LICENČNÍ SMLOUVA

uzavřená dle ustanovení § 2358 a násl. zák. č. 89/2012 Sb., občanského zákoníku., ve znění pozdějších předpisů
ev.č. nabyvatele: 62-2-6230/2018

Smluvní strany:

STOFCOM s.r.o.
Sídlo: Žebětínská 821/70, Kohoutovice, 623 00 Brno
IČO: 25317083
DIČ: CZ25317083
Bankovní spojení: Fio Banka
Číslo účtu: 2000609560/2010
Zapsaná v obchodním rejstříku vedeném Krajským soudem v Brně, oddíl C, vložka C 24979
Zastoupená: Ing. Ondřejem Fialou, jednatelem

(dále jen „Poskytovatel")

a

Česká republika-Hasičský záchranný sbor Jihomoravského kraje
se sídlem: Zubatého 685/1, 614 00 Brno-sever
IČO: 70884099
DIČ: CZ70884099, není plátce DPH
Číslo účtu: 10039881 / 0710
Zastoupená: plk. Ing. Jiřím Pelikánem, krajským ředitelem

(dále jen „Nabyvatel")

uzavírají následující licenční smlouvu:

I.

Předmětem této smlouvy je úplatné poskytnutí práva k užívání antivirového systému ESET Secure Office Plus na 600 počítačích Nabyvateli, k užívání aktualizace virové báze a programových komponent antivirového systému, a dále poskytnutí technické podpory (dále jako „antivirový systém " nebo „předmět smlouvy") po dobu 4 let od účinnosti smlouvy. Podrobná specifikace předmětu smlouvy je uvedena v Příloze č. 1 této smlouvy.

II.

1. Nabyvatel je oprávněn předmět smlouvy užívat na takovém počtu počítačů, který je specifikován v článku I.
2. K užívání předmětu smlouvy je oprávněn pouze Nabyvatel. Nabyvatel není oprávněn převést, postoupit nebo přenechat právo na užívání předmětu smlouvy třetím osobám.

3. Aktualizace virové báze budou uskutečňovány prostřednictvím umožnění internetového přístupu Nabyvatele do databáze Poskytovatele po 24 hodin denně, 365 dní v roce, ve které bude Poskytovatel provádět veškeré aktualizace a Nabyvatel bude tyto aktualizace oprávněn automaticky stahovat na svá vlastní PC.

III.

1. Za poskytnutí práva k užívání antivirového systému spolu s dodávanými aktualizacemi dle této smlouvy zaplatí Nabyvatel Poskytovateli celkovou částku 599.900,- Kč (slovy: pětsetdevadesátdevěttisícdevětsetkorunčeských) + 21% DPH, celkem včetně DPH 725.879,- Kč (slovy: sedmsetdvacetpěttisícosmsetsedmdesátdevětkorunčeských).
2. Na uvedenou částku vystaví Poskytovatel Nabyvateli ihned po účinnosti smlouvy fakturu se splatností 30 dnů. Po doručení účinné smlouvy Nabyvatelem Poskytovateli je Poskytovatel povinen neprodleně, nejpozději do 3 pracovních dnů, poskytnout Nabyvateli práva k užívání předmětu smlouvy. Nesplnění výše uvedených podmínek chápou obě smluvní strany za podstatné porušení smlouvy, které může vést k odstoupení od smlouvy.
3. Strany této smlouvy si sjednávají pro případ, že poskytovatel neposkytne v řádné lhůtě podle čl. III. odst. 2 Nabyvateli práva k užívání předmětu smlouvy povinnost Poskytovatele zaplatit Nabyvateli smluvní pokutu ve výši 0,3 % z celkové ceny za každý i započatý kalendářní den prodlení.
4. V případě, že Nabyvatel ve lhůtě splatnosti nezaplatí Poskytovateli úhradu za užívání antivirového systému stanovenou v odst. 1 a 2 tohoto článku, je Poskytovatel oprávněn znemožnit Nabyvateli antivirový systém aktualizovat.
5. Při nedodržení termínu splatnosti řádně vystaveného daňového dokladu Nabyvatelem je Poskytovatel oprávněn účtovat úrok z prodlení za splnění podmínky podle § 1968 ve výši podle § 1970 občanského zákoníku.

IV.

Nabyvatel je oprávněn užívat antivirový systém podle této smlouvy po dobu 4 let počínaje dnem zpřístupnění předmětu smlouvy k užívání, a to za podmínky uhrazení částky smluvené v článku III. odst. 1.

V.

1. Poskytovatel nepřebírá zodpovědnost za jakékoli újmy na jmění nebo nemajetkové újmy způsobené Nabyvateli nebo třetím osobám kombinací vlivu počítačových infiltrací, jiného software, hardware a použití, případné nepoužití, nebo nemožnosti použít předmět smlouvy. Poskytovatel nezodpovídá ani za újmy, které by mohly vzniknout v souvislosti s užíváním předmětu této licenční smlouvy.
2. Poskytovatel je však povinen za Nabyvatele úplně a bez přispění Nabyvatele vyřídit a urovnat jakékoli oprávněné požadavky třetích osob vyplývající z případných autorských práv (jejich možného porušení, atp.) k antivirovému systému.

VI.

1. Nabyvatel se zavazuje nepoškozovat jakkoliv přímo i nepřímo dobrou pověst Poskytovatele a poskytnutého antivirového systému užívaného ve smyslu této smlouvy a oznamovat Poskytovateli veškeré poznatky, které při využívání antivirového systému získal a které by mohly mít vliv na případné zlepšení tohoto systému nebo by mohly mít vliv na vznik případné škody s provozováním tohoto systému spojené.
2. Způsob a metody činnosti antivirového systému jsou předmětem obchodního tajemství. Nabyvatel není oprávněn zejména používat metody zpětného inženýrství s cílem určit myšlenky nebo principy, které jsou základem jakékoli části programu antivirového systému.

VII.

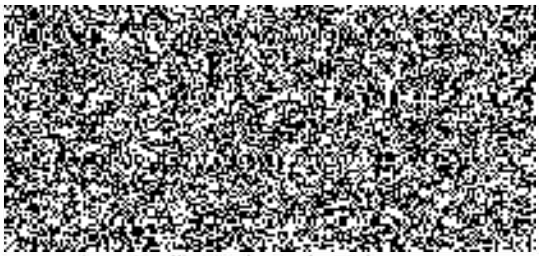
1. Obě smluvní strany se dohodly, že případné vzájemné spory vzniklé z této smlouvy budou přednostně řešeny smírnou cestou vzájemným jednáním a nebude-li dosaženo dohody, bude spor předložen k rozhodnutí místně a věcně příslušnému soudu podle českého práva a věc se bude posuzovat podle právních předpisů platných v České republice.
2. Nastanou-li u některé ze stran okolnosti bránící řádnému plnění ze závazku zřízeného touto smlouvou, je povinna to bez zbytečného odkladu oznámit druhé straně.
3. Veškeré dohody učiněné před podpisem této smlouvy a v jejím obsahu nezahrnuté, pozbývají dnem podpisu smlouvy platnosti bez ohledu na funkční postavení osob, které předsmluvní ujednání učinily.
4. Veškeré změny a doplňky této smlouvy musí mít písemnou formu a budou sjednávány formou postupně číslovaných dodatků k této smlouvě.
5. Licence udělena touto smlouvu nepřechází na případné právní nástupce kterékoli ze smluvních stran a bez předchozího souhlasu Poskytovatele je také nepostupitelná.
6. Tato Smlouva je platně uzavřená dnem připojení podpisu zástupce poslední ze smluvních stran. Smlouva nabývá účinnosti dnem jejího uveřejnění v registru smluv ve smyslu zákona č. 340/2015 Sb., o zvláštních podmínkách účinnosti některých smluv, uveřejňování těchto mluv a o registru smluv (zákon o registru smluv), ve znění pozdějších předpisů. Uveřejnění Smlouvy v registru smluv zajistí Nabyvatel.
7. Smlouva může být ukončena:
   a) písemnou dohodou smluvních stran;
   b) odstoupením od Smlouvy kteroukoliv ze smluvních stran pro porušení této Smlouvy druhou smluvní stranou podstatným způsobem. Účinky odstoupení od této smlouvy nastanou dnem, kdy bude písemné odstoupení strany odstupující druhé straně doručeno;
8. Tato smlouva se vyhotovuje ve dvou stejnopisech, přičemž Poskytovatel a Nabyvatel obdrží po jednom stejnopise.
9. Tato smlouva se řídí úpravou dle zák. č. č. 89/2012 Sb., občanského zákoníku, ve znění pozdějších předpisů. Veškeré údaje a informace, které si strany sdělily při uzavírání této smlouvy, jsou považovány za důvěrné, přičemž žádná ze stran je nesmí zpřístupnit či

sdělit třetí osobě ani je použít v rozporu s jejich účelem pro potřeby vlastní. Poruší-li některá strana tuto povinnost a obohatí-li se tím, vydá druhé straně to, oč se obohatila.

10. Smluvní strany po přečtení této smlouvy prohlašují, že souhlasí s jejím obsahem, že smlouva byla sepsána určitě, srozumitelně, na základě jejich pravé, svobodné a vážné vůle, bez nátlaku na některou ze stran. Na důkaz toho připojují své podpisy.

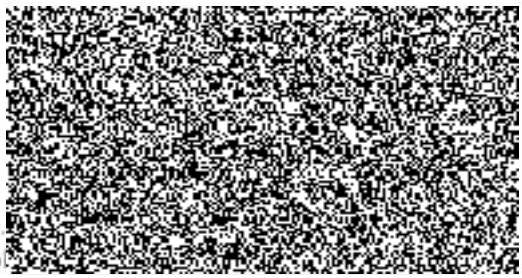
11. Příloha č. 1 – Nabídka a Podrobná specifikace předmětu smlouvy

V Brně dne.....



Ing. Ondřej Fiala, jednatel
Poskytovatel

V Brně dne.....



...
p...
Nabyvatel

NABÍDKA

STOFCOM s.r.o., Žebětínská 821/70, 623 00 Brno - Kohoutovice
Tel.: 547221591
e-mail: stofcom@stofcom.cz, www.stofcom.cz

PRO:
Hasičský záchranný sbor Jihomoravského kraje
Zubatého 685/1
61400 Brno

TEL.: .

ČÍSLO: **NAB1801421**
DATUM: 12.11.2018
VYPRACOVAL: [redacted]
TEL.:
E-MAIL: netopilik@stofcom.cz

Na základě Vaší potávky zasíláme nabídku.

POZICE	NÁZEV A POPIS	MNOŽSTVÍ	CENA / MJ BEZ DPH	CENA CELKEM BEZ DPH	DPH
001	**Nová licence, ESET Secure Office Plus, 4 roky, 600 stanic**	1 ks	599 900,00 Kč	599 900,00 Kč	21%

CELKEM BEZ DPH:	599 900,00 Kč
CELKEM DPH 21%	125 979,00 Kč
CELKEM VČETNĚ DPH:	725 879,00 Kč

V ceně zboží je zahrnut recyklační poplatek a autorské odměny v zákonné výši.
Další informace Vám rádi sdělíme na naší provozovně.

[redacted]

Příloha č. 1 smlouvy – Podrobná specifikace předmět plnění

Produkt

- Podpora operačních systémů MS:

– Windows 7 a vyšší,

– Windows server 2008 R1 a vyšší.

- **Antivirový klient pro systémy:**

– Windows,

– Linux,

– macOS,

– Android.

- Real-Time ochrana před všemi typy PUA a malwaru:

– viry,

– červy,

– trojskými koňmi (backdoor, adware, spyware, rootkit, bootkit, ransomware…).

- **Správa zařízení pro Windows, macOS a Linux umožňující blokaci externích zařízení a médií s podporou whitelistování dle:**

– výrobce, modelu nebo sériového čísla,

– uživatelů nebo skupin (např. administrátorů) v AD,

– lokálního času.

- Možnost blokace přístupu na definované weby nebo domény.

- **Nativní 64-bitové jádro.**

Technologie

- Antivirus, antispyware a anti-phishing pro aktivní ochranu před všemi typy hrozeb.

- IDPS pro ochranu operačního systému a eliminaci aktivit ohrožující bezpečnost zařízení.

- Aktivní i pasivní heuristická analýza pro detekci dosud neznámých hrozeb.

• Systém pro blokaci exploitů využívajících zero-day zranitelností, jenž pokrývá nejpoužívanější vektory útoku:

– Flash Player,

– Javu,

– Microsoft Office,

– webové prohlížeče,

– e-mailové klienty,

– PDF čtečky…

• Pokročilá kontrola RAM paměti pro lepší detekci malwaru využívající silnou obfuskaci a šifrování.

• Možnost zapnutí detekce potenciálně nechtěných, zneužitelných a podezřelých aplikací.

• Cloud kontrola souborů pro urychlení skenování pracující na základě reputace souborů.

• Kontrola souborů v průběhu stahování pro snížení celkového času kontroly.

• Funkce pro ochranu před skriptovými útoky využívajícími:

– JavaScript,

– Windows PowerShell,

– Windows Script Host.

• Funkce ochrany proti zapojení do botnetu pracující s detekcí síťových signatur.

• Ochrana před síťovými útoky skenující síťovou komunikaci a blokující pokusy o zneužití zranitelností na síťové úrovni.

• Kontrola s podporou cloudu pro odesílání a online vyhodnocování neznámých a potenciálně škodlivých aplikací.

• Lokální i cloudový sandbox.

• Speciální modul behaviorální analýzy pro detekce nových typů ransomwaru.

• Systém reputace a cache pro získání informací o závadnosti stahovaných souborů a URL adres.

• Cloudový systém pro detekci nového malwaru ještě nezaneseného v aktualizacích signatur.

• Technologie pro detekci rootkitů obvykle se maskujících za součásti operačního systému.

• Skener firmwaru BIOSu a UEFI.

• Skenování souborů v cloudu (OneDrive & Office 365).

Ostatní

- Podpora Microsoft NAP.

- Velmi nízké systémové nároky umožňující bezproblémové použití i na málo výkonných zařízeních:

– 400 MHz 32-bit (x86) / 64-bit (x64) procesor,

– 128 MB RAM,

– 320 MB volného místa na disku,

– Super VGA (800 x 600).

- Možnost odložení aktualizací a běžných klientských úloh pro lepší využití systémových prostředků.

- **Provádění kontrol při nečinnosti zařízení:**

– vypnuté obrazovce,

– aktivním spořiči obrazovky,

– uzamčení počítače,

– odhlášení uživatele.

- **Šetření baterie notebooku – možnost odložení kontroly / provádění aktualizací, pokud je zařízení napájeno z baterie.**

- Ovládání bezpečnostního programu pomocí Příkazového řádku.

- Možnost řízení šířky pásma pro stahování aktualizací.

- **HIPS s možností definovat pravidla pro systémové registry, procesy, aplikace a soubory.**

- Možnost vrácení i odložení aktualizací modulů.

- Možnost instalovat plnohodnotné antivirové řešení na virtuální stanici/server.

- Modulární instalace.

- Automatická synchronizace bezpečnostních produktů v clusteru.

- **Bezagentové zabezpečení pro VMware vShield a NSX.**

- Možnost importu/exportu nastavení.

- Prezentační režim umožňující potlačení méně důležitých upozornění při práci v celoobrazovkovém režimu aplikace.

- Možnost tvorby výjimek na procesy.

- Ochrana před neautorizovanou změnou nastavení / vyřazení z provozu / odinstalací antimalware řešení a kritických nastavení a souborů operačního systému.

• Možnost vzdáleného definování akce při připojení výměnných médií (kontrolovat, nekontrolovat, nechat na uživateli).

• **Možnost využití sdílené reputační cache v rámci lokální sítě (umožňuje přeskočení skenování stejných souborů, které již byly zkontrolované na jiném zařízeních a tím výrazně zrychlit kontrolu celé sítě).**

• Duální aktualizační profil pro možnost stahování aktualizací z mirroru v lokální síti a zároveň vzdálených serverů při nedostupnosti lokálního mirroru (vhodné pro cestující uživatele s notebooky).

• Kontrola šifrovaných spojení (SSL, TLS, HTTPS, IMAPS…).

• Možnost odesílání e-mailových upozornění a událostí přímo z klienta.

• **Integrovaný komplexní diagnostický nástroj umožňující řešit problémy s infiltrací, jakožto i jiné softwarové a hardwarové nekorektní chování (obsahuje informace procesech, službách, síťových připojeních, ovladačích, problémových položkách v registrech…).**

• **Upozornění při připojení k nezabezpečené bezdrátové síti nebo síti se slabým zabezpečením, jejíž šifrování lze snadno prolomit.**

• **Využití Microsoft Antimalware Scan Interface (AMSI) pro kontrolu skriptů (PowerShell, wscript.exe a cscript.exe).**

• **Podpora Protected Services – službu produktu je možné chránit proti nechtěné modifikaci standardní součástí operačního systému.**

Vzdálená správa

• Webová konzole.

• **Možnost instalace na Windows i Linux.**

• **Předpřipravená virtual appliance pro virtuální prostředí VMware**• Možnost konfigurace linuxové virtual appliance přes uživatelsky přívětivé webové rozhraní Webmin.

• **Nezávislý agent (pracuje i offline) vzdálené správy pro zajištění komunikace a ovládání operačního systému klienta a bezpečnostního programu.**

• **Offline uplatňování politik a spouštění úloh při výskytu definované události (například: odpojení od sítě při nalezení škodlivého kódu).**

• **Server/proxy architektura pro síťovou pružnost – snížení zátěže při stahování aktualizací detekčních modulů výrobce.**

• **Administrace v angličtině a češtině.**

• Instalace a aktualizace bezpečnostního programu.

• **Široké možnosti konfigurace oprávnění administrátorů (například možnost správy pouze části infrastruktury, které konkrétnímu administrátorovi podléhá).**

• Podpora mirroru.

- Zabezpečení přístupu administrátorů do vzdálené správy pomocí 2FA.

- Možnost přihlašování administrátorů pomocí doménových účtů.

- Instalace a odinstalace aplikací 3. stran.

- Vzdálená aktivace bezpečnostního programu.

- **Jedna konzole vzdálené správy pro konfiguraci bezpečnostních produktů na mobilní zařízení (MDM), desktopové systémy, souborové servery, mail servery i ochranu gateway.**

- Export/import konfigurace bezpečnostního programu z klienta.

- Jednorázové testování virtuálních stanic i bez nainstalovaného bezpečnostního programu.

- Správa karantény s možností vzdáleného vymazání / obnovení / obnovení a vyloučení objektu z detekce.

- **Vzdálené získání zachyceného škodlivého souboru z klienta.**

- Jednoduchá aktualizace serveru pro vzdálenou správu pomocí webového rozhraní správcovské konzole.

- Detekce nespravovaných (rizikových) počítačů komunikujících na síti.

- Vzdálené odebrání licence klientovi.

- **Odeslání zprávy na jakékoli zařízení (počítač, mobilní zařízení…), které se následně zobrazí uživateli na obrazovce.**

- Vzdálená odinstalace antivirového řešení 3. strany.

- Vzdálené spuštění jakéhokoli příkazu na cílové stanici pomocí Příkazového řádku.

- Vzdálený restart/vypnutí cílového klienta.

- U mobilních zařízení dostupné vzdálené:

– nalezení,

– uzamknutí,

– odemknutí,

– siréna,

– vymazání obsahu,

– rozšířený reset do továrního nastavení.

- **Možnost navazování úloh pro zautomatizování činností bez zásahu administrátora. Například: Automatická detekce antiviru 3. strany > automatická odinstalace > automatický zpožděný restart pro možnost uložení rozdělané práce klienta > automatická instalace nového bezpečnostního programu > automatická aktivace nového bezpečnostního programu.**

▪ Koncovému klientovi může administrátor vzdáleně ukončit proces, zablokovat síťového spojení, odstranit klíče z registru, odstranit DNS záznam, odstranit soubor, odstranit naplánovanou úlohu, zastavit a odinstalovat službu…

▪ Dynamické skupiny pro možnost definování podmínek, za kterých dojde k automatickému zařazení klienta do požadované skupiny.

▪ Dynamicky se měnící Dashboard s interaktivními přehledy pro okamžité zjištění stavu spravované sítě.

▪ Responzivní design webové konzole vzdálené správy umožňující management klientů pomocí mobilních zařízení (telefonu/tabletu).

▪ Automatické zasílání upozornění při dosažení definovaného počtu nebo procent ovlivněných klientů (například: 5 % všech počítačů / 50 klientů hlásí problémy).

▪ Podpora SNMP Trap, Syslogu.

▪ Podpora vzdálené instalace skriptem nebo pomocí GPO.

▪ Rychlé připojení na klienta pomocí RDP z konzole pro vzdálenou správu.

▪ Reportování stavu antiviru 3. strany, včetně vzdálené správy (instalace/odinstalace aplikací, vynucování aktualizací OS…) klientů chráněných jinými bezpečnostními programy.

▪ Schopnost zaslat reporty a upozornění na e-mail.

▪ Přidání zařízení do vzdálené správy pomocí:

– synchronizace s Active Directory,

– ruční přidání pomocí dle IP adresy nebo názvu zařízení,

– proprietární technologie pro vyhledání nechráněných zařízení v síti.

▪ Několikaminutové automatické zablokování (IP adresy) přístupu do konzole vzdálené správy po několika neúspěšných pokusech o přihlášení.

▪ Možnost vyčítat informace o hardwaru na spravovaných zařízeních (CPU, RAM, diskové jednotky, grafické karty…).

▪ Schopnost zaslat reporty a upozornění na e-mail.

▪ Přehled o všech souborech z celé sítě, které byly odeslány na servery vendora pro hloubkovou analýzu z důvodu možného výskytu škodlivého kódu.

▪ MDM vzdálené správy podporuje operační systémy:

– Android,

– iOS.

Provozní

• Dodavatel musí mít pro případy rozšíření zabezpečení také řešení pro:

– MDM,

– DLP,

– 2FA,

– šifrování,

– EDR.

• Technická podpora v češtině.

• Technická podpora zdarma 12/5 poskytující pomoc na telefonu / přes e-mail / vzdáleně.

• Možnost dokoupení technické podpory 24/7.

• Možnost osobní návštěvy technika zdarma:

– jednou ročně, 4 hodiny práce na místě,

– školení, konzultace, pomoc s instalací / nasazením / aktualizací / ověřením bezpečnostních politik.

Obchodní

- možnost navýšení počtu zabezpečených koncových prvků kdykoliv v průběhu trvání smlouvy za obdobných technických i cenových podmínek jako v základní smlouvě