Smlouva o dílo

Smluvní strany:

Objednatel: **Město Pelhřimov**

se sídlem: Masarykovo náměstí č. 1, 393 01 Pelhřimov

IČO: 00248801

Zastoupené: Ladislav Med, starosta
Ing. Josef Koch, místostarosta

č. účtu: Česká spořitelna, č. účtu 27-9900250/0800

(dále jen jako „Objednatel“)

a

Zhotovitel: **CYBOSEC s.r.o.**

se sídlem: Hradčany 347, 503 53 Smidary

IČO: 04301226

DIČ: CZ04301226

zastoupení: Pavel Jícha, jednatel společnosti

bankovní spojení: FIO Banka, č. [redacted]

zapsaná v obchodním rejstříku vedeném krajským soudem v Hradci Králové, spisová značka C 42008 (pro právnické osoby)

(dále jen jako „Zhotovitel“)

(Objednatel a Zhotovitel dále také společně jako „Smluvní strany“ a každý samostatně jako „Smluvní strana“)

uzavřely níže uvedeného dne, měsíce a roku dle ustanovení § 2586 a násl. zákona č. 89/2012 Sb., občanský zákoník, ve znění pozdějších předpisů, tuto smlouvu o dílo (dále jen „Smlouva“):

I.
Předmět Smlouvy

Zhotovitel se touto smlouvou zavazuje provést na svůj náklad a nebezpečí pro Objednatele za podmínek níže uvedených dílo: **Implementaci systému Bitdefender GravityZone Ultra varianta CLOUD včetně podpory na 36 měsíců.** (dále jen „Dílo“) a Objednatel se zavazuje Dílo převzít a zaplatit za něj Zhotoviteli cenu, která je sjednána v čl. III této Smlouvy. Podrobný systému je uveden v příloze č.1, která je nedílnou součástí této smlouvy.

Předmětem této smlouvy je implementace systému … sestávající z:

- dodávky licencí systému pro 200 koncových stanic Objednatele,
- implementace a instalace systému,
- školení administrátorů,
- podpora na období 36 měsíců.

II.
Cena Díla, platební podmínky

1. Smluvní strany se dohodly, že celková cena díla činí:

- cena díla bez DPH: **385 000** Kč bez DPH (slovy: tři sta osmdesát pět tisíc korun českých)
- DPH: 80 850 Kč
- celkem: **465 850 Kč s DPH**

Nedílnou součástí této smlouvy je Příloha č.2 – položkový rozpočet.

2. Výše uvedená cena díla je sjednána jako **cena maximální**, v které jsou zahrnuty veškeré práce, dodávky a služby nezbytné k řádnému provedení předmětu díla. Zhotovitel zaručuje úplnost rozpočtu a přebírá nebezpečí změny okolností dle § 2620 odst. 2 občanského zákoníku.

3. Smluvní strany se dohodly, že cena díla bude uhrazena na účet Zhotovitele uvedený v záhlaví této smlouvy při předání a převzetí Díla (viz čl. V Smlouvy).

4. Smluvní strany se dohodly, že daňové doklady se základem pro výpočet DPH vyšším než 20.000, - Kč budou obsahovat prohlášení tohoto nebo významově totožného znění: „**Vystavitel tohoto daňového dokladu čestně prohlašuje, že není v insolvenčním ani obdobném řízení, a že se zavazuje zde vyčíslenou DPH uhradit včas a řádně příslušnému správci daně.**“. V případě neuvedení tohoto prohlášení na daňovém dokladu nebude na zde vyčíslenou DPH reflektováno a tato bude objednatelem uhrazena jiným (náhradním) způsobem. Shora uvedené čestné prohlášení musí být uvedeno nad signací daňového dokladu. V opačném případě musí být čestné prohlášení dodavatele znovu opatřeno podpisem a razítkem dodavatele.

5. Smluvní strany se dohodly, že pokud se zhotovitel stane ke dni uskutečnění zdanitelného plnění nespolehlivým plátcem DPH, objednatel je oprávněn provést zajišťovací úhradu DPH na účet příslušného finančního úřadu.

6. Zadavatel nebude poskytovat zálohy.

7. Daňový doklad bude vystaven do 14 kalendářních dnů po převzetí předmětu plnění. Doba splatnosti daňových dokladů je stanovena na 30 kalendářních dnů ode dne doručení daňového dokladu odběrateli. Platby budou probíhat výhradně v CZK a rovněž veškeré cenové údaje budou v této měně.

8. Předání díla bude provedeno na základě předávacího protokolu. Osobami pověřenými k předání díla jsou Ing. Václav Turek za Objednatele a Pavel Jícha za Zhotovitele.

III.

Doba plnění, místo plnění

1. Smluvní strany se dohodly, že Dílo bude Zhotovitelem provedeno nejpozději do 30. 11. 2021.
2. V případě prodlení s provedením předmětu díla (tj. jeho řádným předáním a převzetím – viz čl. V) je Zhotovitel povinen zaplatit Objednateli smluvní pokutu ve výši 0,05 % ze smluvní ceny díla (včetně DPH) za každý započatý den prodlení. Tato smluvní pokuta je započitatelná proti ceně díla.
3. Místem plnění je Město Pelhřimov

IV.
Práva a povinnosti Smluvních stran

1. Objednatel je oprávněn kdykoliv v průběhu Díla kontrolovat, zda je prováděno v souladu s touto Smlouvou.
2. Objednatel se zavazuje poskytovat Zhotoviteli součinnost k provedení Díla, a to ve lhůtě, jíž mu Zhotovitel určí.
3. Zhotovitel postupuje při provádění Díla samostatně.
4. Zhotovitel je povinen dodržet při provádění Díla všechny právní předpisy a příslušné technické normy týkající se předmětné činnosti.

V.
Předání a převzetí Díla

1. K předání a převzetí Díla dojde nejpozději v termínu dle čl. III Smlouvy. Předání a převzetí Díla bude Smluvními stranami písemně potvrzeno (předávací protokol).

2. Zhotovitel se zavazuje předat Dílo bez vad a nedodělků.
3. Smluvní strany se dále dohodly, že budou-li v době předání na Díle viditelné vady či nedodělky, k předání a převzetí Díla dojde až po jejich odstranění. O této skutečnosti bude Smluvními stranami sepsán záznam. Náklady na odstranění vad nese Zhotovitel.

VI.
Odpovědnost za vady, záruka

1. Zhotovitel odpovídá za vady předmětu díla.
2. Vzájemnou dohodou se stanoví záruční doba na předmět díla v délce 36 měsíců.
3. Záruční doba začíná běžet dnem předání a převzetí řádně a úplně provedeného díla (viz čl. V).
4. Zhotovitel se zavazuje zajistit záruční servis na dodanou technologii po dobu 36 měsíců ode dne předání díla.
5. Záruční doba se prodlužuje o dobu počínající datem uplatnění reklamace (vady) a končí dnem odstranění vady.
6. Zahájení vlastní opravy řádně reklamované vady je Zhotovitel povinen zahájit nejpozději do 24 hodin po nahlášení závady. Pokud tak neučiní, je povinen hradit Objednateli smluvní pokutu ve výši 500,-- Kč za každý den, o který nastoupí později. Náklady na odstranění reklamovaných vad nese Zhotovitel; o odstranění vady se vyhotoví písemný záznam, který obsahuje popis vady, termín a způsob jejího odstranění.
7. Pokud Zhotovitel neodstraní vadu díla vůbec, je Objednatel oprávněn odstraněním vad pověřit jiného dodavatele a náklady tohoto odstranění vad požadovat na Zhotoviteli.
8. Záruka zaniká v těchto případech:
    a. systém byl používán v rozporu s návodem k obsluze
    b. závada vznikla nepřípustným zásahem do systému, včetně servisních zásahů a úprav jinou osobou nebo subjektem, než je organizace Zhotovitele
    c. systém je mechanicky poškozen nebo jeho poškození bylo způsobeno vnějšími vlivy (znečištění, cizí látky vniklé do zařízení, přepětí apod.)
    d. poškození bylo způsobeno vlivem neodvratné události (živelná pohroma).
9. Servisní telefon Zhotovitele pro hlášení závad
    - Lokální podpora v CZ
    - Pracovní dny 9:00 - 17:00
        - Tel: [redacted]
        - WEB: https://support.bitdef.cz/submit_ticket
    - Globální podpora výrobce v ENG
    - Doba podpory 24x7
        - [redacted]

VII.
Závěrečná ustanovení

10. Tato Smlouva nabývá platnosti dnem jejího podpisu oběma Smluvními stranami a účinnosti dnem uveřejnění v registru smluv.

11. Tato Smlouva a vztahy z ní vyplývající se řídí právním řádem České republiky, zejména příslušnými ustanoveními zák. č. 89/2012 Sb., občanský zákoník, ve znění pozdějších předpisů.

12. Smluvní strany stvrzují, že plnění z této smlouvy je plněním ve vztahu k veřejnoprávní korporaci a veřejným prostředkům, a tudíž že skutečnosti a údaje uvedené ve smlouvě nejsou obchodním tajemstvím.

13. Smluvní strany podpisem této smlouvy dávají souhlas ke zveřejnění osobních údajů ve smlouvě obsažených pro účely uveřejnění smlouvy a metadat smlouvy v registru smluv zřízeném podle zákona č. 340/2015 Sb. o zvláštních podmínkách účinnosti některých smluv, uveřejňování těchto smluv a o registru smluv (zákon o registru smluv).

14. Smlouva byla vyhotovena ve dvou stejnopisech, z nichž každá Smluvní strana obdrží po jednom vyhotovení.

15. Smluvní strany níže svým podpisem stvrzují, že si Smlouvu před jejím podpisem přečetly, s jejím obsahem souhlasí, a tato je sepsána podle jejich pravé a skutečné vůle, srozumitelně a určitě, nikoli v tísni za nápadně nevýhodných podmínek.

16. Změny a doplňky této smlouvy lze učinit pouze formou písemných dodatků odsouhlasených oběma smluvními stranami.

17. Nedílnými přílohami této smlouvy jsou:

    a. Příloha č.1: Technická specifikace (popis systému)

    b. Příloha č. 2: Položkový rozpočet

V Pelhřimově dne .....

.....

V Praze dne 15.9.2021

[redacted]

Digitálně podepsal [redacted]

.....

[redacted]

Příloha 1 – Technická specifikace (popis systému)

Požadavky zadavatele uvedené v zadávací dokumentaci:

Požadavky na poptávaný systém ochrany koncových stanic a serverů:
1. Detekce nových hrozeb bez nutnosti aktualizace endpointů
2. Plná schopnost detekce/obrany i v režimu offline, včetně dlouhodobého odpojení od sítě
3. Automatická tvorba analýzy útoku, včetně grafického zobrazení a možnosti exportu popisu útoku ve strojově čitelném formátu
4. Možnost manuálního plánování aktualizací
5. Podpora pro ochranu kontejnerů (Docker, Kubernetes)
6. Technická podpora dostupná v režimu 24/7
7. Možnost uvést koncové zařízení do původního stavu před proběhlou hrozbou, včetně rekonstrukce poškozených dat
8. Detekce hrozeb pomocí behaviorální analýzy a přímé pasivní detekce
9. Podpora aplikačního inventáře, včetně zobrazení možných zranitelností skrz programy

Všechny uvedené požadavky nabízený nástroj Bitdefender GravityZone ULTRA varianta CLOUD - SPLŇUJE (nabízí spoustu funkcionalit navíc)

Detailní technický popis nabízeného řešení

Reference technologie

Bitdefender chrání široké spektrum zákazníků od malých firem až po velké korporace, včetně kritické infastruktury státu, nemocnic, školství a státní správy.

Zde uvádíme některé naše zákazníky využívající Bitdefender bezpečnostní řešení v české a slovenské republice.

A mnoho dalších

Více než 150 firem používá v ČR a SK produkt Bitdefender ULTRA s EDR technologií.

Bitdefender GravityZone ULTRA (EDR) detailní popis

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.

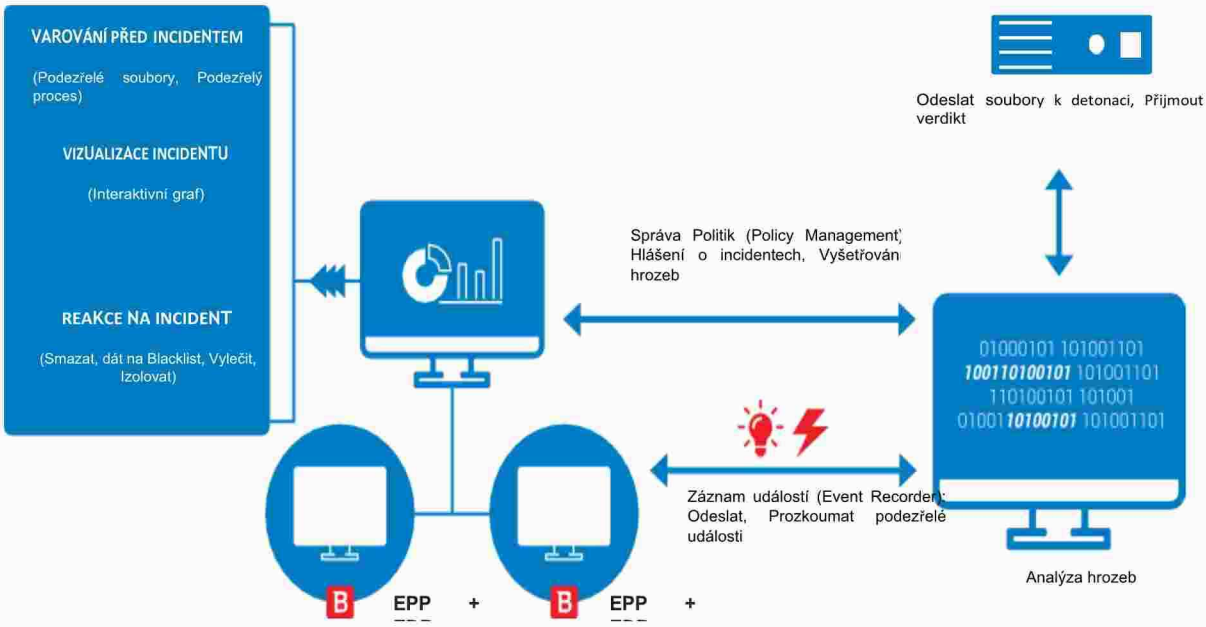
GravityZone Ultra umožňuje podnikovým zákazníkům přesně chránit digitální aktiva i před těmi nejhůře polapitelnými kybernetickými hrozbami a zároveň efektivně reagovat na všechny fáze útoku prostřednictvím:

- 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 i po jeho ukončení (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 aktualizací)

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 zastavuje efektivně útoky.

Jakožto integrovaná sada řešení ochrany koncových bodů zajišťuje GravityZone Ultra konzistentní úroveň zabezpečení pro celé IT prostředí, takže útočníci nenajdou potenciálně 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 rychle společnostem nasadit řešení ochrany koncových bodů a po implementaci vyžaduje menší administrativní úsilí.

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



Výhody

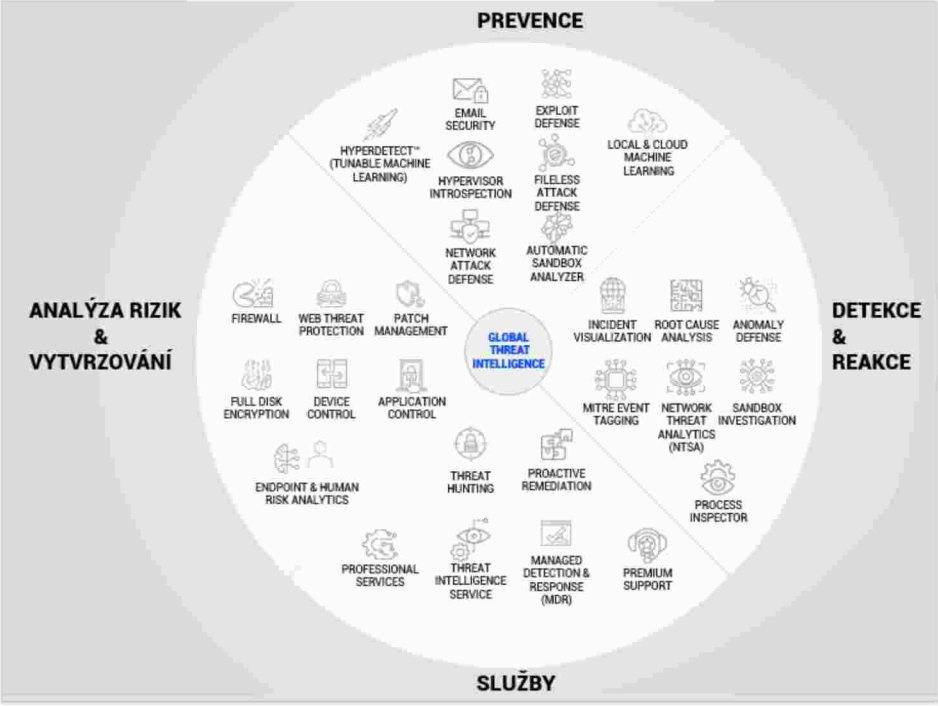
- Detekuje a blokuje bezsouborové malwarové útoky
- Blokuje skriptové útoky
- Rozbalí a analyzuje neznámý malware ještě před spuštěním
- Jediný agent, zabírající minimum prostoru a s nízkým vlivem na výkon systému
- Zabudovaná konzole pro správu fyzických a virtuálních koncových bodů

Ochrana koncových bodů

Bitdefender Endpoint Security HD-komponenta ochrany koncových bodů GravityZone Ultra-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, vícestupňových metod detekce nezaložených na signaturách, a automatické odezvy.

Integrované technologie a služby

Obrázek 2. Bitdefender: Komplexnost bezpečnostního řešení ve čtyřech fázích



Hlavní výhody

Bitdefender GZ ULTRA 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. Bezsouborové 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, HyperDetectTM a Process Inspector pro rozpoznání, zablokování a zastavení bez souborových útoků.V tomto případě jsou útočníky důvěryhodná makra MS Office, která využívají nástroje pro správu systému Windows, jako je PowerShell, pro spouštění 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 Analyzeru pro zachycení a kontrolu skriptů, které upozorní administrátory a zablokují spuštění skriptu, pokud by se pokusil o spuštění škodlivých příkazů. 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. 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

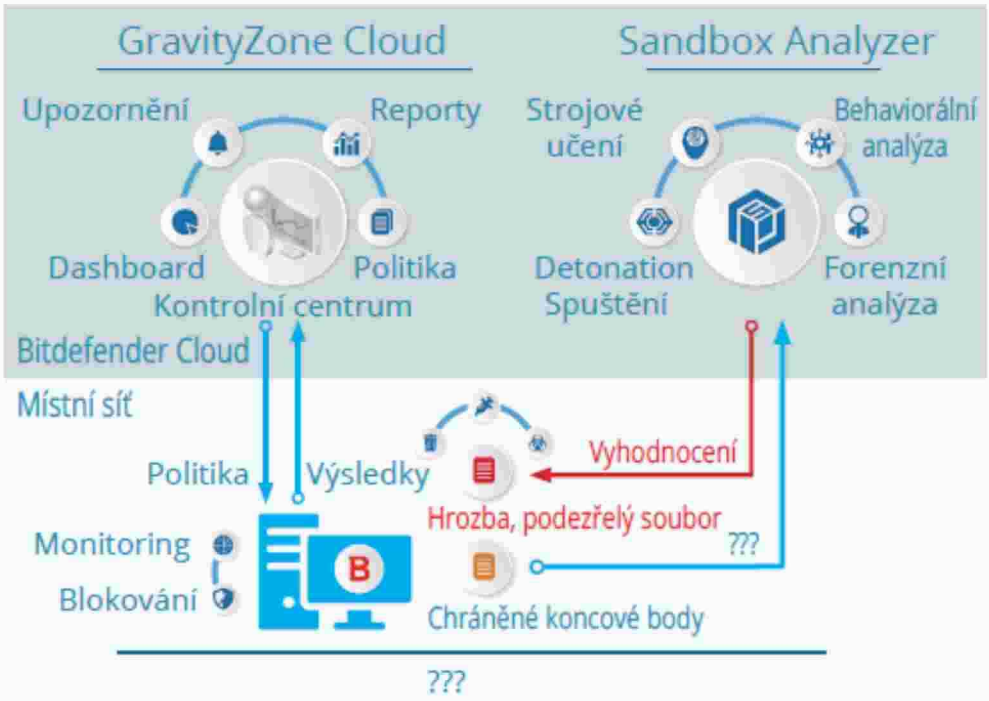
Tato nová vrstva obrany ve fázi před spuštěním obsahuje místní modely strojového učení a pokročilou heuristiku, trénovanou k rozpoznání hackerských nástrojů, exploitů a dalšího malwaru a k blokování hrozeb před spuštěním. Blokuje také podezřelý síťový provoz
Umožňuje správcům zabezpečení nastavit ochranu tak, aby se mohla co nejefektivněji vypořádat s hrozbami, kterým podnik může čelit.

S funkcí „Pouze hlášení" mohou správci systému nastavit a sledovat své nové nastavení politik zabezpečení před jejich uplatněním, a zamezit tak přerušení provozu. S kombinací vysoké viditelnosti a blokování hrozeb unikátní pro Bitdefender mohou správci nastavit HyperDetect na stupeň blokování na normální nebo tolerující úrovneň, ale pokračovat v monitoringu nastavení na agresivní úrovni a tím odhalovat další možná bezpečnostní rizika. 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.

Sandbox Analyzer integrovaný v koncových bodech

Tato výkonná ochranná vrstva proti pokročilým útokům hloubkově analyzuje podezřelé soubory, detonuje je v uzavřeném 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 vyhodnocení o škodlivosti ze Sandbox Analyzeru, Endpoint Security HD okamžitě automaticky zablokuje škodlivý soubor na všech systémech v celém podniku. Funkce automatického odesílání umožňuje správcům systému zvolit si 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 Analyzeru poskytují k hrozbám jasný kontext a pomáhají správcům pochopit jejich chování. Sandbox Analyzer, integrovaný s GravityZone Endpoint agentem, automaticky posílá podezřelé soubory k analýze.

Obrázek 3. Bitdefender: Provázanost jednotlivých vrstev



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, returnoriented-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, přemisťování 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 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.

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.

GravityZone nabízí tu nejlepší ochranu na trhu. Automaticky blokuje/izoluje hrozby, ničí škodlivé procesy a vrací

zpět změny.

Snadné EDR

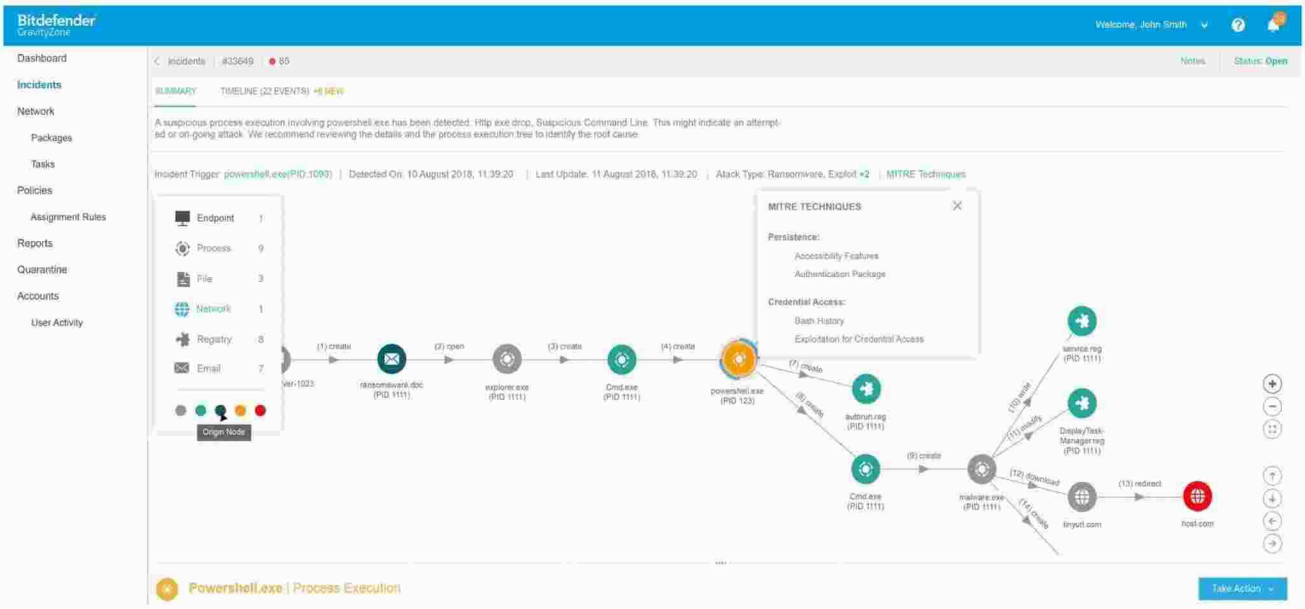
GravityZone Ultra, díky jasné viditelnosti v ukazatelích bezpečnostních metrik útoku (IOC), vyšetřování hrozeb na jedno kliknutí a nápravným reakcím na incidenty, snižuje nároky na zdroje a dovednosti bezpečnostních týmů. Nový datový záznamník bezpečnostních událostí koncových bodů (evenrecorder) je vítaným účinným doplňkem mnohavrstvé ochrany jakožto velmi důležitá součást ucelené ochrany koncových bodů před hrozbami. Jelikož poskytuje rozsáhlé zachycení systémových aktivit (soubory a procesy, instalace programu, načtení modulů, změna registru, síťová připojení atd.), proto umožňuje 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 datech na základě: ukazatelů bezpečnostních metrik útoku (IOCs)tagů v MITRE znalostní databázi procesů, souborů, registrů a jiných parametrů

Obr. 4 Stránka Podrobnosti o incidentech - Poskytuje jasný přehled o incidentu a veškerých detailech útoků.
Správce může snadno získat detailní informace a zareagovat.



.

Přesná detekce umožňuje účinnější bezpečnostní optiku a uvolňuje Vám ruce nezobrazováním 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 dalších forem 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, detekci a reakci, umožňuje rychlou reakci a obnovení koncových bodů do fáze „better then before“. Nástroje pro vyšetřování incidentů, jako analýza kořenových příčin a hlášení karantény, pomáhají administrátorům 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

GravityZone Ultra zahrnuje veškeré 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 a další malware pomocí automatické nápravy.
- Ochrana paměti pro předcházení exploitům.
- Snižuje útočný prostor
- Integrovaný klient obsahující firewall, kontrolu zařízení, filtrování webového obsahu, kontrolu aplikací, správu patchů (přídavný add-ON) a další.

Ochrana Virtualizačních prostředí

Plně zabudovaná komponenta pro Ochranu datového centra GravityZone je řešení pro zabezpečení virtualizovaných prostředí (SVE). Je tím nejpokročilejším řešením zabezpečení virtualizovaných datových center na trhu, optimalizující nejen míru potřebných GPU, ale také provozní náklady.
GravityZone SVE je řešením pro podniky, které spravují i ta největší datová centra. Integrace je snadná a klady této technologie mohou využívat organizace provozující virtuální prostředí všech velikostí.

Hlavní výhody

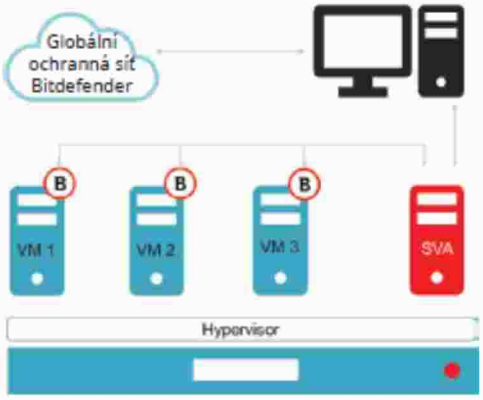
Hbitost

SVE umožnuje 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 fyzických serverů a pracovních stanic. Podporuje centralizovanou správu a automatickou administraci bezpečnostních zásad, které pomáhají zefektivnit IT operace.

Obr. 5 Nasazení SVA ve virtuálním prostředí



Zdokonalené využití infrastruktury

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

Univerzální kompatibilita

Kompatibilní se všemi předními hypervizorními platformami (VMware ESXi, Microsoft Hyper-V, Citrix Xen, Red Hat KVM a Nutanix AHV) a s Windows i Linuxem.

Neomezená lineární škálovatelnost

Můžete využít několika SVA pro zvýšení kapacity skenování s růstem datového centra a tvorbou nových VM. Dalším přínosem je nasazení několika SVA čímž zvýšíte odolnost a zajistíte sdílení zátěže: zátěž při selhání/přetížení SVA může převzít jiný aktivní nebo méně zatížený SVA.

Vrstvená ochrana nové generace

GravityZone Security pro virtualizované prostředí zahrnuje všechny klíčové úrovně zabezpečení Endpoint Security včetně HyperDetect, SandBox analyzeru a metod detekce bez souborových útoků, a poskytuje tak ochranu pro podniková digitální aktiva uložená nebo zpracovávaná v datovém centru.

Funkce

- Navrženo pro umožnění transformace datových center: SDDC, hyper-convergence a hybrid cloud
- Komplexní integrace s VMware, Microsoft, Citrix, AWS pro snížení nákladů. Automatizace instalace a správy nastavení a licencí
- Podpora několika virtualizačních a cloudových prostředí z jediného nasazení
- Souhrnná viditelnost a centralizovaná správa napříč hybridním cloudem
- Výkonná, odolná a škálovatelná architektura na bázi SVA, s podporou všech hypervizorů
- Maximalizovaná hustota VM, nízká zátěž systému při spuštění a optimální výkon aplikací
- Pokročilé vícevrstvé zabezpečení s nepřetržitou ochranou celého hybridního cloudu

GravityZone Control Center

GravityZone Control Center je integrovaná a centralizovaná ovládací konzole poskytující celkový přehled všech součástí správy zabezpečení, včetně zabezpečení koncových bodů, datových center, zabezpečení pro Exchange a pro mobilní zařízení. Může být hostováno v cloudu nebo nasazeno lokálně. Centrum správy GravityZone zastává několik rolí a obsahuje databázový server, aktualizační server, komunikační server a webovou konzoli. Control Center je doručeno jako jeden obraz virtuálního zařízení a může být nasazen za méně než 30 minut. 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.

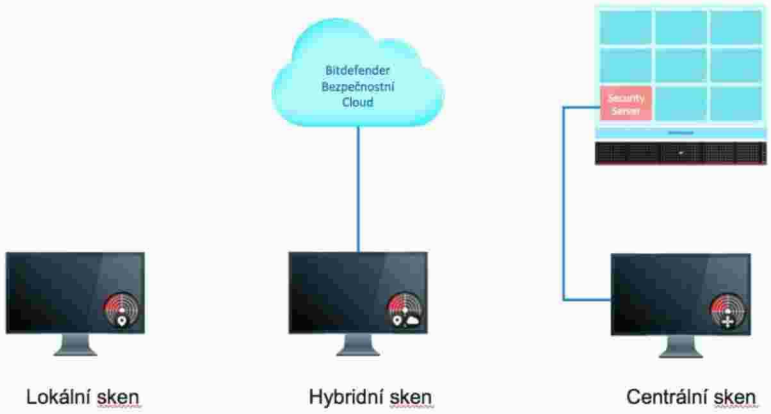
Základní popis GravityZone Architektury řešení (shodný se všemi variantami od verze Enterprise a výš)

Bitdefender GravityZone (dále jen BDGZ) je firemní řešení nabízející nasazení centrální správy všech zařízení ve variantách on-premise (hostované u zákazníka) nebo hostované v cloudu. BDGZ umožňuje spravovat fyzické, virtuální a mobilní koncové body nezávisle na operačním systému, hypervizoru a to vše z jediné centrální konzole. BDGZ řešení se neinstaluje, ale pouze konfiguruje díky využití principu virtuálních appliance (které výrobce poskytuje jako OVA format) ihned připravených k provozu. Řešení je plně škálovatelné od jednotek až po nekonečně mnoho chráněných zařízeních využitím systému klonování virtuálních appliancí. Hlavní technologie, které řadí BDGZ dle nezávislých testů dlouhodobě mezi nejlepší firemní řešení jsou: antivirus a antimalware

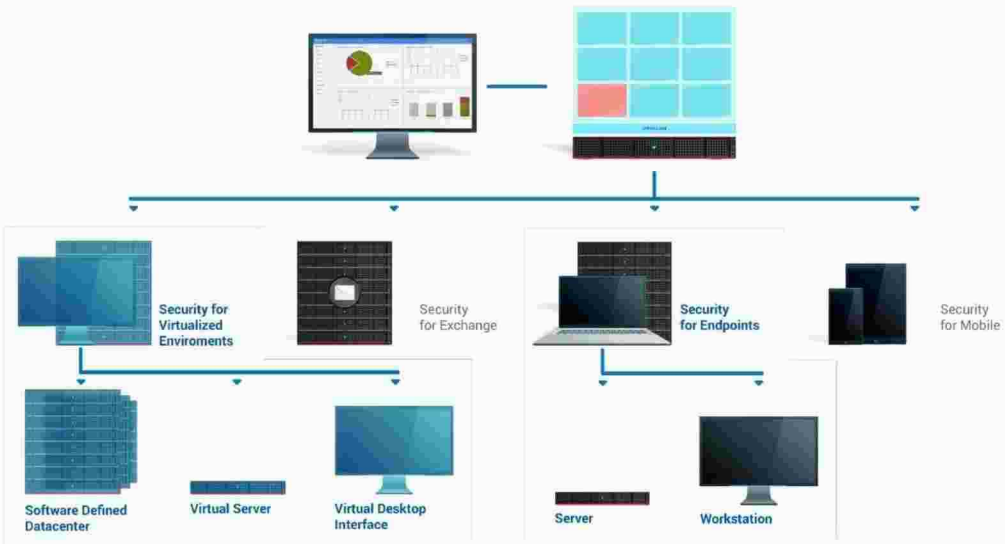
s behaviorální monitoringem, ochrana před hrozbami nultého dne pomocí globální ochranné sítě BDGZ, kontrola aplikací a sandboxing, firewall, kontrola zařízení, kontrola obsahu s antiphishingem a antispamem pro mailservery.

BDGZ nabízí vzdálenou instalaci na neomezené množství stanic včetně automatické odinstalace většiny známých konkurenčních antimalwarových řešeních. BDGZ umožňuje kromě klasického lokální skenování a testování souborů, aplikací, paměti a registrů na hrozby, také možnost využití hybridního a centrálního skenování. V případě hybridního skenování je umožněno přenést částečně zátěž z lokálních zdrojů koncového bodu do globální ochranné sítě Bitdefenderu. V případě centrálního skenování se využívá specializovaných bezpečnostních virtuálních serverů (Security Server), které se o tyto procesy starají. Tyto bezpečnostní virtuální appliance centralizují a deduplikují antimalwarové procesy.

Obrázek 6. Popis skenovacích možností BDGZ



Obrázek 7. Infrastruktura BDGZ přehled všech komponentů včetně centrální správy pro fyzické i virtuální prostředí, včetně podpory pro mobilní zařízení a MS Exchange.

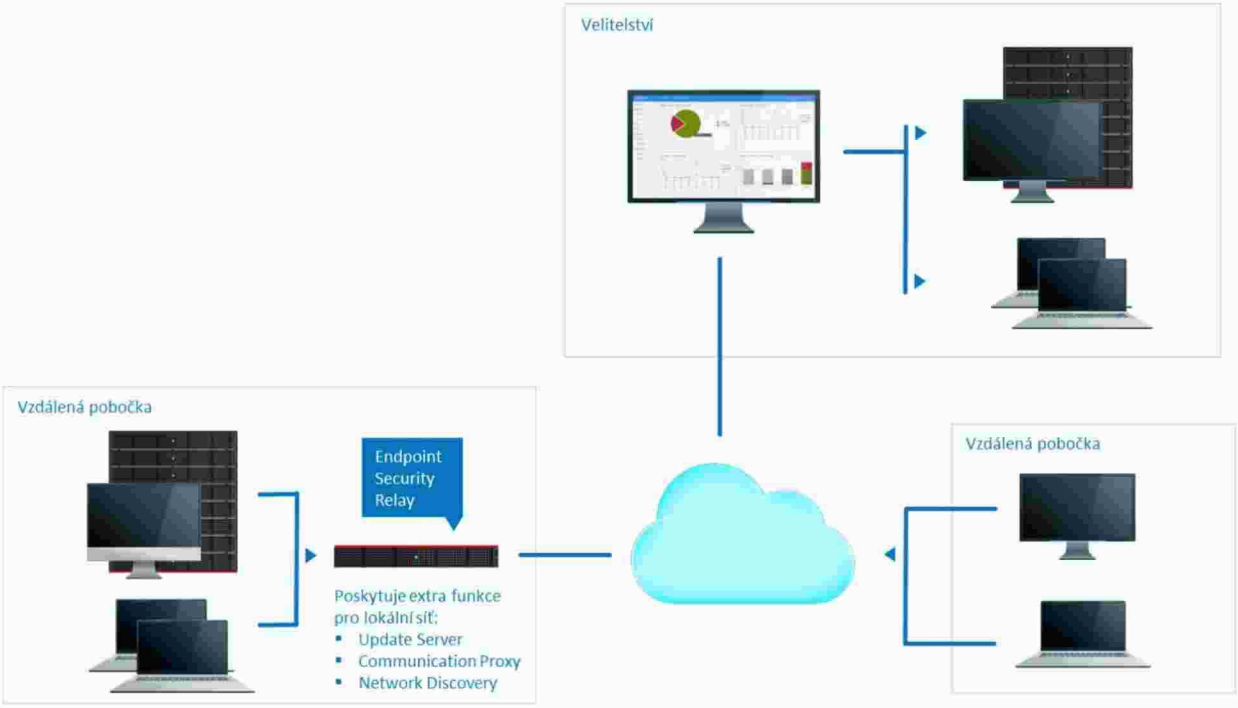


Bitdefender GravityZone komponenty:

- GravityZone Virtuální Appliance (dale jen GZVA) ve formátech .ova, .vhd, .xva, .raw, .ovf.
- GZVA může obsahovat jednu, více nebo všechny následující role:
- Databázového serveru (MongoDB),
- Komunikačního server,
- Update server,
- Webové konzole správy,
- Balanceru,
- Security Serveru. Server pro Centrální skenování (SS) ve formátech -.ova, .vhd, .xva, .raw, .ovf.
- BEST (Bitdefender Endpoint Security Tools) klient přizpůsobitelný OS, na který je nasazen; přizpůsobuje svůj běh tomu, zda se jedná o fyzický nebo virtuální chráněný koncový bod.
- BEST klient s rolí relay,
- extra funkce update serveru, komunikační proxy a network discovery pro lokální síť.

Obrázek 8. Škálování GZVA s využitím vysoké dostupnosti Databáze a role Balanceru

Obrázek 9. Infrastruktura BDGZ s využitím BEST klienta s rolí Relay pro menší pobočky



Funkční vlastnosti řešení

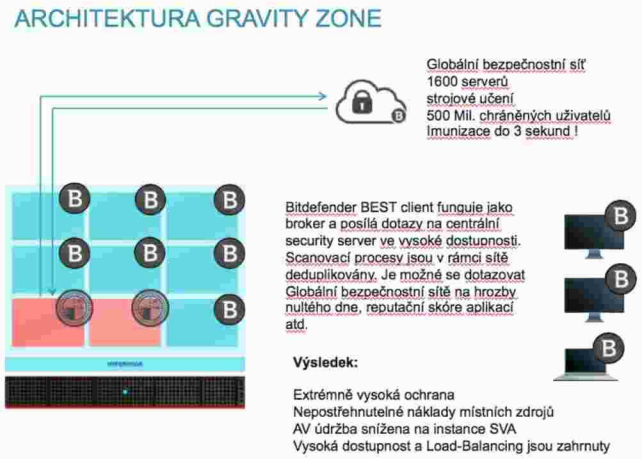
Souhrn technických částí a funkcí řešení BDGZ

BDGZ nabízí následující funkční vlastnosti, které jsou plně v souladu s požadavky ZD:

- nastavení pravidelných naplánovaných skenů,
- nastavitelné pravidelné aktualizace signatur a produktů,
- pokročilý reporting včetně logování,
- automatické upozorňování nejen na malwarové události,
- plně nastavitelné místa lokací pro aktualizace,
- centrální sken, komunikační přenos,
- možnosti detailního nastavení chování klienta na koncovém bodu (silent mode, power user, nastavení hesla pro odinstalaci),
- detailní nastavení pravidel pro firewall včetně nastavení chování dle aktuálně připojené sítě,
- import/export politik,
- Advanced Threat Control (ATC),

- Intrusion detection systém (IDS)sleduje datové toky, hledá v nich pokusy o útok a ty poté zastavuje tak, aby nedošlo k přerušení jiné komunikace. Systém využívá vlastní pravidelně aktualizovanou databázi a umožňuje customizace nastavení, případně výběr použití pouze konkrétních pravidel.
- možnost detailního nastavení přístupových práv uživatelů,
- skenování externích zařízení,
- možnosti vytváření upravitelných instalačních balíčků
- silent instalace – produkt umožňuje tzv. bezodpovědní instalace
- plná podpora vzdálených instalací, která probíhá přes Windows Management Instrumentation, což je součástí všech operačních systémů Windows.
- možnosti upravení již nainstalovaných instalačních balíčků,
- možnost nastavení prověřovaných přípon souborů pro veškeré antimalware procesy,
- možnost nastavení výjimek pro veškeré antimalware procesy,
- aplikační kontrola a povolení nebo blokování aplikací s využitím největší, interní, pravidelně aktualizované databáze aplikací s možností přidávat své vlastní a to manuálně (procházením disku) nebo automaticky s využitím klientské. Kontrola aplikací probíhá zpravidla na základě kontrolního součtu, jména aplikace, cesty na datovém médiu, vnitřní databáze, různých kombinací a dalších v závislosti na konfiguraci.
- kontrola webového přístupu,
- ochrana dat před opuštěním organizace,
- kontrola zařízení (USB, DVD, Bluetooth, Wi-fi…) včetně whitelistu a blacklistu,
- antiphishing engine,
- antispam engine,
- antiransomware engine
- anti-malware engine
- na základě signatur (znalostní databáze) a detekce podezřelého chování (heuristika),
- zero-day attack – ochrana proti útokům a škodlivým kódům, které ještě nejsou známé.

Obrázek 10. Popis architektury BDGZ a BEST klienta



Funkční popis všech základních komponent nabízeného řešení

Bitdefender GravityZone Enterprise a výše (včetně verzí ELITE a ULTRA)

Ochrana pracovních stanic

- Produkt kompletně v českém a anglickém jazyce – klient pro koncové stanice, konzole pro centrální správu, instalační a administrační příručky.
- Instalace a zaškolení administrátorů v ceně implementace.
- Centrální správa a distribuce virových definic.
- Rezidentní ochrana před škodlivými kódy (viry, červi, trojské koně, spyware, adware, phishing, rootkit, ransomware, keyloggery, PUA, ochrana boot sektoru).
- Všechny vrstvy ochrany EPP řízeny, nastavovány, instalovány a rekonfigurovány z jedné centrální správcovské konzole.
- Ochrana proti bezsouborovým útokům.
- Ochrana proti síťovým útokům – brute-force útoky
- Ochrana proti crimeware (botnety, apod.)
- Ochrana proti laterálnímu pohybu malwaru
- Blokování skenování portů
- Možnost rozšíření o další ochrannou vrstvu proti neznámým pokročilým hrozbám a cíleným útokům aplikující pokročilou heuristiku pro odhalování hackovacích nástrojů, exploitů, polymorfního malware, ransomware a techniky skrývání využívané malwarem. Takové rozšíření musí využívat lokální modely strojového učení, tzn. funguje i offline na stanici bez přístupu k síti a nesmí používat méně než 70 000

strojově naučených modelů včetně Perceptronů, Binárních rozhodovacích stromů, Omezených Boltzmannových stroje, Genetických algoritmů, Podpůrných vektorových strojů a Umělých neurálních sítí.

- Možnost rozšíření ochrany o tzn. **Sandboxing**:
- Automatizované prověřování podezřelých souborů v Sandboxu, možnost nechat podezřelou aktivitu probíhat dál, nebo ji pozastavit, dokud nebude výsledek ze Sandboxu k dispozici.
- Možnost nastavit, jaká je maximální doba běhu Sandbox analýzy a kolikrát bude analýza opakována.
- Možnost vypnout či zapnout připojení k internetu při prověřování v Sandboxu.
- Ochrana OS a vybraných aplikací proti zneužití jejich zranitelností klasickými útočnými technikami (např. emulace ROP, Anti-Detour, apod.) i v případě využívání těchto technik neznámými hrozbami.
- Možnost rozšíření o ochranu MS Exchange na úrovni transportu i mailboxů či ochrany transportu pošty pomocí SMTP relay.
- Nastavení produktu v návaznosti na umístění stanice v Active Directory.
- Ochrana elektronické pošty na úrovni protokolů (POP3, SMTP) s možností tyto funkcionality vypnout.
- Kontrola webového provozu včetně SSL.
- Kontrola komprimovaných souborů.
- Kontrola chování aplikací.
- Možnost uchovávat karanténu v centrální lokalitě v SMB/CIFS sdílené složce místo uchovávání karantény na každém jednotlivém PC. Taková karanténa musí být zašifrována a heslo změnitelné pouze z centrální správcovské konzole.
- Automatické aktualizace (v závislosti na síťovém prostředí se aktualizace stahují buď z centrálního uložiště, nebo přímo z Internetu) programu na koncových stanicích i bezpečnostního obsahu nejméně 1x za hodinu
- Ochrana před známými síťovými hrozbami.
- Ochrana před neznámými hrozbami (zero hour / zero day).
- Zaměstnanecká kontrola aplikací - Nástroj pro správu aplikací a seznam povolených položek usnadňují zavedení zásad „implicitně zakázat“, která blokuje všechny aplikace, jež nejsou na seznamu povolených.
- Application control – možnost definovat uživatelům povolené/zakázané aplikace.
- Application control – možnost běhu v „testovacím režimu“ – tzn. možnost ověření funkcionality aniž by docházelo k blokování za účelem odladění pravidel, aby při nasazení nedošlo k okamžitému narušení pracovního procesu uživatelů.
- Web control – možnost definovat uživatelům povolené/zakázané webové stránky a časové okno, ve kterém mohou uživatelé na web přistupovat
- Možnost rozšíření o Patch management – možnost instalovat aktualizace aplikací třetích stran z prostředí centrální správy
- Šifrování pevných disků spravované z centrální konzole – možnost vynutit šifrování disků a možnost kdykoli získat klíč k obnovení takto šifrovaných koncových bodů přímo v rozhraní centrální konzole.
- Blokování neautorizovaných médií a zařízení (Device Control) - Nástroj pro správu zařízení a přístupu jednotlivých zařízení do podnikové sítě IT. Možnost nastavení pravidel dle Device ID tzn. jedno konkrétní zařízení (např. jeden konkrétní flashdisk výrobce XYZ model ABC ver.MNO se sériovým číslem 123456789) a dle Product ID tzn. všechna zařízení jednoho totožného modelu (např. všechny flashdisky výrobce XYZ modelu ABC ver.MNO).

- Detekování hrozeb na základě chování systému.
- Centrální správa (správa všech bezpečnostních řešení z jednoho místa v jedné konzoli).
- Centrální správa jako webová konzole. Instalace na více koncových bodů současně.
- Vzdálená aktivace/deaktivace a vzdálená instalace/odinstalace jakéhokoli (klidně všech) modulů na kterékoli chráněné stanici přímo z centrální konzole bez přerušení ochrany na dané stanici.
- Přednastavené role pro přístup do vzdálené správy.
- Funkce blokování sdílení internetového připojení.
- Funkce monitorování Wi-Fi připojení – logování a hlídání, zda jsou využívané Wi-Fi sítě dostatečně zabezpečeny
- Možnost rozšíření o Endpoint Sensor (EDR)Modul EDR je součástí klientského programu EPP a je možné ho kdykoli zapnout či vypnout bez nutnosti odinstalace řešení či přerušení ochrany koncové stanice přímo z centrální konzole.
- Plně integrovaný do konzole pro centrální správu – tzn. kompletní funkcionalita řízena a kontrolována z centrální konzole včetně prohlížení incidentů, vzdáleného připojení na koncovou stanici či izolování koncového bodu od sítě (komunikace zachována pouze s centrální konzolí)
- Automatické vkládání podezřelých souborů a souborů označených za malware v rámci Incidentu do Sandboxu. Možnost vybrané soubory v rámci incidentu jedním kliknutím odeslat do Sandboxu
- Možnost izolovat koncovou stanici od sítě – bude komunikovat pouze s centrální správou
- Automatické reakce na incidenty a výpis provedených automatizovaných akcí
- Doporučené manuální kroky pro administrátory
- Skener IoC
- Nástroje reakcí na incidenty
- Možnost dalšího rychlého prošetřování incidentů (vyhledání ve VirusTotal či Google) na jedno kliknutí

Ochrana souborových serverů

- Rezidentní ochrana před škodlivými kódy (viry, červi, trojské koně, spyware, adware, phishing, rootkit, ransomware, keyloggery, PUA, ochrana boot sektoru).
- Ochrana proti bezsouborovým útokům.
- Ochrana proti síťovým útokům – brute-force útoky, botnety, apod.
- Ochrana proti laterálnímu pohybu Malwaru. Blokování skenování portů
- Ochrana OS a vybraných aplikací proti zneužití jejich zranitelností klasickými útočnými technikami (např. emulace ROP, Anti-Detour, apod.) i v případě využívání těchto technik neznámými hrozbami.
- Ochrana proti ransomware
- Ochrana před neznámými hrozbami za pomoci agentů využívajících lokální a cloudové strojové učení.
- Detekce chování aplikací
- Application control – spouštění pouze schválených procesů

- Bezagentová ochrana serverů - EPP klient nainstalován na serveru, avšak bez skenovacích enginů – klient slouží pouze pro náhled do systému/provozu koncové stanice a veškeré testování/skenování je zajištěno speciálním virtuálním zařízením určeným pro testování/skenování.
- Centralizované a deduplikované skenování – soubor, který byl právě prověřen na PC1, nebude prověřován znovu na PC2 apod.

Vzdálená správa

- Centrální správa (správa všech bezpečnostních řešení z jednoho místa). Instalace na více koncových bodů současně.
- Vzdálená aktivace/deaktivace a vzdálená instalace/odinstalace jakéhokoli (klidně všech) modulů na kterékoli chráněné stanici přímo z centrální konzole bez přerušení ochrany na dané stanici.
- Přednastavené role pro přístup do vzdálené správy. Možnost přiřazení administračních rolí v centrální konzoli doménovým uživatelům či doménovým skupinám a tudíž umožnění přihlášení do centrální konzole uživatelům, kteří mají práva buď přiřazeny přímo, nebo je má přiřazena bezpečnostní skupina v AD, jíž je uživatel členem. Podpora VDI – virtualizace stanic a aplikací
- Správa všech komponent (PC, server, mobilní zařízení, patch management, šifrování) z jedné konzole

Správa systému:

- Granulární nastavení úrovní ochrany a veškerého nastavení klientů dle organizačních složek či přímo pro jednotlivé koncové stanice.
- Plná integrace s Active Directory – synchronizace organizačních jednotek a objektů z AD, možnost přiřazení pravidel ochrany na jakoukoli organizační jednotku či objekt typu Computer z AD. Možnost automatizace přidělování pravidel dle sítě, ve které se PC nachází, či právě přihlášeného uživatele (možnost nastavit dle uživatelů a skupin v synchronizované AD)
- Plná integrace s VMware vSphere vCenter – tzn. možnost synchronizovat inventář vCenter s centrální konzolí a možnost granulárního nastavení pravidel na jednotlivé prvky v inventáři v Center (tzn. na node, na hostitele, či přímo na jednotlivá VM)
- Možnost rozšíření o Patch management
- Správa licencí, možnost automatizace uvolňování využitých licencí s možností automatického odmazávání neaktivních PC z inventáře.
- Instalace aktualizací klientů odděleně do testovacího prostředí a produkčního prostředí
- Automatizovaná instalace ochrany přímo ze správcovské konzole na jeden či více PC najednou
- Možnost vytvoření pravidel pro dynamické přidělování pravidel na základě
- Cílové požadavky a obecné funkčnosti řešení:
- Systém umožňuje pravidelné i mimořádné aktualizace všech komponent.
- Řešení nabízí plně konfigurovatelný systém pro tvorbu systémových pravidel pro komunikace a komunikační protokoly.
- Dostupnost všech deklarovaných funkcí. Software, včetně centrální konzoly, umožňuje základní monitoring a automatické zasílaní alertů pomocí emailu/http/s, SNMP

Síťová stabilita

- Stažení virových definic pouze jednou do lokálního mirror serveru.
- Možné využití koncových bodů pro ukládání a distribuci virových definic a aktualizací produktu, instalační balíčky, skupinové úkoly a nastavení produktu.
- Podpora protokolu HTTPS.
- Možnost rozšíření o ochranu síťových úložišť typu NAS či jiných zařízení podporujících protokol ICAP.

Ochrana mobilních zařízení (iOS, Android, Windows Phone)

- Ochrana všech aplikací a souborů v telefonu
- Skenování úložiště při jeho napojení
- Možnost vynucení nastavení hesla pro odemknutí telefonu a délky jeho platnosti.
- Možnost vynutit komplexitu hesla - minimální délku, minimální počet speciálních znaků, nemožnost zadat stejné heslo jako X předchozích
- Možnost vynutit akci po X neúspěšných pokusech pro odemknutí
- Vynucení délky prodlení automatického zámku
- Možnost vynucení šifrování (pokud to zařízení podporuje)
- Blokace USB debug módu Webová bezpečnost – blokování phishingových či jinak podvodných stránek a stránek obsahujících malware
- Možnost nastavení výchozí akce pro zařízení, která nesplňují vyžadovaná kritéria
- Možnost vložit profily pro Wi-Fi sítě
- Možnost vložit profily VPN pro iOS zařízení
- Možnost omezení přístupu k webovému obsahu
- Správa plně integrována v jedné, stejné konzoli, jako ochrana EPP
- Možnost léčení dat uložených v interní paměti a na paměťové kartě
- Možnost vzdáleného zamknutí ztraceného či ukradeného zařízení přímo z konzole.
- Možnost vzdáleného mazání všech dat přímo z konzole
- Možnost vzdálené lokalizace telefonu ze správcovské konzole pomocí souřadnic GPS
- Možnost kontroly telefonu i po vložení cizí SIM karty
- Záruka a podpora: Podpora výrobce v České republice
- Komunikace v českém jazyce
- Možnost stahovat nové softwarové verze

Bitdefender GravityZone podporované platformy

Operační systémy

Windows: 10, 8.1, 8, 7
Windows Server:
Windows Server 2019 Core, Windows Server 2019, Windows Server 2016, Windows Server 2016 Core, Windows Server 2012 R2, Windows Server 2012, Windows Small Business Server (SBS) 2011, Windows Server 2008 R2

Windows Tablet and Embedded: Windows 10 IoT Enterprise, Windows Embedded 8.1 Industry, Windows Embedded 8 Standard, Windows Embedded Standard 7, Windows Embedded Compact 7, Windows Embedded POSReady 7, Windows Embedded Enterprise 7

Linux: Ubuntu 14.04 LTS or higher, Red Hat Enterprise Linux / CentOS 6.0 or higher, SUSE Linux Enterprise Server 11 SP4 or higher, OpenSUSE Leap 42.x, Fedora 25 or higher, Debian 8.0 or higher, Oracle Linux 6.3 or higher, Amazon Linux AMI 2016.09 or higher, Amazon Linux 2

macOS: macOS Big Sur (11.0), macOS Catalina (10.15), macOS Mojave (10.14), macOS High Sierra (10.13), macOS Sierra (10.12), OS X El Capitan (10.11)

Mobile: iOS 8.1+, Google Android 4.2+

Hypervizory

VMware vSphere & vCenter Server: 7.0, 6.7U3, 6.7U2a, 6.7U1, 6.7, 6.5, 6.0, 5.5, 5.1, 5.0

VMware Horizon/View: 7.8, 7.7, 7.6, 7.5, 7.1, 6.x, 5.x

VMware Workstation 11.x, 10.x, 9.x, 8.0.6

VMware Player 7.x, 6.x, 5.x

Citrix XenApp & XenDesktop: 7.18, 7.17, 7.16, 7.15 LTSR, 7.6 LTSR

Citrix XenServer: 8.x, 7.x, 6.5, 6.2, 6.5, 5.6, 5.5 (včetně Citrix Xen Hypervisor)
Citrix Virtual Apps & Desktops: 7 1906, 7 1903, 7 1811, 7 1808

Citrix VDI-in-a-Box 5.x

Microsoft Hyper-V: 2012 R2, 2012, 2008 R2

Red Hat Enterprise: 3.0

Red Hat KVM Hypervisor

Oracle VM: 3.0

Oracle VM VirtualBox: 5.2, 5.1

Nutanix Prism with AOS: 5.15, 5.11, 5.10, 5.6, 5.5

Nutanix Prism with AHV: 20170830.395, 20170830.301, 20170830.115

Nutanix Prism: 2018.01.31

Ochrana Microsoft Exchange

GravityZone Security for Exchange nabízí prvotřídní antispam a antimalware pro poštovní server. Zajišťuje bezpečné zpracování zpráv a prostředí pro práci s minimální spotřebou zdrojů. Bitdefender kombinuje všechny potřeby bezpečnostní politiky organizace do jediné platformy, která převezme bezpečnostní úkoly ze serverů a koncových bodů do dedikované GravityZone Virtuální Appliance. GravityZone pomáhá organizacím snižovat

celkové náklady na zabezpečení jejich infrastruktury prostřednictvím jedné optimalizované aplikace s jednoduchou správou a snadným nasazením pro prosazování bezpečnostních politik na poštovních serverech Exchange, virtuálních i fyzických koncových bodů a mobilních zařízeních.

Advanced Pattern Matching (APM) – vysoce účinný heuristický antispamový filtr detekuje neznámé spamy. Strojová neuronová síť s APM filtrem je na velké objemy nevyžádané pošty připravována v Bitdefender labu. Během výcviku se naučí rozlišovat mezi spamem a legitimními e-maily a rozpoznat nové spamové aktivity tím, že srovnává podobnosti s již doručenými zprávami. Tento proces zaručuje vysokou účinnost.

Real Time Data Analysis (RTDA) – filtr využívá Globální síť ochrany pro okamžitou detekci spamu a zaručuje pokročilou ochranu proti hrozbám nultého dne.

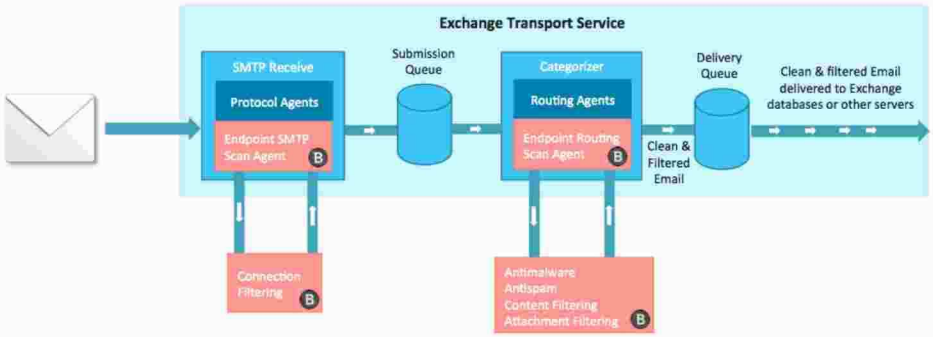
Hlavní výhody

- Nejlepší antispamová ochrana pro mailservery: Golden SPAM+ Virus Bulletin
- Rychlá a jednoduchá instalace
- Antimalware, antivirus, anti-phishing a antispam ochrana v reálném čase
- Bezpečně chrání prostředí Microsoft Exchange proti interním i externím hrozbám

Klíčové výhody

- Několika vrstvá ochrana pro mailservery s behaviorální analýzou a ochranou před zero-day hrozbami
- Filtrování emailové komunikace včetně příloh a kontroly obsahu
- Nastavení prověřovaných přípon souborů pro veškeré antimalware procesy
- Integrace s více AD, Vmware vCenter, Citrix XenServer umožňuje vzdálenou správu
- Bezpečnostní virtuální appliance centralizují a deduplikují antimalwarové procesy
- Řešení umožňuje jak plánované skeny, tak i skeny na vyžádání

- **Ochrana pro Mail Servery**
  Microsoft Exchange 2016, 2013, 2010, 2007
- Pro fyzické i virtuální servery
- Podporované protokoly: SMTP, MAPI, Exchange ActiveSync
- Podporované Role: Edge Transport, Hub Transport a Mailbox (viz obr. 6)



GravityZone Security for Containers

Ochrana, detekce a reakce na kontejnerovou a cloudovou zátěž Bitdefender GravityZone Security for Containers je vysoce výkonné bezpečnostní řešení pro kontejnery a Linux, které je nezávislé na platformě a kombinuje serverovou rozšířenou EDR s pokročilou detekcí exploitů pro Linux, a forenzní analýzou útoků.

Na rozdíl od jiných řešení obsahuje komplexní zásobník vrstev nezávislých na jádře, vytvořený pro Linux a kontejnery, a umožňuje organizacím rozšířit automatizaci a viditelnost napříč cloudovými pracovními úlohami, virtuálními počítači, kontejnery, soukromými a veřejnými cloudy a fyzickými koncovými body.

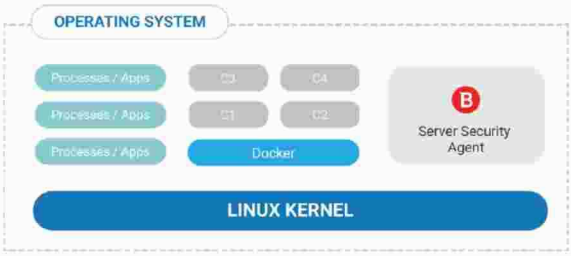
1. **Čím se Bitdefender odlišuje od ostatních řešení?**
   - Komplexní bezpečnostní balíček vytvořený pro kontejnery a Linux–Zatímco jiné produkty se omezují na skenování známých zranitelností nebo hrozeb a soustředí se na systém Windows a koncového uživatele, Bitdefender používá bezpečnostní zásobník vytvořený k ochraně kontejnerů a hostitelů Linuxu za běhu. Identifikuje 0-dny anomálie a TTP pro Linux, stejně jako kontejnery, které byly cílem útoku, a umožňuje rychlé vyšetřování a reakci.
   - Konsolidovaná viditelnost a ochrana napříč infrastrukturami – Vyhněte se přidávání nových bodových řešení a konsolidujte zabezpečení pomocí bezpečnostní platformy Bitdefender GravityZone pro cloudové pracovní zátěže. Zajišťuje široký přehled o hrozbách a ochranu, která pokrývá kontejnery v infrastrukturách IaaS a PaaS, virtuální počítače, cloudové pracovní zátěže, koncové uživatele a servery, Linux a Windows, soukromé a veřejné cloudy.
   - Rozsáhlá automatizace zabezpečení a kompatibilita – Zachovejte agilitu DevOps a provozní efektivitu díky vysoce výkonnému agentovi, automatizovanému nasazení, škálování zabezpečení a zabezpečení Linuxu nezávislému na jádře, které umožňuje upgrade na nové distribuce bez ztráty zabezpečení nebo vzniku problémů.

2. **KLÍČOVÉ SCHOPNOSTI**
   - EDR vytvořená pro Linux a kontejnerové pracovní zátěže, která identifikuje podezřelé chování v reálném čase, umožňuje audit bezpečnostních událostí, forenzní analýzu útoků a rychlou reakci.
   - Linux Advanced Anti-Exploit blokuje útoky na jádro Linuxu, aplikace zero-day a známé exploity
   - Platformově orientovaný, vysoce výkonný bezpečnostní agent zajišťuje minimální dopad na zdroje, zjednodušuje provoz a zvyšuje návratnost investic do cloudu.

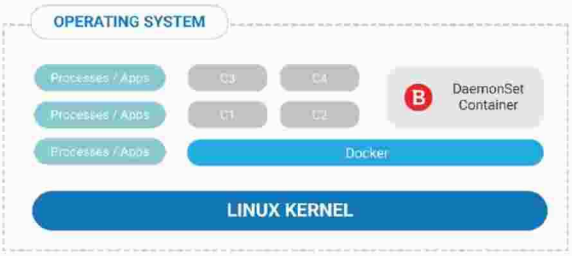
- TTP útočníků mapované na MITRE pro Linux se zaměřují na hrozby specifické pro Linux a zobrazují kontextově bohaté informace.
- Prokázané mistrovství v detekci – Bitdefender dosáhl nejvyššího celkového počtu detekcí a 100% detekce útočných technik pro Linux v hodnoceních MITRE 2021.
- Hlášení incidentů a forenzní analýza s ohledem na kontejnery umožňuje bezpečnostním analytikům s jistotou zahájit vyšetřování a včas zaměřit pátrání.
- Jednotná platforma GravityZone pro CWS zajišťuje konsolidovaný přehled a kontrolu zabezpečení napříč všemi pracovními úlohami, kontejnery, operačními systémy a cloudy.
- Podpora nasazení kontejnerů IaaS i PaaS s modely nasazení hostitelského agenta a sady Daemonset.
- Komplexní bezpečnostní balíček, který zahrnuje správu rizik, antimalware, vyladěnou prevenci pomocí strojového učení, pokročilý Anti-Exploit a rozšířenou EDR.

3. Podpora platformy

- Distribuce Enterprise Linux: Ubuntu 16.04 LTS nebo vyšší, Red Hat Enterprise Linux 7 nebo vyšší, Oracle Linux 7 nebo vyšší, CentOS 7 nebo vyšší, SUSE Linux Enterprise Server 12 SP4 nebo vyšší, openSUSE Leap 15.2, Debian 9 nebo vyšší, Amazon Linux 2.
- Kontejnerové infrastruktury: Amazon ECS, Amazon EKS, Google GKE, Docker, Podman, Kubernetes, Azure AKS



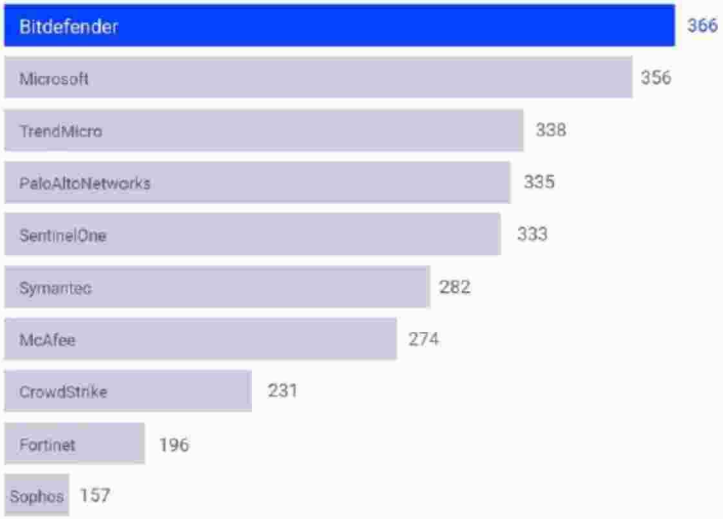
Server Agent - IaaS



DaemonSet - PaaS, cloud-native

4. MITRE 2021 ATT&CK

Nejvyšší celkový počet detekcí a 100% detekce útočných technik pro Linux



Ověřování bitových kopií před spuštěním, nezměnitelné infrastruktury a skenování zranitelností jsou nezbytné, ale nesnižují rizika spuštění způsobená hrozbami ZERO-day, únikem z kontejneru, útoky zevnitř a dalšími útoky. Využíváme odborné znalosti v oblasti vysoce rizikových procesů zabezpečení linuxových serverů prostřednictvím dynamické analýzy běhu a desítek vlastních algoritmů strojového učení, které pohánějí bezkonkurenční pokročilé schopnosti detekce hrozeb, jež kombinujeme s oceňovanými, komplexními ověřenými technologiemi prevence a detekce, abychom účinně zmařili škodlivé aktivity na linuxových serverech a kontejnerových pracovních zátěžích.

Kvalita produktu a významná ocenění

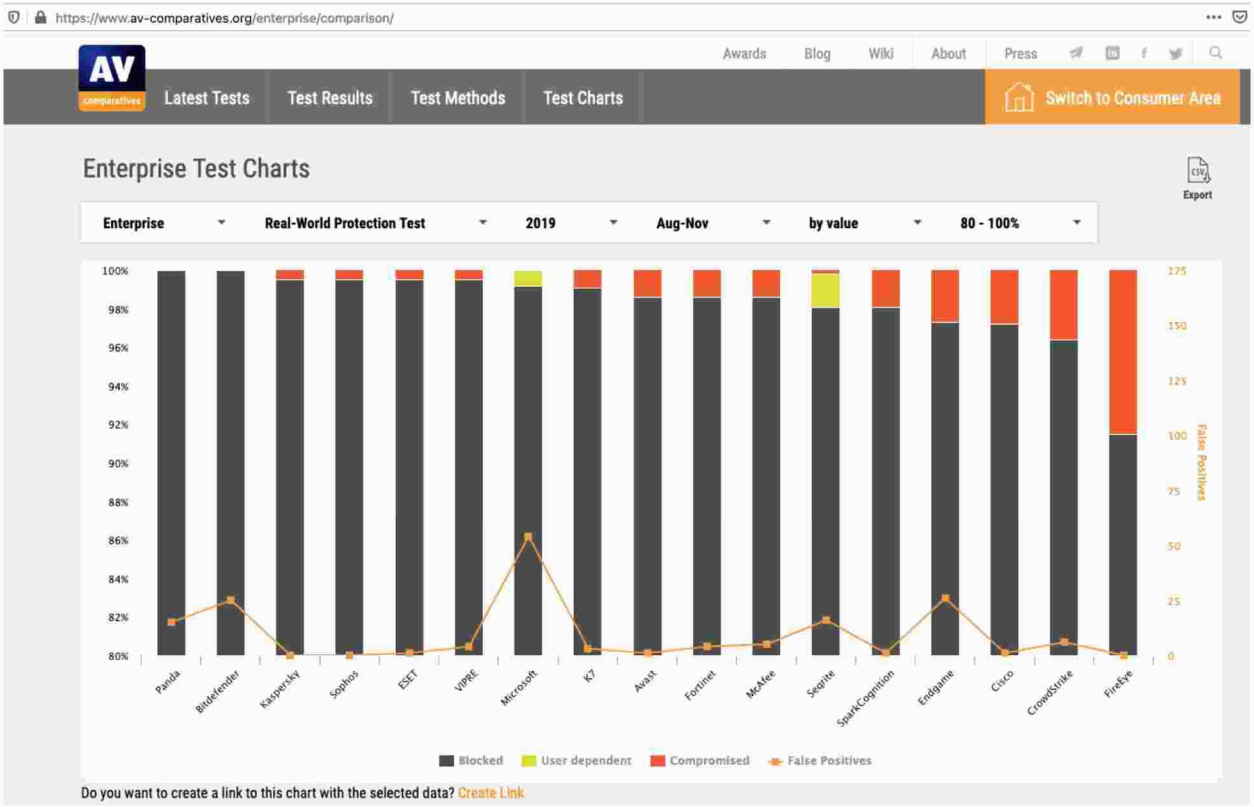
Enhanced Real-World Test 2020 – Enterprise

Advanced Threat Protection – Targeted Attacks, Exploits and Fileless Threats

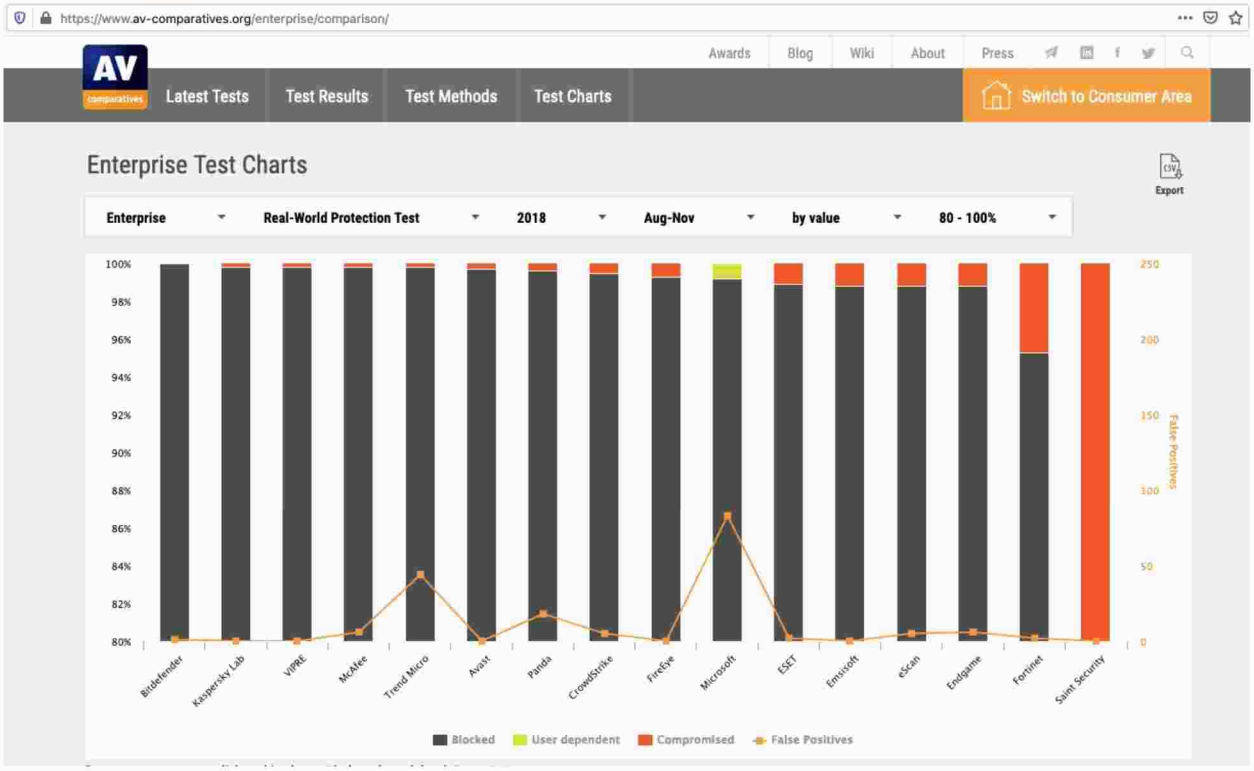
	Test scenarios																
	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	FPs	Score
Avast	◆	✓	✓	✓	✓	◆	✓	✗	✗	✓	✗	✓	✗	✓	✓	N	11
Bitdefender	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	N	15
CrowdStrike	✓	✓	✓	✓	✓	✓	✓	✓	✓	✗	✗	✗	✗	✓	✓	N	11
ESET	✓	◆	✓	✓	✓	✓	✓	✓	✓	✗	✓	✓	✓	✓	✓	N	14
Fortinet	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	Y	N/A
Kaspersky	✓	✓	✓	✓	✓	✗	✓	✓	✓	✓	✓	✓	✓	✓	✓	N	14
SparkCognition	✗	✓	✓	✓	✗	✗	✗	✗	✗	✓	✗	✓	✗	✗	✗	N	5
Vipre	✓	✓	✓	✗	✓	✓	✓	✓	✓	✗	✓	✓	✗	✓	✓	N	12

Link na test zde

Link na testy 2019



Link na testy 2018



Bitdefender získává za posledních 7 let za sebou od nezávislých testovacích organizací ve všech produktových řadách významná ocenění. Přečtěte si více na stránkách uvedených níže.

Product of the Year 2019

AV-Comparatives' 2019 Product of the Year award goes to:

AV-Test Org best protection and best Overall Performance Awards

	Malware Protection March 2019	Performance April 2019	Real-World Protection February-May 2019	Enhanced Real-World August-November	Malware Protection September 2019	Performance October 2019	Real-World Protection August-October 2019
Bitdefender	***	***	***	***	***	***	***
Kaspersky	**	***	***	***	**	***	**
Avast	**	***	**	***	***	***	**
AVG	**	***	**	***	***	***	**
Avira	***	**	***		***	***	***
VIPRE	***	***	***		*	***	***
ESET	**	***	*	***	**	***	*
Norton	**	***	**		***	**	***
Tencent	**	***	***		**	***	**
F-Secure	*	**	**	***	**	***	*
Panda	*	***	**		**	***	**
K7	**	***	*		**	***	**
Total Defense	***	***	*		*	**	***
McAfee	**	***	*		*	***	**
Microsoft	***	*	**		**	**	**
					**	**	**

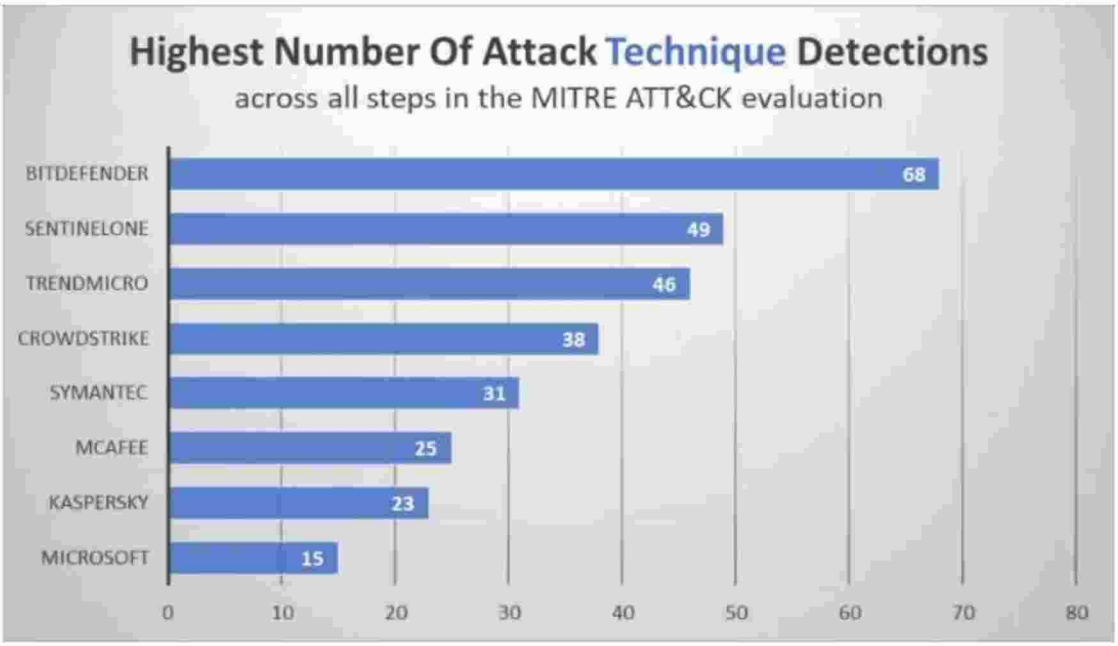
Bitdefender

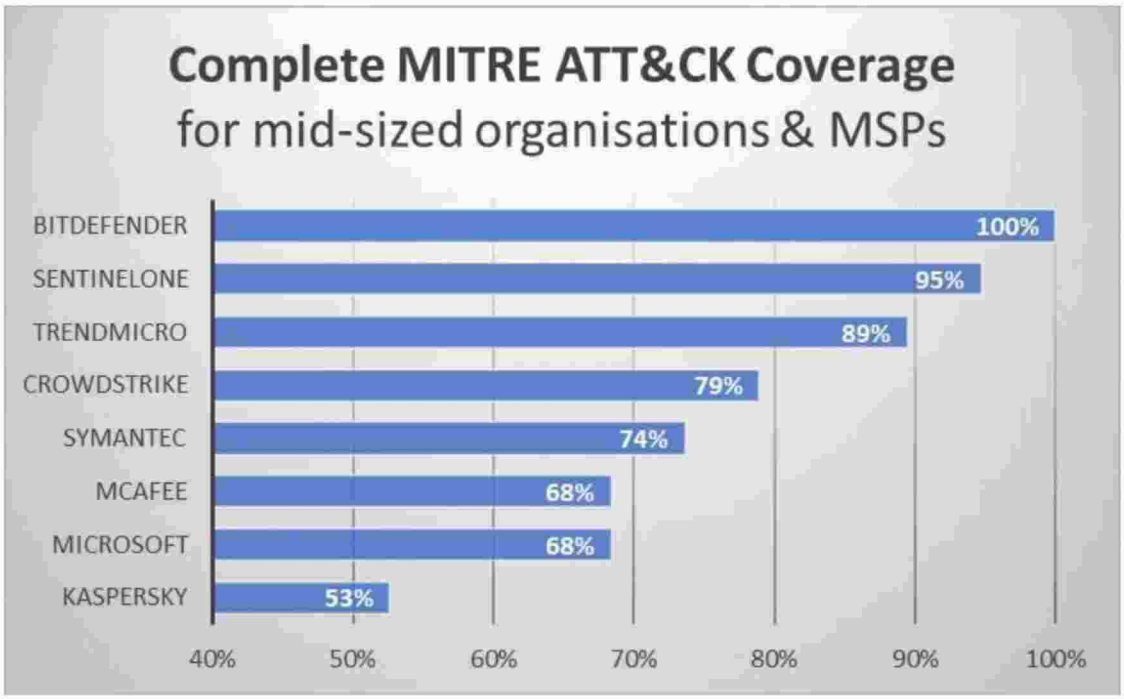
AV-TEST av-test.org 2019 AWARD BEST PROTECTION Bitdefender Endpoint Security (Ultra)

AV comparatives Product of the Year 2019

2020 MITRE ATT&CK. APT29 Evaluation

Bitdefender vyhrál EDR test APT29 u renomované organizaci





VSI Login

VSI Login testy pro virtualizační platformy potvrzují, že Bitdefender GravityZone má nejmenší nároky na provoz a umožňuje nejvyšší hustotu virtualizace na stejném hardware oproti konkurenčním řešením. To vše je možné díky patentovaným technologiím jako jsou central scan s deduplikací a dedikovaným Security Serverům vyvinutým pro virtualizační prostředí.

Figure 2: Baseline – the response time (ms) of an unstressed system

Figure 2 outlines test results of the Baseline measurement. Bitdefender achieves the lowest Baseline response time, which results in better user experience and desktop workload performance when the environment is not stressed.

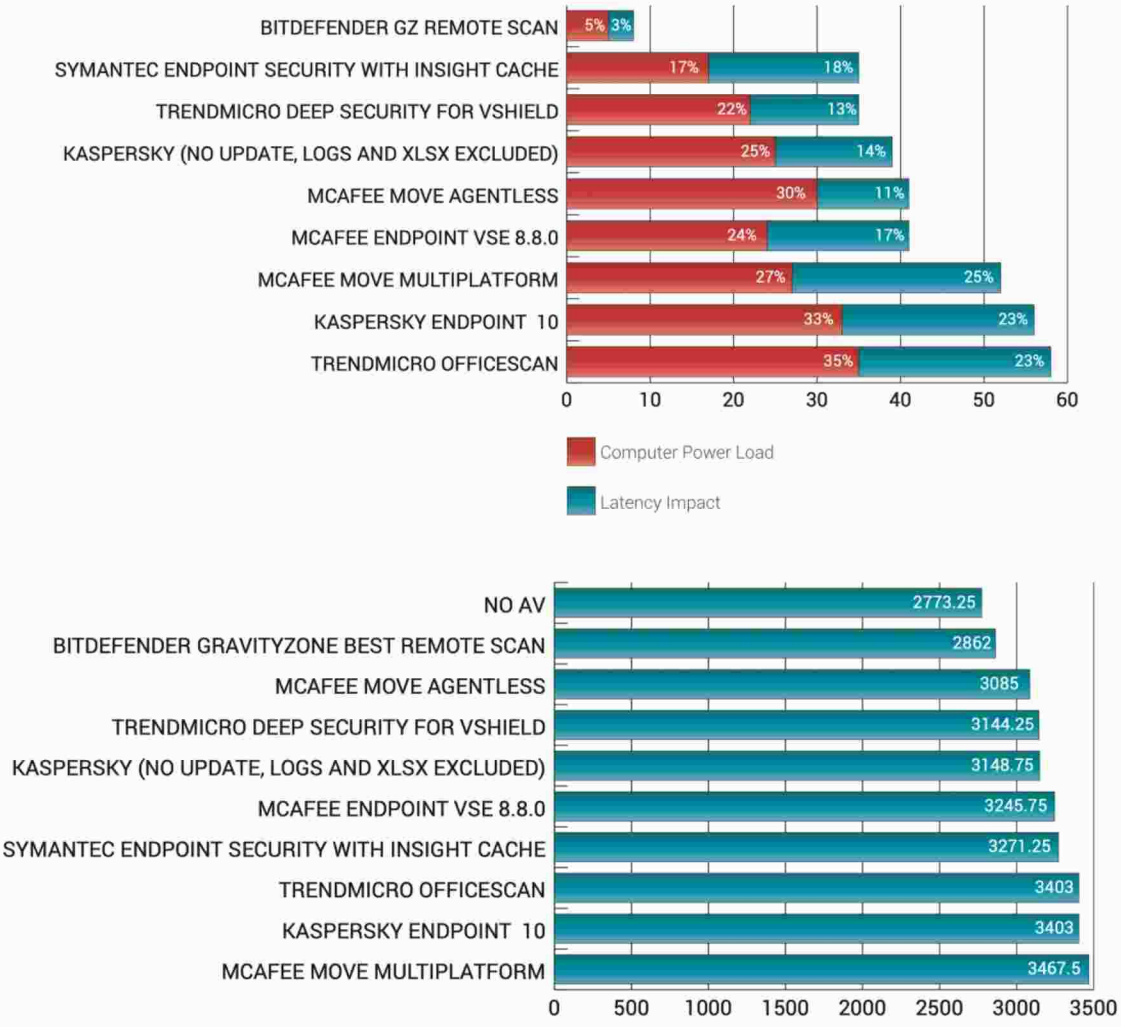


Figure 2: Baseline – the response time (ms) of an unstressed system

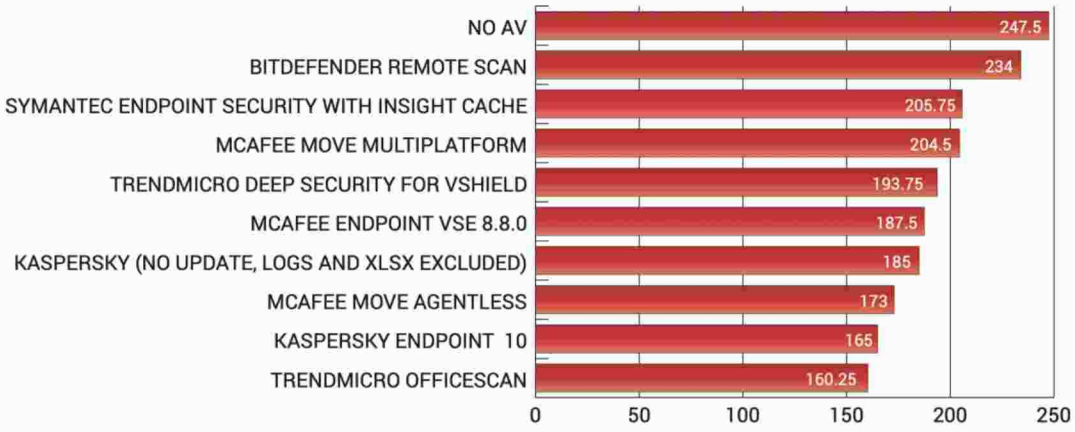


Figure 1: VSImax – the maximum attainable number of VDI sessions

Příloha č. 2 – Položkový rozpočet

Bezpečnostní řešení BITDEFENDER

Licence

Pořadí	Množství	m.j.	P/N	Popis zboží	Cena za 1Ks bez DPH [CZK]	Cena celkem bez DPH [CZK]	Cena celkem s DPH [CZK]
1	230	ks	Bundle	Bitdefender GravityZone Ultra - GOV 36 měsíců	1652	379 960,00	459 751,60
				Celkem bez DPH		**379 960,00 Kč**	
				Celkem s DPH			**459 751,60 Kč**

Implementace

Pořadí	Množství	m.j.	P/N	Popis zboží	Cena za 1Ks bez DPH [CZK]	Cena celkem bez DPH [CZK]	Cena celkem s DPH [CZK]
2	1	Ks	BITDEF_INSTALL	Instalace nástroje a zaškolení administrátora	5040	5 040,00	6 098,40
				Celkem bez DPH		**5 040,00 Kč**	
				Celkem s DPH			**6 098,40 Kč**

Celkem

				Celkem bez DPH		**385 000,00 Kč**	
				Celkem s DPH			**465 850,00 Kč**