S/0625/2023/OIT

SMLOUVA

o udělení licence softwarového produktu

Níže označené smluvní strany----------

statutární město Frýdek-Místek
se sídlem Radniční 1148, Frýdek, 73801 Frýdek-Místek.
osoba oprávněna jednat: Petr Korč, primátor
IČ: 00296643
DIČ: CZ00296643
tel. [redacted]
kontaktní osoba ve věcech technických:
Mgr. René Rozsypal, vedoucí odboru informačních technologií
email [redacted] /tel: [redacted]

- **dále jen nabyvatel**

a

CYBOSEC s.r.o.
se sídlem Hradčany 347, 503 53 Smidary
jejímž jménem jedná Pavel Jícha jako jednatel společnosti
IČ: 04301226
DIČ: CZ04301226
zapsána v obchodním rejstříku vedeném Krajským soudem v Hradci Králové, pod spisovou značkou C 42008
Č. účtu: [redacted]
Tel: [redacted]
Fax: -
E-mail: [redacted]

- **dále jen poskytovatel**
- **nabyvatel a poskytovatel dále jen smluvní strany**

uzavírají v souladu s ustanoveními §1746 odst. 2 a § 2371 a následujících zákona č. 89/2012 Sb., občanský zákoník v platném znění (dále jen „občanský zákoník") a zákona č. 121/2000 Sb., o právu autorském, o právech souvisejících s právem autorským a o změně některých zákonů, v platném znění („autorský zákon") tuto smlouvu k veřejné zakázce „Dodávka a implementace antivirového EDR a XDR systému" následujícího znění a obsahu (dále jen smlouva).

článek 1
PŘEDMĚT SMLOUVY

1. Poskytovatel prohlašuje, že je oprávněn k distribuci programů a služeb, jež tvoří dále specifikovaný předmět této smlouvy, a touto smlouvou poskytuje nabyvateli oprávnění k jeho využívání v rozsahu a za podmínek v této smlouvě vymezených.

2. Předmětem plnění zakázky je dodávka, instalace a konfigurace software antivirové, EDR a XDR ochrany koncových stanic, serverů, uživatelů, poštovních schránek, serverů Microsoft Windows, serverů Linux, virtuálního prostředí VMware vSphere a mobilních zařízení. Dále dodávka, instalace a konfigurace softwarových doplňku umožňující instalaci updatů operačních systémů Microsoft Windows a aplikací a síťové sondy. Plnění veřejné zakázky dále zahrnuje zaškolení zaměstnanců IT nabyvatele, dodání licencí a dokumentů (návodů a nastavení konfigurace). Software musí být určený pro český trh.

3. Popis stávající licence
   Nabyvatel má v současné době zajištěn systém ochrany produktem Bitdefender GravityZone Business Security Enterprise (Cloud Console) 600 Total seats, Bitdefender GravityZone Patch Management 600 Total seats, Bitdefender GravityZone Business Security Enterprise (on premis) 250 Total seats s platností do 14. ledna 2024.

4. Technické parametry
   Poskytovatel musí dodat plně funkční a úplně nakonfigurovaný systém ochrany zařízení nabyvatele (počítače, notebooky, mobilní telefony, servery) dle svých nejlepších znalostí a svědomí, splňující veškeré níže uvedené minimální technické parametry a funkce.

   Případné názvy a popisy uvedené ve specifikaci odkazující na jednotlivá obchodní jména a označení výrobků či obchodních názvů specifikují podmínky požadovaného plnění s tím, že nabyvatel připouští i jiná, kvalitativně a technicky obdobná, řešení za podmínky, že nedojde ke zhoršení požadovaných parametrů technického řešení a bude zachována kompatibilita se stávajícími zařízeními a infrastrukturou nabyvatele.

A. Centrální správa

Popis výrobku	
Výrobce	**Bitdefender**
Modelové označení	[redacted]
Počet licencí	

Musí splňovat následující požadavky:

- nabízené řešení musí být kompletně spravovatelné z jedné konzole centrální správy systému v anglickém jazyce
- jednotné prostředí webové konzole (cloudového řešení prezentující výsledky detekcí s podporou strojivého učení a umělé inteligence) pro správu ochrany fyzických pracovních stanic, serverů (VM) a mobilní zařízení (nadále koncové body) před různými kybernetickými hrozbami, včetně narušení dat, ransomwaru, phishingu, chování koncových bodů v síti, správa oprav a antivirová ochrana. Vizualizace stavů podnikové sítě z hlediska komplexního přehledu o stavu zabezpečení koncových bodů, jejich zranitelností, lidského chování, detekovaných incidentů a blokovaných útoků.
- provozováno formou služby, tak aby bylo možno provozovat plnohodnotně XDR bez ohledu na výpočetní kapacity nabyvatele
- přistupovat odkudkoliv z internetu bez nutnosti připojování a přihlašování do prostředí nabyvatele
- dvou faktorová autentifikace pro přístup do centrální správy
- přehledný dashboard informující o základních nejdůležitějších stavech systému ochrany umožňující customizaci administrátorům

- škálovatelnost přístupů do konzole včetně možnosti nastavení úrovní oprávnění
- vzdálené nasazování klientů
- aktualizace nových verzí klientů (automaticky)
- aktualizace virových databází (automaticky)
- vzdálené nastavování parametrů klientů
- možnost vytváření skupin zařízení s různými parametry nastavení
- synchronizace s Active Directory
- automatická detekce stanice/serveru/mobilního zařízení podle Active Directory
- možnost sledování stavu a počtu a platnosti licencí (aktivní, volné, vyčerpané licence)
- vytváření a aplikace pravidel na skupiny koncových stanic/serverů/mobilních zařízení včetně možnosti okamžitého vynucení pravidel klienta
- možnost definovat výjimky pro kontrolované soubory, procesy, nastavovat plánování kontrol a spouštění kontrol uživatelských stanic v reálném čase
- možnost vzdálené obnovy souborů označených systémem ochrany za škodlivé
- systém umožňující rychle identifikovat hrozby pomocí začlenění heuristik s využitím pokročilých technologií machine learning (ML) a umělé inteligence (AI). Systém musí předvídat a identifikovat konkrétní útoky, stejně jako efektivně identifikovat pokročilý malware před jeho provedením. Za splnění tohoto požadavku se nepovažuje metoda skenování založená na signaturách nebo behaviorálním skenování.
- možnost umístění koncového bodu do karantény (úplná izolace zařízení od produkčního prostředí)
- centrální logování událostí o virových nákazách, hrozbách a provedených kontrolách koncových stanic
- prohledávání logů s možností filtrace
- automatické reportování o stavu a fungování systému a jeho komponent včetně incidentů
- automatické zasílání notifikací o nakažených stanicích, incidentech a hrozbách na email administrátorům
- možnost integrace do SIEM systému prostřednictvím API rozhraní – zasílání bezpečnostních událostí podle typu událostí

B. Ochrana koncových stanic

Musí splňovat následující požadavky:

- klient v českém jazyce
- napojení na centrální správu z bodu 2.3 A
- ochrana před známými hrozbami, škodlivým kódem a pokusy získat citlivé údaje (vir, červ, rootkit, spyware, trojský kůň, keylogger, phishing …)
- rezidentní ochrana
- kontrola hrozeb nepřetržitě monitorující běžící procesy a hodnotící podezřelé chování, jako jsou pokusy: zamaskovat typ procesu, spustit kód v prostoru jiného procesu (unést procesní paměť pro eskalaci oprávnění), replikovat, vyřadit soubory, skrýt před aplikacemi výčtu procesů atd.
- detekce pokročilých útoků a podezřelých aktivit ve fázi před spuštěním
- firewall

- ochrana proti ransomware s funkcionalitou obnovy již zašifrovaných souborů po detekci šifrování
- ochrana proti hrozbám zero-day – vydávání mimořádných aktualizací
- ochrana před infikovanými webovými stránkami
- skenování externích medií (USB, CD, DVD, paměťové karty …)
- automatická aktualizace virových definic
- možnost individuální aktualizace samotného klienta systému ochrany a aktualizace nových virových definic i v případě nedostupnosti centrální konzole (takže s využitím aktualizačního webu výrobce)
- možnost pro administrátory obnovit soubory označené systémem ochrany za škodlivé
- ochrana před modifikací systému ochrany a jeho součástí uživateli koncových stanic (změny a nastavení provádí pouze administrátor – zabezpečeno heslem)
- funkčnost systému ochrany bez nutnosti připojení k centrální správě či internetu
- možnost úplné odinstalace klientů
- podpora operačních systémů Windows 10 a 11 v 64-bit verzích, macOS Big Sur (11.0) a novější

C. Ochrana mobilních zařízení

Musí splňovat následující požadavky:

- napojení na centrální správu z bodu 2.3 A
- rezidentní ochrana
- Anti-Theft – ochrana proti/při odcizení
- možnost uzamknutí a vymazání zařízení na dálku
- Anti-Phishing – detekce škodlivých webových stránek
- detekce škodlivých aplikací včetně možnosti blokovat aplikace
- možnost uplatnění pravidel nastavení – vynucení zámku obrazovky a podobně
- automatická aktualizace virových definic
- podpora operačního systému Android verze 9 a vyšší a iOS 14 a vyšší a 64-bit verze zařízení

D. Ochrana serverů

Musí splňovat následující požadavky:

- napojení na centrální správu z bodu 2.3 A
- podpora Microsoft Exchange 2016 Server za účelem ochrany uživatelů Exchange před hrozbami přenášenými e-mailem
- antivirová ochrana mailboxů
- ochrana před spamem, phishingem a ostatními malwarovými hrozbami v reálném čase
- kontrola přiložených souborů i komprimovaných
- politiky pro doručení/nedoručení zpráv (např. přílohy typu zip, rar, exe, bat atd.)
- automatická aktualizace virových definic
- filtrování zpráv na základě obsahu, rozpoznávání formátu, názvu či velikosti příloh
- možnost nastavení chování při zachycení hrozby (upozornění, nahrazení přílohy, odstranění emailu či přílohy)

- podpora min. pro Windows Server 2016 a novější
- podpora min. pro Linux ve verzích CentOS 7, Debian 9, Red Hat 7 a novějších

E. EDR a XDR ochrana

Musí splňovat následující požadavky:

- prevence, detekce, prověřování a reakce, viditelnost, analýzy, korelované výstrahy při incidentech a automatizované reakce
- integrovat ochranu napříč koncovými body, servery, cloudové aplikace, e-maily, síťový provoz a další
- rekapitulace útoku
- zobrazení, jaké kroky útoku měly největší dopad
- vizualizace v podrobném schématu, kde budou zaznamenávány a znázorněny jednotlivé kroky služeb a procesů předcházejících detekci škodlivého souboru, procesu nebo akce
- usnadnit rozhodovací proces ohledně určení priorit reakcí na útok
- korelace událostí napříč infrastrukturou nabyvatele, se schopností detekovat pokročilé útoky napříč více koncovými body v hybridních infrastrukturách (pracovní stanice, servery nebo kontejnery, na kterých běží různé operační systémy)
- detekci aktivit, které se vyhýbají klasickým mechanismům prevence koncových bodů

F. Kontrola síťového provozu

- nabízený systém musí zajistit sběr, zpracování a vyhodnocování síťového provozu
- sběr veškerého síťového provozu např. prostřednictvím zrcadlením portu (SPAN)
- nabízený systém musí detekovat libovolné zařízení v síti komunikující prostřednictvím IPv4 a IPv6
- tato část systému může být řešena pomocí virtuální appliance i pomocí HW appliance
- poskytuje data pro další části systému ochrany pro vyhodnocování provozu a pro větší visibilitu do provozu nabyvatele

G. Patch management

Musí splňovat následující požadavky:

- udržovat operační systémy a softwarové aplikace aktuální a musí poskytnout komplexní přehled o stavu oprav pro spravované koncové body Windows a Linux
- nasazení aktualizací na nabyvatelem definovanou množinu koncových zařízení (tvorba skupin)
- nasazení výběru aktualizací na vybraná zařízení
- volbu času nasazení aktualizací

H. Sandbox pro Windows

Musí splňovat následující požadavky:

- analyzovat podezřelé spustitelné soubory nebo některé datové soubory např. s makry, jejich chování a hlásit jakékoli změny, které svědčící o škodlivém úmyslu
- zabránit spuštění neznámých hrozeb na koncovém bodu

I. Analýza rizik

Musí splňovat následující požadavky:

- detekce, vyhodnocení a pomáhat napravovat slabiny koncových bodů Windows prostřednictvím kontrol bezpečnostních rizik (na vyžádání nebo naplánovaných prostřednictvím zásad) s přihlédnutím k velkému počtu ukazatelů rizika
- přehled o stavu rizika sítě

5. Požadavky na implementaci

Součástí dodávky antivirového systému bude jeho instalace a implementace v místě plnění zahrnující minimálně:

- zpřístupnění centrální správy
- nastavení centrální správy (včetně pravidel a politik pro všechna zařízení nabyvatele, reporting, alerting, revize aktuálních výjimek)
- revize stávajícího nastavení a přenesení do nabízeného řešení
- odinstalace stávající ochrany ze všech zařízení (cca 550 PC, cca 50 serverů, cca 250 mobilních telefonů)
- instalace nabízeného systému na všechny koncové zařízení
- realizace akceptačních testů a zkušebního provozu
- analýza provozu na veškerých serverech, po instalaci a konfiguraci nabízeného řešení nesmí docházet ke zpomalování serverů a aplikací provozovaných na nich
- vypracování a dodání podrobné technické dokumentace podle skutečného nasazení pro administrátory systému v elektronické podobě (ve formátu MS Office 2013 a vyšší), která musí obsahovat minimálně administrátorskou příručku a kompletní popis nasazené konfigurace a nastavení (technická dokumentace se po předání nabyvateli stává jeho majetkem a může s ní nakládat dle svých potřeb)
- licence současné ochrany jsou platné do 15. 1. 2024. Implementace nového systému ochrany musí plynule navazovat na současnou ochranu, tudíž musí být plně funkční a nakonfigurované na všechny zařízeních nabyvatele nejpozději 14. 1. 2024. V případě nedodržení termínu, bude uplatňovaná sankce 10 000 Kč za každý započatý den
- pokud dojde k dřívější aktivaci licencí nového řešení, nesmí být zkrácena doba jeho plné funkčnosti, která je stanovena na dobu od 15. 1. 2024 do 14. 1. 2027.

Bezodstávkové instalace a konfigurace můžou probíhat za provozu. Práce, které vyžadují odstávku je možno provádět po pracovní době. Veškeré práce mohou probíhat až po předchozí domluvě. Magistrát je v období od 23. 12. 2023 do 1. 1. 2024 uzavřený a nemůže být v tomto období poskytnutá žádná součinnost a toto období se nepočítá do případného zkušebního provozu.

Odstávky je možno provádět v těchto časech:
- pondělí a středa od 17:30 do 19:00
- úterý a pátek od 14:00 do 19:00
- čtvrtek od 15:30 do 19:00
- odstávky po 19 hod. a o víkendu je možno realizovat po individuální domluvě

6. Školení zaměstnanců nabyvatele

Poskytovatel zajistí školení zaměstnanců nabyvatele z odboru IT na veškerý software dodaný v rámci této veřejné zakázky.

- školení musí probíhat v místě plnění VZ a v rozsahu potřebném pro provoz a údržbu nabízeného systému a všech jeho součástí (ukázka, popis, nastavení a vysvětlení jednotlivých součástí systému) minimálně v rozsahu 3x4 hodiny
- školení se zúčastní 6 zaměstnanců nabyvatele (k dispozici je školící místnost s prezentační technikou v místě plnění)

- náklady na školení musí jsou zahrnuty v ceně plnění

7. Akceptační testy a zkušební provoz

   Součástí akceptačních testů a zkušebního provozu, které navrhne poskytovatel, musí být minimálně:

   - prokázání kompletnosti dodávky a splnění všech povinných požadavků
   - prokázání aktivací veškerých licencí aktivačními nebo jinými klíči či prostředky v případě, že je aktivace potřebná
   - poskytovatelem vhodně navržené doplňující testy a kritéria, kterými bude prokázána bezproblémová a plní funkčnost
   - před akceptací a předáním díla do ostrého provozu proběhne 14denní zkušební provoz. Dílo bude předáno do zkušebního provozu proti předávacímu protokolu a musí být již hotovy veškeré konfigurační a implementační práce. Pokud se vyskytnou během testování nebo zkušebního provozu závady, poskytovatel je povinen závady odstranit nejpozději do 8 hodin od nahlášení v pracovní dny v době od 8 hod. do 17 hod.
   - v průběhu zkušebního provozu může nabyvatel průběžně posílat poskytovateli požadavky na úpravy konfigurace, nejpozději však do konce 14. dne zkušebního provozu a poskytovatel musí požadované změny realizovat (pokud to je technicky možné)
   - dokončením díla se rozumí oboustranné odsouhlasení předávacího protokolu po dokončení testovacího provozu, akceptačních testech a případných úpravách v SW konfiguraci

Bezpečnost informací

8. Poskytovatel se zavazuje při poskytování služeb dodržovat pro potřeby zajištění kybernetické bezpečnosti závazky obsažené v ujednáních v příloze č. 1 - **Dohoda o mlčenlivosti,** která je součástí této smlouvy.

článek 2
CENA PLNĚNÍ

1. Cena plnění se sjednává celkem ve výši:

	ks	Jednotková cena	Cena celkem bez DPH	DPH	Cena celkem včetně DPH
A. Ochrana koncových stanic	[redacted]	[redacted]	[redacted]	[redacted]	[redacted]
B. Ochrana serverů					
C. Ochrana mobilních zařízení					
D. Patch management					
CELKEM			2 779 800,-	583 758,-	3 363 558,-

2. Cena plnění dle smlouvy je závazná, nejvýše přípustná, obsahující veškeré náklady poskytovatele s poskytnutím licence.
3. Licence platné 36 měsíců budou hrazeny ve třech platbách. Poskytovatel vystaví daňový doklad za každý rok plnění ve výši 1/3 celkové ceny za jednotlivá období plnění smlouvy, a to vždy k ročnímu výročí platnosti licencí a to:

   i) 1. období od 15.1.2024 do 14.1.2025
   ii) 2. období od 15.1.2025 do 14.1.2026
   iii) 3. období 15.1.2026 do 14. 1. 2027

článek 3
DOBA PLNĚNÍ

1. Licence současné antivirové ochrany končí 14. ledna 2024. Implementace nového řešení musí plynule navazovat na současnou ochranu, tudíž musí být plně funkční nejpozději 15. ledna 2024.
2. Pokud dojde k dřívější aktivaci nového řešení antivirové ochrany, nesmí být zkrácena doba jeho plné funkčnosti, která je stanovena na dobu od 15. ledna 2024 do 14. ledna 2027.

článek 4
PLATEBNÍ PODMÍNKY

1. Podkladem pro zaplacení bude daňový doklad (faktura), který bude obsahovat náležitosti, stanovené daňovými a účetními předpisy.
2. První platba proběhne až po předání a aktivaci licencí, ne však před 15. 1. 2024.
3. Faktura musí mimo jiné náležitosti obsahovat:
   - označení platební doklad – faktura
   - celkovou sjednanou cenu bez DPH
   - celkovou výši DPH
4. Lhůta splatnosti faktury je 14 dnů od doručení kupujícímu.
5. Nabyvatel nebude poskytovat zálohy. Platby budou probíhat výhradně v CZK a to bezhotovostním převodem na účet poskytovatele uvedený v záhlaví této smlouvy nebo v daňovém dokladu, pokud bude odlišný; dnem zaplacení se rozumí okamžik odepsání částky z účtu nabyvatele.
6. Daň z přidané hodnoty bude fakturována ve výši dle právních předpisů platných v době dodání zboží.

článek 5
SMLUVNÍ POKUTY

1. V případě nedodání licence v termínu dohodnutém ve smlouvě, bude poskytovateli účtována smluvní pokuta ve výši 5000 Kč za každý den prodlení.
2. V případě prodlení nabyvatele se zaplacením ceny může poskytovatel požadovat po nabyvateli úrok z prodlení ve výši 0,05 % z fakturované částky bez DPH za každý den prodlení.

článek 6
ZÁVĚREČNÁ USTANOVENÍ

1. Pokud ve smlouvě není výslovně ujednáno jinak, řídí se právní vztahy smluvních stran příslušnými ustanoveními zákona č. 89/2012 Sb., občanského zákoníku, ve znění pozdějších předpisů.
2. Tato smlouva je vyhotovena v elektronické podobě, přičemž obě smluvní strany obdrží její elektronický originál.
3. Nabyvatel jako osoba uvedená v ustanovení § 2 odst. 1 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 uveřejní tuto smlouvu způsobem a ve lhůtě dle tohoto zákona. Smlouva nabývá účinnosti dnem uveřejnění podle tohoto ujednání.
4. Tato smlouva je uzavřena na základě rozhodnutí 28. schůze Rady města Frýdku-Místku ze dne 7. 11. 2023.
5. Poskytovatel bere na vědomí a výslovně souhlasí s tím, že smlouva včetně příloh a případných dodatků bude zveřejněna na profilu zadavatele.

6. Osobní údaje uvedené v této smlouvě jsou zpracovávány v souladu s nařízením Evropského parlamentu a Rady (EU) 2016/679 ze dne 27. dubna 2016 o ochraně fyzických osob v souvislosti se zpracováním osobních údajů a o volném pohybu těchto údajů a o zrušení směrnice 95/46/ES (obecné nařízení o ochraně osobních údajů). Informace o zpracování osobních údajů a právech subjektu údajů jsou zveřejněny na stránkách www.frydekmistek.cz.

Za nabyvatele:

Za poskytovatele:

_____

Petr Korč, primátor

_____

Pavel Jícha, jednatel společnosti

Příloha č. 1 – Dohoda o mlčenlivosti