Smlouva o pořízení licencí na software pro zajištění antivirové ochrany

CYBOSEC s.r.o.
se sídlem: Hradčany 347, 503 53 Smidary
IČO: 04301226
DIČ: CZ04301226
zastoupená: [redacted]dnatelem společnosti
zapsána v obchodním rejstříku vedeném krajským soudem v Hradci Králové, pod spisovou značkou C 42008
bankovní spojení: [redacted]
č. účtu: [redacted]
kontaktní osoba: [redacted]

(dále jako „**poskytovatel**“)

a

Krajská zdravotní, a.s.
se sídlem: Sociální péče 3316/12A, Ústí nad Labem, PSČ 401 13
IČO: 25488627
DIČ: CZ25488627
zastoupená: [redacted]enerálním ředitelem
zapsána v obchodním rejstříku vedeném Krajským soudem v Ústí nad Labem, oddíl B, vložka 1550
bankovní spojení: [redacted]
[redacted]
[redacted]

(dále jako „**nabyvatel**“)

uzavřely níže uvedeného data tuto **smlouvu**

(dále jen „smlouva“).

Poskytovatel a nabyvatel jsou dále označeni rovněž jako „**smluvní strana**“ či společně jako „**smluvní strany**“.

Tato smlouva je uzavřena na základě veřejné zakázky s názvem **„Dodávka antivirového řešení pro Krajskou zdravotní, a.s. 2022 – část 1 - servery“** v souladu s ustanovením § 2079 zákona č. 89/2012 Sb., občanský zákoník (dále jen „**občanský zákoník nebo OZ**“)

Smluvní strany, vědomy si svých závazků v této smlouvě obsažených a s úmyslem být touto smlouvou vázány, dohodly se na následujícím znění smlouvy:

I. ÚVODNÍ USTANOVENÍ

1. Nabyvatel prohlašuje, že:
   - je právnickou osobou řádně založenou a existující podle českého právního řádu, a
   - splňuje veškeré podmínky a požadavky v této smlouvě stanovené a je oprávněn tuto smlouvu uzavřít a řádně plnit závazky v ní obsažené.

2. Poskytovatel prohlašuje, že:

   - je právnickou osobou řádně založenou a existující podle českého právního řádu (*případně upraví prodávající dle právní formy podnikání*), a
   - splňuje veškeré podmínky a požadavky v této smlouvě stanovené a je oprávněn tuto smlouvu uzavřít a řádně plnit závazky v ní obsažené.

II. PŘEDMĚT A ÚČEL SMLOUVY

1. Poskytovatel touto smlouvou poskytuje nabyvateli oprávnění k výkonu nevýhradního nepřenosného práva (dále jen „licence/podlicence“) užívat programové produkty pro komplexní ochranu serverů a pracovních stanic (dále jen „ochranný software“). Ochranný software a počty příslušných licencí jsou specifikovány v příloze č. 1 a 2 této smlouvy. Toto oprávnění je poskytováno za cenu stanovenou v čl. III. této smlouvy, v rozsahu a za podmínek dále v této smlouvě stanovených. Právem užívat ve smyslu této smlouvy se rozumí právo užívání počítačového programu v souladu s omezeními stanovenými zákonem a ustanoveními čl. V této smlouvy.
2. Nabyvatel bude oprávněn nejméně třikrát denně aktualizovat virové báze ochranného software (dále jen "update ochranného software") prostřednictvím internetu, a to po dobu stanovenou v čl. V., odst. 2 této smlouvy. Nabyvatel bude dále oprávněn získat speciální ovladače a další podpůrné informace tak, jak budou aktuálně k dispozici v závislosti na situaci ve virové problematice.
3. Nabyvatel bude oprávněn v rámci této smlouvy aktualizovat ochranný software (dále jen "upgrade ochranného software") v případě, že během doby uvedené v čl. V., odst. 3 této smlouvy bude distribuována nová verze ochranného software.
4. Poskytovatel se zavazuje po dobu platnosti této smlouvy poskytovat nabyvateli technickou podporu v českém jazyce v oblasti IT bezpečnosti prostřednictvím své hot-line na telefonním čísle [redacted] a prostřednictvím help desku e-mail: [redacted] a to v době od 8:00 do 17:00 hodin ve státem uznané pracovní dny.

   (celkově dále také „předmět plnění“)
5. Nabyvatel se zavazuje za plnění poskytovatele uvedené v této smlouvě uhradit poskytovateli celkovou cenu stanovenou v čl. III této smlouvy a dále se zavazuje vyvinout součinnost k převzetí ochranného software a dodržování všech podmínek licence stanovených zákonem, touto smlouvou a licenčním ujednáním výrobce ochranného software.
6. Kontaktní osoby – za poskytovatele:

   a) [redacted]

   b) -
7. Kontaktní osoby – za nabyvatele:

   a) [redacted]

   [redacted]

   Jakékoliv změny v osobách či adresách budou poskytovatelem nabyvateli oznámeny písemnou formou nejdéle do 5 (pěti) pracovních dnů.
8. Poskytovatel touto smlouvou garantuje nabyvateli splnění zadání Veřejné zakázky a všech z toho vyplývajících podmínek a povinností převzatých poskytovatelem v rámci zadávacího

řízení podle zadávací dokumentace Veřejné zakázky a nabídky poskytovatele. Tato garance je nadřazena ostatním podmínkám a garancím uvedeným v této smlouvě. Pro vyloučení jakýchkoli pochybností znamená, že:

- v případě jakékoliv nejistoty ohledně výkladu ustanovení této smlouvy budou tato ustanovení vykládána tak, aby v co nejširší míře zohledňoval účel Veřejné zakázky vyjádřený zadávací dokumentací Veřejné zakázky;
- v případě chybějících ustanovení této smlouvy budou použita dostatečně konkrétní ustanovení zadávací dokumentace Veřejné zakázky.

9. Poskytovatel se zavazuje, že po dobu platnosti této smlouvy garantuje nabyvateli ceny dle přílohy č. 1 této smlouvy, na dodání dalšího předmětu plnění na rámec této smlouvy, který by byl požadován nabyvatelem v souladu se zákonem č. 134/2016 Sb. o zadávání veřejných zakázek, ve znění pozdějších předpisů.

III. CENA, PLATEBNÍ PODMÍNKY

1. Celková cena za plnění předmětu plnění smlouvy byla stanovena dohodou smluvních stran ve výši 317 600,- Kč bez daně z přidané hodnoty (dále také „DPH“).
2. K celkové ceně podle odst. 1. tohoto článku bude připočtená DPH platná v den uskutečnění zdanitelného plnění a za její určení a vyčíslení v souladu s právními předpisy nese odpovědnost poskytovatel.
3. Celková cena určená postupem dle odst. 1. a 2. tohoto článku je cena konečná a nepřekročitelná a zahrnuje veškeré náklady spojené s realizací předmětu plnění Smlouvy, vč. všech licenčních poplatků, základní e-mailové a telefonické podpory výrobců a certifikovanou technickou podporu poskytovatele v rozsahu stanoveném touto Smlouvou.
4. Cena bude nabyvatelem uhrazena na základě daňového dokladu (faktury) vystaveného poskytovatelem. Daňový doklad (faktura) musí splňovat náležitosti daňového a účetního dokladu podle zákona č. 563/1991 Sb., o účetnictví, ve znění pozdějších předpisů, zákona č. 235/2004 Sb., o dani z přidané hodnoty, ve znění pozdějších předpisů a musí mít náležitosti obchodní listiny dle § 435 OZ. Nedílnou součástí daňového dokladu musí být nabyvatelem potvrzený předávací protokol.
5. Daňový doklad (faktura) musí za účelem možnosti prokázání legálního nabytí licencí na užívání software obsahovat minimálně katalogové číslo licence na užívání software (Product Number), přesné a úplné označení licence na užívání software (včetně licenční edice a verze), počet dodaných kusů licencí na užívání software a jejich cenu. Nesplnění této podmínky je důvodem k vrácení daňového dokladu (faktury) poskytovateli k přepracování. Lhůta splatnosti nového daňového dokladu (faktury) začíná běžet dnem prokazatelného převzetí nového daňového dokladu (faktury) nabyvatelem.
6. Splatnost každého daňového dokladu (faktury) vystaveného poskytovatelem je 60 dnů ode dne jeho doručení nabyvateli. Poskytovatel se zavazuje předat či odeslat daňový doklad (fakturu) nabyvateli nejpozději následující pracovní den po jeho vystavení na adresu uvedenou v záhlaví této smlouvy nebo elektronicky na email **uctarna@kzcr.eu**.
7. V případě, že daňový doklad výše uvedené náležitosti nebude splňovat nebo bude obsahovat nesprávné údaje, vrátí nabyvatel daňový doklad do dne splatnosti daňového dokladu k opravení bez jeho proplacení. Splatnost opraveného daňového dokladu je 60 dní ode dne jeho prokazatelného doručení nabyvateli na adresu nabyvatele uvedenou v záhlaví této Smlouvy nebo elektronicky na e-mail **uctarna@kzcr.eu**. Ke splatnosti nastalé na základě předchozího nabyvatelem vráceného daňového dokladu se nepřihlíží.

8. Platby dle smlouvy budou probíhat výhradně v korunách českých (Kč) a rovněž veškeré cenové údaje budou v této měně.

9. Smluvní strany považují za okamžik splnění peněžitých závazků vyplývajících z této smlouvy okamžik odeslání peněžité platby z bankovního účtu povinné smluvní strany na účet oprávněné smluvní strany uvedený v záhlaví této smlouvy.

IV. PŘEDÁNÍ A PŘEVZETÍ OCHRANNÉHO SOFTWARE

1. Místem plnění je sídlo nabyvatele uvedené v záhlaví této smlouvy. Osobou oprávněnou k převzetí plnění za nabyvatele je jedna z osob uvedených v čl. II., odst. 7 této smlouvy

2. Poskytovatel se zavazuje předat nabyvateli předmět plnění nejpozději do 60 dní ode dne účinnosti smlouvy.

3. Nabyvatel je oprávněn s takto předaným ochranným software nakládat v souladu s ustanoveními této smlouvy.

4. Odevzdání předmětu plnění a dodacích listů potvrdí jedna z oprávněných osob každé smluvní strany dle čl. II, odst. 6 a 7 této smlouvy na datovaném předávacím protokole, vyhotoveném poskytovatelem ve dvou kopiích. Každá smluvní strana si ponechá jednu kopii.

5. Poskytovatel je spolu s dodávkou licencí na užívání software povinen:

   a) doložit oficiální potvrzení výrobce nebo zastoupení výrobce v České republice o určení dodávaného předmětu plnění pro český trh a koncového zákazníka Krajská zdravotní a.s.

   b) dodat licenční ujednání, platná k datu dodání licencí na užívání software a všechny licenční materiály, které jsou součástí daných licencí na užívání software (např. licenční číslo, licenční klíč, licenční certifikát, licenční oprávnění, štítek prokazující pravost licence, instalační média, hardwarový klíč, dokumentace vztahující se k licenci, apod.). Nesplnění této podmínky bude v procesu akceptace předmětu plnění klasifikováno jako podstatná vada plnění (vada bránící následnému používání předmětu plnění)

   c) vystavit konečnou fakturu, která bude obsahovat všechny náležitosti, nezbytné k prokázání legálního nabytí licencí na užívání software, které jsou předmětem plnění. Minimálně musí pro každou licenci na užívání software obsahovat přesnou a úplnou specifikaci licence na užívání software (ve tvaru shodném s tím, jak licence na užívání software rozlišuje výrobce software – např. product number, výrobce software, název software, verze software, typ licence, jazyková mutace, bitová verze, časové omezení nebo další upřesňující údaje, jimiž výrobce software svoje licence rozlišuje), počet dodaných licencí (či vyjádření, že jde o licenci bez omezení počtu instalací nebo přístupů) a s výjimkou licencí typu OEM také jejich cenu. Nesplnění této podmínky bude důvodem k vrácení faktury poskytovateli k přepracování, přičemž lhůta splatnosti nové faktury začne běžet dnem prokazatelného převzetí nové faktury nabyvatelem.

6. Akceptace řešení - pokud se při akceptaci řešení ukáže, že řešení nevyhovuje kterémukoliv požadavku, specifikovanému v zadávací dokumentaci veřejné zakázky, je nabyvatel oprávněn odmítnout plnění převzít, přičemž poskytovatel vrátí veškeré již zaplacené úhrady, poskytovatel navíc zaplatí smluvní pokutu ve výši 500.000 Kč bez DPH.

V. PODMÍNKY LICENCE

1. Nabyvatel je oprávněn užívat každou licenci pouze pro vlastní potřebu, v souladu s jejím určením a za podmínek stanovených zákonem, touto smlouvou a za podmínek stanovených v licenčním ujednání výrobce.
2. Nabyvatel je oprávněn provádět update ochranného software ve smyslu čl. II., odst. 2 této smlouvy po dobu 36 měsíců ode dne podpisu předávacího protokolu dle čl. IV., odst. 4 této smlouvy.
3. Nabyvatel je oprávněn provádět upgrade ochranného software ve smyslu čl. II., odst. 3 této smlouvy po dobu 36 měsíců ode dne podpisu předávacího protokolu dle čl. IV., odst. 4 této smlouvy.
4. Nabyvatel není oprávněn bez předcházejícího písemného souhlasu poskytovatele jakýmkoliv způsobem postoupit, přenechat, zapůjčit, umožnit užívání, či jinak dočasně či trvale poskytnout oprávnění tvořící součást licencí nebo licence třetí osobě.
5. Licence udělené na základě této smlouvy, resp. práva a povinnosti přecházejí při zániku nabyvatele na jeho právního nástupce.

VI. ZÁRUKY A ODPOVĚDNOST ZA ŠKODU

1. Poskytovatel zaručuje nabyvateli vlastnosti ochranného software ve stejném rozsahu, v jakém jsou zaručeny držitelem autorských práv.
2. Poskytovatel je povinen zajistit, aby předmět plnění dle této smlouvy byl bez právních vad, zejména aby nebyl zatížen žádnými právy třetích osob, z nichž by pro nabyvatele vyplynul jakýkoliv finanční nebo jiný závazek ve prospěch třetí strany nebo která by jakkoliv omezovala užití předmětu plnění. V případě porušení tohoto závazku je poskytovatel v plném rozsahu odpovědný za případné následky takového porušení, přičemž právo nabyvatele na případnou náhradu škody a smluvní pokutu zůstává nedotčeno.
3. Poskytovatel prohlašuje, že nejpozději ke dni podpisu této smlouvy bude mít sjednáno pojištění odpovědnosti za škody způsobené jím a jeho případnými subdodavateli v souvislosti s výkonem jeho podnikatelské činnosti třetí osobě v minimální výši 20.000.000,- Kč. Poskytovatel je povinen udržovat pojištění v platnosti minimálně v rozsahu požadovaném touto smlouvou, po celou dobu účinnosti této smlouvy. Kopie pojistné smlouvy tvoří přílohu č. 4 této smlouvy. Pokud by v důsledku pojistného plnění nebo jiné události mělo dojít k zániku pojistného krytí, k omezení rozsahu pojištěných rizik, ke snížení stanovené minimální výše pojistného krytí v pojištění, nebo k jiným změnám, které by znamenaly zhoršení podmínek oproti původnímu stavu, je poskytovatel povinen učinit příslušná opatření tak, aby pojištění bylo udrženo tak, jak je požadováno v tomto ustanovení.

VII. SANKCE

1. V případě, že nabyvatel nedodrží sjednaný termín splatnosti daňového dokladu, je poskytovatel oprávněn požadovat z dlužné částky úrok z prodlení ve výši 0,005 % za každý den prodlení.
2. Nabyvatel má právo na smluvní pokutu ve výši 0,05 % z celkové ceny za každé porušení smlouvy, jakož i za každý i jen započatý den trvání tohoto porušení a za každý případ samostatně.
3. Klasifikace vad pro účely této smlouvy:

a) výpadek centrální správy či závažné nedostatky znemožňující použití centrální správy, vážné odchylky od schválené specifikace

b) chyba v důležité funkci aplikace (centrální správa, klient), která má vliv na funkčnosti provozu, centrální správa nebo klienti nefungují v souladu se schválenou specifikací

4. Poskytovatel je povinen zaplatit nabyvateli následující smluvní pokutu za dobu výpadku dle klasifikace vad uvedené v odst. 4 tohoto článku (výpadek se počítá od nahlášení incidentu)

   a) po dvou pracovních dnech za každý započatý den 1.000 Kč

   b) po pěti pracovních dnech za každý započatý den 2.000 Kč

5. V případě porušení povinnosti poskytovatele mít sjednáno platné pojištění v rozsahu a za podmínek sjednaných v čl. 6 odst. 3 této smlouvy vzniká nabyvateli nárok na zaplacení smluvní pokuty ve výši 1 000 Kč za každý, byť i započatý den prodlení s řádným splněním této povinnosti.

6. Veškeré smluvní pokuty dle smlouvy jsou splatné do 30 kalendářních dnů ode dne doručení výzvy k jejich zaplacení povinné smluvní straně. Smluvní pokuty je nabyvatel oprávněn započíst ve smyslu ust. § 1982 OZ proti i nesplatné pohledávce poskytovatele na úhradu ceny. Sjednáním smluvní pokuty podle tohoto článku není dotčeno právo nabyvatele na náhradu škody vzniklé z porušení povinností utvrzovaných smluvní pokutou, a to i ve výši přesahující sjednanou smluvní pokutu tzn., že smluvní strany se dohodly, že § 2050 OZ se nepoužije.

7. Pokud by poskytovatel jakoukoliv část plnění prováděl prostřednictvím subdodavatele, odpovídá poskytovatel za plnění a úkony subdodavatele stejným způsobem a ve stejném rozsahu, jakoby plnění poskytoval a úkony činil sám poskytovatel.

8. Zaplacením uvedených smluvních pokut není dotčeno právo nabyvatele na náhradu škody vzniklé z porušení povinnosti, ke které se smluvní pokuta vztahuje.

VIII. OPRÁVNĚNÉ OSOBY

1. Každá ze smluvních stran jmenuje oprávněnou osobu, popř. zástupce oprávněné osoby. Oprávněné osoby budou zastupovat smluvní stranu ve všech záležitostech souvisejících s plněním této smlouvy.

2. Oprávněné osoby jsou oprávněny jménem stran provádět veškeré úkony dle této smlouvy, a připravovat dodatky ke smlouvě pro jejich písemné schválení osobám oprávněným zavazovat strany (statutárním orgánům), nebo jejich zplnomocněným zástupcům.

3. Jména oprávněných osob jsou uvedena v příloze č. 2 této smlouvy.

4. Smluvní strany jsou oprávněny změnit oprávněné osoby, jsou však povinny na takovou změnu druhou smluvní stranu písemně upozornit, přičemž změna oprávněné osoby se stane účinnou doručením předmětného oznámení druhé smluvní straně. Zmocnění zástupce oprávněné osoby musí být písemné s uvedením rozsahu zmocnění.

IX. OSTATNÍ USTANOVENÍ

1. Poskytovatel se zavazuje po celou dobu obchodní spolupráce dodržovat platné právní předpisy a provádět veškerá plnění v souladu s platným právním řádem

2. Poskytovatel tímto uděluje souhlas se zveřejněním této smlouvy v souladu s povinnostmi nabyvatele, jakožto subjektu povinného dle zákona č. 340/2015 Sb. o zvláštních podmínkách

účinnosti některých smluv, uveřejňování těchto smluv a o registru smluv (zákon o registru smluv), ve znění pozdějších předpisů.

3. Poskytovatel se zavazuje zachovávat dle zákona č. 110/2019 Sb., o zpracování osobních údajů, mlčenlivost o osobních údajích a o bezpečnostních opatřeních, jejichž zveřejnění by ohrozilo zabezpečení osobních údajů, a to i po ukončení plnění smlouvy, v případě jejího ukončení dohodou, odstoupením od ní.
4. Tato smlouva bude v úplném znění uveřejněna v registru smluv nabyvatelem.
5. Poskytovatel se zavazuje nezpřístupnit údaje o dodávkách poskytovaných nabyvateli třetí osobě, pokud pro něj taková povinnost nevyplývá ze zákona nebo pravomocného rozhodnutí příslušného soudního či správního orgánu.
6. Obě smluvní strany jsou povinny oznámit druhé smluvní straně jakoukoliv změnu údajů uvedených v záhlaví této smlouvy, a to písemně bez zbytečného odkladu poté, kdy se o příslušné změně dozví.

X. PLATNOST A ÚČINNOST SMLOUVY

1. Tato smlouva nabývá platnosti dnem jejího podpisu oprávněnými osobami obou smluvních stran a účinnosti dnem jejího uveřejnění v registru smluv.
2. Nabyvatel je oprávněn od smlouvy (popřípadě její části) písemně odstoupit jen z důvodu podstatného porušení smlouvy poskytovatelem (odstoupení od smlouvy ze strany nabyvatele nesmí být spojeno s uložením jakékoliv sankce k tíži nabyvatele), přičemž za podstatné porušení smlouvy se bude považovat zejména porušení jakékoliv povinnosti poskytovatele vyplývající z této smlouvy a její nesplnění ani v dodatečné přiměřené lhůtě, kterou nabyvatel poskytovateli k tomu poskytne (nevylučuje – li to charakter porušené povinnosti); v pochybnostech se má za to, že dodatečná lhůta je přiměřená, pokud činila alespoň 5 (pět) pracovních dnů.
3. Odstoupením od smlouvy nejsou dotčena ustanovení týkající se smluvních pokut, úroků z prodlení, řešení sporů a ustanovení týkající se těch práv a povinností, z jejichž povahy vyplývá, že mají trvat i po odstoupení (zejména jde o povinnost poskytnout peněžitá plnění za plnění poskytnutá před účinností odstoupení).
4. Nabyvatel je oprávněn smlouvou kdykoliv vypovědět bez uvedení důvodu, výpovědní lhůta je stanovena na 3 měsíce. Výpovědní lhůta začíná běžet prvním dnem měsíce následujícího po doručení písemné výpovědi.

XI. ZÁVĚREČNÁ USTANOVENÍ

1. Práva a povinnosti vzniklé na základě této smlouvy nebo v souvislosti s touto smlouvou se řídí právním řádem České republiky, zejména OZ.
2. Smluvní strany se zavazují vyvinout maximální úsilí k odstranění vzájemných sporů vzniklých na základě této smlouvy nebo v souvislosti s touto smlouvou a k jejich vyřešení zejména prostřednictvím jednání kontaktních osob nebo pověřených zástupců.
3. K dosažení účelu této smlouvy jsou si smluvní strany povinny vzájemně poskytovat potřebné informace a nezbytnou součinnost.
4. Jakékoliv změny závazkového právního vztahu založeného smlouvou mohou být činěny toliko písemnými datovanými pořadově číslovanými dodatky podepsanými oprávněnými osobami obou smluvních stran.

5. Poskytovatel bere na vědomí, že je osobou povinou spolupůsobit při výkonu finanční kontroly dle § 2 písm. e) zákona č. 320/2001 Sb., o finanční kontrole ve veřejné správě a o změně některých zákonů, ve znění pozdějších předpisů a zavazuje se, že umožní všem subjektům oprávněným k výkonu kontroly projektu, z jehož prostředků je dodání zboží hrazeno, provést kontrolu dokladů souvisejících s plněním smlouvy, a to po dobu danou právními předpisy ČR k jejich archivaci.
6. Poskytovatel bere na vědomí a výslovně souhlasí s tím, že tato smlouva včetně případných dodatků bude nabyvatelem zveřejněna.
7. Smluvní strany tímto shodně prohlašují, že tato smlouva ani její přílohy neobsahují žádné informace nebo skutečnosti, které smluvní strany nebo i jen jedna z nich považují za obchodní tajemství ve smyslu § 504 OZ.
8. Poskytovatel se rovněž zavazuje pro případ, že se v průběhu plnění předmětu smlouvy dostane do kontaktu s osobními údaji, že je bude ochraňovat a nakládat s nimi plně v souladu s příslušnými právními předpisy.
9. Tato smlouva se vyhotovuje ve dvou stejnopisech, z nichž každý má platnost originálu. Nabyvatel obdrží jeden stejnopis, poskytovatel obdrží jeden stejnopis.
10. Ujednání této smlouvy jsou vzájemně oddělitelná. Pokud jakákoli část závazku podle této Smlouvy je nebo se stane neplatnou či nevymahatelnou, nebude to mít vliv na platnost a vymahatelnost ostatních závazků podle této smlouvy a smluvní strany se zavazují nahradit takovouto neplatnou nebo nevymahatelnou část závazku novou, platnou a vymahatelnou částí závazku, jejíž předmět bude nejlépe odpovídat předmětu původního závazku. Pokud by smlouva neobsahovala nějaké ujednání, jehož stanovení by bylo jinak pro vymezení práv a povinností odůvodněné, smluvní strany učiní vše pro to, aby takové ustanovení bylo do Smlouvy doplněno.
11. Smluvní strany prohlašují, že smlouva byla uzavřena podle jejich pravé a svobodné vůle, určitě, vážně a srozumitelně, a že nebyla uzavřena v tísni či za nápadně nevýhodných podmínek. Na důkaz pravdivosti tohoto prohlášení připojují smluvní strany ke smlouvě své podpisy.

Přílohy:

Příloha č. 1:	Kalkulace ceny
Příloha č. 2:	Specifikace ochranného software
Příloha č. 3:	Oprávněné osoby
Příloha č. 4:	Kopie pojistné smlouvy

[redacted]

Příloha č. 1 smlouvy - Kalkulace ceny

	Cena bez DPH	DPH	Cena s DPH
Dodávka Licence Bitdefender GravityZone Business Security Premium (Elite) pro 85 serverů, platnost licence 36 měsíců			
Dodávka Licence Bitdefender GravityZone Business Security Premium (Elite) pro 150 serverů, platnost licence 36 měsíců			
Implementace antivirového řešení - servery			
Podpora licencí na servery na období 36 měsíců podpora společnosti IS4 security s.r.o.			
Celkem	**317600**	**66696**	**384296**

[redacted]

Příloha č. 2 smlouvy - Specifikace ochranného software

Příloha č. 3a Technická specifikace

„Dodávka antivirového řešení pro Krajskou zdravotní, a.s. 2022 – část 1 - servery“

1. **Specifikace zabezpečení**
   - Předmětem je řešení zabezpečení operačních systémů na virtuálních a fyzických serverech.
   - Musí jít o moduly jednoho výrobce a tyto moduly musí být integrovány do jednoho celku s jedinou centrální správou. Centrální správa bude implementovat jako software na virtuální Windows server 2022.
   - V případě požadavku na použití stávající infrastruktury, musí být jasně specifikovány požadavky na takovou infrastrukturu. Součástí dodávky musí být veškeré potřebné programové vybavení, tj. všechny licence potřebné pro instalaci a provoz.
   - Podpora ve formě NBD (oprava do druhého pracovního dne), záruka a plná licence na dodaný software a všechny jeho komponenty musí být minimálně na 3 roky od dne nasazení s možností dalšího prodloužení.

2. **Požadované funkce antivirové ochrany**
   - Podpora operačních systémů MS: Windows Server 2012 R2, Windows Server 2016, Windows Server 2019 a Windows Server 2022
   - Podpora MS Exchange 2010, MS Exchange 2016 a vyšší.
   - integrované řešení pro koncovou ochranu serverů – licence pro 85 fyzických serverů a 150 virtuálních serverů
   - použití „lehkého“ klienta pro virtuální servery – prostředí virtualizace VMWARE 6.7 a vyšší
   - Real-time ochrana před všemi druhy malwaru : viry,červy,trojskými koňmi (backdoor, adware, spyware, rootkit, bootkit, ransomware, zero day)
   - přesná identifikace známých i neznámých hrozeb nízké zatížení systému - rychlé startování systému a malé nároky na systémové zdroje (max. do 10%), vytížení RAM do 1GB.
   - rychlá kontrola - inteligentní dynamická vyrovnávací paměť, která minimalizuje diskové operace
   - Napojení na centrální správu ze které lze instalovat, spravovat a konfigurovat antivirové klienty.
   - Funkcionalita zajišťující centrální stahování aktualizací a jejich distribuci na klienty
   - Instalace sw aktualizací v rámci aktualizačního procesu antivirových signatur.
   - Aktualizace virové databáze minimálně 4x denně.
   - Možnost plánovaného skenování serverů.
   - Definice výjimek
   - Možnost skriptovat klientskou část.
   - Virový trezor

- Správa zařízení umožňující blokaci všech medií s podporou whitelistování na základě definice.
- Možnost blokace přístupu na definované weby nebo domény.
- Podpora virtuálního prostředí: VMware vSphere
- Integrace s Active Directory na úrovni uživatel/skupina
- Logování incidentů
- Blokování C&C komunikace
- Kontrola a správa vyjímatelných zařízení (USB vyjímatelná zařízení, optická média, infračervené přenosy, bluetooth, disketové jednotky, multimediální zařízení)
- Aplikační kontrola
- blokování neznámých malware kategorie „Crypto-Ransomware“ a jiných
- ochrana MBR,UEFI

3. Instalace

- zadavatel požaduje instalaci řešení do virtualizačního prostředí VMware verze 6.7 a vyšší, dodavatel v rámci nabídky specifikuje požadavky na potřebné prostředky ve virtualizačním prostředí
- dodavatel zajistí instalaci a implementaci serverové části předmětu plnění na virtuální server, který připraví zadavatel na základě požadavků dodavatele
- dodavatel zajistí kompletní instalaci, konfiguraci a zprovoznění celého předmětu plnění
- dodavatel zajistí odinstalaci původního antivirového řešení

4. Update

- dodavatel zajistí update předmětu plnění i update virových databází po dobu 3 let

5. Specifikace podpory

- podpora od výrobce po dobu platnosti licence
- 5x výjezd za rok v pracovní době dle požadavků zadavatele v rámci podpory
- Lokální podpora (minimálně 8x5) v českém jazyce od certifikovaných odborníků: hotline, helpdesk, podpora administrace
- Garantovanou rychlost řešení problému do dvou hodin od nahlášení problému
- Zajištění technického školení (administrace a instalace) pro dvě osoby na úrovni profesional

6. Akceptační podmínky

- Instalace na všech zadavatelem definovaných serverech
- Ověření funkčnosti antivirových testů
- Ověření automatizovaného pouštění testů
- Ověření funkčnosti update programu i virových definic
- Ověření znalostí administrátorů zadavatele složením certifikačního testu.

Požadavky na předmět plnění uvedené v tomto dokumentu jsou závazné, jejich nedodržení bude považováno za nesplnění zadávacích podmínek s následkem vyloučení dodavatele z účasti na veřejné zakázce.

Dodavatel prohlašuje, že jím nabízené plnění splňuje všechny požadavky uvedené v této příloze

Společnost CYBOSEC s.r.o.

Je předním dodavatelem technologií Bitdefender v České republice s vysoce školeným týmem odborníků. Vybrali jsme pro zadavatele Krajská zdravotní, a.s. řešení postavené na prémiovém produktu **Bitdefender Gravity Zone Business Security Premium (ELITE)**, které nejen, že splňuje všechny požadavky zadavatele, ale jde výrazně výše nad jejich rámec. Nad rámec požadovaných funkcionalit bychom rádi uvedli několik klíčových:

- HyperDetect™ (Inteligentní strojové učení) - Engine využívající strojového učení a pokročilou heuristiku. Detekuje sofistikované hrozby a cílené útoky, blokuje hackerské nástroje, bezsouborové útoky, zero-day útoky, anomálie a další nebezpečný neznámý malware.
- Ransomware Mitigation – Vytváří průběžně zálohu souborů v reálném čase. V případě ransomwarového útoku obnoví veškeré soubory do původního stavu a tím zabraňuje ztrátě dat.
- Analýza primární příčiny – Zobrazuje detail útoku a odhaluje počátek a způsob vedení útoku. Výrazně usnadňuje řešení bezpečnostních incidentů. Každý incident dostává automaticky skóre dle závažnosti a tím usnadňuje prioritizaci řešení incidentů.
- Sandbox Analyzer – Automaticky odesílá podezřelé soubory k bezpečné detonaci, analyzuje a poskytuje vyhodnocení v reálném čase. Detekuje zero-day a cílené útoky.

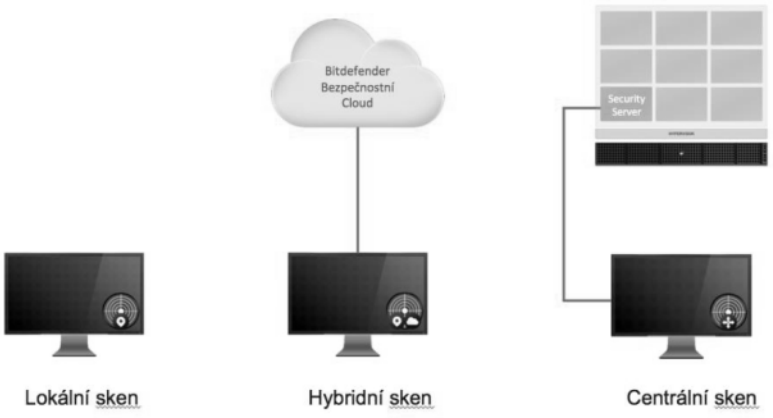
Podrobný popis nabízeného řešení pokročilé ochrany koncových bodů

Základní popis GravityZone Architektury řešení

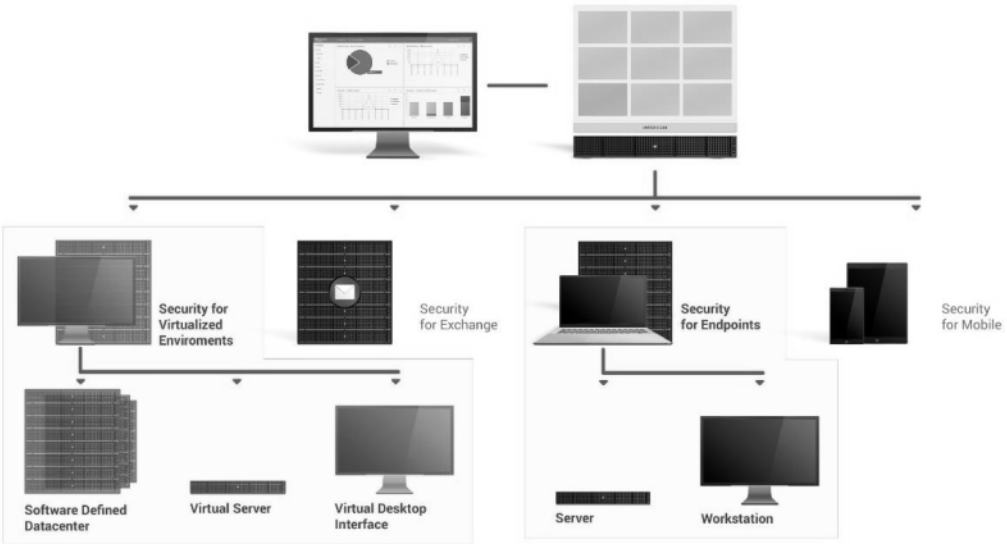
Bitdefender GravityZone (dále jen **BDGZ**) je firemní řešení nabízející nasazení centrální správy všech zařízení ve variantách on-premise (hostované u zákazníka) nebo hostované v cloudu. BDGZ umožňuje spravovat fyzické, virtuální a mobilní koncové body nezávisle na operačním systému, hypervizoru a to vše z jediné centrální konzole správy. 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 i lokální skenování a testování souborů, aplikací, paměti a registrů na hrozby ve variantách 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.



Obr.1 Popis skenovacích možností BDGZ

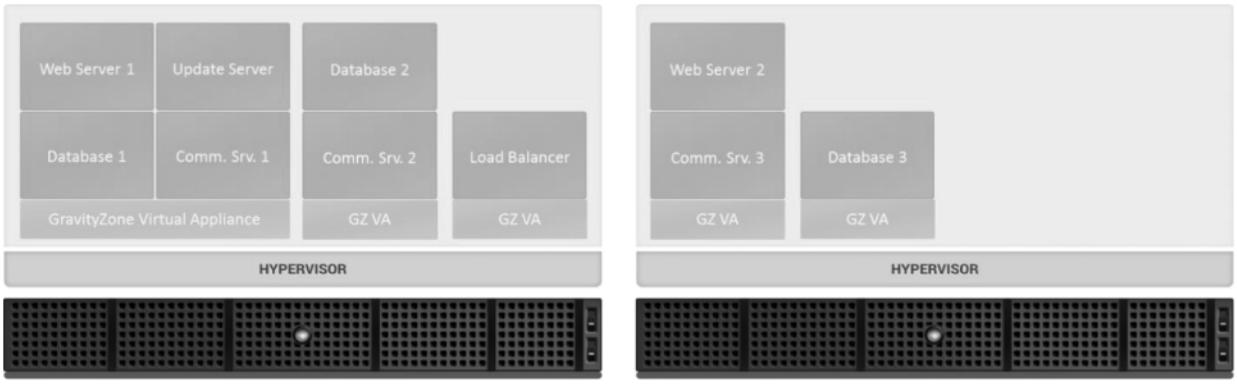


Obr.2 Infrastruktura BDGZ přehled všech komponentů včetně centrální správy pro fyzické i virtuální prostředí, včetně podpory pro mobilní zařízení a MS Exchange.

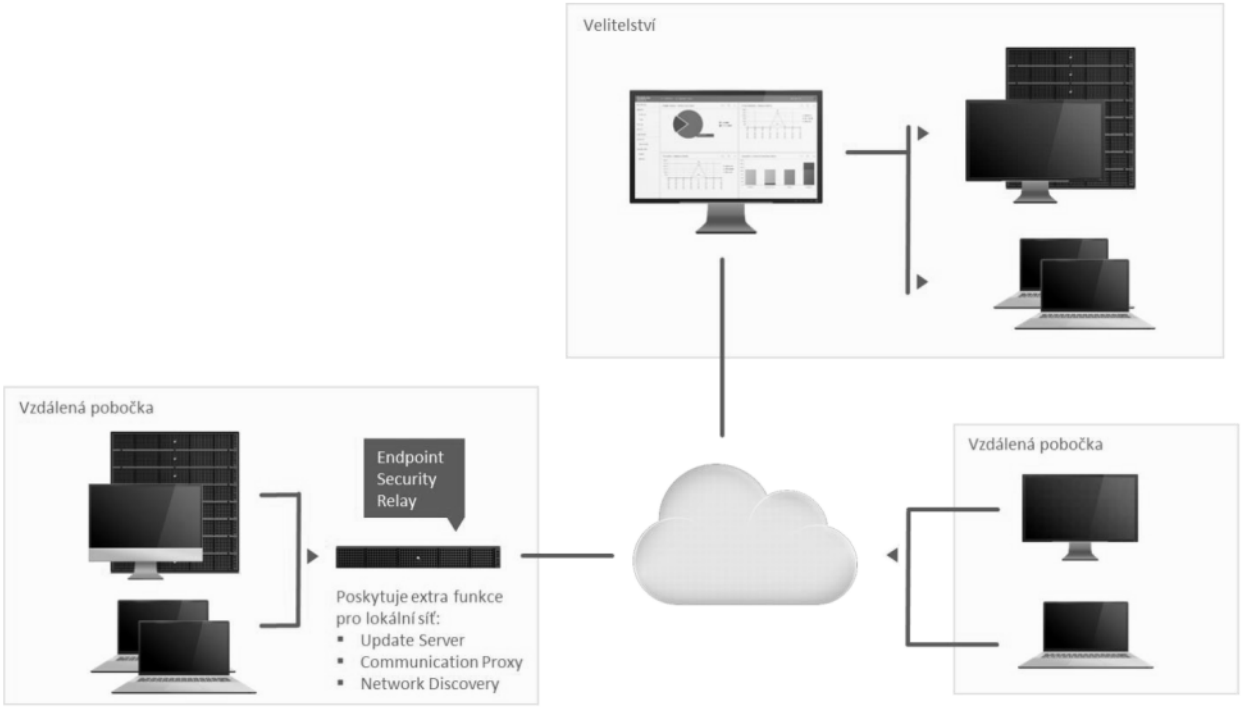
Bitdefender GravityZone komponenty:

- 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.



Obr.3 Škálování GZVA s využitím vysoké dostupnosti Databáze a role Balanceru

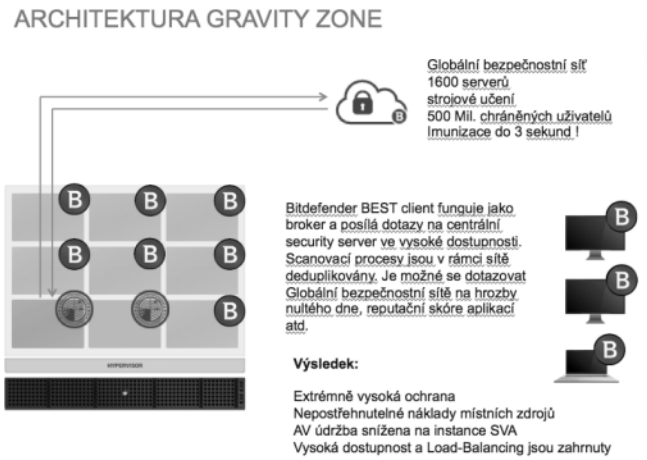


Obr. 4 Infrastruktura BDGZ s využitím BEST klienta s rolí Relay pro menší pobočky

Funkční vlastnosti řešení

Souhrn technických částí a funkcí řešení BDGZ

- 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.



Obr.5 Popis architektury BDGZ a BEST klienta

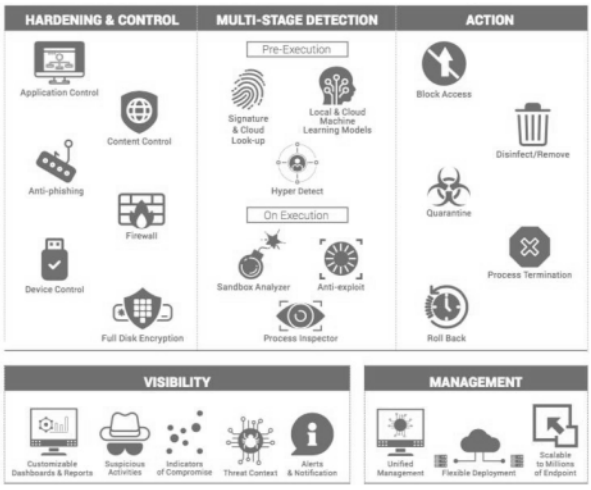
Bitdefender Endpoint Security (GravityZone Business Security Premium (ELITE))

Security Hyperdetect & Sandbox Analyzer

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 (ELITE) - 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, vícestupňových metod detekce nezaložených na signaturách, a automatické odezvy.

Hlavní výhody

Endpoint Security Premium (Elite) 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 (Elite) 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 (Elite) je 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, 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

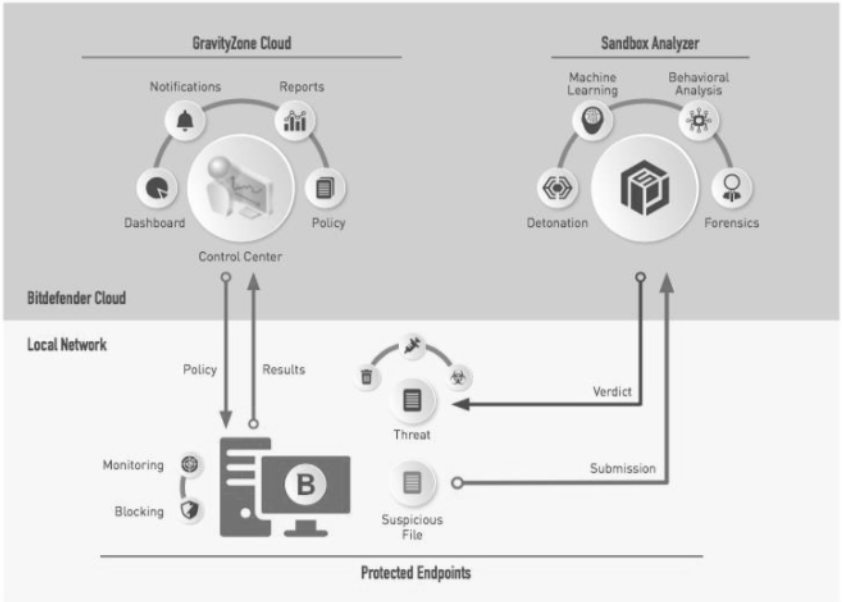
umožňuje správcům zabezpečení nastavit obranu tak, aby se mohla co nejefektivněji vypořádat s hrozbami, kterým podnik může čelit. S funkcí „Pouze hlášení" mohou správci zabezpečení uspořádat a sledovat své nové

zásady zabezpečení před jejich zveřejněním, a zamezit tak přerušení 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. 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 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 Analyzeru, Endpoint Security (Elite) 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 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. Po doručení rozsudku o škodlivosti ze Sandbox Analyzeru, Endpoint Security 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 Analyzéru 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, 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.

Šifrování celého disku
Šifrování celého disku spravované skrze GravityZone pomocí Windows BitLocker a Mac FileVault, využívající výhod technologií 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.

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

Funkční popis všech základních komponent nabízeného řešení

Bitdefender GravityZone Business Security Premium (Elite)

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) .
- 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.

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.

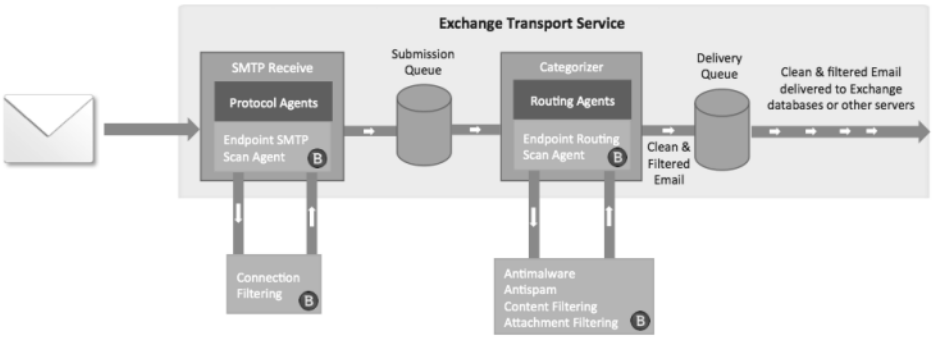
Hlavní výhody

- 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

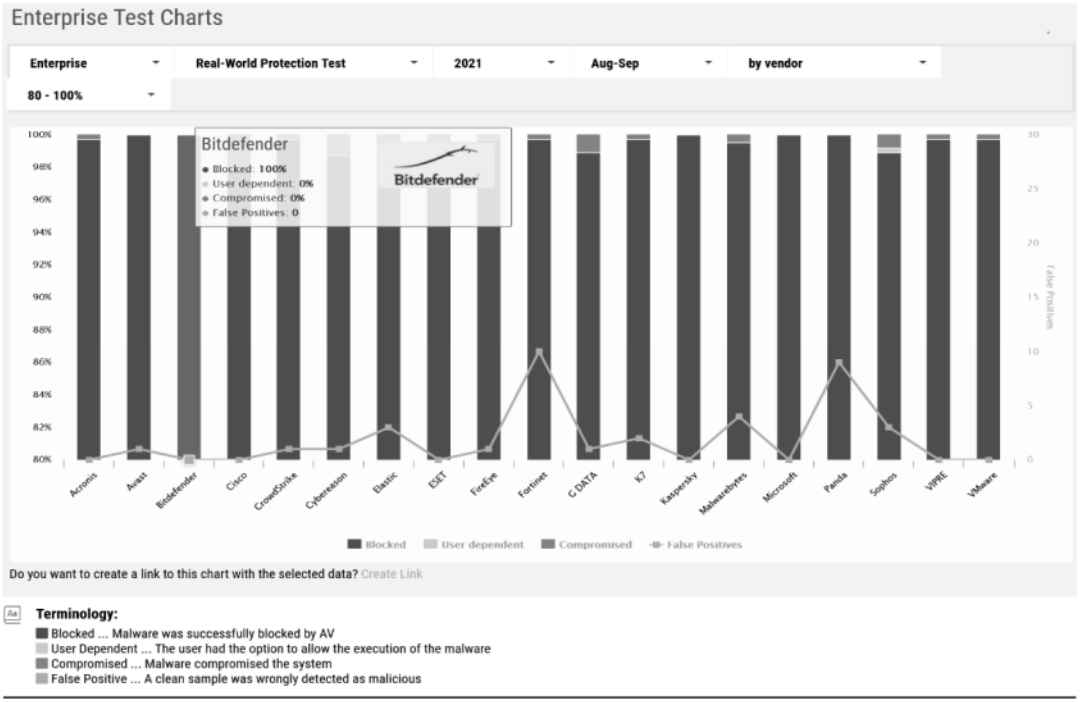
Klíčové výhody

- 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)



Kvalita produktu a významná ocenění



https://www.av-comparatives.org/awards/bitdefender/

Bitdefender získává za posledních 5 let za sebou od nezávislých testovacích organizací ve všech produktových řadách významná ocenění, přičemž **54 % všech testů vyhrál.**

AV-TEST Award 2021
for Bitdefender

lasti kybernetické bezpečnosti

Best protection for corporate users:
Bitdefender Endpoint Security (Ultra)

Příloha č. 3 smlouvy - Oprávněné osoby

Za nabyvatele:

- ve věcech smluvních:

Jméno a příjmení	[redacted]
Adresa	[redacted]
E-mail	[redacted]
Telefon	[redacted]
Fax	-

- ve věcech obchodních a ve věcech technických a realizačních:

Jméno a příjmení	[redacted]
Adresa	[redacted]
E-mail	[redacted]
Telefon	[redacted]
Fax	-

Za poskytovatele:

- ve věcech smluvních:

Jméno a příjmení	[redacted]
Adresa	[redacted]
E-mail	[redacted]
Telefon	[redacted]
Fax	-

- ve věcech obchodních a ve věcech technických a realizačních:

Jméno a příjmení	[redacted]
[redacted]	[redacted]
E-mail	[redacted]
[redacted]	+420 736 174 250
Fax	-

Příloha č. 4: Kopie pojistné smlouvy

V180

GENERALI
ČESKÁ POJIŠŤOVNA

TC99110006011

POJISTNÁ SMLOUVA
Pojištění [redacted]

SMLUVNÍ STRANY

Pojistitel
Generali Česká pojišťovna a.s., Spálená 75/16, Nové Město, 110 00 Praha 1, IČO: 452 72 956, DIČ: CZ699001273, je zapsaná v obchodním rejstříku vedeném Městským soudem v Praze, spis. zn. B 1464, člen skupiny Generali, zapsané v italském registru pojišťovacích skupin, vedeném IVASS, pod číslem 026 (dále jen pojišťovna)

Pojišťovací zprostředkovatel
Samostatný zprostředkovatel (SZ)
Titul, jméno, příjmení, titul za jménem / obchodní firma
Generali Česká Distribuce a.s.
IČO: 44795084
Adresa sídla – ulice: Na Pankráci, číslo popisné: 1658/121
Obec – část obce: Praha 4, PSČ: 140 00

Vázaný zástupce (VZ)
Titul, jméno, příjmení, titul za jménem / obchodní firma
[redacted]
IČO: 65426053
Adresa sídla – ulice: Azalková, číslo popisné: 1172
Obec – část obce: Praha, PSČ: 102 00
[redacted]

O221118802148

Pojistník

Název	CYBOSEC s.r.o., zapsaná v C 42008 rejstříku KS Hradec Králové
IČO	04301226
Adresa	Hradčany 347, 503 53 Smidary, ČESKÁ REPUBLIKA
Plátce DPH	ANO
E-mail	[redacted]

Korespondenční adresa je shodná s adresou pojistníka.

Pojištěný
Pojištěný je shodný s pojistníkem, pokud není dále u jednotlivých pojištění uvedeno jinak.

I. POJISTNÁ DOBA
Pojištění se sjednává na dobu od **00:00 hod.** dne **13. 11. 2020** do konce pojistného roku ve smyslu ujednání této pojistné smlouvy. Tato pojistná smlouva se sjednává s **automatickou prolongací**. Datum obnovy je stanoven na **13. 11.** každého kalendářního roku.

Dohodou obou smluvních stran byla v této pojistné smlouvě provedena s účinností ode dne 6. 5. 2022 změna a od tohoto data je platná tato verze pojistné smlouvy.

V161

GENERALI ČESKÁ POJIŠŤOVNA

Z-VPPP82/**N**

TC99004101023

O221118802658

Generali Česká pojišťovna a.s., Spálená 75/16, Nové Město, 110 00 Praha 1, IČO: 452 72 956, DIČ: CZ699001273, je zapsaná v obchodním rejstříku vedeném Městským soudem v Praze, spis. zn. B 1464, člen skupiny Generali, zapsané v italském registru pojišťovacích skupin, vedeném IVASS, pod číslem 026 (dále „pojišťovna")

Pojistka

Pojištění podnikatele a právnických osob

potvrzení o uzavření pojistné smlouvy číslo 4284246677

Pojistník

Název firmy	CYBOSEC s.r.o.
Adresa	Hradčany 347, 503 53 Smidary, ČESKÁ REPUBLIKA
IČO	04301226

Pojištění podnikatele a právnických osob

Pojištění odpovědnosti

Pojistná událost
Pojistnou událostí je vznik povinnosti pojištěného nahradit škodu nebo újmu uvedenou v pojistné smlouvě či pojistných podmínkách, se kterou je spojena povinnost pojišťovny poskytnout pojistné plnění.

Pojistná nebezpečí
Pojistným nebezpečím jsou skutečnosti a události vymezené v pojistné smlouvě jako možná příčina vzniku pojistné události.

Oprávněnou osobou z tohoto pojištění je pojistník.

Podmínky, rozsah pojištění a pojistných nebezpečí stanoví pojistná smlouva a Všeobecné pojistné podmínky pro pojištění majetku a odpovědnosti VPPMO-P-01/2020.

Pojištění v základním rozsahu se sjednává s limitem pojistného plnění	20 000 000 Kč
Pojištění v základním rozsahu se sjednává s územním rozsahem	Česká republika
Pojištění v základním rozsahu se sjednává se spoluúčastí	5000 Kč

Počátek a doba pojištění

Pojištění se sjednává na dobu od 13. 11. 2021 do 12. 11. 2022.
Pojištění se sjednává s automatickou prolongací.

Pojišťovna potvrzuje, že údaje obsažené v pojistce jsou platné ke dni jejího vydání.

Platnost pojistky od: 6. 5. 2022

S pozdravem

Generali Česká pojišťovna a.s.

[redacted]

strana 1 z 1

[redacted]