OPERATOR ECONOMIC

_____

(*denumirea/numele*)

FORMULAR DE OFERTA

Către

MUNICIPIUL TIMISOARA
BV. C.D.LOGA NR.1, TIMISOARA

1. Examinând documentația de atribuire, subsemnații....., reprezentanți ai ofertantului ..... (*denumirea/numele ofertantului*), ne oferim ca, în conformitate cu prevederile şi cerințele cuprinse în documentația mai sus menționată, sa furnizam **„Upgrade licență antivirus Bitdefender" pentru Primăria Municipiului Timişoara** *(valabilitate licenta- 24 luni)* pentru suma de ..... (*suma în litere şi în cifre*) RON fara TVA, la care se adaugă taxa pe valoarea adăugată în valoare de ..... (*suma în litere şi în cifre*) RON fara TVA.

2. Ne angajăm ca, în cazul în care oferta noastră este stabilită câştigătoare, sa furnizam produsul conform celor mentionate in contract.

3. Ne angajăm sa menținem aceasta oferta valabilă pentru o durata de **45 zile**, şi ea va rămâne obligatorie pentru noi şi poate fi acceptată oricând înainte de expirarea perioadei de valabilitate.

4. Pana la încheierea şi semnarea contractului de achiziție publica aceasta oferta, împreună cu comunicarea transmisă de dumneavoastră, prin care oferta noastră este stabilită câştigătoare, vor constitui un contract angajant între noi.

5. Am înțeles şi consimțim ca, în cazul în care oferta noastră este stabilită ca fiind câştigătoare, sa constituim garanția de buna execuție în conformitate cu prevederile din documentația de atribuire.

6. Înțelegem ca nu sunteți obligați sa acceptați oferta cu cel mai mic pret sau orice alta oferta pe care o puteți primi.

Data .....

.....,

(nume, prenume,semnătură si stampila)

in calitate de ..... legal autorizat să semnez oferta pentru şi în numele ..... (*denumirea/numele operatorului economic)*

Operator economic,

_____

(denumirea/numele)

Modul de <u>prezentare a ofertei tehnice</u> privind atribuirea contractului de furnizare "Upgrade licența antivirus Bitdefender" pentru Primăria Municipiului Timișoara

Prin prezenta documentatie, subsemnatul..... (nume si prenume in clar a persoanei autorizate), reprezentant al ..... (denumirea ofertantului), detaliez concret modul de realizare a acestui contract, in functie de cerintele minime impuse de autoritatea contractanta prin documentatie:

Cerinte impuse de autoritatea contractanta prin documentatie	***Modul de indeplinire de catre ofertant al cerintelor impuse prin documentatie (se va completa de catre ofertant)***
SPECIFICAȚII TEHNICE – pentru update program antivirus BITDEFENDER **A. CONSOLA DE MANAGEMENT** 1. Instalare si configurare: 1. Pachetul de instalare va fi livrat ca o masina virtuala bazata pe sistem de operare Linux securizat care contine toate rolurile sau serviciile necesare. Consola nu va necesita o licenta suplimentara pentru sistemul de operare. Imaginea de tip template se va putea importa in: a. VMware vSphere b. Citrix XenServer c. Microsoft Hyper-V d. Red Hat Enterprise Virtualization e. KVM f. Oracle VM. 2. Consola de management se livreaza cu o baza de date inclusa care este de tip non-relationala, pentru o functionare cat mai rapida, fara a fi nevoie de licente aditionale. 3. Solutia va fi scalabila, astfel ca oricare dintre roluri sau servicii pot fi instalate separat pe mai multe masini virtuale sau pe aceeasi masina virtuala. 4. Masinile de scanare pentru mediile virtuale VMware si Citrix se insteaza la distanta prin task din consola de management, iar pentru alte platforme se descarca separat din interfata web a produsului. 5. Rolurile principale trebuie sa fie cel putin similare cu: Server cu baza de date, Server de comunicatie, Server de actualizare, Server de Web. 6. Solutia va include aditional si un modul de	

balansare (load balancer) pentru cazurile in care mai multe masini virtuale ale componentei de management sunt instalate cu acelasi rol (pentru Load Balancing si performanta/redundanta). 7. Solutia va include un mecanism de configurare a disponibilitatii pentru Serverul cu baze de date (clustering pentru redundanta). Astfel, baza de date se va putea instala de mai multe ori, pe mai multe masini virtuale. 2. Cerinte generale: 1. Interfata consolei de management va fi in limba romana. 2. Interfata clientului de securitate, care se instaleaza pe statii si servere, va fi in limba romana. 3. Manualul de instalare a produsului va fi in limba romana. 4. Manualul de administrare a produsului va fi in limba romana. 5. Solutia va include un modul de update server prin care se asigura actualizarea de produs si a semnaturilor. 6. Solutia va pemite activarea/dezactivarea actualizarilor de produs/semnaturi. 7. Notificarile – prezente in interfata, notificarile necitite sunt evidentiate, trimise catre una sau mai multe adrese de email, alerteaza administratorul in cazul unor probleme majore: licentiere, detectie virusi, actualizari de produs disponibile). 8. Solutia va permite integrarea cu un server Syslog pentru raportarea evenimentelor antimalware. 9. Solutia va permite instalarea serviciului de SMNP prin care se pot raporta statusul masinilor din cadrul componentei de management. 3. Panou de monitorizare si raportare (Dashboard): 1. Rapoartele din panoul de monitorizare vor putea fi configurate specificand numele raportului, tipul raportului, tinta raportului, optiuni specifice pentru orice tip de raport (de exemplu pentru raportul de actualizare - care este intervalul dupa care o statie este considerata neactualizata). 2. Panoul central contine rapoarte pentru toate modulele suportate. 3. Rapoartele din panoul central de comanda permit: adaugarea altor rapoarte, stergerea lor si rearanjarea. 4. Inventarierea retelei – managementul securitatii: 1. Solutia se va integra cu domenii Active Directory multiple, VMware vCenter, Citrix Xen si importa inventarul acestor platforme. 2. Pentru integrarea cu Active Directory, se va putea defini si intervalul (in ore) de sincronizare si forta sincronizarea.	

3. Se permite descoperirea masinilor din Microsoft Hyper-V, Red Hat VM, Oracle VM, KVM. 4. Se permite descoperirea statiilor statii fizice neintegrate in Active Directory (Workgroup) cu ajutorul Network discovery. 5. Solutia va oferi optiuni de cautare, sortare si filtrare dupa numele sistemului, sistem de operare si adresa IP. 6. Solutia va permite instalarea la distanta sau manual a clientilor antimalware pe masini fizice/virtuale. 7. Solutia va permite selectarea modulelor componente atunci cand se creaza pachetul clientului care se instalează pe mașinile fizice/virtuale. 8. Solutia va permite lansarea de task-uri de scanare, actualizare, instalare, dezinstalarea la distanta pentru clientul antimalware. 9. Solutia va oferi posibilitatea de repornire a masinilor fizice de la distanta. 10. Solutia va oferi informatii detaliate despre fiecare task si se fiseaza daca task-ul s-a finalizat sau nu cu succes. 11. Solutia va permite configurarea centralizata a clientilor antimalware prin intermediul politicilor 12. Se vor oferi in consola de management informatii detaliate ale obiectelor din consola: Nume, IP, Sistem de operare, Grup, Politica atribuita, Ultimele actualizare, Versiunea produsului, Versiunea de semnaturi. 5. Politici: 1. Solutia va permite configurarea setarilor clientului antimalware prin intermediul unei singure politici ce contine setari pentru toate module 2. Politica va contine optiuni specifice de activare/dezactivare si configurarea functionalitatilor precum scanarea antimalware la cerere, firewall, controlul accesului la Internet, controlul aplicatiilor, scanarea traficului web,controlul dispozitivelor, power user. 3. Solutia permite aplicarea politicilor pe masini client, grupuri de masini, pool-uri de resourse (VMware), domeniu, unitati organizationale sau useri de active directoy. 4. Politica sa poate fi schimbata automat in functie de: a. User-ul logat pe statie b. IP sau clasa de IP al statiei c. Gateway-ul alocat d. DNS serverul alocat e. Clientul este/nu este in acceasi retea cu infrastructura de management f. Tipul retelei (lan, wireless) 6. Rapoarte: 1. Solutia va contine rapoarte care prezinta	

statusul masinilor clientil din punct de vedere al actualizarilor, fisierelor malware detectate, aplicatiile blocate, site-urilor web blocate. 2. Rapoartele programate pot fi trimise catre un numar nelimitat de adrese de email (nu este nevoie sa aiba un cont in consola de management). 3. Solutia va permite vizualizarea rapoartelor curente programate de administrator. 4. Solutia va permite exportarea rapoartelor in format .pdf si detaliile ca format .csv. 7. Carantina: 1. Solutia va permite restaurarea fisierelor carantinate in locatia originala sau intr-o cale configurabila. 2. Carantina va fi locala, pe fiecare statia administrata si va fi administrata, fie local, fie din consola de magement 3. Permite descarcarea fisierelor carantinate doar pentru masinile virtuale protejate prin modulul mediilor virtuale integrat cu VMware vShield. 8. Utilizatori: 1. Administrarea se va putea face pe baza de roluri. 2. Roluri multiple predefinite: Administrator companie, Administrator retea, Reporter sau rol personalizat. a. Administrator companie: administreaza arhitectura consolei de management; b. Administrator retea: administreaza serviciile de securitate; c. Reporter: monitorizeaza si genereaza rapoarte. 3. Utilizatorii pot fi importati din Microsoft Active Directory sau creati in consola de management. 4. Se va permite configurarea detaliata a drepturilor administrative, permitand selectarea serviciilor si obiectelor pentru care un utilizator poate face modificari. 5. Se va permite deconectarea automata a oricarui tip de utilizator dupa un anumit timp pentru o protectie sporita a datelor afisate in consola de administrare. Acest interval se poate personaliza de administratorul solutiei. 9. Log-uri: 1. Inregistrarea actiunilor utilizatorilor. 2. Se vor oferi informatii detaliate pentru fiecare actiune a unui utilizator. 3. Se va permite filtrarea actiunilor utilizator dupa numele utilizatorului, actiune. 10. Actualizare: 1. Se permite definirea de locatii de actualizare multiple. 2. Se permite activarea/dezactivarea actualizarilor de produs si semnaturi. 3. Se permite actualizarea produsului intr-o retea	

fara acces la Internet. 4. Orice client antivirus sa poata fi configurat sa livreze update-urile catre alt client antivirus 5. Modulul de actualizare din consola de management, permite testarea noilor versiuni de pachete de instalare ale clientului antimalware, inainte de a fi instalate pe toate statiile din retea, evitand posibile probleme ce pot afecta serverele sau statiile critice. 11. Certificate: 1. Accesul la consola de management sa se faca doar prin HTTPS. 2. Serverul web, din consola centrala de management trebuie sa permita importarea de certificate digitale eliberate de o autoritate de certificare autorizata sau proprie organizatiei. 3. Solutia permite afisarea in consola de management informatii despre certificate: nume, autoritatea emitenta, data eliberarii si data expirarii certificatelor eliberate. **B. PROTECTIE STATII SI SERVERE FIZICE/VIRTUALE** 1. Caracteristici generale minimale si eliminatorii: 1. Pentru reducerea la minim a consumului de resurse, solutia antimalware trebuie sa permita instalarea personalizata a modulelor detinute (de exemplu, sa permita instalarea solutiei antimalware fara modulul de control al accesului web, modul de control al dispozitivilelor sau modulul firewall). 2. Cerinte de sistem: • Sisteme de operare pentru statii de lucru: Windows 10, Windows 8, Windows 7, Windows Vista (SP1), Windows XP (SP3), Mavericks (10.9.x), Mountain Lion (10.8.x), Lion (10.7.x) • Sisteme de operare embedded: Windows Embedded 8.1 Industry, Windows Embedded 8 Standard, Windows Embedded Standard 7, Windows Embedded POSReady 7, Windows Embedded Enterprise 7, Windows Embedded POSReady 2009, Windows Embedded Standard 2009, Windows XP Embedded with Service Pack 2, Windows XP Tablet PC Edition • Sisteme de operare pentru servere: Windows Server 2012 R2, Windows Server 2012, Windows Small Business Server (SBS) 2011, Windows Small Business Server (SBS) 2008, Windows Server 2008 R2, Windows Server 2008, Windows Small Business Server (SBS) 2003, Windows Server 2003 R2, Windows Server 2003 with Service Pack 1, Windows Home Server • Sisteme de operare Linux: Red Hat Enterprise Linux / CentOS 5.6 sau mai recent, Ubuntu	

10.04 LTS sau mai recent, SUSE Linux Enterprise Server 11 sau mai recent, OpenSUSE 11 sau mai recent, Fedora 15 sau mai actual and Debian 5.0 sau mai recent. • Sisteme de operare MAC: Mac OS X El Capitan (10.11.x), Mac OS X Yosemite (10.10.5), Mac OS X Mavericks (10.9.5), Mac OS X Mountain Lion (10.8.5) 3. Administrare si instalare remote: 1. Inainte de instalare, administratorul va putea particulariza pachetele de instalare cu modulele dorite: firewall, content control, device control, power user. 2. Instalarea se va putea face in mai multe moduri: a. prin descarcarea directa a pachetului pe statia pe care se va face instalarea; b. prin instalarea la distanta, direct din consola de management 3. Instalarea clientilor la distanta in alte locatii decat cele in care este instalata consola de management se va face prin intermediul unui alt client antivirus existent in locatiile respective pentru a minimiza traficul in WAN. 4. In consola vor fi disponibile informatii despre fiecare statie: numele statiei, IP, sistem de operare, module instalate, politica aplicata, informatii despre actualizari etc. 5. Din consola se va putea trimite o singura politica pentru configurarea integrala a clientului de pe statii/servere. 6. Consola va include o sectiune, „Audit", unde se vor mentiona toate actiunile intreprinse fie de administratori fie de reporteri, cu informatii detaliate: logare, editare, creare, delogare, mutare etc. 7. Posibilitatea creari unui singur pachet de instalare, utilizabil atat pentru sistemele de operare pe 32 de biti cat si pentru cele pe 64 de biti. 8. Posibilitatea creari unui singur pachet de instalare, utilizabil pentru statii (fizice si/sau virtuale), servere (fizice si/sau virtuale), exchange. 9. Posibilitatea de a crea pachetele de instalare de tip web installer sau kit full. 10. Administratorul va putea crea grupuri sau chiar subgrupuri, unde va putea muta statiile/serverele din retea pentru cele care nu sunt integrate domeniu. 11. Permite selectarea clientului care va realiza descoperirea statiilor din retea, altele decat cele integrate in domeniu. 4. Caracteristici si functionalitati principale ale modulului antimalware: 1. Scanarea automata in timp real va putea fi setata sa nu scaneze arhive sau fisiere mai mari de « x » MB, marimea fisierelor putand fi definita de administratorul solutiei,	

2. Definirea pana la 16 nivele de profunzime pentru scanarea in arhive. 3. Scanarea euristica comportamentala prin simularea unui calculator virtual in interiorul caruia sunt rulate aplicatii cu potential periculos protejand sistemul de virusii necunoscuti prin detectarea codurilor periculoase a caror semnatura nu a fost lansata inca. 4. Scanarea oricarui suport de stocare a informatiei (CD-uri, harduri externe, unitati partajate etc). De asemenea, se va putea anula scanarea in cazul in care sunt detectate unitati care au informatii stocate mai mult de « x » MB. 5. Scanarea automata a emailurilor la nivelul statiei de lucru pentru POP3/SMTP. 6. Configurarea cailor ce urmeaza a fi scanate la cerere. 7. Clientii antimalware pentru workstation sa permita definirea unor liste de excludere de la scanarea in timp real si la cerere a anumitor directoare, discuri, fisiere, extensii sau procese. 8. Cu ajutorul unei baze de date complete cu semnaturi de spyware si a euristicii de detectie a acestui tip de programe, produsul va trebui sa ofere protectie anti-spyware. 9. Posibilitatea de configura scanarile programate sa se execute cu prioritate redusa 10. Produsul antimalware poate fi configurat sa foloseasca scanarea in cloud, si partial scanarea locala. Pentru statiile ce nu au suficiente resurse hardware, scanarea se poate face cu o masina de scanare instalata in retea. 11. Administratorul poate personaliza și motoarele de scanare, având posibilitatea de a alege între mai multe tehnologii de scanare: • Scanare locală, când scanarea se efectuează pe stația de lucru locală. Modul de scanare locală este potrivit pentru mașinile puternice, având toate semnăturile și motoarele stocate local. • Scanarea hibrid cu motoare light (Cloud public), cu o amprentă medie, folosind scanarea în cloud și, parțial, semnături locale. Acest mod de scanare oferă avantajul unui consum mai bun de resurse, fără să implice scanarea locală. • Scanarea centralizată în Cloud-ul privat, cu o amprentă redusă, necesitând un server de securitate pentru scanare. În acest caz, nu se stochează local nicio semnătură, iar scanarea este transferată către serverul de securitate. • Scanare centralizată (Scanare în cloud privat cu server de securitate) cu fallback* pe Scanare locală (motoare full) • Scanare centralizată (Scanare în cloud privat cu server de securitate) cu fallback* pe Scanare hibrid (cloud	

public cu motoare light) 12. Pentru o protectie sporita, solutia antimalware trebuie sa aiba 3 tipuri de detectie: bazata pe semnaturi, bazata de comportamentul fisierelor si bazata pe monitorizarea proceselor. 13. Pentru o protectie sporita, solutia antimalware trebuie sa poata scana paginile HTTP. 14. Pentru o mai buna gestionare a antimalware instalat pe statii, produsul va include optiunea de setare a unei parole pentru protectia la dezinstalare. 15. Pentru siguranta utilizatorului, clientul va include un modul de antiphishing. 16. Solutia ofera protectie in timp real pe masinile cu sistem de operare Linux in conformitate cu versiunea de kernel instalata. 17. Pe masinile virtuale parte a unui pool instalarea clientului antimalware se face doar pe masina de tip template, dupa care se recompune pool-ul de masini virtuale. 5. Firewall: 1. Posibilitatea de a configura reguli de firewall pentru aplicatii sau conectivitate. 2. Modulul poate fi instalat/dezinstalat in functie de preferinta administratorului. 3. Posibilitatea de a defini retele de incredere pentru masina destinatie. 6. Carantina: 1. Produsul antimalware sa permita trimiterea automata a fisierelor din carantina catre laboratoarele antimalware ale producatorului. 2. Trimiterea continutului carantinei va putea fi expediat in mod automat, la un interval definit de administrator. 3. Produsul antimalware sa permita stergerea automata a fisierelor carantinate mai vechi de o anumita perioada, pentru a nu incarca inutil spatiul de stocare. 4. Posibilitatea de a restaura un fisier din carantina in locatia lui originala. 5. Modulul de carantina va permite rescanarea obiectelor dupa fiecare actualizare de semnaturi. 7. Protectia datelor: 1. Produsul permite blocarea datelor confidentiale (pin-ul cardului, cont bancar etc) transmise prin HTTP sau SMTP prin crearea unor reguli specifice. 8. Controlul continutului: 1. Consola va avea integrat un modul dedicat controlului accesului la Internet cu urmatoarele particularitati: a. Permite blocarea accesului la Internet pentru anumite masini client sau grupuri de masini. b. Permite blocarea accesului la Internet pe intervale orare.	

c. Permite blocarea paginilor de internet care contin anumite cuvinte cheie. d. Permite controlul accesului numai la anumite pagini de internet specificate de administrator; e. Permite blocarea accesului la anumite aplicatii definite de administrator; f. Permite restrictionarea accesului pe anumite pagini de internet dupa anumite categorii prestabilite (ex: online dating, violenta, pornografie etc). 9. Controlul dispozitivelor: 1. Modulul poate fi instalat/dezinstalat in functie de preferinta administratorului. 2. Modulul va permite controlul urmatoarelor tipuri de dispozitive: a. Bluetooth Devices b. CDROM Devices c. Floppy Disk Drives d. Security Policies 153 e. IEEE 1284.4 f. IEEE 1394 g. Imaging Devices h. Modems i. Tape Drives j. Windows Portable k. COM/LPT Ports l. SCSI Raid m. Printers n. Network Adapters o. Wireless Network Adapters p. Internal and External Storage 3. Modulul va permite configurarea de reguli prin care se vor defini permisiunile pentru dispozitivele conectate la masina client. 4. Modulul va permite configurarea de excluderi pentru diferite tipuri de dispozitive pentru care s-au configurat reguli. 10. Power User: 1. Modulul poate fi instalat/dezinstalat in functie de preferinta administratorului. 2. Modulul permite posibilitatea de a acorda utilizatorilor drepturi de Power User. Utilizatorii vor putea accesa si modifica setarile clientului antimalware dintr-o consola dispobibila local pe masina client. 3. Administratorul va putea suprascrie din consola setarile aplicate de utilizatorii Power User. 11. Actualizare: 1. Posibilitatea efectuarii actualizarii la nivel de statie in mod silentios (fara avertizare). 2. Sistem de actualizare cascadat folosind unul sau mai multe servere de actualizare (cascadate). 3. Actualizarea pentru locatiile remote prin intermediul unui client antimalware care are si rol de server de actualizare.	

C. PROTECTIE SI SECURITATE PENTRU TELEFOANELE MOBILE DE TIP SMARTPHONE

1. Cerinte minime de sistem:
   - Telefoane cu sistem de operare iOS 5+: Apple iPhone si tablete iPad
   - Telefoane cu sistem de operare Android 2.2+

2. Caracteristici:
   1. Permite asocierea unui dispozitiv cu un utilizator din Active Directory.
   2. Instalarea se face prin trimiterea unui email catre utilizator cu detaliile de instalare.
   3. Activarea dispozitivului mobil in consola de management sa se faca prin scanarea unui cod QR.
   4. Pachetele de instalare se vor putea descarca de pe Apple App Store si Google Play.
   5. Se vor putea intreprinde urmatoarele actiuni:
      a. Blocarea dispozitivului;
      b. Deblocarea dispozitivului;
      c. Stergerea datelor si revenirea la setarile din fabrica;
      d. Localizarea dispozitivului;
      e. Scanarea dispozitivului(doar pentru cele cu sistem de operare Android);
      f. Criptarea memoriei dispozitivului(doar pentru cele cu sistem de operare Android).
   6. Consola va permite raportarea dispozitivelor: active, inactive, deconectate, cu sistemul de operare modificat astfel incat utilizatorul sa aiba acces total asupra lui (rooted or jailbroken devices).

3. Setari de securitate:
   1. In cazul in care un dispozitiv nu este conform cu setarile dorite, se vor putea intreprinde automat actiunile:
      a. Ignorare;
      b. Blocarea accesului;
      c. Blocarea dispozitivului;
      d. Stergerea datelor si revenirea la setarile din fabrica;
      e. Stergerea dispozitivului din consola.
   2. Se va putea impune blocarea dispozitivelor cu ajutorul unei parole. Aceasta parola va putea fi configurata sa contina:
      a. Parola simpla sau complexa (in functie de cerintele sistemului de operare);
      b. Numere si litere;
      c. O lungime minima definita de administrator;
      d. Un numar minim de caractere speciale, definit de adiministrator;
      e. Perioada de expirare a parolei. Perioada va putea fi definita de

adiministrator;
   f. Configurarea restrictiei refolosirii parolei;
   g. Numarul de introduceri incorecte a parolei, de catre utilizator;
   h. Perioada de autoblocare a dispozitivului dupa un numar de minute definite de adiministrator.
3. Se vor putea genera mai multe profiluri care vor stabili reguli de securitate pentru conectivitatea la Wi-Fi sau VPN (numai pentru sistemul de operare iOS) dar si unele legate de accesul la anumite pagini de internet.
4. Profilurile de Wi-Fi vor contine urmatoarele optiuni:
   a. Generale – se defineste SSID precum si tipul securitatii retelei;
   b. Setari TCP/IP – atat pentru protocolul IPv4 dar si pentru IPv6;
   c. Setari de proxy – dezactivat, automat sau configurat manual.
5. Profilurile acces pagini de internet pentru sistemul de operare Android includ optiuni precum:
   a. Permiterea, blocarea sau programarea pentru anumite zile si intervale orare a accesului la anumite pagini de internet;
   b. Crearea unor exceptii pentru blocarea sau permiterea accesului catre anumite pagini de internet.
6. Profilurile acces pagini de internet pentru sistemul de operare iOS inlcud optiuni de activare sau dezactivare a:
   a. Utilizarii browser-ului Safari;
   b. Optiunii de completare automata a informatiilor;
   c. Alertarii utilizatorului in cazul accesarii unor pagini frauduloase;
   d. Javascript;
   e. Pop-up-urilor;
   f. Cookie-uri.

D. PROTECTIE SI SECURITATE PENTRU SERVERELE EMAIL MICROSOFT EXCHANGE

1. Produsul va oferi protectie antimalware, antispam (inclusiv antiphishing), precum si filtrare de atasamente si continut, prin integrarea cu serverul Microsoft Exchange. De asemenea, va permite scanarea antimalware la cerere a bazelor de date Exchange.
2. Produsul va asigura scanarea atasamentelor si a continutului mesajelor in timp real, fara a afecta vizibil performanta serverului de mail.
3. Actualizarea antimalware trebuie sa poata fi facuta automat la un interval de maxim 1 ora, precum si la cerere.
4. In afara de detectia pe baza de semnaturi, modulul de protectie antimalware va trebui sa includa si scanare euristica comportamentala,

prin simularea unui calculator virtual in interiorul caruia sunt rulate si analizate aplicatii cu potential periculos, pentru a proteja sistemul de virusii necunoscuti prin detectarea codurilor periculoase a caror semnatura nu a fost lansata inca. 5. Produsul va oferi optiuni multiple de actiune la identificarea unui atasament virusat (dezinfectare, stergere, mutare in carantina). 6. Cu ajutorul unei baze de date complete cu semnaturi de spyware si a euristicii de detectie a acestui tip de programe, produsul va oferi protectie anti-spyware pentru a preveni furtul de date confidentiale. 7. Produsul va oferi protectie antispam, cu o baza de semnaturi actualizabila prin internet. 8. Modulul antispam va trebui sa includa un filtru URL cu o baza de adrese URL cunoscute a fi folosite in mesaje spam, precum si un filtru de caractere pentru detectarea automata a mesajelor scrise cu caractere chirilice sau asiatice. 9. Produsul va trebui sa ofere filtru RBL care sa identifice spam-ul prin sincronizarea cu anumite baze de date online care contin liste de servere de mail cunoscute ca fiind la originea acestui tip de mesaje. 10. Produsul va trebui sa ofere un serviciu/filtru online pentru imbunatatirea protectiei impotriva valurilor de spam nou aparute. 11. Produsul va oferi posibilitatea de a defini politici de filtrare antimalware, antispam, a continutului sau atasamentelor pentru diferite grupuri sau utilizatori. 12. Actualizarea produsului va fi configurabila si se va putea realiza de pe internet, direct sau printr-un proxy, sau din cadrul retelei de pe un server de actualizare propriu. 13. Produsul va trebui sa ofere statistici atat referitoare la scanarea antivirus cat si la scanarea antispam. 14. Produsul se va integra in cadrul consolei de management unitar al solutiei antivirus. 15. Pentru usurinta accesului la setarile produsului din diferite medii de operare, produsul va avea consola de administrare web. **ALTE SERVICII SOLICITATE** A. Ofertantul va asigura furnizarea serviciilor de şcolarizare cu privire la utilizarea şi configurarea solutiei pentru 2 persoane din cadrul Compartimentului Servicii Informatice si de Comunicaţii la sediul beneficiarului. B. Se vor asigura următoarele servicii pentru o perioada de 24 luni de la semnarea contractului. 1.Actualizarea bazei de senaturi de virusi şi a motoarelor de scanare. 2.Actualizarea versiunii şi generaţiei de produs.	

3.Suport tehnic prin e-mail și chat non stop 24/24 ore, 7/7 zile pe saptămână, inclusiv în zilele sâmbătă și duminică și zilele sărbătoare legale, în limba română asigurat de către producătorul soluției. 4.Pentru orice virus pe care producătorul nu îl identifică și dezinfectează se va livra antidotul în cel mai scurt timp posibil de la trimiterea unei monstre a virusului. 5.Distribuirea unor mesaje de atenționare de urgență prin e-mail în cazul apariției unor noi viruși distructivi sau cu potențial de răspândire rapidă. ***Perioada de valabilitate a licentei va fi de <u>24 luni</u>, de la data mentionată în ordinul de incepere.***	

Data completării _____

Operator economic

.....

(semnătura autorizată si stampila)

CONTRACT DE FURNIZARE
nr..... data.....

Preambul
În temeiul L 98/2016 privind achiziţiile publice cu modificările şi completările ulterioare şi a HG 395/2016 pentru aprobarea Normelor metodologice de aplicare a prevederilor referitoare la atribuirea contractului de achiziţie publică/acordului-cadru din Legea nr. 98/2016 privind achiziţiile publice cu modificările şi completările ulterioare, se încheie prezentul contract, între:

1. Părţi contractante

MUNICIPIUL TIMIŞOARA, prin Primar, cu sediul în Timişoara, bv. C. D. Loga nr. 1, cod fiscal 14756536, tel. 0256-408.367, fax 0256-204.177, reprezentată prin Dominic Fritz - Primar în calitate de **Achizitor**, pe de o parte **şi**

..... , cu sediul in, str. ....., nr. ....., tel. ....., fax: ....., înregistrată la Oficiul Registrului Comerţului sub nr. ....., CUI ....., reprezentată prin ....., administrator, în calitate de **FURNIZOR**, pe de alta parte.

2. Definiţii

2.1.- În prezentul contract următorii termeni vor fi interpretaţi astfel:
a. **contract** - reprezintă prezentul contract si toate Anexele sale.
b. **achizitor si furnizor-** părţile contractante, aşa cum sunt acestea numite în prezentul contract;
c. **preţul contractului** - preţul plătibil furnizorului de către achizitor, în baza contractului, pentru îndeplinirea integrală şi corespunzătoare a tuturor obligaţiilor asumate prin contract;
d. **produse** – Upgrade licenţă antivirus pentru Primăria Municipiului Timişoara, pe care furnizorul are obligaţia de a le furniza conform specificatiilor din referatul de necesitate , respectiv contractului;
e. **forţa majoră** - un eveniment mai presus de controlul părţilor, care nu se datorează greşelii sau vinei acestora, care nu putea fi prevăzut la momentul încheierii contractului şi care face imposibilă executarea şi respectiv, îndeplinirea contractului; sunt considerate asemenea evenimente: războaie, revoluţii, incendii, inundaţii sau orice alte catastrofe naturale, restricţii apărute ca urmare a unei carantine, embargo, enumerarea nefiind exhaustivă ci enunţiativă.
Nu este considerat forţă majoră un eveniment asemenea celor de mai sus care, fără a crea o imposibilitate de executare, face extrem de costisitoare executarea obligaţiilor uneia din părţi;
f. **zi** –zi calendaristică; an -365 de zile.

3. Interpretare

3.1. În prezentul contract, cu excepţia unei prevederi contrare cuvintele la forma singular vor include forma de plural şi viceversa, acolo unde acest lucru este permis de context.
3.2. Termenul „zi" sau „zile" sau orice referire la zile reprezintă zile calendaristice dacă nu se specifică în mod diferit.

CLAUZE OBLIGATORII

4. Obiectul principal al contractului

4.1.- Furnizorul se obligă să furnizeze Upgrade licenţă antivirus Bitdefender pentru Primăria Municipiului Timişoara, în conformitate cu cerinţele impuse, oferta tehnică si oferta financiara cu cantitatile aferente anexe la prezentul contract.

5. Preţul contractului

5.1.Preţul convenit pentru îndeplinirea contractului, plătibil furnizorului de către achizitor, este de **.....lei**, la care se adaugă TVA. Preţurile unitare sunt cele declarate în oferta financiară depusă.

27. Limba care guvernează contractul

27.1- Limba care guvernează contractul este limba română.

28. Comunicări

28.1- (1) Orice comunicare dintre părţi, referitoare la îndeplinirea prezentului contract, trebuie să fie transmisă în scris.

(2) Orice document scris trebuie înregistrat atât în momentul transmiterii cât şi în momentul primirii.

28.2- Comunicările între părţi se pot face şi prin telefon, telegramă, telex, fax sau e-mail cu condiţia confirmării în scris a primirii comunicării.

29. Legea aplicabilă contractului

29.1- Contractul va fi interpretat conform legilor din România.

Părţile au înţeles să încheie astăzi.....prezentul contract în trei exemplare, câte unul pentru fiecare parte.

ACHIZITOR,

MUNICIPIUL TIMIŞOARA
P R I M A R
DOMINIC FRITZ

FURNIZOR,

.....
reprezentantă prin .....,

DIRECŢIA ECONOMICĂ
SLAVITA DUBLES

PT. SEF SERVICIUL JURIDIC
CRISTINA BOZAN

BIROU UNITATE DE DIGITALIZARE SI
ASISTENTA INFORMATICA
FLOREA VIOREL

ROMÂNIA
JUDEŢUL TIMIŞ
MUNICIPIUL TIMIŞOARA
BIROU UNITATE DE DIGITALIZARE SI
ASISTENTA INFORMATICA
Nr. SC2020-288911 08.12.2020

APROBAT,
Primar
DOMINIC FRITZ

REFERAT DE NECESITATE ŞI OPORTUNITATE
privind achizitionarea „Upgrade licenţa antivirus",
pentru Primăria Municipiului Timişoara

1. **Obiectul contractului**
   Achizitie "Upgrade licenţa antivirus", pentru Primăria Municipiului Timişoara

2. **Codul CPV**
   Codul CPV: 48761000-0 „Pachete software antivirus"

3. **Necesitatea si oportunitatea achizitiei**
   Scopul acestei achiziții constă în necesitatea siguranței și integrității informațiilor deținute prin protecția acestora impotriva pierderii, distrugerii sau divulgarii neautorizate.
   În luna octombrie a anului 2014, Primaria Municipiului Timişoara a încheiat contractul 236/30.09.2014 prin care s-a achiziționat o licenta antivirus Bitdefender pentru toată infrastructura informatică.
   În vederea asigurării exploatării la parametrii proiectaţi a sistemelor informatice din Primăria Municipiului Timişoara, ţinând cont de cerinţele de securitate şi integritate a datelor din sistemul informaţional al instituţiei, se impune prelungirea licenţei antivirus pentru echipamentele informatice ale Primăriei Municipiului Timişoara,
   Având în vedere că în data de 07 februarie 2021 expira perioada de valabilitate a licentei achizitionate anul acesta pentru protejarea infrastructurii informatice a echipamentelor informatice, este necesară demararea procedurilor de achiziție.

4. **Descrierea succinta a achizitiei**
   Achizitiea „Upgrade licenţa antivirus" asigura ținerea la zi a definițiilor de viruși tinand cont de faptul că toate activitățile din cadrul Primăriei Timişoara se desfășoară folosind echipamente informatice ce trebuie protejate de atacuri informatice.

   Produsul este o platforma integrata pentru managementul securitatii, gandita ca o solutie modulara. Produsul contine urmatoarele module:
   A. O consola de management care asigura functionalitati de administrare;
   B. Protectie statii si servere fizice/virtuale;
   C. Protectie si securitate pentru telefoanele mobile de tip smartphone cu sistem de operare iOS sau Android;
   D. Protectie si securitate pentru serverele email Microsoft Exchange;

SPECIFICAŢII TEHNICE – pentru update program antivirus BITDEFENDER

A. CONSOLA DE MANAGEMENT

1. Instalare si configurare:
   1. Pachetul de instalare va fi livrat ca o masina virtuala bazata pe sistem de operare Linux securizat care contine toate rolurile sau serviciile necesare. Consola nu va necesita o licenta suplimentara pentru sistemul de operare. Imaginea de tip template se va putea importa in:
      a. VMware vSphere
      b. Citrix XenServer
      c. Microsoft Hyper-V
      d. Red Hat Enterprise Virtualization
      e. KVM
      f. Oracle VM.
   2. Consola de management se livreaza cu o baza de date inclusa care este de tip non-relationala, pentru o functionare cat mai rapida, fara a fi nevoie de licente aditionale.
   3. Solutia va fi scalabila, astfel ca oricare dintre roluri sau servicii pot fi instalate separat pe mai multe masini virtuale sau pe aceeasi masina virtuala.
   4. Masinile de scanare pentru mediile virtuale VMware si Citrix se insteaza la distanta prin task din consola de management, iar pentru alte platforme se descarca separat din interfata web a produsului.
   5. Rolurile principale trebuie sa fie cel putin similare cu: Server cu baza de date, Server de comunicatie, Server de actualizare, Server de Web.
   6. Solutia va include aditional si un modul de balansare (load balancer) pentru cazurile in care mai multe masini virtuale ale componentei de management sunt instalate cu acelasi rol (pentru Load Balancing si performanta/redundanta).
   7. Solutia va include un mecanism de configurare a disponibilitatii pentru Serverul cu baze de date (clustering pentru redundanta). Astfel, baza de date se va putea instala de mai multe ori, pe mai multe masini virtuale.

2. Cerinte generale:
   1. Interfata consolei de management va fi in limba romana.
   2. Interfata clientului de securitate, care se instaleaza pe statii si servere, va fi in limba romana.
   3. Manualul de instalare a produsului va fi in limba romana.
   4. Manualul de administrare a produsului va fi in limba romana.
   5. Solutia va include un modul de update server prin care se asigura actualizarea de produs si a semnaturilor.
   6. Solutia va pemite activarea/dezactivarea actualizarilor de produs/semnaturi.
   7. Notificarile – prezente in interfata, notificarile necitite sunt evidentiate, trimise catre una sau mai multe adrese de email, alerteaza administratorul in cazul unor probleme majore: licentiere, detectie virusi, actualizari de produs disponibile).
   8. Solutia va permite integrarea cu un server Syslog pentru raportarea evenimentelor antimalware.
   9. Solutia va permite instalarea serviciului de SMNP prin care se pot raporta statusul masinilor din cadrul componentei de management.

3. Panou de monitorizare si raportare (Dashboard):
   1. Rapoartele din panoul de monitorizare vor putea fi configurate specificand numele raportului, tipul raportului, tinta raportului, optiuni specifice pentru orice tip de raport (de exemplu pentru raportul de actualizare - care este intervalul dupa care o statie este considerata neactualizata).
   2. Panoul central contine rapoarte pentru toate modulele suportate.

3. Rapoartele din panoul central de comanda permit: adaugarea altor rapoarte, stergerea lor si rearanjarea.

4. Inventarierea retelei – managementul securitatii:
   1. Solutia se va integra cu domenii Active Directory multiple, VMware vCenter, Citrix Xen si importa inventarul acestor platforme.
   2. Pentru integrarea cu Active Directory, se va putea defini si intervalul (in ore) de sincronizare si forta sincronizarea.
   3. Se permite descoperirea masinilor din Microsoft Hyper-V, Red Hat VM, Oracle VM, KVM.
   4. Se permite descoperirea statiilor statii fizice neintegrate in Active Directory (Workgroup) cu ajutorul Network discovery.
   5. Solutia va oferi optiuni de cautare, sortare si filtrare dupa numele sistemului, sistem de operare si adresa IP.
   6. Solutia va permite instalarea la distanta sau manual a clientilor antimalware pe masini fizice/virtuale.
   7. Solutia va permite selectarea modulelor componente atunci cand se creaza pachetul clientului care se instalează pe maşinile fizice/virtuale.
   8. Solutia va permite lansarea de task-uri de scanare, actualizare, instalare, dezinstalarea la distanta pentru clientul antimalware.
   9. Solutia va oferi posibilitatea de repornire a masinilor fizice de la distanta.
   10. Solutia va oferi informatii detaliate despre fiecare task si se fiseaza daca task-ul s-a finalizat sau nu cu succes.
   11. Solutia va permite configurarea centralizata a clientilor antimalware prin intermediul politicilor
   12. Se vor oferi in consola de management informatii detaliate ale obiectelor din consola: Nume, IP, Sistem de operare, Grup, Politica atribuita, Ultimele actualizare, Versiunea produsului, Versiunea de semnaturi.

5. Politici:
   1. Solutia va permite configurarea setarilor clientului antimalware prin intermediul unei singure politici ce contine setari pentru toate module
   2. Politica va contine optiuni specifice de activare/dezactivare si configurarea functionalitatilor precum scanarea antimalware la cerere, firewall, controlul accesului la Internet, controlul aplicatiilor, scanarea traficului web,controlul dispozitivelor, power user.
   3. Solutia permite aplicarea politicilor pe masini client, grupuri de masini, pool-uri de resourse (VMware), domeniu, unitati organizationale sau useri de active directoy.
   4. Politica sa poate fi schimbata automat in functie de:
      a. User-ul logat pe statie
      b. IP sau clasa de IP al statiei
      c. Gateway-ul alocat
      d. DNS serverul alocat
      e. Clientul este/nu este in acceasi retea cu infrastructura de management
      f. Tipul retelei (lan, wireless)

6. Rapoarte:
   1. Solutia va contine rapoarte care prezinta statusul masinilor clientil din punct de vedere al actualizarilor, fisierelor malware detectate, aplicatiile blocate, site-urilor web blocate.
   2. Rapoartele programate pot fi trimise catre un numar nelimitat de adrese de email (nu este nevoie sa aiba un cont in consola de management).
   3. Solutia va permite vizualizarea rapoartelor curente programate de administrator.
   4. Solutia va permite exportarea rapoartelor in format .pdf si detaliile ca format .csv.

7. Carantina:

1. Solutia va permite restaurarea fisierelor carantinate in locatia originala sau intr-o cale configurabila.
2. Carantina va fi locala, pe fiecare statia administrata si va fi administrata, fie local, fie din consola de magement
3. Permite descarcarea fisierelor carantinate doar pentru masinile virtuale protejate prin modulul mediilor virtuale integrat cu VMware vShield.

8. Utilizatori:
   1. Administrarea se va putea face pe baza de roluri.
   2. Roluri multiple predefinite: Administrator companie, Administrator retea, Reporter sau rol personalizat.
      a. Administrator companie: administreaza arhitectura consolei de management;
      b. Administrator retea: administreaza serviciile de securitate;
      c. Reporter: monitorizeaza si genereaza rapoarte.
   3. Utilizatorii pot fi importati din Microsoft Active Directory sau creati in consola de management.
   4. Se va permite configurarea detaliata a drepturilor administrative, permitand selectarea serviciilor si obiectelor pentru care un utilizator poate face modificari.
   5. Se va permite deconectarea automata a oricarui tip de utilizator dupa un anumit timp pentru o protectie sporita a datelor afisate in consola de administrare. Acest interval se poate personaliza de administratorul solutiei.

9. Log-uri:
   1. Inregistrarea actiunilor utilizatorilor.
   2. Se vor oferi informatii detaliate pentru fiecare actiune a unui utilizator.
   3. Se va permite filtrarea actiunilor utilizator dupa numele utilizatorului, actiune.

10. Actualizare:
   1. Se permite definirea de locatii de actualizare multiple.
   2. Se permite activarea/dezactivarea actualizarilor de produs si semnaturi.
   3. Se permite actualizarea produsului intr-o retea fara acces la Internet.
   4. Orice client antivirus sa poata fi configurat sa livreze update-urile catre alt client antivirus
   5. Modulul de actualizare din consola de management, permite testarea noilor versiuni de pachete de instalare ale clientului antimalware, inainte de a fi instalate pe toate statiile din retea, evitand posibile probleme ce pot afecta serverele sau statiile critice.

11. Certificate:
   1. Accesul la consola de management sa se faca doar prin HTTPS.
   2. Serverul web, din consola centrala de management trebuie sa permita importarea de certificate digitale eliberate de o autoritate de certificare autorizata sau proprie organizatiei.
   3. Solutia permite afisarea in consola de management informatii despre certificate: nume, autoritatea emitenta, data eliberarii si data expirarii certificatelor eliberate.

B. PROTECTIE STATII SI SERVERE FIZICE/VIRTUALE

1. Caracteristici generale minimale si eliminatorii:
   1. Pentru reducerea la minim a consumului de resurse, solutia antimalware trebuie sa permita instalarea personalizata a modulelor detinute (de exemplu, sa permita instalarea solutiei antimalware fara modulul de control al accesului web, modul de control al dispozitivilelor sau modulul firewall).

2. Cerinte de sistem:
   - Sisteme de operare pentru statii de lucru: Windows 10, Windows 8, Windows 7, Windows Vista (SP1), Windows XP (SP3), Mavericks (10.9.x), Mountain Lion (10.8.x), Lion (10.7.x)

- Sisteme de operare embedded: Windows Embedded 8.1 Industry, Windows Embedded 8 Standard, Windows Embedded Standard 7, Windows Embedded POSReady 7, Windows Embedded Enterprise 7, Windows Embedded POSReady 2009, Windows Embedded Standard 2009, Windows XP Embedded with Service Pack 2, Windows XP Tablet PC Edition
- Sisteme de operare pentru servere: Windows Server 2012 R2, Windows Server 2012, Windows Small Business Server (SBS) 2011, Windows Small Business Server (SBS) 2008, Windows Server 2008 R2, Windows Server 2008, Windows Small Business Server (SBS) 2003, Windows Server 2003 R2, Windows Server 2003 with Service Pack 1, Windows Home Server
- Sisteme de operare Linux: Red Hat Enterprise Linux / CentOS 5.6 sau mai recent, Ubuntu 10.04 LTS sau mai recent, SUSE Linux Enterprise Server 11 sau mai recent, OpenSUSE 11 sau mai recent, Fedora 15 sau mai actual and Debian 5.0 sau mai recent.
- Sisteme de operare MAC: Mac OS X El Capitan (10.11.x), Mac OS X Yosemite (10.10.5), Mac OS X Mavericks (10.9.5), Mac OS X Mountain Lion (10.8.5)

3. Administrare si instalare remote:
   1. Inainte de instalare, administratorul va putea particulariza pachetele de instalare cu modulele dorite: firewall, content control, device control, power user.
   2. Instalarea se va putea face in mai multe moduri:
      a. prin descarcarea directa a pachetului pe statia pe care se va face instalarea;
      b. prin instalarea la distanta, direct din consola de management
   3. Instalarea clientilor la distanta in alte locatii decat cele in care este instalata consola de management se va face prin intermediul unui alt client antivirus existent in locatiile respective pentru a minimiza traficul in WAN.
   4. In consola vor fi disponibile informatii despre fiecare statie: numele statiei, IP, sistem de operare, module instalate, politica aplicata, informatii despre actualizari etc.
   5. Din consola se va putea trimite o singura politica pentru configurarea integrala a clientului de pe statii/servere.
   6. Consola va include o sectiune, „Audit", unde se vor mentiona toate actiunile intreprinse fie de administratori fie de reporteri, cu informatii detaliate: logare, editare, creare, delogare, mutare etc.
   7. Posibilitatea creari unui singur pachet de instalare, utilizabil atat pentru sistemele de operare pe 32 de biti cat si pentru cele pe 64 de biti.
   8. Posibilitatea creari unui singur pachet de instalare, utilizabil pentru statii (fizice si/sau virtuale), servere (fizice si/sau virtuale), exchange.
   9. Posibilitatea de a crea pachetele de instalare de tip web installer sau kit full.
   10. Administratorul va putea crea grupuri sau chiar subgrupuri, unde va putea muta statiile/serverele din retea pentru cele care nu sunt integrate domeniu.
   11. Permite selectarea clientului care va realiza descoperirea statiilor din retea, altele decat cele integrate in domeniu.

4. Caracteristici si functionalitati principale ale modulului antimalware:
   1. Scanarea automata in timp real va putea fi setata sa nu scaneze arhive sau fisiere mai mari de « x » MB, marimea fisierelor putand fi definita de administratorul solutiei,
   2. Definirea pana la 16 nivele de profunzime pentru scanarea in arhive.
   3. Scanarea euristica comportamentala prin simularea unui calculator virtual in interiorul caruia sunt rulate aplicatii cu potential periculos protejand sistemul de virusii necunoscuti prin detectarea codurilor periculoase a caror semnatura nu a fost lansata inca.
   4. Scanarea oricarui suport de stocare a informatiei (CD-uri, harduri externe, unitati partajate etc). De asemenea, se va putea anula scanarea in cazul in care sunt detectate unitati care au informatii stocate mai mult de « x » MB.
   5. Scanarea automata a emailurilor la nivelul statiei de lucru pentru POP3/SMTP.
   6. Configurarea cailor ce urmeaza a fi scanate la cerere.

7. Clientii antimalware pentru workstation sa permita definirea unor liste de excludere de la scanarea in timp real si la cerere a anumitor directoare, discuri, fisiere, extensii sau procese.
8. Cu ajutorul unei baze de date complete cu semnaturi de spyware si a euristicii de detectie a acestui tip de programe, produsul va trebui sa ofere protectie anti-spyware.
9. Posibilitatea de configura scanarile programate sa se execute cu prioritate redusa
10. Produsul antimalware poate fi configurat sa foloseasca scanarea in cloud, si partial scanarea locala. Pentru statiile ce nu au suficiente resurse hardware, scanarea se poate face cu o masina de scanare instalata in retea.
11. Administratorul poate personaliza și motoarele de scanare, având posibilitatea de a alege între mai multe tehnologii de scanare:
    - Scanare locală, când scanarea se efectuează pe stația de lucru locală. Modul de scanare locală este potrivit pentru mașinile puternice, având toate semnăturile și motoarele stocate local.
    - Scanarea hibrid cu motoare light (Cloud public), cu o amprentă medie, folosind scanarea în cloud și, parțial, semnături locale. Acest mod de scanare oferă avantajul unui consum mai bun de resurse, fără să implice scanarea locală.
    - Scanarea centralizată în Cloud-ul privat, cu o amprentă redusă, necesitând un server de securitate pentru scanare. În acest caz, nu se stochează local nicio semnătură, iar scanarea este transferată către serverul de securitate.
    - Scanare centralizată (Scanare în cloud privat cu server de securitate) cu fallback* pe Scanare locală (motoare full)
    - Scanare centralizată (Scanare în cloud privat cu server de securitate) cu fallback* pe Scanare hibrid (cloud public cu motoare light)

12. Pentru o protectie sporita, solutia antimalware trebuie sa aiba 3 tipuri de detectie: bazata pe semnaturi, bazata de comportamentul fisierelor si bazata pe monitorizarea proceselor.
13. Pentru o protectie sporita, solutia antimalware trebuie sa poata scana paginile HTTP.
14. Pentru o mai buna gestionare a antimalware instalat pe statii, produsul va include optiunea de setare a unei parole pentru protectia la dezinstalare.
15. Pentru siguranta utilizatorului, clientul va include un modul de antiphishing.
16. Solutia ofera protectie in timp real pe masinile cu sistem de operare Linux in conformitate cu versiunea de kernel instalata.
17. Pe masinile virtuale parte a unui pool instalarea clientului antimalware se face doar pe masina de tip template, dupa care se recompune pool-ul de masini virtuale.

5. Firewall:
    1. Posibilitatea de a configura reguli de firewall pentru aplicatii sau conectivitate.
    2. Modulul poate fi instalat/dezinstalat in functie de preferinta administratorului.
    3. Posibilitatea de a defini retele de incredere pentru masina destinatie.

6. Carantina:
    1. Produsul antimalware sa permita trimiterea automata a fisierelor din carantina catre laboratoarele antimalware ale producatorului.
    2. Trimiterea continutului carantinei va putea fi expediat in mod automat, la un interval definit de administrator.
    3. Produsul antimalware sa permita stergerea automata a fisierelor carantinate mai vechi de o anumita perioada, pentru a nu incarca inutil spatiul de stocare.
    4. Posibilitatea de a restaura un fisier din carantina in locatia lui originala.
    5. Modulul de carantina va permite rescanarea obiectelor dupa fiecare actualizare de semnaturi.

7. Protectia datelor:
    1. Produsul permite blocarea datelor confidentiale (pin-ul cardului, cont bancar etc) transmise prin HTTP sau SMTP prin crearea unor reguli specifice.

8. Controlul continutului:
   1. Consola va avea integrat un modul dedicat controlului accesului la Internet cu urmatoarele particularitati:
      a. Permite blocarea accesului la Internet pentru anumite masini client sau grupuri de masini.
      b. Permite blocarea accesului la Internet pe intervale orare.
      c. Permite blocarea paginilor de internet care contin anumite cuvinte cheie.
      d. Permite controlul accesului numai la anumite pagini de internet specificate de administrator;
      e. Permite blocarea accesului la anumite aplicatii definite de administrator;
      f. Permite restrictionarea accesului pe anumite pagini de internet dupa anumite categorii prestabilite (ex: online dating, violenta, pornografie etc).

9. Controlul dispozitivelor:
   1. Modulul poate fi instalat/dezinstalat in functie de preferinta administratorului.
   2. Modulul va permite controlul urmatoarelor tipuri de dispozitive:
      a. Bluetooth Devices
      b. CDROM Devices
      c. Floppy Disk Drives
      d. Security Policies 153
      e. IEEE 1284.4
      f. IEEE 1394
      g. Imaging Devices
      h. Modems
      i. Tape Drives
      j. Windows Portable
      k. COM/LPT Ports
      l. SCSI Raid
      m. Printers
      n. Network Adapters
      o. Wireless Network Adapters
      p. Internal and External Storage
   3. Modulul va permite configurarea de reguli prin care se vor defini permisiunile pentru dispozitivele conectate la masina client.
   4. Modulul va permite configurarea de excluderi pentru diferite tipuri de dispozitive pentru care s-au configurat reguli.

10. Power User:
    1. Modulul poate fi instalat/dezinstalat in functie de preferinta administratorului.
    2. Modulul permite posibilitatea de a acorda utilizatorilor drepturi de Power User. Utilizatorii vor putea accesa si modifica setarile clientului antimalware dintr-o consola dispobibila local pe masina client.
    3. Administratorul va putea suprascrie din consola setarile aplicate de utilizatorii Power User.

11. Actualizare:
    1. Posibilitatea efectuarii actualizarii la nivel de statie in mod silentios (fara avertizare).
    2. Sistem de actualizare cascadat folosind unul sau mai multe servere de actualizare (cascadate).
    3. Actualizarea pentru locatiile remote prin intermediul unui client antimalware care are si rol de server de actualizare.

C. PROTECTIE SI SECURITATE PENTRU TELEFOANELE MOBILE DE TIP SMARTPHONE

1. Cerinte minime de sistem:
   - Telefoane cu sistem de operare iOS 5+: Apple iPhone si tablete iPad
   - Telefoane cu sistem de operare Android 2.2+

2. Caracteristici:
   1. Permite asocierea unui dispozitiv cu un utilizator din Active Directory.
   2. Instalarea se face prin trimiterea unui email catre utilizator cu detaliile de instalare.
   3. Activarea dispozitivului mobil in consola de management sa se faca prin scanarea unui cod QR.
   4. Pachetele de instalare se vor putea descarca de pe Apple App Store si Google Play.
   5. Se vor putea intreprinde urmatoarele actiuni:
      a. Blocarea dispozitivului;
      b. Deblocarea dispozitivului;
      c. Stergerea datelor si revenirea la setarile din fabrica;
      d. Localizarea dispozitivului;
      e. Scanarea dispozitivului(doar pentru cele cu sistem de operare Android);
      f. Criptarea memoriei dispozitivului(doar pentru cele cu sistem de operare Android).
   6. Consola va permite raportarea dispozitivelor: active, inactive, deconectate, cu sistemul de operare modificat astfel incat utilizatorul sa aiba acces total asupra lui (rooted or jailbroken devices).

3. Setari de securitate:
   1. In cazul in care un dispozitiv nu este conform cu setarile dorite, se vor putea intreprinde automat actiunile:
      a. Ignorare;
      b. Blocarea accesului;
      c. Blocarea dispozitivului;
      d. Stergerea datelor si revenirea la setarile din fabrica;
      e. Stergerea dispozitivului din consola.
   2. Se va putea impune blocarea dispozitivelor cu ajutorul unei parole. Aceasta parola va putea fi configurata sa contina:
      a. Parola simpla sau complexa (in functie de cerintele sistemului de operare);
      b. Numere si litere;
      c. O lungime minima definita de administrator;
      d. Un numar minim de caractere speciale, definit de adiministrator;
      e. Perioada de expirare a parolei. Perioada va putea fi definita de adiministrator;
      f. Configurarea restrictiei refolosirii parolei;
      g. Numarul de introduceri incorecte a parolei, de catre utilizator;
      h. Perioada de autoblocare a dispozitivului dupa un numar de minute definite de adiministrator.
   3. Se vor putea genera mai multe profiluri care vor stabili reguli de securitate pentru conectivitatea la Wi-Fi sau VPN (numai pentru sistemul de operare iOS) dar si unele legate de accesul la anumite pagini de internet.
   4. Profilurile de Wi-Fi vor contine urmatoarele optiuni:
      a. Generale – se defineste SSID precum si tipul securitatii retelei;
      b. Setari TCP/IP – atat pentru protocolul IPv4 dar si pentru IPv6;
      c. Setari de proxy – dezactivat, automat sau configurat manual.
   5. Profilurile acces pagini de internet pentru sistemul de operare Android includ optiuni precum:

a. Permiterea, blocarea sau programarea pentru anumite zile si intervale orare a accesului la anumite pagini de internet;
b. Crearea unor exceptii pentru blocarea sau permiterea accesului catre anumite pagini de internet.

6. Profilurile acces pagini de internet pentru sistemul de operare iOS inlcud optiuni de activare sau dezactivare a:
   a. Utilizarii browser-ului Safari;
   b. Optiunii de completare automata a informatiilor;
   c. Alertarii utilizatorului in cazul accesarii unor pagini frauduloase;
   d. Javascript;
   e. Pop-up-urilor;
   f. Cookie-uri.

D. PROTECTIE SI SECURITATE PENTRU SERVERELE EMAIL MICROSOFT EXCHANGE

1. Produsul va oferi protectie antimalware, antispam (inclusiv antiphishing), precum si filtrare de atasamente si continut, prin integrarea cu serverul Microsoft Exchange. De asemenea, va permite scanarea antimalware la cerere a bazelor de date Exchange.
2. Produsul va asigura scanarea atasamentelor si a continutului mesajelor in timp real, fara a afecta vizibil performanta serverului de mail.
3. Actualizarea antimalware trebuie sa poata fi facuta automat la un interval de maxim 1 ora, precum si la cerere.
4. In afara de detectia pe baza de semnaturi, modulul de protectie antimalware va trebui sa includa si scanare euristica comportamentala, prin simularea unui calculator virtual in interiorul caruia sunt rulate si analizate aplicatii cu potential periculos, pentru a proteja sistemul de virusii necunoscuti prin detectarea codurilor periculoase a caror semnatura nu a fost lansata inca.
5. Produsul va oferi optiuni multiple de actiune la identificarea unui atasament virusat (dezinfectare, stergere, mutare in carantina).
6. Cu ajutorul unei baze de date complete cu semnaturi de spyware si a euristicii de detectie a acestui tip de programe, produsul va oferi protectie anti-spyware pentru a preveni furtul de date confidentiale.
7. Produsul va oferi protectie antispam, cu o baza de semnaturi actualizabila prin internet.
8. Modulul antispam va trebui sa includa un filtru URL cu o baza de adrese URL cunoscute a fi folosite in mesaje spam, precum si un filtru de caractere pentru detectarea automata a mesajelor scrise cu caractere chirilice sau asiatice.
9. Produsul va trebui sa ofere filtru RBL care sa identifice spam-ul prin sincronizarea cu anumite baze de date online care contin liste de servere de mail cunoscute ca fiind la originea acestui tip de mesaje.
10. Produsul va trebui sa ofere un serviciu/filtru online pentru imbunatatirea protectiei impotriva valurilor de spam nou aparute.
11. Produsul va oferi posibilitatea de a defini politici de filtrare antimalware, antispam, a continutului sau atasamentelor pentru diferite grupuri sau utilizatori.
12. Actualizarea produsului va fi configurabila si se va putea realiza de pe internet, direct sau printr-un proxy, sau din cadrul retelei de pe un server de actualizare propriu.
13. Produsul va trebui sa ofere statistici atat referitoare la scanarea antivirus cat si la scanarea antispam.
14. Produsul se va integra in cadrul consolei de management unitar al solutiei antivirus.
15. Pentru usurinta accesului la setarile produsului din diferite medii de operare, produsul va avea consola de administrare web.

ALTE SERVICII SOLICITATE

A. Ofertantul va asigura furnizarea serviciilor de şcolarizare cu privire la utilizarea şi configurarea solutiei pentru 2 persoane din cadrul Compartimentului Servicii Informatice si de Comunicaţii la sediul beneficiarului.

B. Se vor asigura următoarele servicii pentru o perioada de 24 luni de la semnarea contractului.

1.Actualizarea bazei de senaturi de virusi şi a motoarelor de scanare.

2.Actualizarea versiunii şi generaţiei de produs.

3.Suport tehnic prin e-mail şi chat non stop 24/24 ore, 7/7 zile pe saptămână, inclusiv în zilele sâmbătă şi duminică şi zilele sărbătoare legale, în limba română asigurat de către producătorul soluţiei.

4.Pentru orice virus pe care producătorul nu îl identifică şi dezinfectează se va livra antidotul în cel mai scurt timp posibil de la trimiterea unei monstre a virusului.

5.Distribuirea unor mesaje de atenţionare de urgenţă prin e-mail în cazul apariţiei unor noi viruşi distructivi sau cu potenţial de răspândire rapidă.

5. Valoarea estimata

Valoarea estimata a fost calculată ţinând cont de mărimea infrastructurii informatice a Primăriei Municipiului Timişoara, respectiv de numărul echipamentelor ce trebuie protejate de atacuri informatice. Primaria Municipiului Timişoara deţine un server de mail ce gazduieşte aproximativ 600 de căsuţe de mail, 550 de calculatoare, 20 de tablete, 25 servere virtuale şi 120 de staţii virtuale. La calculul valorii estimate s-a luat in considerare si suplimentarea numarului de statii, laptopuri si tablete.

Valoarea estimata a fost stabilita pe baza de cost istoric, respectiv prin inventarierea platilor efectuate in baza contractelor avute in derulare, pentru achizitionarea de produse similare cu cele care fac obiectul prezentului referat, la care a fost aplicata rata anuala a inflatiei. Detaliem mai jos modul de calcul al valorii estimate:

Nr. crt.	**Denumire**	**Valoare (lei, fara TVA)**
1	Licenta antivirus conform contract nr. 236/30.09.2014 (12 luni)	40.241,27
2	Prelungire licenta antivirus conform comanda nr. 450/16.10.2015 (12 luni)	38.627
3	Prelungire licenta antivirus conform comanda nr. 1230/18.11.2016 (12 luni)	38.627
4	Prelungire licenta antivirus conform contract nr. 5/23.01.2018	26.543,61
5	Prelungire licenta antivirus conform contract nr.13/30.01.2019	40.911,85
6	Prelungire licenta antivirus conform contract nr.10/29.01.2020	40.230
	Media aritmetica este de	37.530,12

Avand in vedere cele consemnate mai sus, estimam o valoare a achizitiei de **80.000 lei, fara TVA**, respectiv 95.200 lei cu TVA.

Perioada de valabilitate a licentei va fi de 24 luni, de la data mentionată în ordinul de incepere.

6. Gradul de prioritate al necesitatii

Având în vedere că în data de 07 februarie 2021 expira perioada de valabilitate a licentei, pentru protejarea infrastructurii informatice, a echipamentelor informatice, este necesară demararea procedurii de achiziție în vederea prelungirii licenței antivirus.

BIROU UNITATE DE DIGITALIZARE SI
ASISTENTA INFORMATICA
FLOREA VIOREL

BIROU UNITATE DE DIGITALIZARE SI
ASISTENTA INFORMATICA
MARASCU IONEL SORIN

BIROU UNITATE DE DIGITALIZARE SI
ASISTENTA INFORMATICA
BORDEA CORNELIA