Bitdefender®

BUILT FOR RESILIENCE

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 170 zemích. Pomocí mnohavrstvé ochrany s využitím strojového učení a umělé inteligence umí odhalovat a zablokovat i ty nejsofistikovanější útoky (Ransomware, bez souborové, cílené atd.)

Bitdefender
GravityZone

PRAVIDELNĚ VÍTĚZÍ V TESTECH

AV-TEST Award 2021, 3 ocenění v roce 2021

Gartner peerinsights region—customers' choice 2021

Ocenění "Volba zákazníků" v roce 2021, Gartner Peer Insights "Voice of the Customer"

AV comparatives CERTIFIED ATP Enterprise 2021

Nejlepší celkový výsledek v AV-Comparatives Endpoint Prevention & Response Report

MITRE ENGENUITY | ATT&CK® Evaluations

Nejlepší celkový výsledek ve 4. kole soutěže MITRE Engenuity ATT&CK® Enterprise Evaluations

FORRESTER®

Strong Performer. The Forrester Wave: Endpoint Detection and Response Providers, Q2 2022

THE RADICATI GROUP, INC.
A TECHNOLOGY MARKET RESEARCH FIRM

Největší hráč v oblasti Radicati APT Protection MQ 2021

GravityZone Business Security Enterprise

Dokonalé řešení pro ochranu koncových bodů: pokročilá prevence, rozšířená detekce, účinná reakce a analýza rizik.
GravityZone Business Security Enterprise (dříve známá jako GravityZone Ultra) kombinuje celosvětově nejúčinnější platformu pro ochranu koncových bodů EPP spolu s funkcemi Endpoint Detection and Response (EDR), která vám pomáhá chránit infrastrukturu koncových bodů (pracovní stanice, servery a kontejnery) v celém životním cyklu hrozeb, a to s vysokou účinností a efektivitou.

Tato technologie korelace napříč koncovými body posouvá detekci a viditelnost hrozeb na novou úroveň tím, že využívá funkce XDR (eXtended Detection and Response) pro detekci pokročilých útoků napříč všemi koncovými body v hybridních infrastrukturách (pracovní stanice, servery a kontejnery s různými operačními systémy).

Díky zabudované analýze rizik (rizika generovaná koncovým bodem a uživateli) a inovacím v oblasti hardeningu, nativně minimalizuje útočný povrch koncového bodu, a tím útočníkům ztěžuje průnik.

Spolu s pokročilým funkcemi prevence, včetně detekce anomálií a ochrany proti zneužití, blokuje GravityZone Business Security Enterprise sofistikované hrozby v počátečních fázích útoku. Rychlé třídění výstrah a vyšetřování incidentů pomocí časové osy útoku a s výstupy ze sandboxu umožňují správcům systému rychle reagovat a zastavit probíhající útoky jediným kliknutím myši.

Zajišťuje konzistentní zabezpečení všech koncových bodů se systémy Windows, Linux nebo Mac ve fyzické, virtualizované nebo cloudové infrastruktuře. Podporuje integraci s již existujícími nástroji pro bezpečnostní operace, včetně Splunku, a je optimalizována pro technologie datových center, včetně všech hlavních hypervizorů, čímž sníží potřebu řešení od více dodavatelů.

Jak GravityZone Business Security Enterprise 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 útoku v celém jeho životním cyklu, od prvního kontaktu, pokusu o zneužití až po snahu o setrvání v systému.

eXtended Endpoint Detection and Response (XEDR)

Nová funkce detekce a reakce na koncových bodech rozšiřuje možnosti analýzy EDR o korelace událostí ze všech koncových bodů v organizaci a tím vám pomáhá 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 2008, což vedlo ke zvýšení detekce hrozeb s nízkým počtem falešně pozitivních výsledků a zároveň umožnilo zastavovat neznámé hrozby před jejich spuštěním, nebo při jejich spuštění.

Hyperdetect - využívá strojové učení a heuristickou analýzu

HyperDetect je bezpečnostní vrstva, která zlepšuje obranu proti pokročilým hrozbám, jako jsou útoky bez souborů, cílené útoky, podezřelé soubory, síťový provoz, exploity, ransomware a další.

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.

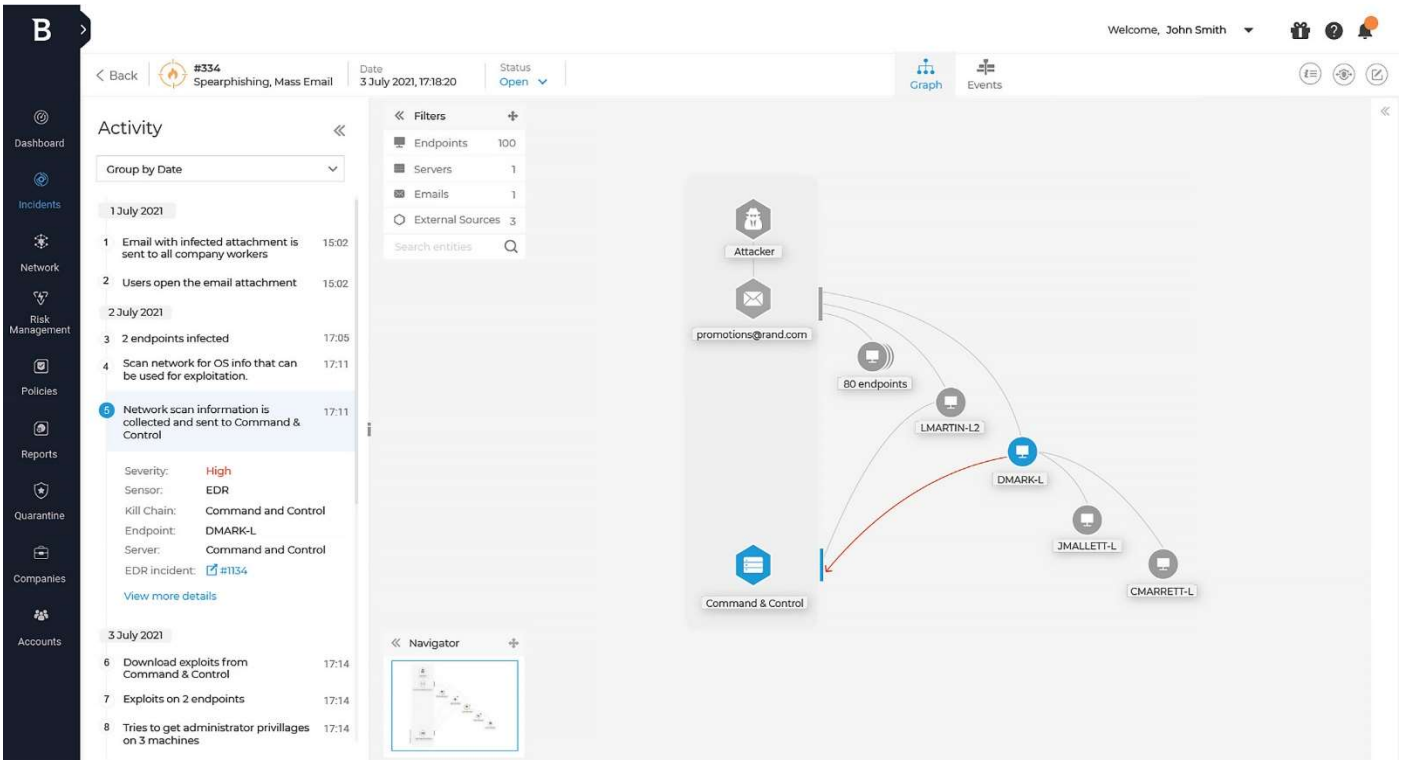
Obrana před bez souborovým útokem

Detekce a blokování malwaru založeného na skriptech, bez souborů.

Rozšířené vyšetřování incidentů a inteligentní reakce pro rozvinuté systémy

GravityZone Business Security Enterprise 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.

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 např. zadávání přihlašovacích údajů na webových stránkách s nešifrovanou komunikací, 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 Business Security Enterprise 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 útočníka.

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.

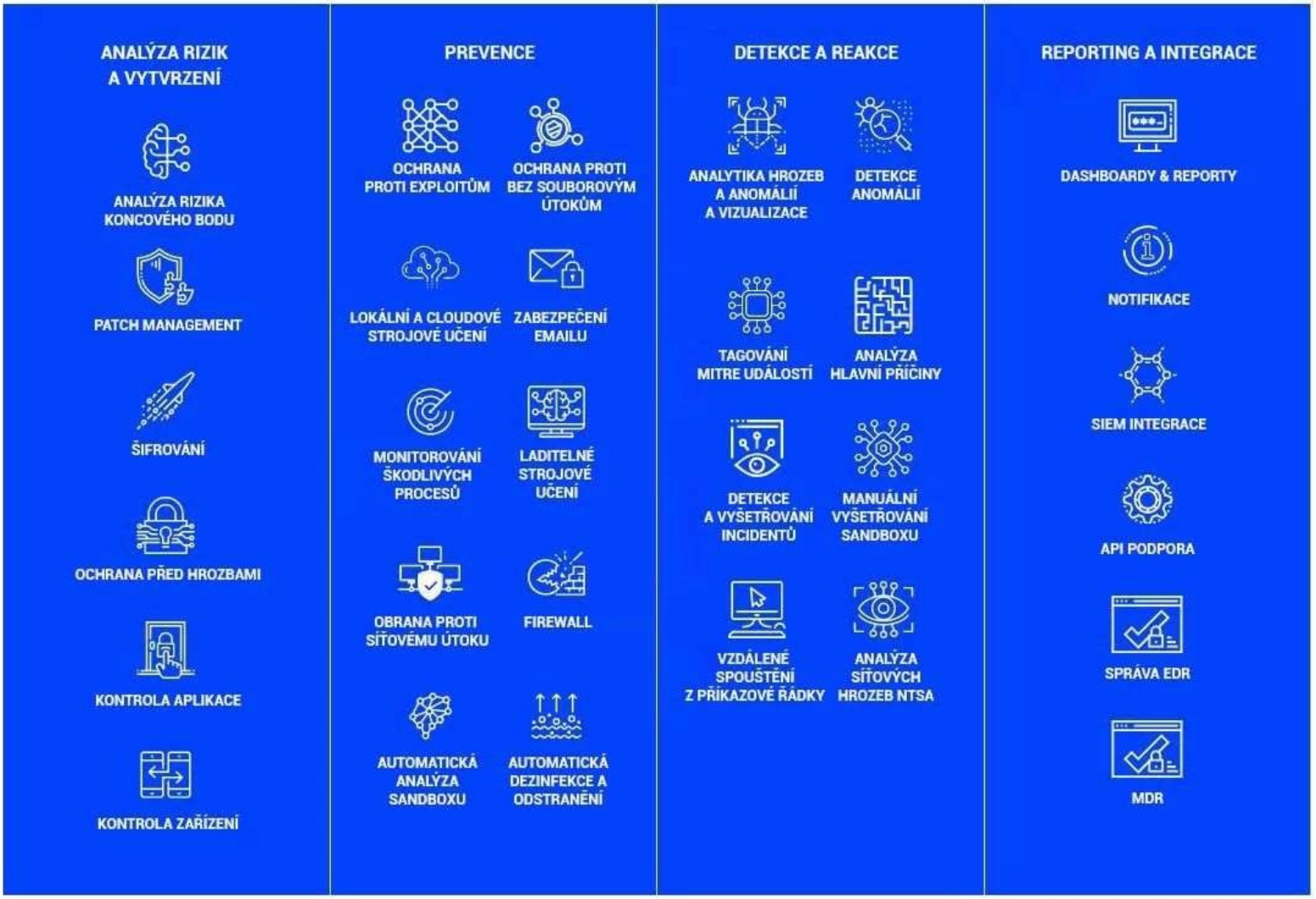
Pokrytí napříč platformami a integrace API třetích stran
Pokrývá všechny podnikové koncové body se systémem Windows, Linux nebo Mac ve fyzické, virtualizované nebo cloudové infrastruktuře, a poskytuje konzistentní zabezpečení napříč celou

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 Business Security Enterprise

Vytvořeno pro zvýšení kybernetické odolnosti

Bitdefender GravityZone Business Security Enterprise 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 Business Security Enterprise: Jednotná prevence, rozšířená detekce, reakce a analýza rizik

Bitdefender
GravityZone

eXtended Endpoint Detection and Response Business Security (XEDR)

Bitdefender v červenci 2021 představil další evoluci řešení pro detekci a reakci na koncové body - eXtended EDR (XEDR), přidáním analytiky a korelace bezpečnostních událostí napříč koncovými body do řešení Bitdefender Endpoint Detection and Response (EDR) a GravityZone Business Security Enterprise, 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-premise 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 zajišťuje včasnou detekci 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
GravityZone

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	Kontroly na koncových bodech a sítích před spuštěním i při spuštění
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 infrastrukturu organizace proti sofistikovaným nebo cíleným útokům. Díky pokročilým detekčním a reportovacím schopnostem chrání před těžko polapitelnými 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
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 Bitdefender, 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.

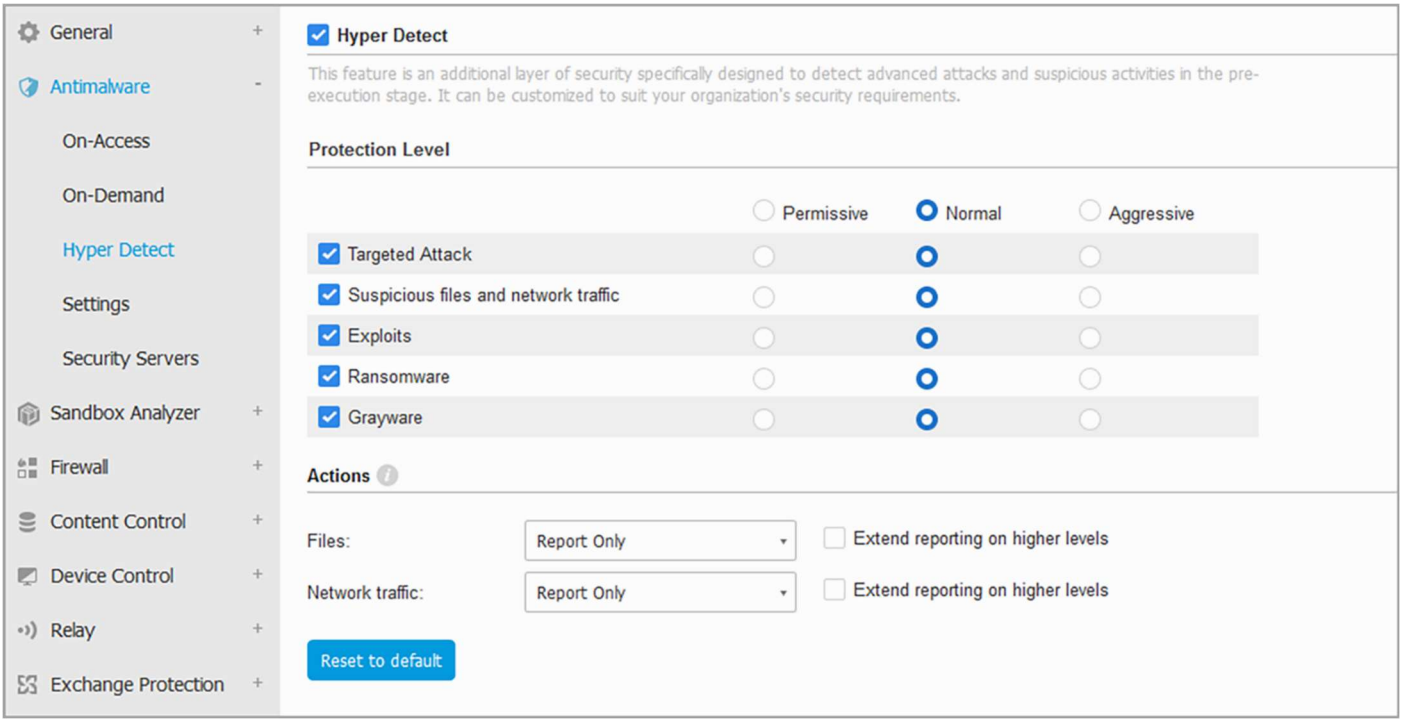
Více informací najdete na stránce produktu na našem webu Bitdefender.cz

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".

GravityZone Business Security Premium

Ochrana koncových bodů nové generace. Vylepšeno o analýzu lidských rizik. GravityZone Business Security Premium (původně známá jako GravityZone Elite) chrání vaši organizaci před celým spektrem sofistikovaných kybernetických hrozeb. S více než 30 technologiemi zabezpečení založenými na strojovém učení, poskytuje GravityZone několik vrstev obrany, které trvale překonávají konvenční zabezpečení koncových bodů, což dokazují nezávislé testy.

Jeden agent, jedno konzolové řešení pro fyzické, virtuální, mobilní a cloudové koncové body a e-mail. GravityZone Business Security Premium přidává do vašeho bezpečnostního ekosystému lidský prvek, minimalizuje režii správy a poskytuje vám všudypřítomný přehled a kontrolu.

Vlastnosti & výhody

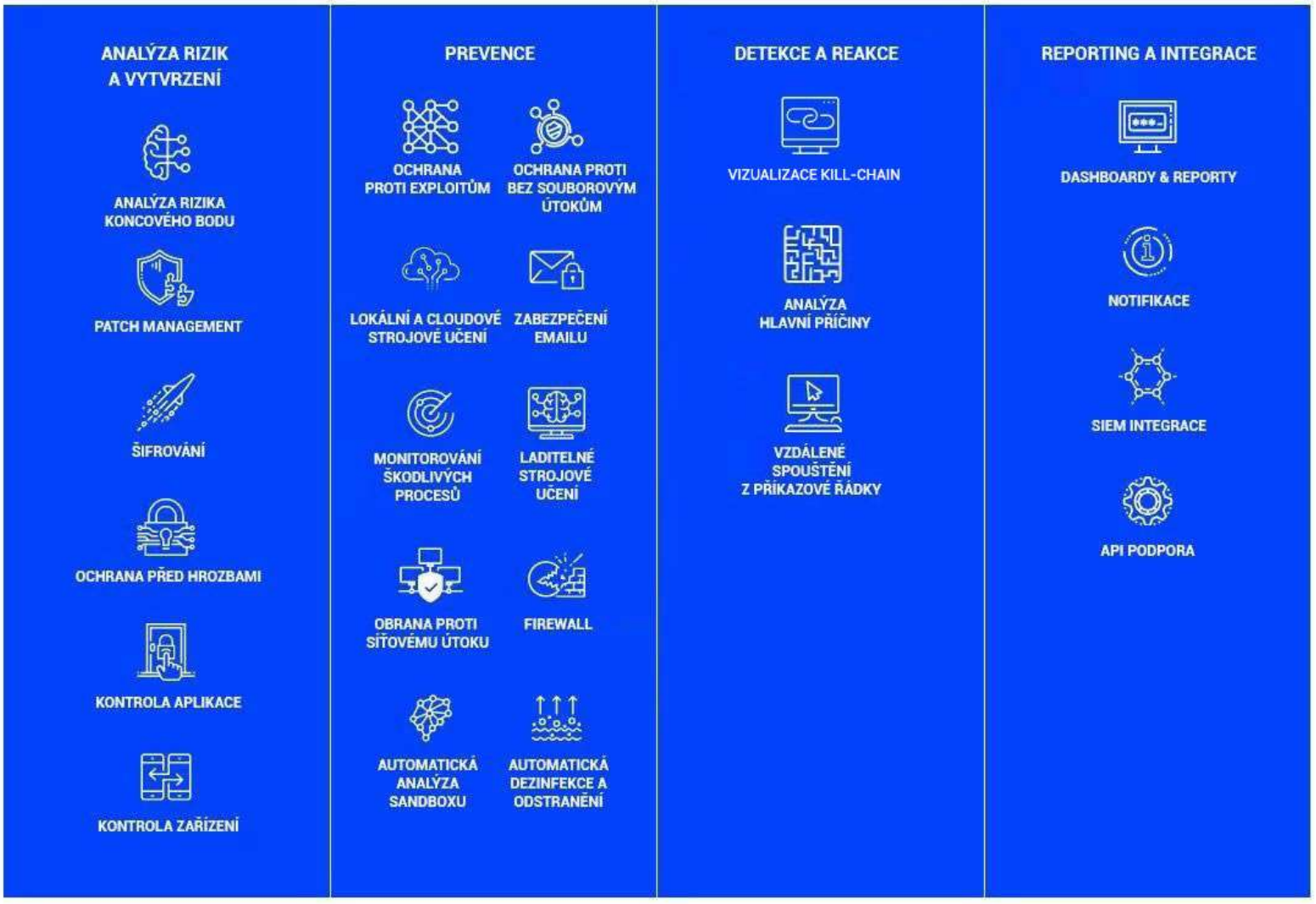
- Analýza lidských rizik pomáhá identifikovat činnosti a chování uživatelů, které představují bezpečnostní riziko pro organizaci
- HyperDetect™ blokuje útoky bez souborů již před spuštěním. Obsahuje modely strojového učení a technologii skryté detekce útoků. Tvoří další vrstvu zabezpečení, která je speciálně navržena k odhalování pokročilých útoků a podezřelých aktivit ve fázi před jejich spuštěním.
- Řízení rizik a analýza nepřetržitě skenuje koncové body na chybné konfigurace a zranitelnosti aplikací, a vydává doporučení pro stanovení priorit a odstranění chyb.
- Prevence a potlačování ransomwaru se skládá z automatických, aktuálních záložních kopií uživatelských souborů
- Obrana proti síťovým útokům pomocí nové vrstvy zabezpečení koncového bodu sítě, určené k detekci a prevenci útoků využívajících síťové zranitelnosti.
- Forenzní analýza a vizualizace útoků zvyšuje úroveň přehledu o hrozbách v organizaci a odhaluje širší souvislosti útoků na koncové body. Umožňuje zaměřit se na konkrétní hrozby a provést nápravná opatření.
- Sandbox Analyzer zajišťuje preventivní detekci pokročilých útoků automatickým odesíláním souborů, které vyžadují další analýzu, do cloudového sandboxu a přijímáním nápravných opatření na základě výsledků.
- Strojové učení předpovídá a blokuje pokročilé útoky. Bitdefender využívá strojové učení v celém svém portfoliu.

odolných proti neoprávněné manipulaci, bez použití stínových kopií, z funkcí blokování a prevence (Fileless Attack Defense; Network Attack Defense; Advanced Anti-Exploit; Machine Learning Anti-Malware); z několika detekčních vrstev (kontrola procesů, monitorování registru, kontrola kódu, Hyper Detect) a z technologií pro zmírnění rizika pro uživatele a systém.

Skenovací engine, HyperDetect, Sandbox Analyzer, Content Control, Global Protective Network jsou jen některé příklady technologií Bitdefender, které využívají strojové učení.

Technologie GravityZone Business Security Premium

Integrovaná platforma pro ochranu koncových bodů, řízení rizik a forenzní analýzu útoků



GravityZone Business Security

Konzistentní a neustále vylepšovaná ochrana, v kombinaci s řízením rizik a hodnocením zranitelnosti. Zabezpečení s efektivním využitím zdrojů, které poskytuje vysoký výkon a ochranu a zároveň umožňuje centralizovanou správu, snadné nasazení s minimálními nároky na technické dovednosti. Nejlépe vyhovuje potřebám podnikové kybernetické bezpečnosti a umožňuje vám vybrat si mezi cloudovou nebo lokální hostovanou konzolí pro správu.

GravityZone Business Security kombinuje strojové učení a heuristiku se signaturami a dalšími technikami, a nabízí ochranu proti všem typům malwaru a hrozbám, jako je phishing, ransomware, exploity a zero-days. Průkopnické a patentované technologie, jako je Process Inspector a algoritmy strojového učení, jsou neustále vyvíjeny, trénovány a používány od roku 2008.

Vlastnosti & výhody

Obrana proti síťovým útokům. Získejte novou úroveň ochrany před útoky, jejichž cílem je získat přístup do systému využíváním zranitelností sítě. Rozšiřte chráněné oblasti o zabezpečení založené na síti, které blokuje hrozby, jako jsou útoky Brute Force, Password Stealers a Network Exploits.

Pokročilé monitorování chování aplikací. Bitdefender Process Inspector trvale sleduje běžící procesy, zda nevykazují známky škodlivého chování. Průkopnická a proprietární technologie, která byla uvedena na trh v roce 2008 jako (AVC), byla neustále zdokonalována a udržuje Bitdefender o krok napřed před vznikajícími hrozbami.

Více vrstev zabezpečení koncových bodů. Vaše stolní počítače, notebooky a servery jsou chráněny vrstveným zabezpečením: strojové učení, heuristika, signatury, ochrana paměti a nepřetržité sledování běžících procesů, blokování malwaru, dezinfekce a karanténa.

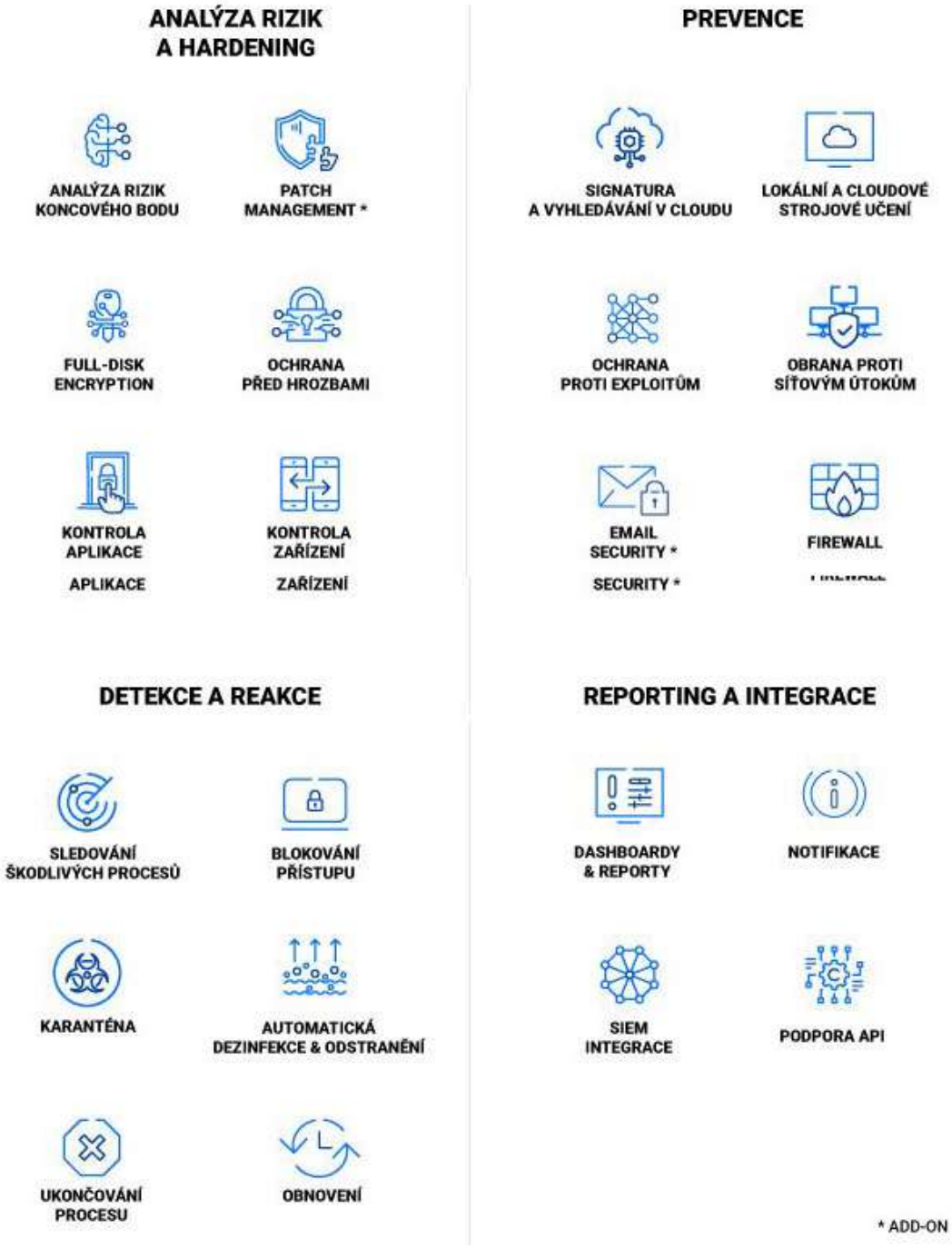
Webové zabezpečení - hardware není potřeba. Dedikované servery ani více zaměstnanců IT nebude třeba, protože GravityZone centralizuje všechny funkce zabezpečení do jedné konzole. Zaměstnanci nikdy nemusí aktualizovat nebo monitorovat bezpečnostní aktivity. Můžete ušetřit čas vzdálenou instalací ochrany na všechny nechráněné počítače pomocí jednoduchého a komplexního postupu. Bezpečnostní řešení lze nasadit buď v místním prostředí, nebo ho hostovat v Bitdefender cloudu.

AI a strojové učení zdokonalené v průběhu let. Umělá inteligence a strojové učení jsou nezbytné k boji proti sofistikovaným hrozbám. Na rozdíl od jiných prodejců má Bitdefender dlouholeté zkušenosti s vylepšováním těchto technologií a výsledky to jasně ukazují: lepší míra detekce s méně falešnými poplachy.

Největší cloud Security Intelligence. S více než 500 miliony chráněných strojů provádí Bitdefender Global Protective Network 11 miliard dotazů denně a pomocí strojového učení a korelace událostí detekuje hrozby bez zpomalení uživatelů.

Technologie GravityZone Business Security

Adaptivní vrstvená architektura, která zahrnuje kontrolu koncových bodů, prevenci, detekci, obnovu a transparentnost.



A LA CARTE

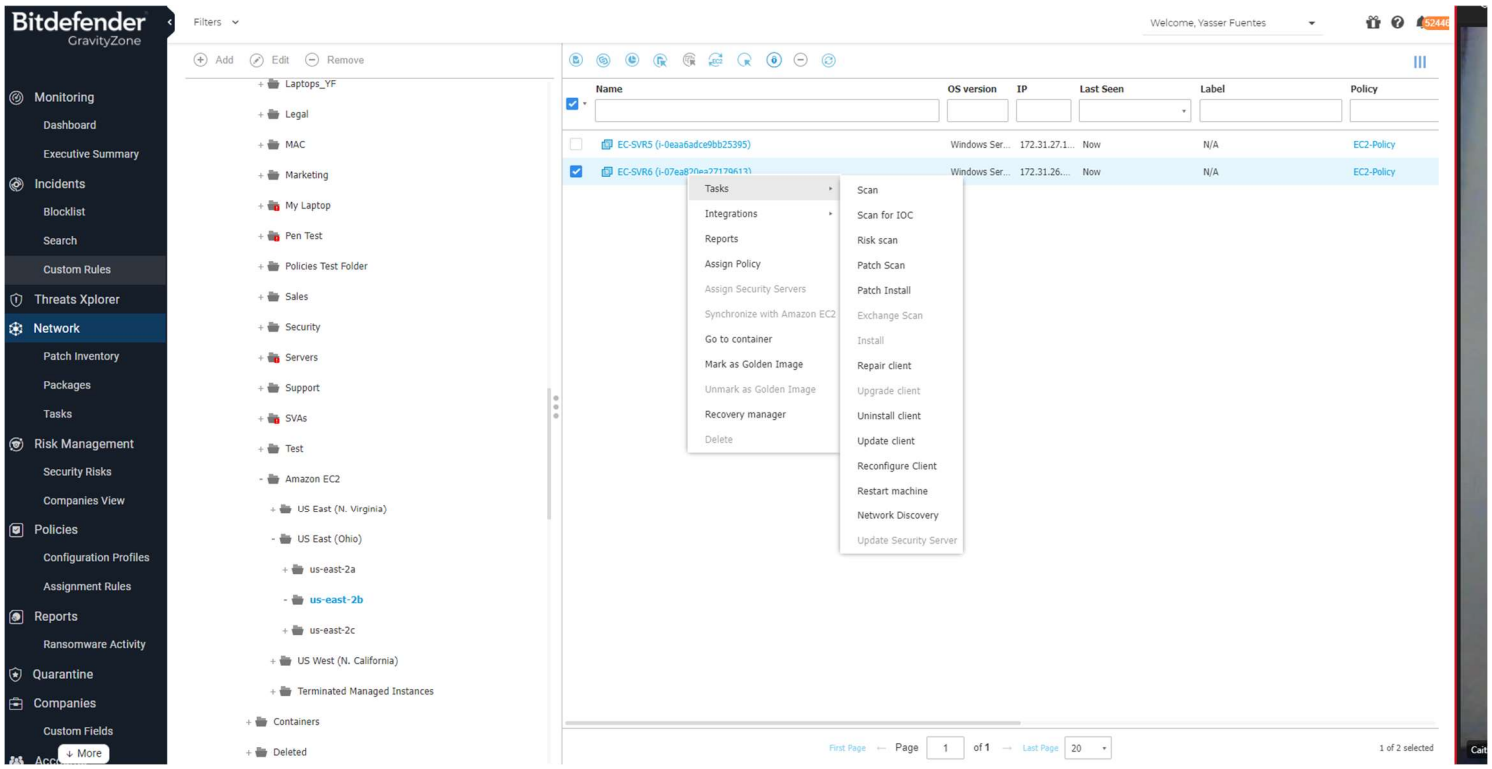
GravityZone Security for Servers

GravityZone Security for Servers poskytuje vysoce výkonnou ochranu ve všech privátních datových centrech a veřejných cloudech.

GravityZone urychluje nasazení a ve velké míře automatizuje bezpečnostní pracovní postupy, prostřednictvím integrace s cloudovými platformami pro pracovní prostředí, jako jsou AWS, Citrix Hypervisor, Nutanix AHV a VMware vCenter Server a veřejnými cloudy, jako jsou Amazon a Azure.

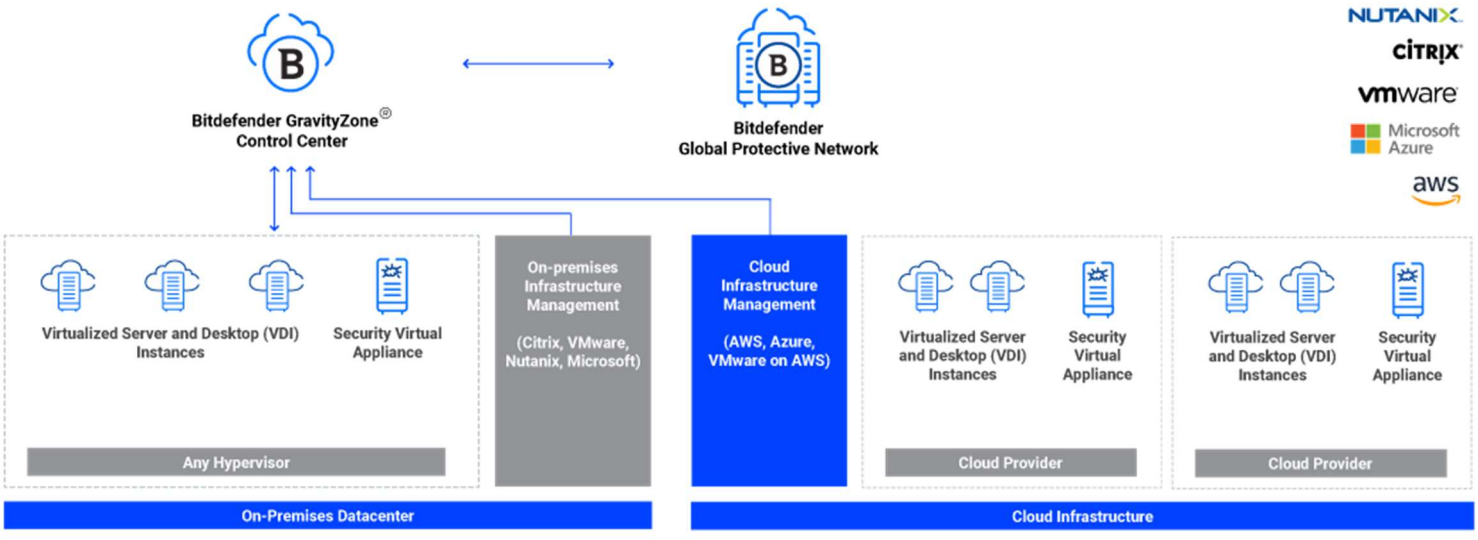
Správcovská konzole je od základu vyvinuta pro virtualizovaná a cloudová prostředí, podporuje všechny hypervisory a je kompatibilní s jakoukoli cloudovou infrastrukturou. Z jedné správy může chránit více hypervisorů, cloudů a hostovaných operačních systémů.

GravityZone Security for Servers minimalizuje zátěž virtuálního stoje, díky použití ultra lehkého agenta, patentované antimalwarové heuristice a algoritmům ukládání do mezipaměti, které snižují náročnost na výkon. Výsledkem je výrazné snížení latence a tím i zefektivnění práce koncových uživatelů, protože aplikace mají k dispozici více zdrojů CPU, paměti a IOPS.



Vlastnosti & výhody

- Nižší náklady na infrastrukturu díky efektivní architektuře a patentovaným bezpečnostním algoritmům, zvýšená hustota virtuálních počítačů až o 55 %
- Urychluje nasazení a automatizuje bezpečnostní pracovní postupy prostřednictvím integrace s cloudovými platformami, jako jsou AWS, Citrix Hypervisor, Nutanix AHV a VMware vCenter Server.
- Podporuje všechny hypervisory a je kompatibilní s jakoukoli cloudovou infrastrukturou. Ze stejného nasazení může chránit více hypervisorů, cloudů a hostovaných operačních systémů. Firmy mohou rozšířit ochranu i mimo servery a cloudová prostředí na fyzické koncové body, mobilní zařízení a poštovní schránky Exchange.
- Přehled, kontrola a správa zabezpečení všech pracovních zátěží v jakémkoli virtualizovaném nebo cloudovém prostředí pomocí jedné centrální platformy.
- Bezproblémová integrace s jakýmkoli prostředím s univerzální kompatibilitou - nezávislé na platformě a operačním systému, kompatibilní se všemi distribucemi Linuxu, bez nutnosti vlastní integrace.
- Bitdefender používá pro servery speciálně vytvořený technologický stack a konzistentně vyhrává nezávislé testy prevence a detekce, přičemž v testu Comparatives 2020 APT zastavil 100 % hrozeb, a v hodnocení MITRE ATT&CK, zveřejněném v roce 2021, vykázal nejvyšší počet odhalených útoků.



Technologické schéma

GravityZone Security for Workstations

Pokročilá kybernetická ochrana pro zajištění chodu vaší firmy. Díky adaptivní, vrstvené ochraně nabízí GravityZone Security for Workstations nejlepší ochranu před sofistikovanými hrozbami, s minimální dopadem na výkon.

Vzhledem k tomu, že v poslední době čelíme rychle se šířícím sofistikovaným útokům, potřebují organizace zabezpečení koncových bodů, které se dokáže přizpůsobit novým hrozbám, identifikovat a blokovat dosud neznámý malware a ransomware. Patentované technologie strojového učení, v kombinaci se schopností monitorovat chování a odhalovat techniky útoků, umožňuje GravityZone detekovat a preventivně blokovat hrozby, které tradiční antivirová ochrana přehlíží.

GravityZone se dodává jako virtuální zařízení spravované u zákazníka nebo v cloudu, a lze ji snadno nasadit a škálovat tak, aby chránila libovolný počet koncových bodů, s integrovanou redundancí a vysokou dostupností.

Vlastnosti & výhody

- **Detekce a zastavení útoků.** Bitdefender Process Inspector je technologie detekce anomálií chování, která poskytuje ochranu před dosud neznámými hrozbami ve fázi jejich spouštění.
- **Sandbox Analyzer zlepšuje detekci cílených útoků**. zajišťuje detekci pokročilých útoků před jejich spuštěním automatickým odesláním souborů, které vyžadují další analýzu, do cloudového sandboxu, a na základě zjištěných skutečností provádí nápravná opatření.
- **Pokročilý Anti-Exploit**. Vrstva Bitdefender Memory Protection chrání před známými i neznámými exploity zaměřenými na chyby prohlížeče a aplikací ve fázi spuštění.
- **Kontrola a zabezpečení koncových bodů**. Bitdefender Endpoint Protection obsahuje mnoho funkcí, které společně snižují plochu útoku: Ochrana před webovými hrozbami, brána firewall, kontrola aplikací a zařízení.
- ***(Add-on) HyperDetect™ blokuje útoky před jejich spuštěním**. Obsahuje modely strojového učení a technologii skryté detekce útoků. Tvoří další vrstvu zabezpečení, která je speciálně navržena k odhalování pokročilých útoků a podezřelých aktivit ve fázi před jejich provedením.

** Add-on je volitelně dokoupitelné rozšíření.*

SPECIALITY & ADD-ON

GravityZone Security for Containers

Vysoce výkonné zabezpečení kontejnerů a serverových prostředí Linuxu, které je nezávislé na verzi jádra.
Bitdefender GravityZone Security for Containers chrání kontejnerové a cloudové pracovní prostředí 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 Linux koncové body poslední verzi linuxového jádra, což umožňuje nasazení nových distribucí, jakmile na ně chce vaše organizace přejít, aniž by vás to omezovalo v zabezpečení.

Forenzní analýza a vizualizace útoků zvyšují úroveň přehledu o hrozbách v organizaci a odhalují širší souvislosti útoků na kontejnery. Umožní vám zaměřit se na konkrétní hrozby a přijmout nápravná opatření pro všechny kontejnery a pracovní stanice v hybridních a multi-cloudových prostředích

Vlastnosti & výhody

- EDR vytvořená pro Linux a kontejnerové pracovní stanice
- 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
- Pokročilý nástroj Anti-Exploit pro Linux
- Jednotná platforma GravityZone pro CWS i mimo ni
- TTP útočníka mapované na MITRE pro Linux
- Zaměřuje se na hrozby specifické pro systém Linux a zobrazuje kontextově bohaté informace
- EDR Podporuje jednotný přehled a řízení všech pracovních stanic, kontejnerů, operačních systémů a cloudů

Bitdefender
GravityZone

GravityZone Security for Email

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

Vlastnosti & výhody

- **Více bezpečnostních systémů** využívá kombinaci pokročilých technologií k odhalování spamu i sofistikovanějších, cílených phishingových a podvodných útoků.
- **Výkonný nástroj** umožňuje kontrolu nad doručováním e-mailů a filtrování zpráv na základě atributů, jako je velikost, zdroj, cíl, klíčová slova a další.
- 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".
- **Ochrana při kliknutí** přepisuje odkazy ve zprávách a chrání zaměstnance v reálném čase tím, že blokuje a upozorňuje uživatele na škodlivé odkazy.
- **Využívá pokročilou analýzu chování**, která zahrnuje více než 10 000 algoritmů analyzujících více než 130 proměnných extrahovaných z každé e-mailové zprávy, pro silnou detekci a prevenci hrozeb
- **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.

GravityZone Patch Management

Bezpečnostní záplaty na známé zranitelnosti
Zvyšte zabezpečení, udržujte systémy aktuální a snižte složitost IT pomocí automatického záplatování.

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.

Automatizované záplatování může pomoci zajistit soulad vaší organizace s klíčovými předpisy o zabezpečení dat, jako jsou GDPR, HIPAA, PCI DSS a další.

Vlastnosti & výhody

- Aktualizace operačního systému a největší množiny softwarových aplikací
- Automatické a ruční aktualizace
- GravityZone Patch Management poskytuje podrobné informace o záplatách (CVE, BuletinID), rychlé nasazení chybějících záplat a blacklisting záplat - možnost dočasně zabránit instalaci záplat
- 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 klíčové pilíře 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

IS4 security s.r.o.
Country Partner Bitdefender
ČR/SK

Jordánská 391, 198 00 Praha 9
Česká republika
tel.: +420 245 501 800
email: info@is4security.cz

Technická podpora

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