje technologie EDR, analýzy rizik a hardeningu v jednom jediném agentovi a jedné konzoli a využívá 30 vrstev pokročilých technik k úspěšnému zastavení narušení v celém životním cyklu hrozeb, od prvního kontaktu, zneužití, setrvání a škodlivé aktivity.

eXtended Endpoint Detection and Response (XEDR)

Nová funkce detekce a reakce na koncové body rozšiřuje možnosti analýzy EDR a korelace událostí za hranice jednoho koncového bodu, aby vám pomohla efektivněji řešit komplexní kybernetické útoky zahrnující více koncových bodů. XEDR vám jedinečným způsobem poskytuje vizualizace hrozeb na úrovni organizace, abyste se mohli zaměřit na vyšetřování a efektivněji reagovat.

Zabezpečení koncového bodu a člověka na základě analýzy rizik

Bitdefender engine pro analýzu rizik vám umožňuje průběžně vyhodnocovat, upřednostňovat a zpřísňovat chybné konfigurace a nastavení zabezpečení koncových bodů pomocí přehledného seznamu priorit. Identifikuje také akce a chování uživatelů, které představují bezpečnostní riziko pro vaši organizaci.

Zjednodušením a automatizací bezpečnostních operací, a neustálým zmenšováním plochy útoku, dosáhnete nejvyšší úrovně ochrany s nejnižšími náklady na provoz.

Nejúčinnější ochrana koncových bodů na světě
Výsledkem špičkové ochrany, kterou v současné době licencuje více než 150 předních technologických společností, je více než 30 technologií ochrany vyvinutých za posledních 20 let špičkovými výzkumníky, matematiky a datovými vědci společnosti Bitdefender. Kvalitu Bitdefenderu potvrzují i výsledky nezávislých testů, kdy např. v letech 2018 až 2021 získal Bitdefender většinu 1. míst ve srovnávacích testech AV.

Lokální a cloudové strojové učení
Bitdefender poprvé spustil strojové učení v roce 2009, což vedlo ke zvýšení detekce hrozeb s nízkým počtem falešně pozitivních výsledků, které mohou zastavit neznámé hrozby před jejich spuštěním a při jejich spuštění.

Hyperdetect - nastavitelné strojové učení
Umožňuje týmům IT vyladit ochranu citlivých podnikových služeb s nejvyšším rizikem.

Obrana proti anomáliím
Pokročilá technologie strojového učení, která sleduje systémové služby a monitoruje techniky skrytých útoků. Dokáže chránit vlastní aplikace před škodlivými útoky.

Cloudový Sandbox
Zajišťuje předběžnou detekci pokročilých útoků automatickým odesíláním souborů, které vyžadují další analýzu, do cloudového sandboxu, a přijímáním nápravných opatření na základě výsledku šetření.

Obrana proti síťovým útokům
Detekce a blokování nových typů hrozeb v dřívějších fázích útočného řetězce, jako jsou útoky hrubou silou, krádeže hesel a postranní pohyb.

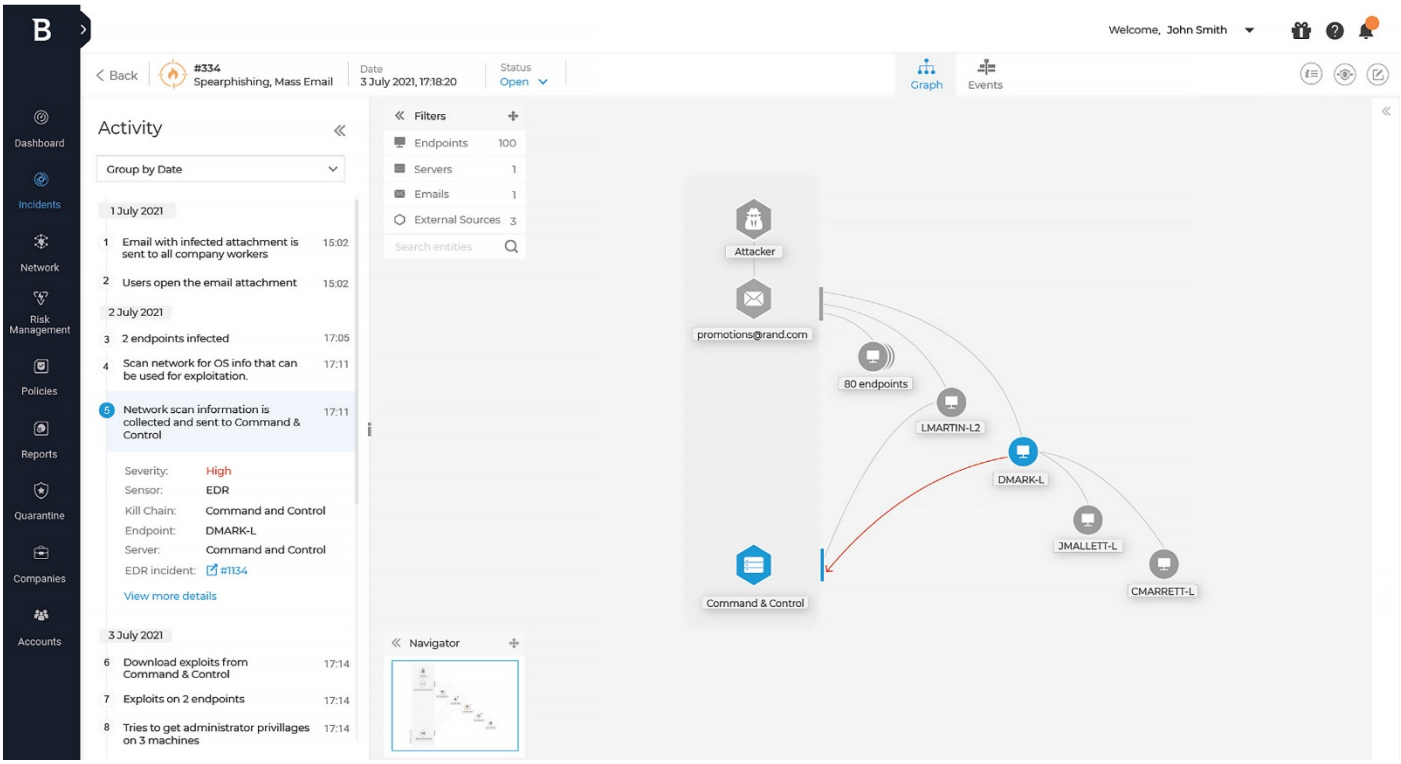
Exploit Defense
Několik mechanismů pro prevenci zneužití chrání paměť a blokuje útoky před zneužitím systémů, což snižuje nároky na zpracování.

Obrana před bez souborovým útokem
Detekce a blokování malwaru založeného na skriptech, bez souborů, obfuskovaného a vlastního malwaru s automatickou nápravou.

Rozšířené vyšetřování incidentů a inteligentní reakce pro rozvinuté systémy

GravityZone Ultra umožňuje efektivní vyšetřování incidentů a rychlou reakci pro obnovení koncových bodů do stavu "lepšího než předtím". Nástroje pro vyšetřování incidentů, jako je Extended Incident View, poskytují přehled o bezpečnostních incidentech na úrovni organizace a pomáhají bezpečnostním týmům ověřovat podezřelé aktivity a adekvátně reagovat na kybernetické hrozby. Pokročilé vyhledávání aktuálních a historických dat na základě IOC, značek MITRE a dalších relevantních artefaktů, umožňuje rychlou identifikaci hrozeb, které se mohou skrývat v infrastruktuře koncových bodů.

Na základě informací získaných z koncových bodů během vyšetřování poskytuje jednotné rozhraní pro řízení nástrojů pro okamžitou úpravu zásad a/nebo záplatování zjištěných zranitelností, aby se předešlo budoucím incidentům a zlepšilo se zabezpečení prostředí.



Rozšířený pohled na incident poskytuje přehled o incidentu na úrovni organizace. Bezpečnostní analytik může snadno získat podpůrné důkazy a účinně reagovat. Analýza rizik koncových bodů pro nepřetržitou správu útočné plochy

Klíčové vlastnosti

eXtended Endpoint Detection and Response (XEDR)
Tato technologie korelace napříč koncovými body, známá jako eXtended EDR, posouvá detekci hrozeb a jejich viditelnost na novou úroveň tím, že využívá funkce XDR pro detekci pokročilých útoků napříč více koncovými body v hybridních infrastrukturách (pracovní stanice, servery nebo kontejnery s různými OS).

Integrovaná analýza lidských rizik a rizik koncového bodu
Průběžně analyzujte rizika pomocí stovek faktorů, abyste odhalili a upřednostnili konfigurační rizika pro všechny koncové body a umožnili automatické akce na jejich posílení. Identifikuje akce a chování uživatelů, které představují bezpečnostní riziko pro organizaci, jako je používání nešifrovaných webových stránek pro přihlašování na webové stránky, špatná správa hesel, používání kompromitovaných USB, opakované infekce atd.

Vrstvená obrana
Technologie bez signatur, včetně pokročilého lokálního a cloudového strojového učení, technologie analýzy chování, integrovaného sandboxu a vytvrzení (hardening) zařízení, fungují jako vysoce účinná vrstvená ochrana proti sofistikovaným hrozbám.
Integrovaná analýza lidských rizik a rizik koncového bodu

Vyšetřování a reakce na incidenty s nízkými náklady
Rychlé třídění upozornění a vyšetřování incidentů pomocí časové osy útoku a výstupu ze sandboxu umožňuje týmům pro reakci na incidenty rychle reagovat a zastavit probíhající útoky (reakce na jedno kliknutí).

Moderní prevence a detekce nové generace s automatickou nápravou
Nejlepší prevence na světě a funkce detekce, založené na chování při spuštění, zabraňují spuštění pokročilých hrozeb v podnikové infrastruktuře a zastavují je. Díky pokročilým funkcím prevence, jako jsou PowerShell Defense, Exploit Defense a Anomaly Detection, blokuje GravityZone Ultra moderní útoky v dřívějších fázích útočného řetězce, v době před jejich provedením, čímž zajišťuje neprůstřelnost zabezpečení vaší organizace. Po zjištění aktivní hrozby se spustí automatická reakce pro zablokování dalšího poškození nebo postranních pohybů.

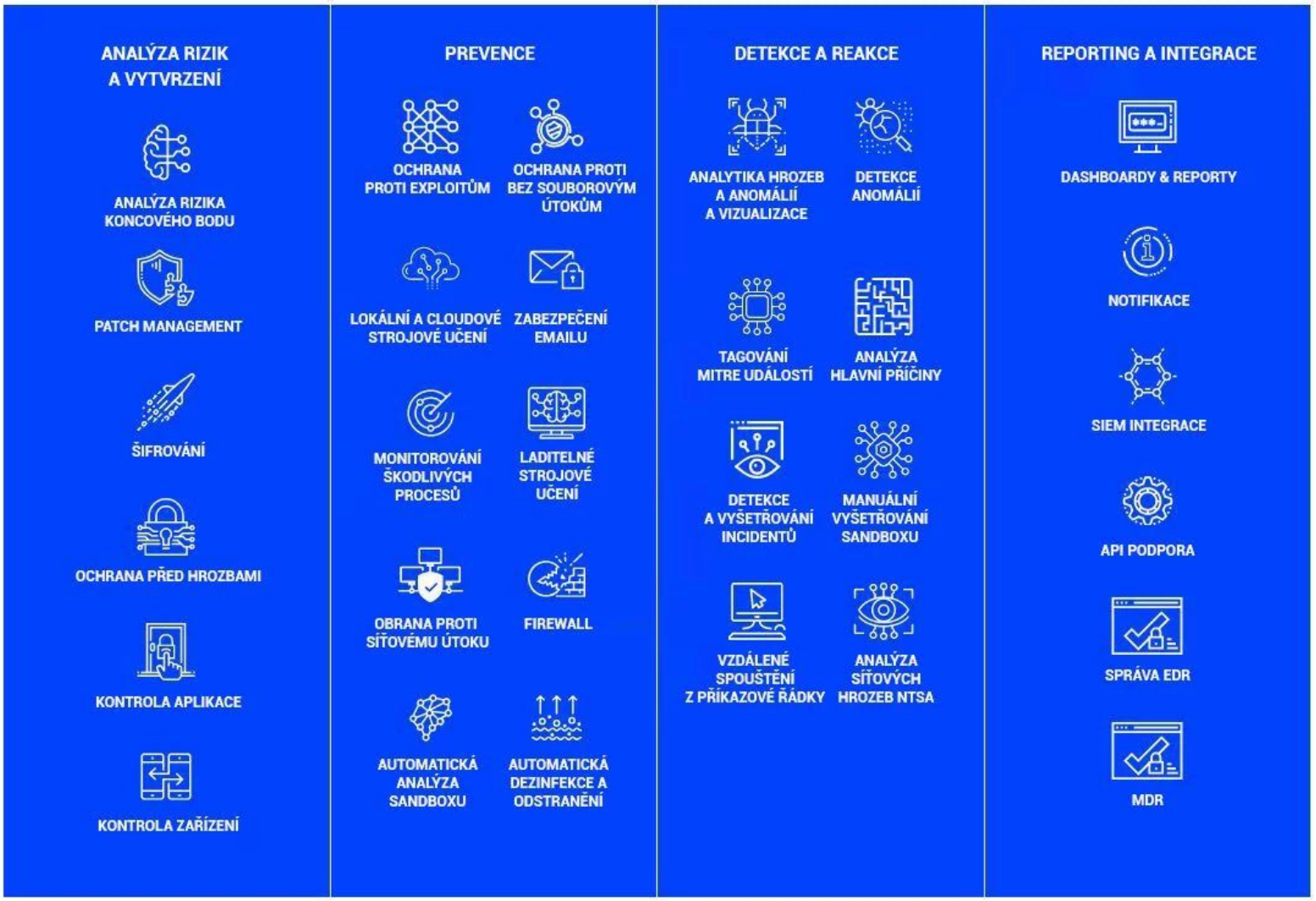
Ochrana proti síťovým útokům
Bitdefeder Network Attack Defense, nová vrstva zabezpečení koncového bodu sítě navržená tak, aby detekovala a zabránila pokusům o útok, které využívají síťové zranitelnosti, blokuje několik síťových útoků založených na datovém toku, jako je Brute Force, Password Stealers nebo Lateral Movement, ještě předtím, než se mohou spustit. Network Attack Defense také generuje incidenty EDR a je důležitým zdrojem informací pro korelace incidentů EDR.

Pokrytí napříč platformami a integrace API třetích stran
Pokrývá všechny podnikové koncové body se systémem Windows, Linux nebo Mac ve fyzické, virtualizované nebo cloudové infrastruktuře, a poskytuje konzistentní zabezpečení napříč celou infrastrukturou. Podporuje integraci s již existujícími nástroji pro bezpečnostní operace (včetně Splunku) a je optimalizován pro technologie datových center včetně všech hlavních hypervizorů.

Technologie GravityZone Ultra

Vytvořeno pro zvýšení kybernetické odolnosti

Bitdefender GravityZone Ultra spoléhá na architekturu jednoho agenta/jedné konzole, která poskytuje kompletní sadu bezpečnostních funkcí, přehled z jednoho okna a integrovanou správu v celém podnikovém prostředí: pracovní stanice (fyzické i virtuální), servery a cloudové pracovní zátěže. GravityZone je cloudově orientované řešení, ale podporuje také nasazení v lokálních prostředích, pokud to vyžadují předpisy nebo obchodní požadavky.



Bitdefender GravityZone Ultra: Jednotná prevence, rozšířená detekce, reakce a analýza rizik

eXtended Endpoint Detection and Response Business Security (XEDR)

Bitdefender v červenci 2021 dnes představil další evoluci řešení pro detekci a reakci na koncové body - eXtended EDR (XEDR) s přidáním analytiky a korelace bezpečnostních událostí napříč koncovými body do řešení Bitdefender Endpoint Detection and Response (EDR) a GravityZone Ultra, jednotné platformy pro prevenci, detekci a reakci na koncové body a analýzu rizik. Tyto nové funkce zvyšují účinnost zabezpečení pro identifikaci a zastavení šíření útoků ransomwaru, pokročilých trvalých hrozeb (APT) a dalších sofistikovaných útoků dříve, než ovlivní provoz podniku.

Díky integrované detekci a reakci napříč operačními systémy (Windows, Linux, Mac) a hybridními prostředími (veřejný a soukromý cloud, on-premises) poskytuje Bitdefender komplexní pohled na bezpečnostní operace v reálném čase, což výrazně zlepšuje schopnost organizací všech velikostí, dokonce i těch, které nemají bezpečnostní analytiky na plný úvazek, odhalovat skryté útoky, které by při izolované analýze a detekci na jednotlivých koncových bodech zůstaly nepovšimnuty.

Sofistikované útoky navržené tak, aby se vyhnuly detekci bezpečnostních technologií, často napodobují "normální" procesy nebo se provádějí ve více fázích prostřednictvím různých vektorů včetně koncových bodů, sítí, dodavatelských řetězců, hostovaných IT a cloudových služeb. Bitdefender XEDR zabraňuje komplexním útokům tím, že přijímá, zkoumá a koreluje telemetrii napříč koncovými body, aby odhalil indikátory kompromitace (IOC), techniky APT, signatury malwaru, zranitelnosti a abnormální chování. Toto pokročilé monitorování automatizuje včasnou detekci scénářů útoku a poskytuje pracovníkům zabezpečení a IT jednotný přehled o tom, kde útok začal.

Nové funkce XEDR také vylepšují řízenou detekci a reakci (MDR) Bitdefender tím, že poskytují větší přehled a kontext incidentu během vyšetřování, aby se urychlilo ověřování hrozeb, reakční akce a náprava.

Více informací o **EDR a jeho praktické použití** najdete ve dvoudílném videu na našem blogu

Bitdefender Ransomware Mitigation

Ransomware je již dlouhou dobu lukrativním byznysem, který kyberzločincům vynáší miliardy na zaplacených výkupných. Nyní, když už je ziskovost ransomwaru prokázána, hledají zločinecké organizace nové a nové způsoby, jak na svých investicích ještě více vydělat, což povede k čím dál více sofistikovaným útokům na firmy a organizace.

Jak Bitdefender GravityZone poráží ransomware?
Jako adaptivní vrstvené bezpečnostní řešení poskytuje Bitdefender GravityZone několik funkcí proti ransomwaru, přičemž všechny jeho vrstvy spolupracují při prevenci, detekci a nápravě.

Více blokovacích vrstev	Koncový bod a síť, před provedením a při spuštění, na bázi souborů a bez souborů
Více detekčních vrstev	Kontrola procesů, monitorování registrů, kontrola kódu, hyperdetekce
Více vrstev obnovy	Účinný rollback z místního počítače, vzdáleného systému nebo bezpečnostního incidentu
Adaptivní obranné mechanismy	Pokročilý Anti-Exploit, adaptivní heuristika, konfigurovatelné strojové učení
Technologie pro minimalizaci rizik	Automatické opravování zranitelností, chybné konfigurace systému, chování uživatelů
Zálohy odolné proti neoprávněné manipulaci	Nepoužívá se zranitelná stínová kopie, ransomware nemůže odstranit zálohy.
Vzdálené blokování ransomwaru	Blokuje vzdálené a síťové útoky ransomwaru, a zařazuje IP adresy útočníků na černou listinu.
Čištění v rámci celé organizace	Vzdálené ukončování procesů, snadná globální karanténa a odstraňování souborů

Příklady použití **Případ použití Bitdefender Ransomware Mitigation** najdete ve videu na našem blogu.

Stáhněte si příručku „**Ransomware - Prevence a zmírnění škod pomocí Bitdefender GravityZone**“

Sandbox Analyzer

Bitdefender Sandbox Analyzer je bezpečnostní řešení, které posiluje bezpečnostní infrastrukturu organizace proti sofistikovaným nebo cíleným útokům. Díky pokročilým detekčním a reportovacím schopnostem chrání před těžko zachytitelnými a přetrvávajícími hrozbami, které se snaží proniknout do vaší sítě.

Pokročilá detekce a viditelnost
Kombinuje vlastní toky zpravodajských informací o hrozbách s proprietárním strojovým učením a detekcí chování pro maximální přesnost v reálném čase. Zobrazuje interaktivní vizualizační grafy bezpečnostních incidentů pro hloubkovou forenzní analýzu. Detekuje velmi sofistikované, na míru vytvořené hrozby cílící na konkrétní prostředí pomocí golden image support.

Kompatibilní a efektivní
Prevence a detekce jsou prováděny plně na místě, bez souborů odeslaných pro skenování mimo vaši síť. Využívá AI a inteligenci hrozeb Bitdefender vytvořenou z více než 500 milionů uživatelů na celém světě, aby byla zachována přesná detekce v reálném čase na místní úrovni. Odhaluje nejpokročilejší typy malwaru, jako jsou APT nebo C2, a to prostřednictvím technologií anti-evasion a anti-fingerprint.

Integrovaný, automatizovaný, škálovatelný
Aby se prolínal s architekturou zabezpečení, integruje se nativně s technologiemi Bitdefenderu, a prostřednictvím API s dalšími prvky zabezpečení. Automatizuje proces výběru a odesílání souborů pro provedení karantény, a umožňuje autonomní reakci. Běží jako virtuální zařízení, může být snadno upraven tak, aby podporoval rostoucí toky dat.

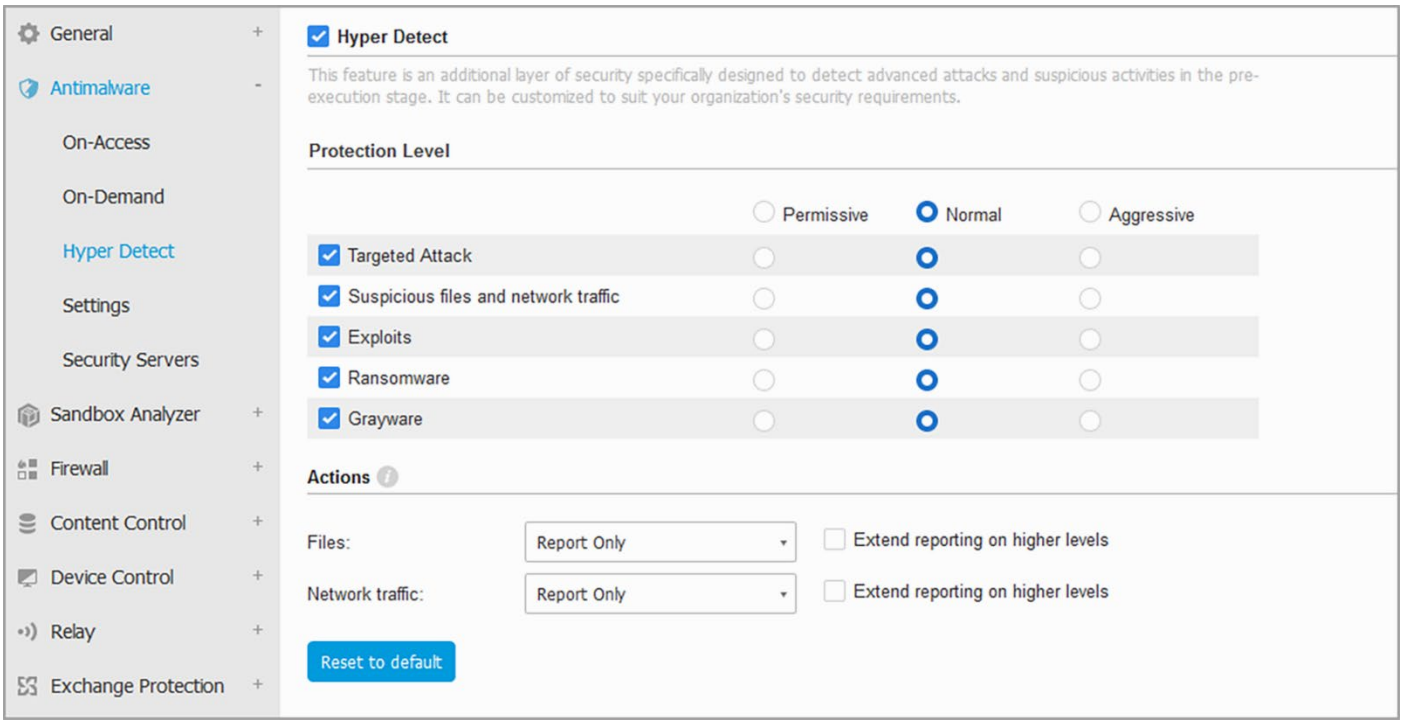
Více informací najdete na stránce produktu na našem webu Bitdefender.cz

Stáhněte si Datasheet „**GravityZone™ Sandbox Analyzer**“

HyperDetect

Tato obranná vrstva ve fázi před spuštěním obsahuje lokální modely strojového učení a pokročilé heuristiky vycvičené k odhalování hackerských útoků, nástrojů, exploitů a obfuskačních technik malwaru, aby bylo možné zablokovat sofistikované hrozby ještě před jejich spuštěním. Detekuje také způsoby šíření a stránky, které hostí sady zneužití, a blokuje podezřelý webový provoz.

HyperDetect umožňuje správcům zabezpečení upravit obranu tak, aby co nejlépe čelila konkrétním rizikům, kterým organizace pravděpodobně čelí. Díky funkci "pouze hlášení" mohou správci zabezpečení před zavedením nové obranné politiky připravit a sledovat její průběh, čímž se eliminuje přerušení provozu. V kombinaci vysoké viditelnosti a agresivního blokování, která je pro Bitdefender jedinečná, mohou uživatelé nastavit HyperDetect tak, aby blokoval na normální nebo povolené úrovni, a zároveň pokračovat v automatickém hlášení na agresivní úrovni, čímž odhalí včasné indikátory kompromitace.



HyperDetect umožňuje správcům zabezpečení upravit agresivitu obrany a nabídnout možnost. jedinečnou kombinaci blokování a viditelnosti hrozeb. Například blokování na úrovni "Normální".a hlášení na úrovni "Agresivní".

SPECIALITY & ADD-ON

GravityZone Security for Containers

Vysoce výkonné zabezpečení kontejnerů a serverových zátěží Linuxu, které je nezávislé na platformě.
Bitdefender GravityZone Security for Containers chrání kontejnerové a cloudové pracovní zátěže před moderními útoky na Linux a kontejnery pomocí prevence hrozeb s umělou inteligencí, technologií proti zneužití specifických pro Linux, a detekce a reakce na kontext (EDR).

Na rozdíl od jiných řešení nevyžaduje agent Bitdefender pro koncové body pro Linux komponenty linuxového jádra, což umožňuje nasazení nových distribucí, jakmile na ně chce vaše organizace přejít, aniž by vás to omezovalo v zabezpečení.

S naším platformově orientovaným, vysoce výkonným zabezpečením pracovních zátěží získáte konzistentní přehled a kontrolu nad všemi kontejnery a pracovními zátěžemi v hybridních a multicloudových prostředích.

Vlastnosti & výhody

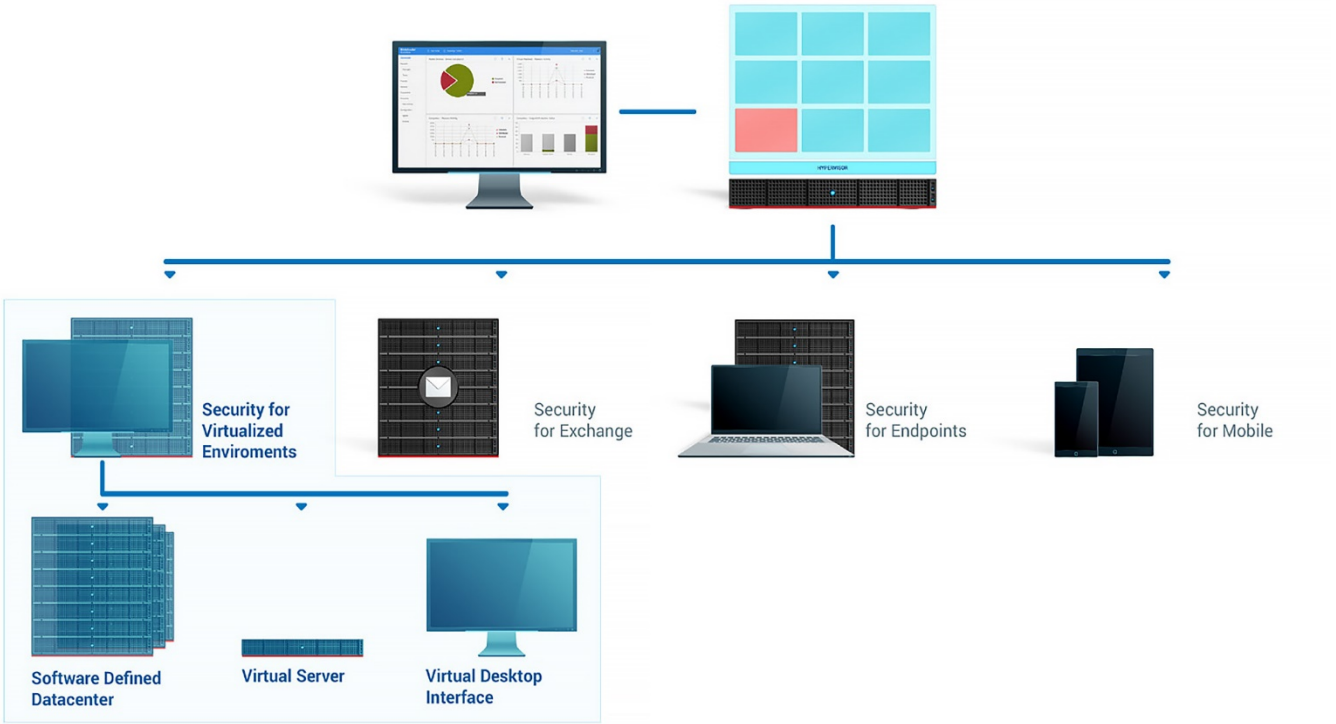
- EDR vytvořená pro Linux a kontejnerové pracovní zátěže
- Detekuje hrozby v reálném čase a umožňuje rychlou reakci
- Vysoce výkonný bezpečnostní agent nezávislý na platformě
- Zajišťuje minimální dopad na zdroje, zjednodušuje provoz a zvyšuje návratnost investic do cloudu
- Kontextově orientované hlášení incidentů a forenzní analýza
- EDR vytvořená pro Linux a kontejnerové pracovní zátěže
- Pokročilý nástroj Anti-Exploit pro Linux
- Blokuje jádro Linuxu, aplikace zero-day a známé exploit útoky
- TTP útočníka mapované na MITRE pro Linux
- Zaměřuje se na hrozby specifické pro systém Linux a zobrazuje kontextově bohaté informace
- Jednotná platforma GravityZone pro CWS i mimo ni
- EDR Podporuje jednotný přehled a řízení všech pracovních zátěží, kontejnerů, operačních systémů a cloudů.

GravityZone Security for Virtualized Environments

Vysoce výkonné zabezpečení pro hybridní a multicloudová prostředí
Bitdefender GravityZone Security for Virtualized Environments (SVE) je platformově orientované řešení ochrany navržené pro virtualizaci a hybridní cloud. Poskytuje osvědčené, vysoce výkonné zabezpečení v privátních i veřejných cloudových prostředích a přispívá k tomu, že společnost Bitdefender byla uznána jako lídr v nejnovější zprávě Forrester WaveTM: Cloud Workload Security, Q4 2019.

Podniky přijímají GravityZone SVE, aby minimalizovaly dopady na výkon zabezpečení cloudových výpočetních zdrojů a automatizovaly správu zabezpečení díky bezproblémové integraci s technologiemi VMware, Citrix, Nutanix a předními veřejnými cloudy, jako jsou Amazon a Azure.

Účelově vytvořený bezpečnostní zásobník cloudu a architektura s vysokou dostupností nabízejí robustní ochranu proti sofistikovaným útokům. GravityZone SVE konsoliduje správu zabezpečení nejen pro pracovní zátěže v hybridních a multicloudových prostředích, ale také pro fyzické desktopy, servery, mobilní zařízení a e-mail.



Bitdefender GravityZone (SVE) je nejpokročilejší bezpečnostní řešení pro virtualizovaná datová centra na trhu, pokud jde o antimalwarovou ochranu virtuálních počítačů, které optimalizuje nejen poměr konsolidace, ale také provozní náklady. GravityZone SVE je navrženo jako podnikové řešení schopné podporovat největší datová centra. Integrace do produkčního prostředí je však mimořádně jednoduchá a výhody technologie lze využít ve virtuálních prostředích libovolné velikosti.

GravityZone Email Security

Vícevrstvé cloudové zabezpečení e - mailů pro vaši organizaci a MSP.
S řešením GravityZone Email Security mohou organizace využívat kompletní ochranu podnikové elektronické pošty, která přesahuje rámec malwaru a dalších tradičních hrozeb, jako jsou spam, viry, rozsáhlé phishingové útoky a škodlivé adresy URL. Zabraňuje podvodům a vydávání se za někoho jiného, využívá několik předních bezpečnostních motorů a behaviorálních technologií k analýze obsahu příchozích a odchozích e-mailů, adres URL a příloh.

Vlastnosti & výhody

- **Více antivirových mechanismů založených na signaturách a chování** nabízí ochranu před všemi formami malwaru, včetně variant zero-day.
- **Ochrana při kliknutí** přepisuje adresy URL v e-mailových zprávách a chrání uživatele při kliknutí pomocí flexibilních zásad a stránek s upozorněním na blokování a varování.
- Možnost vynucení **šifrování TLS** a omezení komunikace s jinými e-mailovými servery, které nepodporují protokol TLS.
- **SecureMail** poskytuje jednoduché řešení šifrování e-mailů pro ochranu citlivých dat při přenosu.
- **Monitorování omezení odesílání** automaticky chrání před pokusy o odesílání velkého množství odchozích zpráv a pomáhá tak zabránit zařazení domény a IP na černou listinu.
- **Podpora protokolů SPF, DKIM a DMARC**, které pomáhají chránit proti útokům typu "vydávání se za někoho jiného".
- **Prevence Directory harvesting attack (DHA**) blokuje útoky directory harvesting tím, že uzavře spojení s příjemcem, jakmile je dosaženo prahové hodnoty neplatné / falešné e-mailové adresy.
- **Nearby (cousin) Domains** porovnává domény odesílatele s legitimními názvy domén a identifikuje blízké domény (které se od skutečného názvu domény liší o jeden nebo dva znaky).
- **Blokování příloh souborů** zahrnuje kontrolu MIME příloh a schopnost detekovat archivy chráněné heslem.
- **Opakované porovnávání vzorů**, algoritmická analýza, analýza na úrovni připojení a ověřování odesílatele/serveru, v kombinaci se zpravodajstvím o hrozbách, přináší další výkonnou vrstvu zabezpečení, která chrání uživatele služby Microsoft 365.
- Funkce **Executive Tracking** využívá údaje synchronizované ze služby Active Directory k automatickému zjišťování skutečných jmen uživatelů v polích záhlaví a obálek s adresami, aby byla zajištěna ochrana proti útokům typu "vydávání se za jiné osoby" a CEO podvodům.

GravityZone Patch Management

Bezpečnostní a jiné než bezpečnostní záplaty.
I když je phishing hlavní příčinou narušení bezpečnosti, stejně důležitá je správa a záplatování interních systémů. Analytická společnost Gartner předpovídá, že "do konce roku 2020 bude 99 % zneužívaných zranitelností i nadále patřit mezi ty, které jsou známé odborníkům na bezpečnost a IT".

Přídavný modul Patch Management, plně integrovaný do platformy GravityZone, umožňuje organizacím udržovat operační systémy a softwarové aplikace aktuální a poskytuje komplexní přehled o stavu záplat v celé instalační základně systému Windows. Modul záplatování poskytuje aktualizace pro celou flotilu pracovních stanic, fyzických serverů nebo virtuálních serverů.

Modul GravityZone Patch Management obsahuje několik funkcí, například skenování záplat na vyžádání / plánované skenování záplat, automatické / ruční záplatování nebo hlášení chybějících záplat.

Podniky, které záplatují své koncové body, posílí svou bezpečnostní pozici a soulad s předpisy a zároveň zvýší provozní efektivitu.

Vlastnosti & výhody

- Aktualizace operačního systému a největší množiny softwarových aplikací
- Automatické a ruční aktualizace
- Podrobné informace o aktualizacích - CVE, ID bulletinu, závažnost záplaty, kategorie záplaty
- Možnost nastavení různých plánů pro bezpečnostní a jiné než bezpečnostní aktualizace
- Rychlé nasazení chybějících aktualizací
- Možnost distribuovat aktualizace ze serveru relay, což snižuje síťový provoz.
- Specifické zprávy o aktualizacích, které pomáhají společnostem prokázat dodržování předpisů
- Automatické upozornění správce IT na chybějící bezpečnostní/nebezpečnostní aktualizace.

GravityZone Full Disk Encryption

Původní, osvědčený šifrovací doplněk pro zabezpečení firemních dat.
Data jsou v digitální ekonomice nejdůležitějším aktivem. Ochrana důvěrných dat, splnění požadavků na dodržování předpisů a prevence nákladných úniků dat, jsou klíčovými pilíři strategie ochrany podnikových dat.

GravityZone Full Disk Encryption je řešení, které pomáhá společnostem dodržovat předpisy týkající se dat, a předcházet ztrátě citlivých informací v případě ztráty nebo odcizení zařízení.

GravityZone Full Disk Encryption šifruje bootovací i ne bootovací svazky, na pevných discích, ve stolních počítačích a noteboocích, a poskytuje jednoduchou vzdálenou správu šifrovacích klíčů.

Toto řešení poskytuje centralizovanou správu nástrojů BitLocker (v systému Windows), FileVault a nástroje příkazového řádku diskutil (obojí v systému macOS), přičemž využívá výhod nativního šifrování zařízení a zajišťuje optimální kompatibilitu a výkon. Vyměnitelné disky nejsou šifrovány.

Vlastnosti & výhody

- Nativní, osvědčené šifrování, které využívá šifrovací mechanismy poskytované systémy Windows a Mac
- Jedna konzola pro ochranu koncových bodů a správu šifrování
- Specifické zprávy o šifrování, které pomáhají společnostem prokázat shodu s předpisy
- Vynucení ověřování před spuštěním systému

KONTAKTNÍ INFORMACE

Bitdefender GOLD PARTNER

CYBOSEC s.r.o.
Bitdefeder GOLD Partner

Hradčany 347, Smidary
Česká republika

+420 736 174 250
pavel.jicha@cybosec.com

Technická podpora

Provozní doba:	Po - Pá (09:00 - 17:00)
tel.:	+420 245 501 801
email:	helpdesk@bitdef.cz
web:	support.bitdef.cz

CYBOSEC We build the Trust

Bitdefender

Datasheet

GravityZone Patch Management

Aktualizujte a zabezpečujte systémy pomocí automatického záplatování.

Neopravené bezpečnostní chyby v oblíbených aplikacích představují významnou hrozbu pro bezpečnost IT. Avšak správa a administrace aktualizací softwaru může být pro IT oddělení zdlouhavá a časově náročná. GravityZone Patch Management umožňuje automatizovat záplatování operačních systémů a aplikací pomocí přesných kontrolních mechanismů a robustního reportování. Pokrývá celou instalační základnu systému Windows: pracovní stanice, fyzické servery i virtuální servery.

GravityZone Patch Management překonává ostatní řešení díky velmi rychlému skenování záplat, podpoře nejširší základny aplikací třetích stran, detailním možnostem a vysoké spolehlivosti. Konsolidací záplatování a zabezpečení dále snížíte náklady a zefektivníte správu a reportování. Přídavný modul Patch Management, plně integrovaný do platformy GravityZone, umožňuje organizacím udržovat operační systémy a softwarové aplikace aktuální, a poskytuje komplexní přehled o stavu záplat v celé instalační základně systému Windows.
Modul GravityZone Patch Management zahrnuje několik funkcí, například skenování záplat na vyžádání / plánované skenování záplat, automatické / ruční záplatování, nebo hlášení chybějících záplat. Podniky, které záplatují své koncové body, posilují svou bezpečnostní pozici a kompatibilitu s požadavky právních nařízení, a současně zvyšují provozní efektivitu.

Hlavní výhody:

- **Minimalizace bezpečnostních rizik** - výrazné zkrácení doby potřebné k opravě kritických zranitelností.
- **Zlepšení kybernetické hygieny a produktivity vašeho IT týmu** - automatizujte skenování záplat, jejich nasazení a reportování.
- **Zjednodušení reportování o záplatách a o souladu s právními předpisy** - splnění požadavků na řízení rizik
- **Snížení nákladů** - konsolidace správy záplat a zabezpečení koncových bodů u jediného dodavatele a na jediné platformě.
- **Zvýšení produktivity zákazníků** - s aktuálními aplikacemi a menším počtem problémů ,nebo se zpomalením systémů.

Bitdefender
BUILT FOR RESILIENCE

Přehledně

Modul GravityZone Patch Management podporuje automatické i ruční záplatování. Poskytuje organizaci větší flexibilitu a efektivitu při správě záplat, díky možnosti vytvářet inventář záplat, plánovat skenování záplat, omezit automatické záplatování na aplikace preferované správcem, měnit plánování bezpečnostních a jiných záplat, a odložit restartování u záplat vyžadujících restart.

Hlavní výhody

- Zajišťuje soulad s legislativními požadavky na zabezpečení informací, jako jsou GDPR, HIPAA a PCI DSS.
- Podporuje automatické i manuální záplatování, což organizacím poskytuje větší flexibilitu a efektivitu celého procesu, a to jak na pracovišti, tak vzdáleně.
- Udržuje operační systémy a softwarové aplikace v aktuálním stavu, a poskytuje komplexní přehled o stavu záplat v celé instalační základně systému Windows, čímž snižuje riziko pokročilých útoků.

"Bitdefender Patch Management je fantastický. Pokud se objeví oprava zero-day, Bitdefender dokáže rychle aktualizovat celou organizaci nejnovější bezpečnostní záplatou. Dodržování záplat se zvýšilo ze 75 na téměř 99 procent. Dříve bylo obvyklé, že pracovní stanice ve vzdálených lokalitách zůstávaly roky bez aktualizace."

Arcidiecéze USA,
IT Director

Funkce a vlastnosti

Nejrychlejší skenování a nasazení záplat

GravityZone Patch Management dokáže během několika sekund prohledat systémy a najít chybějící záplaty. Po identifikaci lze tyto záplaty rychle nasadit pomocí automatických nebo ručních postupů.

Podpora největší množiny aplikací třetích stran, operačních systémů Windows a Linux.

Snadno záplatujete nejen operační systémy Windows a Linux, ale také nejrozsáhlejší seznam aplikací, které vaši zákazníci s největší pravděpodobností používají. Centralizujte záplatování napříč lokalitami, fyzickými i virtuálními pracovními stanicemi a servery.

Vylepšené pracovní postupy s flexibilním automatizovaným a řízeným záplatováním

Můžete vytvářet inventář záplat, plánovat skenování záplat, vybírat aplikace, které mají být automaticky záplatovány, měnit plánování bezpečnostních a jiných záplat, a odkládat restarty po instalacích záplat.

ANALÝZA RIZIK A HARDENING

- ANALÝZA RIZIK KONCOVÉHO BODU
- PATCH MANAGEMENT*
- FULL-DISK ENCRYPTION*
- OCHRANA PŘED HROZBAMI
- KONTROLA APLIKACE
- KONTROLA ZAŘÍZENÍ

PREVENCE

- SIGNATURY A ZABLOKOVÁNÍ CLOUDU
- LOKÁLNÍ & CLOUDOVÉ STROJOVÉ UČENÍ
- OCHRANA PROTI EXPLOITŮM
- NETWORK ATTACK DEFENSE
- EMAIL SECURITY*
- FIREWALL
- OCHRANA PROTI BEZ SOUBOROVÝM ÚTOKŮM

DETEKCE A REAKCE

- SLEDOVÁNÍ ŠKODLIVÝCH PROCESŮ
- BLOKOVÁNÍ PŘÍSTUPU
- KARANTÉNA
- AUTOMATICKÁ DEZINFEKCE & ODSTRANĚNÍ
- UKONČOVÁNÍ PROCESU
- OBNOVENÍ

REPORTING A INTEGRACE

- DASHBOARDY & REPORTY
- NOTIFIKACE
- SIEM INTEGRACE
- PODPORA API

* ADD-ON

Bitdefender
BUILT FOR RESILIENCE

IS4 security s.r.o.
Country Partner Bitdefeder ČR & SK
Jordánská 391, 198 00 Praha 9

Tel.: + 420 245 501 800
email: info@bitdef.cz
web: www.bitdefender.cz

Společnost Bitdefender je lídrem v oblasti kybernetické bezpečnosti, která ve své třídě poskytuje nejlepší řešení prevence, detekce a reakce na hrozby po celém světě. Bitdefender střeží miliony spotřebitelských, podnikových a vládních prostředí, a je jedním z nejdůvěryhodnějších odborníků v oblasti eliminace hrozeb, ochrany soukromí a dat, a zajištění kybernetické odolnosti. Díky rozsáhlým investicím do výzkumu a vývoje objeví laboratoře Bitdefender Labs každou minutu více než 400 nových hrozeb, a denně ověří přibližně 40 miliard dotazů na výskyt hrozeb. Společnost je průkopníkem průlomových inovací v oblasti antimalwaru, zabezpečení IoT, behaviorální analytiky a umělé inteligence, a její technologie si licencuje více než 150 nejuznávanějších světových technologických značek. Společnost Bitdefender byla založena v roce 2001 a má zákazníky ve více než 170 zemích s pobočkami po celém světě.

Více informací najdete na https://www.bitdefender.cz

NABÍDKA

NAB-23-215
Vystaveno: 23.8.2023

Dodavatel:
CYBOSEC s.r.o.
Hradčany 347
503 53 Smidary
Česká republika

IČO: 04301226
DIČ: 04301226

Kontaktní údaje:

Pavel Jícha
pavel.jicha@cybosec.com
+420736174250

Odběratel:
Město Ostrov

IČO: 00254843
DIČ: CZ00254843

Jáchymovská 1
36301 Ostrov
Česká republika

Kontaktní údaje:

Položka	Množství	Cena za jednotku	Sleva %	Celkem	Sazba DPH	Celkem vč. DPH
Bitdefender GravityZone Business Security ENTERPRISE EDR / XDR - GOV 36 měsíců	206	1 980,00 Kč	5	387 486,00 Kč	21 %	468 858,06 Kč
Bitdefender GravityZone Patch Management ADDON - GOV 36 měsíců	206	1 015,00 Kč	0	209 090,00 Kč	21 %	252 998,90 Kč
Instalace a konfigurace nástroje - SENIOR TECHNIK	1	0,00 Kč	0	0,00 Kč	21 %	0,00 Kč
Certifikované zaškolení obsluhy - ADMIN BASIC (6 HOD)	1	0,00 Kč	0	0,00 Kč	21 %	0,00 Kč

Rozpis DPH

Sazba %	Základ	Daň
21%	596 576,00 Kč	125 280,96 Kč

Konečná cena: **596 576,00 Kč**
Konečná cena vč. DPH: **721 856,96 Kč**