Kúpna zmluva č. Z202214146_Z

uzatvorená v zmysle §409 a nasl. Obchodného zákonníka

I. Zmluvné strany

1.1 Objednávateľ:

Obchodné meno:	Mesto Trenčín
Sídlo:	Mierové námestie 2, 91164 Trenčín, Slovenská republika
IČO:	00312037
DIČ:	2021079995
IČ DPH:	SK 2021079995
Bankové spojenie:	IBAN: SK61 7500 0000 0000 2558 1243
Telefón:	0326504265

1.2 Dodávateľ:

Obchodné meno:	AUTOCONT s.r.o.
Sídlo:	Krasovského 14, 85101 Bratislava, Slovenská republika
IČO:	36396222
DIČ:	2020105428
IČ DPH:	SK2020105428
Bankové spojenie:	IBAN: SK53 0900 0000 0050 3080 8601
Telefón:	+421 2 3278 8811

II. Predmet zmluvy

2.1 Všeobecná špecifikácia predmetu Zmluvy:

Názov:	Antivírusová ochrana koncových zariadení Eset Protect Advanced pre 275 počítačov na 36 mesiacov
Kľúčové slová:	Antivírusová ochrana
CPV:	48761000-0 - Antivírusový softvérový balík; 60000000-8 - Dopravné služby (bez prepravy odpadu)
Druh/y:	Tovar; Služba

2.2 Funkčná a technická špecifikácia predmetu Zmluvy:

Položka č. 1: Antivírusová ochrana koncových zariadení Eset Protect Advanced alebo lepší ekvivalent

Funkcia
Antivírusová ochrana pre 275 koncových zariadení (počítačov, notebookov, serverov) na platforme Windows na 36 mesiacov s platnosťou od 2. 12. 2022 do 2.12 2025
Súčasťou dodávky sú aj implementačné práce vrátane inštalácii (resp. výmeny) licencií na koncové stanice, servery v rozsahu počtu požadovaných licencií , nastavenie bezpečnostných politík podľa požiadaviek objednávateľa, nastavenie centrálnej konzoly resp. správy v termíne najneskôr do 2.12.2022
Antivírusové riešenie pre koncové body a servery :
- podporované klientske platformy - OS: Windows, Linux, MacOS, Android, všetko v slovenskom jazyku
- natívna podpora architektúr pre platformy Windows a MacOS: x86, x64, ARM64
- antimalware, antiransomware, antispyware a anti-phishing na aktívnu ochranu pred všetkými typmi hrozieb
- personálny firewall pre zabránenie neautorizovanému prístupu k zariadeniu so schopnosťou automatického prebratia pravidiel z brány Windows Firewall
- modul pre ochranu operačného systému a elimináciu aktivít ohrozujúcich bezpečnosť zariadenia s možnosťou definovať pravidlá pre systémové registre, procesy, aplikácie a súbory
- ochrana pred neautorizovanou zmenou nastavenia / vyradenie z prevádzky / odinštalovaním antimalware riešenia a kritických nastavení a súborov operačného systému

- aktívna aj pasívna heuristická analýza pre detekciu doposiaľ neznámych hrozieb
- systém na blokáciu exploitov zneužívajúcich zero-day zraniteľností, ktorý pokrýva najpoužívanejšie vektory útoku: sieťové protokoly, Flash Player, Javu, Microsoft Office, webové prehliadače, e-mailových klientov, PDFčítačky…
- systém na detekciu malwaru už na sieťovej úrovni poskytujúci ochranu aj pred zneužitím zraniteľností na sieťovej vrstve.
- kontrola šifrovaných spojení (SSL, TLS, HTTPS, IMAPS…)
- anti-phishing so schopnosťou detekcie homoglyph útokov
- kontrola RAM pamäte pre lepšiu detekciu malwaru využívajúceho silnú obfuskáciu a šifrovanie
- cloud kontrola súborov pre urýchlenie skenovania fungujúca na základe reputácie súborov
- kontrola súborov v priebehu sťahovania pre zníženie celkového času kontroly
- kontrola súborov pri zapisovaní na disk a extrahovaní archivačných súborov
- detekcia s využitím strojového učenia
- funkcia ochrany proti zapojeniu do botnetu pracujúca s detekciou sieťových signatúr
- ochrana pred sieťovými útokmi skenujúca sieťovú komunikáciu a blokujúca pokusy o zneužitie zraniteľností na sieťovej úrovni
- kontrola s podporou cloudu pre odosielanie a online vyhodnocovanie neznámych a potenciálne škodlivých aplikácií
- lokálny sandbox
- modul behaviorálnej analýzy pre detekciu správania nových typov ransomwaru
- systém reputácie pre získanie informácií o závadnosti súborov a URL adries
- cloudový systém na detekciu nového malwaru ešte nezaneseného v aktualizáciách signatúr
- technológia na detekciu rootktitov obvykle sa maskujúcich za súčasti operačného systému
- skener firmvéru BIOSu a UEF
- skenovanie súborov v cloude OneDrive
- funkcionalita pre klientov MS Windows - Antimalware, Antispyware, Personal Firewall, Personal IPS, Application Control, Device control, Security Memory (zabraňuje útokom na bežiace aplikácie), kontrola integrity systémových komponentov
- funkcionalita pre klientov MacOS - Personal Firewall, Device control, autoupgrade
- možnosť aplikovania bezpečnostných politík aj v offline režime na základe definovaných podmienok
- ochrana proti pokročilým hrozbám (APT) a 0-day zraniteľnostiam
- podpora automatického vytvárania dump súborov na stanici na základe nálezov
- okamžité blokovanie/mazanie napadnutých súborov na stanici (s možnosťou stiahnutia administrátorom na ďalšiu analýzu)
- duálny aktualizačný profil pre možnosť sťahovania aktualizácií z mirroru v lokálnej sieti a zároveň vzdialených serverov pri nedostupnosti lokálneho mirroru (pre cestujúcich používateľov s notebookmi)
- možnosť definovať webové stránky, ktoré sa spustia v chránenom režime prehliadača, pre bezpečnú prácu s kritickými systémami alebo internetovým bankovníctvo
- aktívne ochrany pred útokmi hrubou silou na protokol SMB a RDP
- možnosť zablokovania konkrétnej IP adresy po sérii neúspešných pokusov o prihlásenie pre protokoly SMB a RDP s možnosťou výnimiek vo vnútorných sieťach
- automatické aktualizácie bezpečnostného softvéru s možnosťou odloženia reštartu stanice
- „zmrazenie“ na požadovanej verzii – produkt je možné nakonfigurovať tak, aby nedochádzalo k automatickému povyšovaniu majoritných a minoritných verzií najmä na staniciach, kde sa vyžaduje vysoká stabilita
Integrovaná cloudová analýza neznámych vzoriek :
- funkcia cloudového sandboxu je integrovaná do produktu pre koncové a serverové zariadenia, tzn. Cloudový sandbox nemá vlastného agenta, nevyžaduje inštaláciu ďalších komponentov či už v rámci produktu alebo implementácie HW prvku do siete
- sandbox umožňujúci spustenie vzoriek malwaru pre: Windows, Linux
- možnosť využitia na koncových bodoch a serveroch pre aktívnu detekciu škodlivých súborov
- analýza neznámych vzoriek v rade jednotiek minút
- optimalizácia pre znemožnenie obídenia anti-sandbox mechanizmami
- schopnosť analýzy rootkitov a ransomvéru
- schopnosť detekcie a zastavenie zneužitia alebo pokusu o zneužitie zero day zraniteľnosti

- riešenie pracuje s behaviorálnou analýzou
- kompletný výsledok o zanalyzovanom súbore vrátane informácie o nájdenom i nenájdenom škodlivom správaní daného súboru
- manuálne odoslanie vzorky do sandboxu
- možnosť proaktívnej ochrany, kedy je potenciálna hrozba blokovaná, pokiaľ nie je známy výsledok analýzy zo sandboxu
- neobmedzené množstvo odosielaných súborov
- všetka komunikácia prebieha šifrovaným kanálom
- okamžité odstránenie súboru po dokončení analýzy v cloudovom sandboxe
- možnosť voľby, aké kategórie súborov do cloudového sandboxu budú odchádzať (spustiteľné súbory, archívy, skripty, pravdepodobný spam, dokumenty atp.)
- veľkosť odoslaných súborov do cloudového sandboxu môže dosahovať až 64MB
- výsledky analyzovaných súborov sú dostupné a automatizovane distribuované všetkým serverom a staniciam naprieč organizáciou, tak aby nedochádzalo k duplicitnému testovaniu
Šifrovanie celých diskov :
- podpora platforiem Windows a MacOS
- správa cez centrálny manažment
- unikátna technológia pre platformu Windows (nevyužíva sa BitLocker)
- podpora Pre-Boot autentizácie
- podpora TMP modulu
- podpora Opal samošifrovacích diskov
- možnosť definovať počet chybne zadaných pokusov
- možnosť definovať zložitosť a dĺžku autentizačného hesla
- možnosť obmedziť platnosť autentizačného hesla
- podpora okamžitého zmazania šifrovacieho kľúča a následné uzamknutie počítača
- recovery z centrálnej konzoly
Management konzola pre správu všetkých riešení v rámci ponúkaného balíka :
- webová konzola
- možnosť inštalácie na Windows aj Linux
- predpripravená virtual appliance pre virtuálne prostredie VMware, Microsoft Hyper-V a Microsoft Azure, Oracle Virtual Box
- server/proxy architektúra pre sieťovú pružnosť – zníženie záťaže pri sťahovaní aktualizácií detekčných modulov výrobcu
- možnosť prebudenia klientov pomocou Wake On Lan
- vzdialené vypnutie, reštart počítača alebo odhlásenie všetkých užívateľov
- možnosť konfigurácie virtual appliance cez užívateľsky prívetivé webové rozhranie Webmin
- nezávislý manažment agent pre platformy Windows, Linux a MacOS
- management agent pre architektúry na platformy Windows a MacOS x86, x64, ARM64
- nezávislý agent (pracuje aj offline) vzdialenej správy pre zabezpečenie komunikácie a ovládania operačného systému klienta
- offline uplatňovanie politík a spúšťanie úloh pri výskyte definovanej udalosti (napríklad: odpojenie od siete pri nájdení škodlivého kódu)
- administrácia v najpoužívanejších jazykoch vrátane slovenčiny
- široké možnosti konfigurácie oprávnení administrátorov (napríklad možnosť správy iba časti infraštruktúry, ktoré konkrétnemu administrátorovi podlieha)
- zabezpečenie prístupu administrátorov do vzdialenej správy pomocou 2FA
- podpora štítkov/tagovania pre jednoduchšiu správu a vyhľadávanie
- správa karantény s možnosťou vzdialeného vymazania / obnovenia / obnovenia a vylúčenia objektu z detekcie
- vzdialené získanie zachyteného škodlivého súboru z klienta
- detekcia nespravovaných (rizikových) počítačov komunikujúcich na sieti
- podpora pre inštalácie a odinštalácie aplikácií 3. strán

- vyčítanie informácií o verziách softvéru 3. strán
- možnosť vyčítať informácie o hardvéri na spravovaných zariadeniach (CPU, RAM, diskové jednotky, grafické karty..)
- možnosť vyčítať sériové číslo zariadenia
- možnosť vyčítať voľné miesto na disku
- detekcia aktívneho šifrovania BitLocker na spravovanej stanici
- zobrazenie časovej informácie o poslednom boote stanice
- odoslanie správy na počítač / mobilné zariadenie, ktoré sa následne zobrazí užívateľovi na obrazovke
- vzdialená odinštalovanie antivírusového riešenia 3. strany
- vzdialené spustenie akéhokoľvek príkazu na cieľovej stanici pomocou Príkazového riadka
- dynamické skupiny pre možnosť definovania podmienok, za ktorých dôjde k automatickému zaradeniu klienta do požadovanej skupiny a automatickému uplatneniu klientskej úlohy
- automatické zasielanie upozornení pri dosiahnutí definovaného počtu alebo percent ovplyvnených klientov (napríklad: 5 % všetkých počítačov / 50 klientov hlási problémy)
- podpora SNMP Trap, Syslogu a qRadar SIEM
- podpora formátov pre Syslog správy: CEF, JSON, LEEF
- podpora inštalácie skriptom - *.bat, *.sh, *.ini (GPO, SSCM…)
- rýchle pripojenie na klienta pomocou RDP z konzoly pre vzdialenú správu
- reportovanie stavu klientov chránených inými bezpečnostnými programami
- schopnosť zaslať reporty a upozornenia na e-mail
- konzola podporuje multidoménové prostredie (schopnosť pracovať s viacerými AD štruktúrami)
- konzola podporuje multitenantné prostredie (schopnosť v jednej konzole spravovať viac počítačových štruktúr)
- podpora VDI prostredia (Citrix, VMware, SCCM, apod)
- podpora klonovania počítačov pomocou golden image
- podpora inštancií klonov
- podpora obnovy identity počítača pre VDI prostredie na základe FQDN
- možnosť definovať viacero menných vzorov klonovaných počítačov pre VDI prostredie
- pridanie zariadenia do vzdialenej správy pomocou: synchronizácia s Active Directory, ručné pridanie pomocou podľa IP adresy alebo názvu zariadenia, pomocou sieťového skenu nechránených zariadení v sieti, Import cez csv súbor

Technické vlastnosti	**Jednotka**	**Minimum**	**Maximum**	**Presne**
Dĺžka licencie	mesiac			36
Počet stolových a prenosných počítačov	kus			275
Technické vlastnosti	**Hodnota/Charakteristika**			

2.3 Osobitné požiadavky na plnenie:

Názov
Vrátane dopravy na miesto plnenia
Vrátane inštalácie na mieste plnenia.
Dodávateľ predloží do 3 pracovných dní od uzavretia zmluvy na EKS elektronický rozpis položiek tovaru v zložení: názov tovaru, označenie výrobku/ opis tovaru, cena jednotlivého tovaru za ks bez DPH, cena jednotlivého tovaru za ks s DPH, cena celkom bez DPH, cena celkom s DPH.
Obstarávateľ požaduje do 3 pracovných dní od vygenerovania zmluvy na EKS predložiť kontaktné údaje osoby, ktorá je za dodávateľa oprávnená vo veciach plnenia zmluvy.
Objednávateľ má nárok na zmluvnú pokutu vo výške 300 €za každé aj opakované takéto porušenie tejto zmluvy.
Samotné antivírusové riešenie t j. samotná aplikácia na koncovom zariadení dostupná v slovenskom jazyku, príp. v českom jazyku
Poskytnutie zľavy pre verejnú správu resp. samosprávu

Do ceny obstarávanej softvérovej licencie vo všeobecnosti musia byť zahrnuté celkové náklady a to hlavne: náklady na podporu a údržbu softvéru (ročný poplatok výrobcovi softvéru, ak je potrebný) a náklady na záruky spojené s prevádzkou softvéru.
Objednávateľ neposkytuje preddavky ani zálohy. Dodávateľ je oprávnený fakturovať len tovar, ktorý bol Objednávateľom podľa dodacieho listu skutočne prevzatý. Dodací list podpísaný oprávneným zástupcom Objednávateľa bude prílohou faktúry. Splatnosť faktúry, ktorá musí spĺňať náležitosti daňového dokladu je 30 dní odo dňa jej doručenia objednávateľovi.
Platba sa uskutoční po dodaní a prevzatí tovaru na základe vystavenej faktúry, ktorej súčasťou bude dodací list potvrdenýobjednávateľom.
Ak je Dodávateľ identifikovaný pre DPH v inom členskom štáte EÚ a tovar bude do SR prepravený z iného členského štátu EÚ, tento Dodávateľ nebude pri plnení Zmluvy fakturovať DPH. Vo svojej Kontraktačnej ponuke však musí uviesť príslušnú sadzbu a výšku DPH podľa zákona č. 222/2004 Z.z. a cenu vrátane DPH. Objednávateľ nie je zdaniteľnou osobou a v tomto prípade je/bude registrovaný pre DPH podľa § 7 zákona č. 222/2004 Z.z. a bude povinný odviesť DPH v SR podľa zákona č. 222/2004 Z.z..

Názov	Upresnenie

2.4 Prílohy opisného formulára Zmluvy:

Popis	Názov súboru

III. Zmluvné podmienky

3.1 Miesto plnenia Zmluvy:

Štát: Slovenská republika
Kraj:
Okres:
Obec:
Ulica: Mesto Trenčín , Mierové nám1/2,911 64 Trenčín

3.2 Čas / lehota plnenia zmluvy:

25.11.2022 12:41:00 - 09.12.2022 12:51:00

3.3 Dodávané množstvo/ rozsah zmluvného plnenia:

Jednotka: celok v zmysle vyššie uvedených požiadaviek
Požadované množstvo: 1,0000

3.4 Práva a povinnosti zmluvných strán podľa tejto Zmluvy sa spravujú Obchodnými podmienkami elektronickej platformy verzia 1.2, účinná odo dňa 3.11.2022 , ktoré tvoria neoddeliteľnú prílohu tejto Zmluvy.

IV. Zmluvná cena

4.1 Celková cena predmetu Zmluvy bez DPH: 5 916,67 EUR

4.2 Sadzba DPH: 20,00

4.3 Celková cena predmetu Zmluvy vrátane DPH: 7 100,00 EUR

V. Záverečné ustanovenia

5.1 Táto Zmluva bola uzavretá automatizovaným spôsobom v rámci Elektronického kontraktačného systému a v zmysle Obchodných podmienok elektronickej platformy verzia 1.2, účinná odo dňa 03.11.2022, ktoré tvoria jej prílohu č. 1.

5.2 Táto Zmluva nadobúda platnosť dňom jej uzavretia a účinnosť za podmienok definovaných v Obchodných podmienkach elektronickej platformy uvedených v bode 5.1 tejto zmluvy.

5.3 Táto Zmluva vrátane jej príloh predstavuje úplnú dohodu zmluvných strán o jej predmete. Vedľajšie dohody k tejto zmluve neexistujú.

5.4 Táto Zmluva je vyhotovená v elektronickej podobe v štyroch vyhotoveniach, po jednom pre každú zmluvnú stranu, jedno vyhotovenie bude zaslané na zverejnenie v Centrálnom registri zmlúv Úradu vlády Slovenskej republiky a jedno bude zverejnené v Centrálnom registri zmlúv Trhoviska.

5.5 Túto Zmluvu bude možné meniť a dopĺňať za podmienok stanovených príslušnými všeobecne záväznými právnymi predpismi len vo forme písomného a číslovaného dodatku podpísaného oboma zmluvnými stranami.

5.6 Táto Zmluva má nasledovné prílohy:
Príloha č.1 Obchodné podmienky elektronickej platformy verzia 1.2, účinná odo dňa 03.11.2022, https://portal.eks.sk/SpravaOpet/Opet/VerejnyDetail/

Príloha č.2 Vlastný návrh plnenia zákazky Z202214146

V Bratislave, dňa 23.11.2022 13:58:01

Objednávateľ:
Mesto Trenčín
konajúci prostredníctvom osoby poverenej zastupovať Objednávateľa v rámci elektronického trhoviska

Dodávateľ:
AUTOCONT s.r.o.
konajúci prostredníctvom osoby poverenej zastupovať Dodávateľa v rámci elektronického trhoviska