Bitdefender

Bitdefender GravityZone Ultra Suite

Odhalte a zastavte těžko polapitelné hrozby s hbitostí a přesností

GravityZone Ultra je kompletní řešení Endpoint Security navržené od základu jako integrované EPP nové generace a snadno použitelné EDR. Nabízí prevenci, detekci hrozeb, automatickou reakci, poskytuje detailní viditelnost před ohrožením i po něm, efektivní automatické třídění výstrah, snadné vyšetřování, pokročilé vyhledávání a možnosti řešení incidentu na jeden klik.

GravityZone Ultra je postavena na vysoce efektivní prevenci, vlastními automatizovanými technologiemi detekce hrozeb a dále na následných reakcích na ně, a proto výrazně omezuje počet incidentů vyžadujících manuální analýzu a snižuje provozní náklady spolu s nároky potřebnými pro provoz řešení EDR. Díky tomu že poskytuje jednoho agenta pro všechny integrované funkce ochrany, a zároveň je spravovatelné pomocí jedné ucelené centrální konzole, tak je snadné ho nasadit a integrovat s ostatními prvky stávající bezpečnostní architektury.

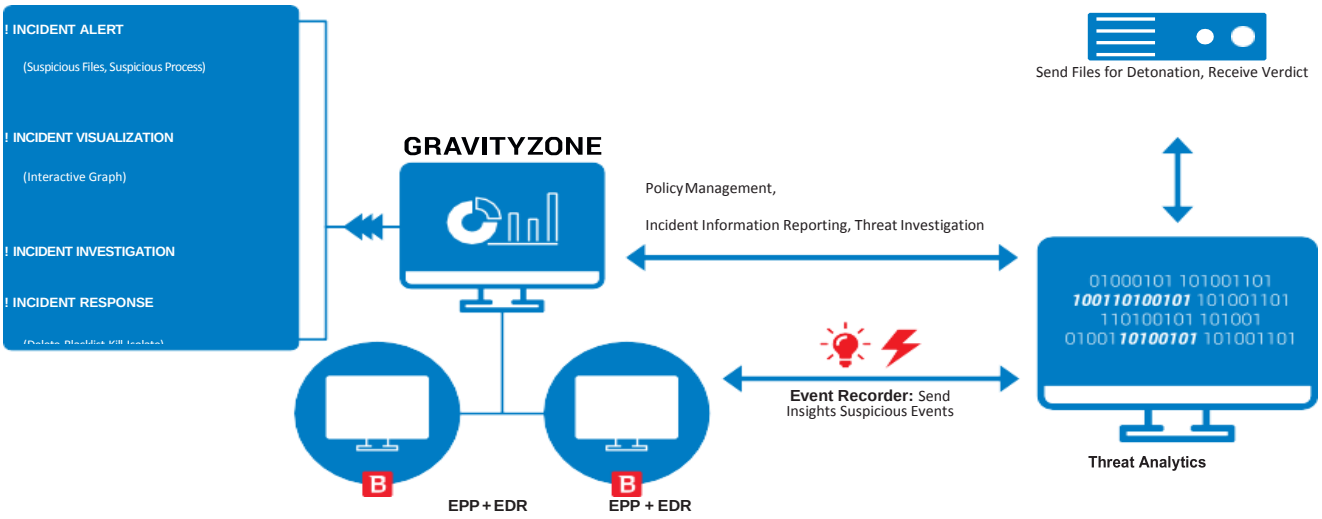
GravityZone Ultra umožňuje podnikovým zákazníkům přesně chránit digitální aktiva i před těmi nejhůře polapitelnými kybernetickými hrozbami a zároveň efektivně reagovat na všechny fáze útoku prostřednictvím:

- Redukce útočné plochy (pomocí firewallu, řízení přístupu aplikací, kontroly obsahu a správy záplat)
- Ochrany dat (pomocí doplňkového modulu určeného pro šifrování celého pevného disku)
- Detekce a odstranění škodlivého malware před spuštěním (pomocí laditelného strojového učení, kontroly procesů v reálném čase a analýzy karantény)
- Detekce hrozeb v reálném čase a jejich automatické nápravy
- Viditelnost útoku před a po něm (Root Cause Analysis)
- Rychlého třídění incidentů, jejich šetření a následných reakcí na ně
- Vyhledávání v aktuálních a historických bezpečnostních datech
- Postupnému zlepšování stavu bezpečnosti (prostřednictvím doplňkového modulu správy záplat)

Výsledkem je jednoduchá plynulá prevence proti hrozbám, dosažená hloubková viditelnost, přesná detekce incidentů a inteligentní reakce na ně, což vede celkově k výraznému snížení rizika hrozeb, vystavování se nákazám a efektivně zastavuje útoky.

Jakožto integrovaná sada řešení ochrany koncových bodů zajišťuje **GravityZone Ultra** konzistentní úroveň zabezpečení pro celé IT prostředí, takže útočníci nenajdou žádné špatně chráněné koncové body, které by následně mohli využít k škodlivým akcím proti organizaci. **GravityZone Ultra** spoléhá na jednoduchou integrovanou architekturu s centralizovanou správou, a to jak pro koncové body, tak pro datová centra. Umožňuje společnostem rychle nasadit řešení ochrany koncových bodů a po implementaci vyžaduje menší administrativní úsilí.

Sandbox Analyzer:



Obrázek 1. Bitdefender XDR: Prevence, detekce a reakce v jednom programu, spravovaném konzolí GravityZone

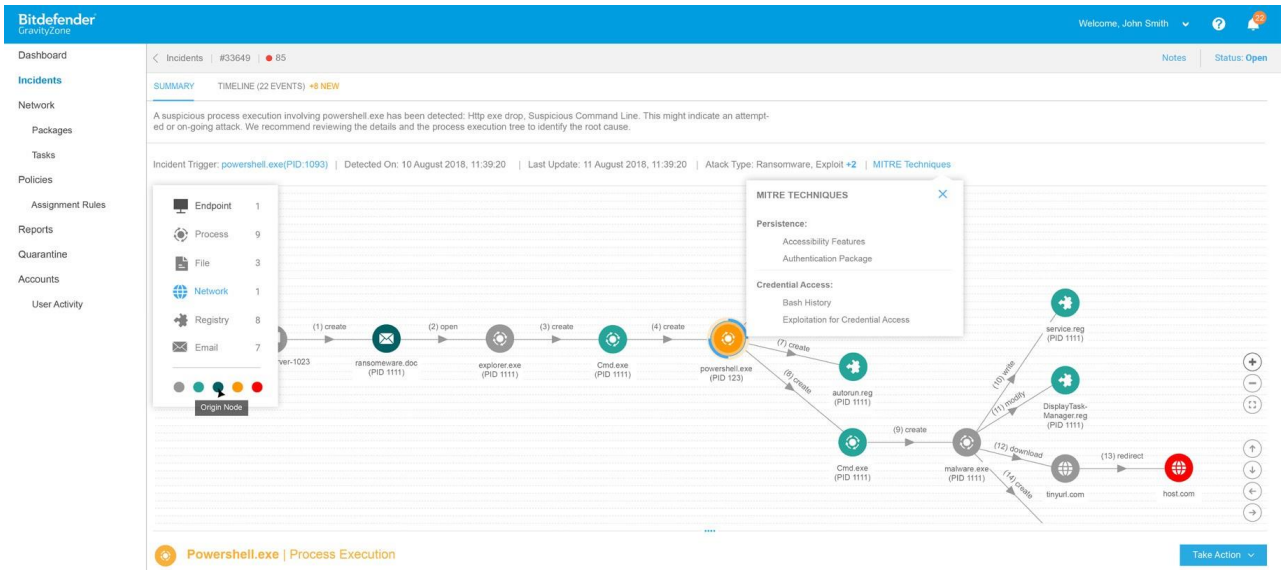
Snadné EDR

GravityZone Ultra, díky jasné viditelnosti v ukazatelích bezpečnostních metrik útoku (IOC), vyšetřování hrozeb na jedno kliknutí a nápravným reakcím na incidenty, snižuje nároky na zdroje a dovednosti bezpečnostních týmů. Nový datový záznamník bezpečnostních událostí koncových bodů (even recorder) je vítaným účinným doplňkem mnohavrstvé ochrany jakožto velmi důležitá součást ucelené ochrany koncových bodů před hrozbami. Jelikož poskytuje rozsáhlé zachycení systémových aktivit (soubor a proces, instalace programu, načtení modulů, změna registru, síťová připojení atd.), umožňuje tak širokou vizualizaci celého řetězce událostí zapojených do útoku napříč celou firemní infrastrukturou.

Hlavní výhody

GravityZone Ultra rozšiřuje celkovou ochranu koncových bodů nad rámec tradičních funkcí EPP a poskytuje tak analytikům a týmům zodpovědným za řešení bezpečnostních incidentů nástroje, které opravdu potřebují k účinné rychlé analýze podezřelých činností, jejich následnému vyšetřování a provádění přiměřených obranných reakcí na pokročilé hrozby:

- Detekce v reálném čase a automatická náprava
- Rychlé třídění incidentů, vyšetřování a reakce detekce podezřelé aktivity
  - Ověření podezřelé aktivity a třídění výstrah
  - Odpověď incidentu jedním kliknutím
- Forenzní analýza před a po útoku (Root Cause Analysis)
- Hledání v aktuálních a historických dat ech na základě:
  - ukazatelů bezpečnostních metrik útoku (IOCs)
  - tagů v MITRE znalostní databázi
  - procesů, souborů, registrů a jiných parametrů



Obrázek 2. Stránka Podrobnosti o incidentech poskytuje jasný přehled o „Dosahu útočné detonace" incidentu. Provozovatel může snadno získat podpůrné důkazy a zareagovat.

Přesná detekce umožňuje účinnější bezpečnostní optiku a uvolňuje Vám ruce zamezením zbytečných upozornění

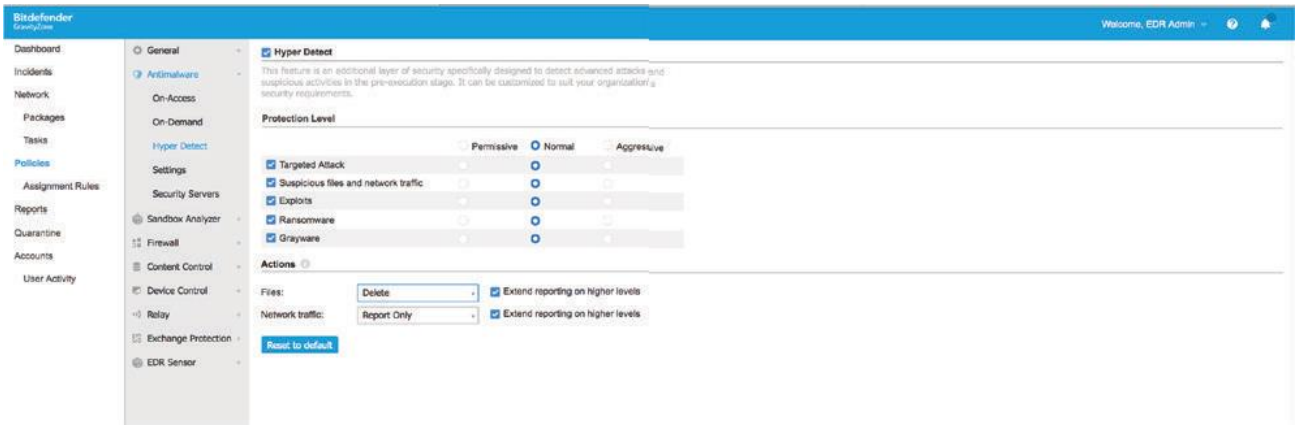
Pro ruční analýzu a vyřešení jsou uváděny pouze relevantní, související a závažné události. Šum a nadbytečné informace jsou udržovány na minimu, protože převážná většina útoků a pokročilých útoků je zablokována ve fázi před nebo při spuštění. Těžko polapitelné hrozby, včetně bezsouborového malwaru, exploitů, ransomwaru a obfuskovaného malwaru, jsou neutralizovány pomocí vysoce výkonných vrstvených technologií prevence pro koncové body nové generace, a kontroly procesů založené na bázi chování při spuštění. Automatická odezva a oprava eliminují nutnost lidského zásahu v blokování útoků.

Dokonale přesná detekce umožňuje bezpečnostnímu personálu zaměřit se pouze na skutečné incidenty a hrozby:

- Minimalizuje šum a rozptylování od falešných poplachů
- Snižuje množství incidentů pomocí účinné prevence hrozeb
- Eliminuje ruční nápravu blokovaných útoků s automatickou nápravou a opravou

Jednoduché šetření incidentů a chytrá odezva pro lepší ochranu

GravityZone Ultra, jakožto integrované řešení pro prevenci a detekci a reakci, umožňuje rychlou reakci a obnovení koncových bodů do fáze „lepší než dříve“. Nástroje pro vyšetřování incidentů, jako analýza kořenových příčin a hlášení karantény, pomáhají týmům zabezpečení ověřovat podezřelé činnosti a přiměřeně reagovat na počítačové hrozby. Pokročilé vyhledávání současných a historických dat na základě IOC, MITRE tagů a dalších relevantních artefaktů, umožňuje rychlou identifikaci hrozeb, které by se mohly skrývat v infrastruktuře koncových bodů.



Ucelená bezpečnostní platforma pro sledování koncových bodů v jediném agentu a jednotné konzoli

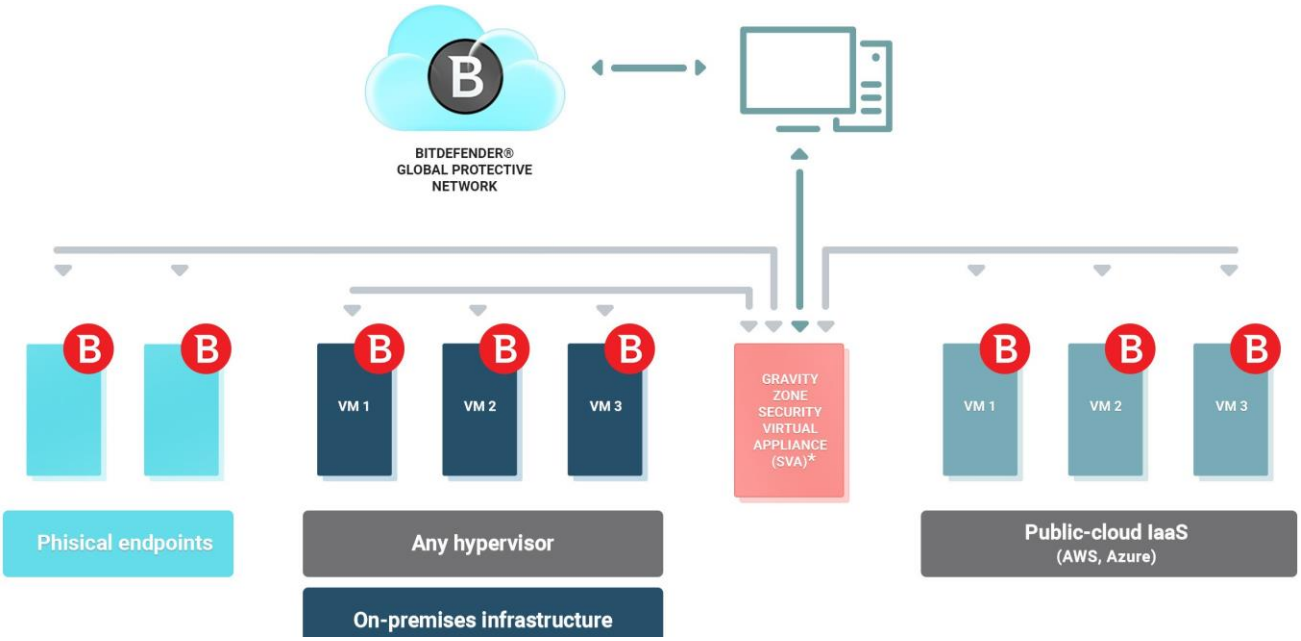
GravityZone Ultra zahrnuje veškeré ztvrzené řízení prevence nové generace zahrnuté v **Endpoint Security HD** a **GravityZone Elite**:

- Minimalizuje vystavení se hrozbám pomocí silné prevence.
- Detekce na bázi strojového učení a chování blokuje neznámé hrozby před nebo při spuštění.
- Odhaluje a blokujte skriptový, bezsouborový, obfuskovaný a vlastní malware pomocí automatické nápravy.
- Ochrana paměti k předcházení exploitům.
- Snižuje plochu útoku umožněním jednoduchého ovládání bezpečnosti IT.
- Integrovaný klient obsahující firewall, kontrolu zařízení, filtrování webového obsahu, kontrolu aplikací, správu patchů a další.

Obrázek 3. Bitdefender GravityZone Ultra: Ucelená bezpečnostní platforma, EPP + EDR, pro sledování koncových bodů.

Ochrana datového centra

Nedílnou součástí **GravityZone Ultra**, **GravityZone Security for Virtualized Environments**, je jeho bezpečnostní komponenta pro zabezpečení serveru a VDI navržená pro agilitu, provozní efektivitu a snižování nákladů na infrastrukturu v softwarově definovaných, hyperkonvertovaných a hybridních cloudových prostředích.



* Implementace bez agentů jsou podporovány také s VMware® vShieldTM nebo NSXTM

Ochrana datového centra

Vyšší provozní efektivita a obratnost
Kompatibilní s více cloudovými platformami a všemi hypervizory (např. VMware® ESXiTM, Citrix® XenServer®, Microsoft® Hyper-V, Nutanix® AHV, KVM, RedHat® Enterprise Virtualization nebo jejich kombinace), GravityZone pomáhá zefektivnit IT a bezpečnostní operace, a zároveň zlepšit dodržování předpisů. Sjednocená řídicí konzole **GravityZone** zjednodušuje nasazení a správu zabezpečení, umožňuje automatizované zajišťování zabezpečení, centralizované vymáhání politik a viditelnost jednoho skla v heterogenních a distribuovaných prostředích. Integrace s nástroji pro správu virtualizace (např. VCenter Server, XenServer a Nutanix Prism) dává GravityZone povědomí o operačním kontextu základní infrastruktury v reálném čase, včetně inventáře globálního virtuálního stroje (VM). V důsledku toho může GravityZone automaticky aplikovat bezpečnostní zásady vhodné pro VM, které sledují pracovní vytížení bez ohledu na to, kde v hybridním cloudu se nacházejí, což umožňuje týmům IT pro operace IT rozdělit tisíce zabezpečených virtuálních počítačů během několika hodin.

Špičkový výkon a využití infrastruktury
Patentované bezpečnostní algoritmy GravityZone a jejich efektivní design, který eliminuje potřebu použití agentů náročných na zdroje uvnitř každého virtuálního počítače, umožňují až o 35% vyšší hustotu virtualizace a 17% rychlejší odezvu aplikace než konkurence, což podporuje lepší využití infrastruktury a vynikající konečné využití uživatelské zkušenosti.

Neomezená lineární škálovatelnost
Modulární a odolná architektura GravityZone poskytuje škálovatelnost pro bezpečné nasazení na úrovni operátora. Platforma může být na vyžádání rozšířena lineárním a efektivním způsobem přidáním bezpečnostních virtuálních zařízení nebo násobením rolí serveru Control Center, pokud je to požadováno.

Univerzální kompatibilita
Kompatibilní se všemi předními platformami hypervisoru (VMware ESXi, Microsoft Hyper-V, Citrix Xen, Red Hat KVM a Nutanix AHV) a Windows i Linux jako hostující OS.

Řídicí centrum GravityZone

GravityZone Ultra Control Center je integrovaná a centralizovaná konzole pro správu, která poskytuje pohled ze všech skleněných oken na všechny komponenty správy zabezpečení, včetně zabezpečení koncových bodů, zabezpečení datových center a cloudů, a zabezpečení pro Exchange. Pro **GravityZone Ultra** je k dispozici pouze konzole hostovaná v cloudu. **Středisko správy GravityZone** zahrnuje více rolí a obsahuje databázový server, komunikační server, aktualizační server a webovou konzoli.

GravityZone Ultra je k dispozici s cloudovou konzolí. Chrání stolní počítače, servery a poštovní schránky Exchange. Servery by měly tvořit méně než 35% celkových jednotek.

Podrobné systémové požadavky naleznete na www.bitdef.cz

Bitdefender

Bitdefender je světová společnost specializující se na bezpečnostní technologie, poskytující špičkové řešení kybernetické bezpečnosti a pokročilou ochranu před hrozbami pro více než 500 milionů uživatelů ve více než 150 zemích. Bitdefender již od roku 2001 vydává oceňované technologie pro zabezpečení podniků i spotřebitelů a je upřednostňovaným poskytovatelem jak v zabezpečení hybridní infrastruktury, tak v ochraně koncových bodů. Prostřednictvím výzkumu a vývoje, spojenectví a partnerství, Bitdefender je spolehlivě napřed a dodává robustní zabezpečení, na které se můžete spolehnout.
Více informací naleznete na http://www.bitdef.cz

Všechna práva vyhrazena. © 2020 Bitdefender. Všechny zde uvedené ochranné známky, obchodní názvy a produkty jsou majetkem jejich příslušných vlastníků. PRO VÍCE INFORMACÍ NAVŠTIVTE: bitdef.cz