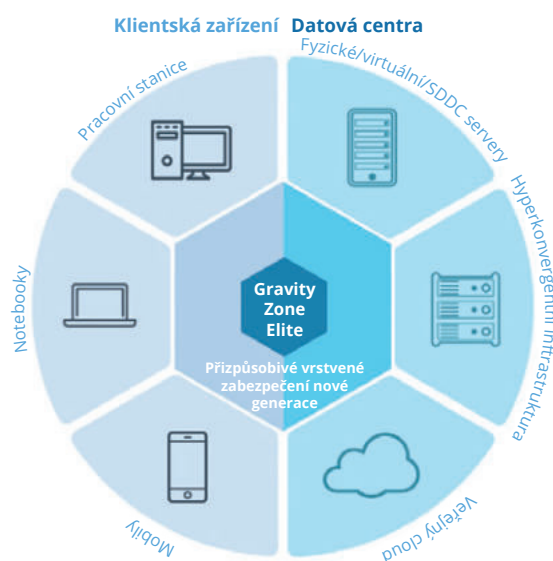


Bitdefender GravityZone Elite Suite

Vrstvená bezpečnostní platforma nové generace

Bitdefender GravityZone Elite Suite byla navržena pro ochranu podniků proti celé škále komplikovaných kyberútoků s rychlostí a přesností. Elite spojuje osvědčený přístup vrstveného zabezpečení Bitdefenderu se svými nástroji a technologiemi nové generace pro poskytnutí vysoké úrovně výkonu a ochrany koncových bodů napříč podnikovým prostředím: stolních počítačů, notebooků, telefonů, fyzických a virtuálních serverů.

GravityZone Elite zaručuje stálou úroveň ochrany pro celé IT prostředí omezením špatně chráněných koncových bodů, které by mohly být zneužity jako výchozí body pro škodlivou činnost proti organizaci. Opírá se o jednoduchou integrovanou architekturu s centralizovaným řízením pro koncové body i datové centrum. Cloudové a on-premise možnosti nasazení konzole jsou vhodné pro prostředí připravená na cloud, i pro přísně regulovaná prostředí.



Výhody:

- Detekuje a blokuje bezsouborové malwarové útoky.
- Blokuje skriptové útoky.
- Rozbalí a analyzuje neznámý malware ještě před spuštěním.
- Jediný agent, zabírající minimum prostoru a s nízkým vlivem na výkon systému.
- Zabudovaná konzole pro správu fyzických a virtuálních koncových bodů.

Ochrana koncových bodů

Bitdefender Endpoint Security HD – komponenta ochrany koncových bodů GravityZone Elite – chrání podniky proti celé škále komplikovaných kyberútoků s rychlostí, přesností, nízkou správní režií a minimálním vlivem na výkon systému. Řešení nové generace eliminuje nutnost provozu více řešení ochrany koncových bodů na jednom zařízení díky kombinaci preventivních kontrol, víceúrovňových metod detekce nezaložených na signaturách, a automatické odezvy.

Hlavní výhody

Rozpoznejte a zabraňte celé škále pokročilých hrozeb a neznámého malwaru.

Endpoint Security HD ničí pokročilé hrozby a neznámý malware, včetně ransomware, které obcházejí tradiční řešení ochrany koncových bodů. Pokročilé útoky jako PowerShell, skriptové, bezsouborové útoky a sofistikovaný malware lze rozpoznat a zablokovat ještě před spuštěním.

Rozpoznejte a zastavte bezsouborový malware.

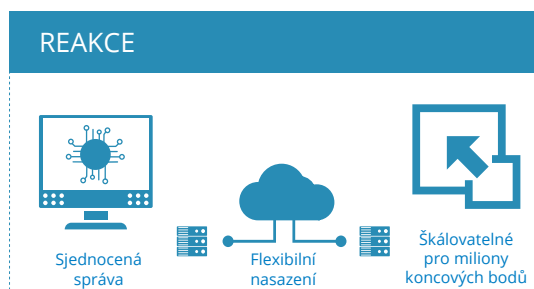
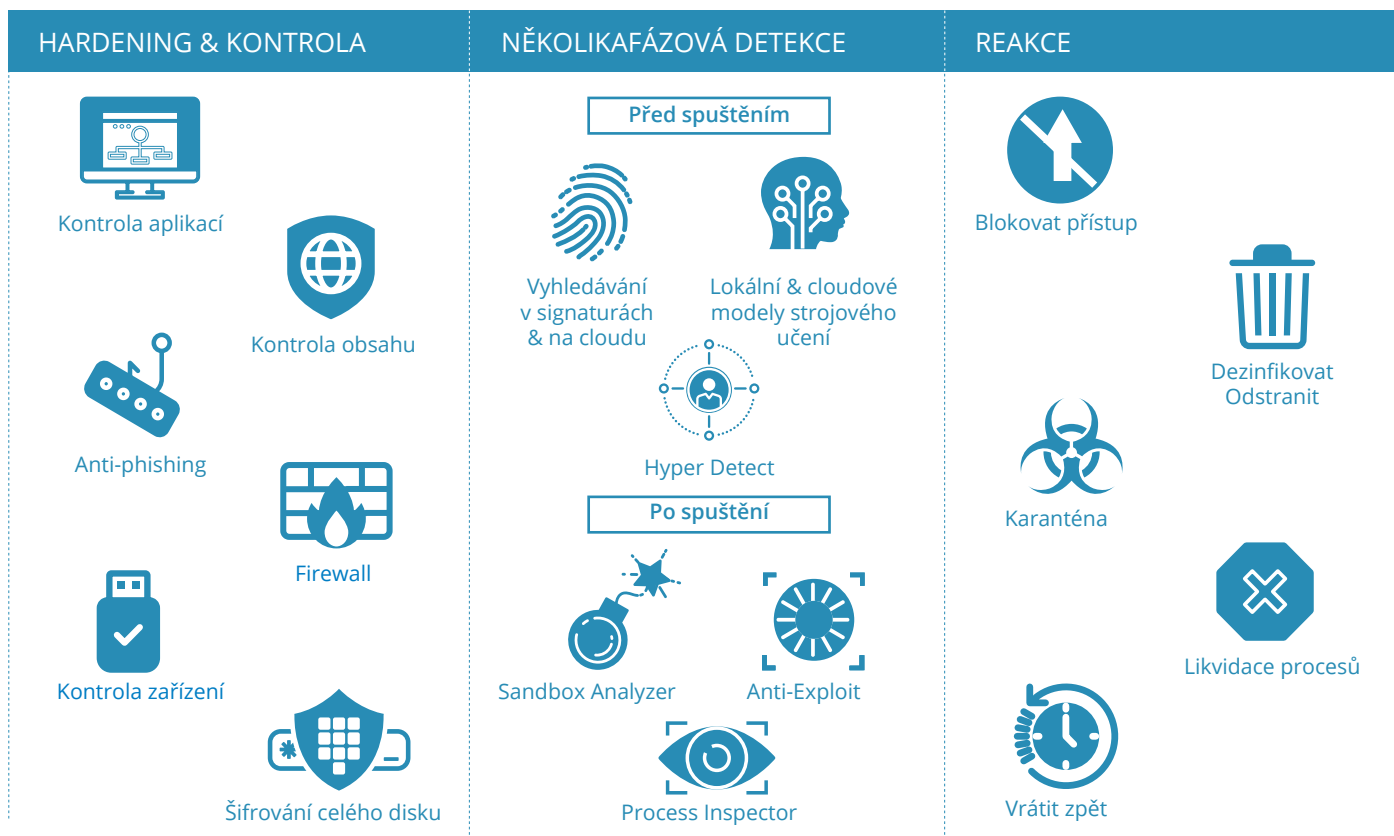
Bzsouborové malwarové útoky spouštějí škodlivé kódy přímo v paměti. Protože se na disku nevyskytuje žádný soubor, většina antivirových řešení vyvinutých pro analýzu souborů tyto útoky nezaznamená. Bitdefender využívá Advanced Anti-Exploit, HyperDetect™ a Process Inspector pro rozpoznání, zablokování a zastavení bezsouborových útoků.

Zastavte Makro a skriptové útoky.

V tomto případě jsou útočníky důvěryhodná makra MS Office, která využívají nástroje pro správu systému Windows, jako je PowerShell, pro spuštění skriptů a stahování škodlivých kódů, které spustí útoky. Protože se jedná o „důvěryhodné“ nástroje systému Windows, většina produktů ochrany koncových bodů, včetně takzvaných poskytovatelů antivirové ochrany nové generace, neprovádí důkladnou kontrolu skriptů, jako jsou PowerShell, WMI, interpreti Javascriptu atd. Bitdefender přidává metody Command-line Analyzery pro zachycení a kontrolu skriptů, které upozorní administrátory a zablokují spuštění skriptu, pokud by se pokusil o spuštění škodlivých příkazů.

Zautomatizujte sanaci hrozeb a odezvy.

Jakmile je rozpoznána hrozba, Endpoint Security HD ji okamžitě neutralizuje pomocí úkonů jako ukončení procesu, uložení do karantény, odstranění a obnovení do stavu před škodlivými



změnami. V reálném čase sdílí informace s GPN, informační službou Bitdefenderu na bázi cloudu o hrozbách, a celosvětově tak zabraňuje podobným útokům.

Získejte kontext hrozby a viditelnost.

Unikátní schopnost Bitdefender Endpoint Security HD identifikovat a hlásit podezřelou činnost poskytuje administrátorům včasné varování před škodlivým chováním, jako jsou podezřelé požadavky operačního systému, úhybné manévry a připojení k příkazovým a ovládacím centrům.

Funkce

Strojové učení.

Technologie strojového učení používají vysoce trénované strojové modely a algoritmy pro předpověď a blokování pokročilých útoků. Modely strojového učení Bitdefenderu využívají 40 000 statických a dynamických funkcí a jsou neustále zkoušeny na bilionech vzorků čistých i škodlivých souborů, nashromážděných z více než 500 milionů koncových bodů po celém světě. Tímto se výrazně zvyšuje efektivita při detekci malwaru a minimalizují se plané poplachy.

HyperDetect.

Tato nová vrstva obrany ve fázi před spuštěním obsahuje místní

Zvyšte provozní efektivitu s jediným agentem a integrovanou konzolí.

Jediný integrovaný agent Bitdefenderu pro ochranu koncových bodů eliminuje přetížení agenta. Modulární design nabízí maximální pružnost a umožňuje administrátorům nastavit zásady zabezpečení. GravityZone automaticky přizpůsobuje instalační balíček a minimalizuje vliv agenta na výkon systému. Zkonstruovaný od základů až po post-virtualizační a post-cloudové struktury zabezpečení, GravityZone poskytuje jednotnou platformu pro správu zabezpečení pro ochranu fyzických, virtualizovaných a cloudových prostředí.

modely strojového učení a pokročilou heuristiku, trénované k rozpoznání hackerských nástrojů, exploitů a technik obfuskace malwaru a k blokování hrozeb před spuštěním. Také rozpoznává metody dodávání, stránky hostující exploitové soupravy, a blokuje podezřelý síťový provoz. HyperDetect umožňuje správcům zabezpečení nastavit obranu tak, aby se mohla co nejeftivněji vypořádat s hrozbami, kterým podnik může čelit. S funkcí „Pouze hlášení“ mohou správci zabezpečení uspořádat a sledovat své nové zásady zabezpečení před jejich zveřejněním, a zamezit tak přerušování provozu. S kombinací vysoké viditelnosti a blokování hrozeb unikátní pro Bitdefender mohou uživatelé nastavit HyperDetect pro blokování na normální nebo tolerující úrovni, ale pokračovat v přijímání hlášení na agresivní úrovni a odhalovat časné ukazatele ohrožení.

Sandbox Analyzer integrovaný v koncových bodech.

Tato výkonná ochranná vrstva proti pokročilým útokům hloubkově analyzuje podezřelé soubory, detonuje zatížení uzavřené ve virtuálním prostředí hostovaném Bitdefenderem, analyzuje jejich chování a hlásí škodlivé záměry. Sandbox Analyzer, integrovaný s GravityZone Endpoint agentem, automaticky posílá podezřelé soubory k analýze. Po doručení rozsudku o škodlivosti ze Sandbox Analyzáru, Endpoint Security HD okamžitě automaticky zablokuje škodlivý soubor na všech systémech v celém podniku. Funkce automatického odesílání umožňuje správcům zabezpečení si zvolit mód „monitorování“ nebo „blokování“, a zabránit tak v přístupu k souboru, dokud o něm neobdrží verdikt. Správci také mohou posílat soubory k analýze ručně. Bohaté forenzní informace Sandbox Analyzáru poskytují k hrozbám jasný kontext a pomáhají správcům pochopit jejich chování.

Pokročilý Anti-Exploit.

Technologie prevence exploitů chrání paměť a zranitelné aplikace, jako jsou prohlížeče, čtečky dokumentů, multimediální soubory a runtime (tj. Flash, Java). Pokročilé mechanismy sledují postupy při přístupu k paměti pro rozpoznání a blokování exploitových technik, jako ověření volajícího API, pivotní zásobník, return-oriented-programming (ROT) a další.

Process Inspector.

Process Inspector pracuje v režimu nulové důvěry (zero-trust) a nepřetržitě monitoruje všechny procesy spuštěné v operačním systému. Vyhledává podezřelé aktivity a neobvyklé chování procesů, jako jsou pokusy o zastření typu procesu, spuštění kódu v prostoru jiného procesu (ovládnutí procesové paměti pro zvýšení úrovně oprávnění), replikace, přemísťování souborů, skrývání se před aplikacemi zobrazujícími výčet běžících procesů a další. Podniká náležitá nápravná opatření, včetně ukončení procesu a vrácení změn, které proces provedl. Je vysoce efektivní v rozpoznávání neznámého, pokročilého malwaru i bezsouborových útoků, včetně ransomwaru.

Anti-phishing a filtrování zabezpečení webu.

Filtrování zabezpečení webu umožňuje skenování příchozího

Ochrana datových center

GravityZone Security pro Virtualizovaná prostředí (SVE) využívá vrstvené obrany nové generace Bitdefender Endpoint Security HD, aby poskytl podnikům ve své třídě nejlepší zabezpečení pro pracovní zátěž serverů své třídy, VDI a cloudů, zatímco maximalizuje výkonnost infrastruktury a provozní efektivitu. GravityZone SVE je navržen jako řešení pro podniky, které dokáže podpořit i ta největší datová centra.

Hlavní výhody

Hbitost

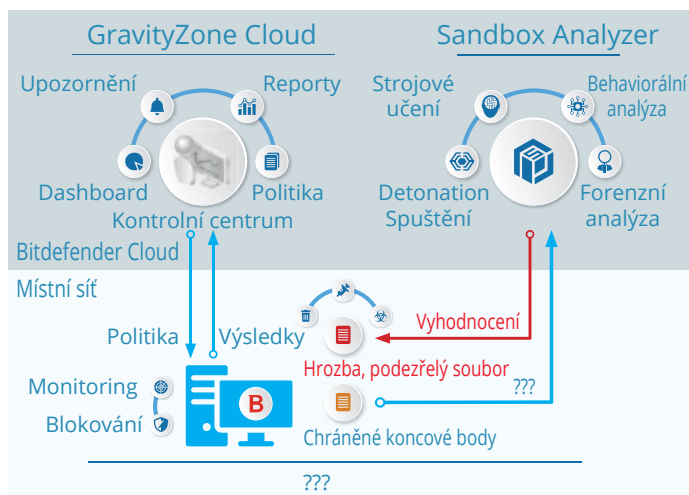
SVE umožňuje automatizované zabezpečení napříč životním cyklem datového centra jak při zavádění, tak při každodenních bezpečnostních operacích ve vysoce dynamickém virtuálním prostředí. Je integrovaná s VMware (vCenter, vShield, NSX), Citrix XenCenter a s platformou Nutanix Enterprise Cloud a poskytuje rychlá automatická opatření.

Provozní výkonnost

Jednotná ovládací konzole GravityZone Control Center usnadňuje nasazení zabezpečení, správu a aktualizace, a poskytuje soustředěnou viditelnost do všech virtuálních a hmotných serverů a pracovních stanic. Podporuje centralizovanou tvorbu a automatickou administraci bezpečnostních zásad, které pomáhají zefektivnit IT operace, zatímco zlepšují soulad.

Zdokonalené využití infrastruktury

Centralizované skenování a nízká náročnost agenta výrazně snižují využití paměti, místa na disku, činnosti CPU a I/O na hostitelských serverech, zatímco zvyšují hustotu VM a návratnost investic v IT infrastruktuře.



síťového přenosu, včetně SSL, přenosu http a https v reálném čase pro zabránění stažení malware na koncový bod. Ochrana proti phishingu automaticky blokuje phishing a podvodné webové stránky.

Šifrování celého disku

Šifrování celého disku spravované skrze GravityZone pomocí Windows BitLocker a Mac FileVault, využívající výhod technologii zabudovaných v operačních systémech.

Kontrola koncových bodů a hardening.

Správa koncových bodů na základě bezpečnostních zásad zahrnuje firewall, kontrolu zařízení s USB skenováním, a kontrolu webového obsahu s kategorizací URL.

Odezva a zamezení dalšímu šíření.

GravityZone nabízí tu nejlepší čistící technologii na trhu. Automaticky blokuje/izoluje hrozby, ničí škodlivé procesy a vrací zpět změny.

Univerzální kompatibilita

Kompatibilní se všemi virtualizačními platformami (jako jsou VMware® ESXi™, Microsoft® Hyper-V™, Citrix® XenServer®, Red Hat® Enterprise Virtualization®, KVM a Nutanix® Acropolis), s Microsoft Active Directory a oběma hostujícími operačními systémy Windows® a Linux®, GravityZone usnadňuje nasazení, odhalování koncových bodů a správu zásad.

Neomezená lineární škálovatelnost

Můžete využít několika SVA pro zvýšení kapacity skenování s růstem datového centra a tvorbou nových VM. Jakmile existující SVA dosáhne určitého prahu zatížení, můžete nasadit nové a přizpůsobovat růst.

Vrstvená obrana nové generace

GravityZone Security pro virtualizovaná prostředí zahrnuje všechny klíčové úrovně zabezpečení Endpoint Security včetně HyperDetect, Sandbox analyzáru a metod detekce bezsouborových útoků, a poskytuje tak vedoucí ochranu pro podniková digitální aktiva uložená nebo zpracovávaná v datovém centru.

Bitdefender

Zabezpečení pro mobilní zařízení iOS a Android

Toto řešení je navrženo pro podporu kontrolovaného přijetí konceptu „Přines si své vlastní zařízení“ (BYOD) důsledným prosazováním zásad zabezpečení na zařízeních všech uživatelů. Jako výsledek jsou mobilní zařízení pod kontrolou a všechny citlivé obchodní informace, které obsahují, jsou chráněny. Administrativní zátěž je snížena díky vždy aktuálnímu stavu vyhovujících a nevyhovujících zařízení.

Zabezpečení pro Exchange servery

Poskytuje několikvrstevnou ochranu pro posílání zpráv: antispam, antiphishing, antivirus a antimalware s analýzou chování, ochranou proti zero-day hrozbám a filtrováním e-mailového provozu, včetně filtrování příloh a obsahu. Antimalwarové skenování lze stáhnout z chráněných mailových serverů na centralizované bezpečnostní servery. Správa a vytváření přehledů je centralizována a umožňuje jednotné zásady pro koncové body a zasílání zpráv.

GravityZone Control Center

GravityZone Control Center je integrovaná a centralizovaná ovládací konzole poskytující celkový přehled všech součástí správy zabezpečení, včetně zabezpečení koncových bodů, zabezpečení datových center, zabezpečení pro Exchange a zabezpečení pro mobilní zařízení. Může být hostováno na cloudu nebo nasazeno lokálně. Centrum správy GravityZone zastává několik rolí a obsahuje databázový server, komunikační server, aktualizací server a webovou konzoli. Pro větší podniky je možné ho nakonfigurovat tak, aby využíval několik virtuálních zařízení s více instancemi specifických rolí s vestavěným vyrovnávačem zatížení pro škálovatelnost a vysokou dostupnost.

Podrobné systémové požadavky naleznete na www.bitdefender.cz

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.bitdefender.cz>



Všechna práva vyhrazena. © 2017 Bitdefender. Všechny zde uvedené ochranné známky, obchodní názvy a produkty jsou majetkem jejich příslušných vlastníků. PRO VÍCE INFORMACÍ NAVŠTIVTE: bitdefender.cz

