UNIVERSITATEA TEHNICĂ GHEORGHE ASACHI din IAȘI
DIRECȚIA GENERALA ADMINISTRATIVA
SERVICIUL ACHIZITII PUBLICE

UNIVERSITATEA TEHNICĂ
„GHEORGHE ASACHI" DIN IAȘI
REGISTRATURA
-29-
Nr. 40003 / 03.12. 2021

INVITAȚIE DE PARTICIPARE

Serviciul Achizitii Publice invită operatorii economici interesați să depună ofertă pentru atribuirea contractului de achiziție publică „Servicii de mentenanta, drept de utilizare, update software antivirus".

1. Informații generale

1.1 **Achizitor**

Denumirea: Universitatea Tehnică "Gheorghe Asachi" din Iași
Serviciul Achiziții Publice
Adresa: str. Prof.dr.docent Dimitrie Mangeron, nr. 67, Imobil T
Responsabil achiziție: ing. Șerban VLONGA
Telefon: 0232702360
Email: vlonga@tuiasi.ro

1.2 **Publicarea invitației de participare și a documentelor anexate**

www.tuiasi.ro/administratie/achizitii-publice

1.3 **Depunerea ofertelor**

Ofertele se vor publica pe site-ul www.e-licitatie.ro până pe data de 07.12.2021 ora 12.00 și vor avea codul CPV indicat la punctul 2.3 din invitatia de participare publicată pe site-ul universității www.tuiasi.ro/administratie/achizitii-publice, întregul lot fiind publicat în SEAP ca un singur reper cu denumirea „ Servicii de mentenanta, drept de utilizare, update software antivirus -invitația nr. ..40003.....", având prețul unitar egal cu valoarea exclusiv TVA a întregului lot. Ofertanții vor transmite oferta tehnico-economică detaliată la adresa de e-mail vlonga@tuiasi.ro până pe data de 07.12.2021 ora 12.00.

1.4 **Modul de elaborare a ofertei**

- ✓ Ofertantul trebuie să elaboreze oferta pentru toate produsele/serviciile/lucrările din caietul de sarcini. Dacă sunt împărțite pe loturi, ofertantul va trebui să facă ofertă pentru toate produsele dintr-un lot. Nu vor fi luate în considerare ofertele din care lipsesc repere solicitate prin caietul de sarcini anexat.
- ✓ **Propunerea tehnico-financiară**
  Ofertantul va elabora propunerea tehnico-financiară astfel încât aceasta sa respecte în totalitate cerințele prevazute în Caietul de sarcini si sa furnizeze toate informatiile solicitate cu privire la preț precum şi la alte condiții financiare şi comerciale legate de obiectul contractului de achiziție publică. Oferta depusă trebuie să îndeplinească în totalitate specificaţiile tehnice minime obligatorii, dupa cum au fost acestea stabilite în caietul de sarcini.

1.5 **Prezentarea ofertei**

Limba de redactare a ofertei:	Română
Moneda în care este exprimat prețul contractului:	Lei
Perioada minimă de valabilitate a ofertei:	30 zile

1.6 **Termen limită pentru solicitarea clarificărilor privind invitația de participare/caietul de sarcini:**

06.12.2021

2. Obiectul contractului

2.1 **Tip contract:**

Lucrări ☐;

Produse ☐;

Servicii ☑;

2.2 **Denumire contract:**

Lot 1: Servicii de mentenanta, drept de utilizare, update software antivirus

2.3 **Descrierea contractului**

Servicii de mentenanta, drept de utilizare, update software antivirus cod CPV72260000-5 conform **Caiet de sarcini anexat**

Nr. Crt.	Nr. lot	Cod CPV	Denumire produs/serviciu/lucrare	Cant.	Specificații tehnice
0	1	2	3	4	5
1	Lot 1	72260000-5	Servicii de mentenanta, drept de utilizare, update software antivirus	1buc	Servicii de mentenanta, drept de utilizare, update software antivirus conform caiet de sarcini

2.4 **Valoarea estimativă a contractului:**

Lot1 86.000,00 lei (fără T.V.A.) cu caracter de regularitate pe 3 ani cu plati anuale egale fara actualizarea pretului.

2.5 **Termen de livrare/ prestare a serviciilor**

Lot1 max. 5 zile de la semnarea contractului/comenzii.

2.6 **Sursa/Surse de finanțare:**

Finanțare de baza.

Locația lucrărilor, locul de livrare a produselor sau de prestare a serviciilor:

Rectorat Imobil T str. Dr. Docent D. Mangeron, nr. 67, D.I.C.D.

3. **Procedura aplicată pentru atribuirea contractului de achizitie publică:**
   Achiziție directă
4. **Informații detaliate și complete cu privire la criteriul aplicat pentru stabilirea ofertei câștigătoare**
   Prețul cel mai scăzut
5. **Garantia de buna executie (în cazul contractelor de servicii de proiectare/lucrări) Nu este cazul.**
6. **Plata prețului contractului**
   Se va face prin O.P., în contul de Trezorerie indicat de către operatorul economic, în maxim 30 zile de la confirmarea fiecărei facturi, (se poate factura lunar funcție de prestările efectuate) în baza facturii fiscale, contractului de achiziție și a notei de recepție. Prețul contractului nu se actualizează. Contract cu caracter de regularitate pe 3 ani cu plati anuale egale fara actualizarea pretului.
7. **Anunț de atribuire**
   În urma finalizării achiziției directe, autoritatea contractantă va publica, pe pagina proprie de internet www.tuiasi.ro/administratie/achizitii-publice, un anunț de atribuire în termen de 15 zile de la data încheierii contractului.

Aprobat,
Director General Administrativ,
Dr.ing. Sorin Avram IACOBAN

Întocmit
Ing. Șerban VLONGA

CAIET DE SARCINI

Caietul de sarcini face parte integrantă din documentaţia pentru elaborarea şi prezentarea ofertei şi constituie ansamblul cerinţelor pe baza cărora se elaborează de către fiecare ofertant propunerea tehnică.

Caietul de sarcini conţine, în mod obligatoriu, specificaţii tehnice.

Cerinţele impuse vor fi considerate ca fiind minimale. În acest sens orice ofertă prezentată, care se abate de la prevederile Caietului de sarcini, va fi luată în considerare, dar numai în măsura în care propunerea tehnică presupune asigurarea unui nivel calitativ superior cerinţelor minimale din Caietul de sarcini.

Ofertarea de produse cu caracteristici tehnice inferioare celor prevăzute în caietul de sarcini şi termene de livrare care depăşesc termenul de livrare stabilit prin invitaţia de participare atrage descalificarea ofertantului.

Propunerea tehnică a operatorilor economici va contine următoarele:

- **denumirea, producatorul şi marca produselor ce vor fi ofertate;**
- **cantităţile produselor ofertate;**
- **specificaţiile tehnice ale produselor ofertate;**
- **fişele tehnice ale produselor emise de producator, prospecte, file de catalog, standarde recunoscute pe plan internaţional, din care sa reiasă caracteristicile tehnice ofertate;**
- **link catre pagina producatorului;**
- **respectarea caracteristicilor tehnice minimale, completare cu caracteristici suplimentare ofertate dacă există;**
- **termenul de livrare al produselor;**
- **perioada de garanţie/support tehnic acordată produselor. Operatorii economici au obligaţia de a garanta buna funcţionare a acestora pe toată perioada de valabilitate a contractului.**

Nu sunt admise loturi din care lipsesc repere (este un singur lot). Oferta tehnică va fi prezentată comparativ, pe 2 coloane, respectiv: specificaţii cerute – specificaţii oferite.

NOTĂ :
Specificaţile tehnice care indică o anumită origine, sursă, producţie, un procedeu special, o marcă de fabrică sau de comerţ, un brevet de invenţie, o licenţă de fabricaţie, sunt mentionate doar pentru identificarea cu usurinta a tipului de produs şi NU au ca efect favorizarea sau eliminarea anumitor operatori economici sau a anumitor produse. Aceste specificatii vor fi considerate ca având menţiunea de « sau echivalent ».

a) Suport tehnic - mentenanţă şi update:

Perioada suport tehnic, ce incude mentenanţă şi update, ce va fi precizată de ofertant, va fi cel puţin egală cu cea prevăzută în caietul de sarcini. Perioada de suport tehnic începe din momentul recepţiei serviciului. În perioada de suport tehnic, toate intervenţiile autorizate vor fi gratuite.

Ofertantul va trebui să aibă un serviciu de asistenta tehnică in limba română. În timpul perioadei de suport tehnic, ofertantul va constata problemele în maxim 2 zile de la anunţarea acesteia şi va remedia, când este necesar, în termen de maxim 15 zile de la anunţarea problemei, pe cheltuiala sa.

Ofertantul va pune la dispoziţia beneficiarului, cel puţin două nume, adrese şi numere de telefon pentru suport tehnic. Ofertantul va asigura suportul tehnic gratuit în funcţionarea normală a produselor pe toată perioada de garanţie.

b) Condiţiile şi termenele de prestare:

Termenul de livrare a subscripţiei (cheie de licenţiere ce da drept de utilizare) este: conform invitaţiei de participare.

Ofertantul trebuie să precizeze în ofertă termenul de livrare şi că este de acord cu condiţiile stipulate mai jos.

Contractul se încheie la Universitatea Tehnica "Gheorghe Asachi" din Iaşi, Strada Prof. dr. docent Dimitrie Mangeron, nr. 67.

Livrarea cheii de licenţiere va fi efectuată în format electronic.

Ofertantul va asigura manualele de utilizare în limba română şi engleză.

c) Condiţiile şi termenele de recepţie:

Recepţia cantitativă se va efectua la sediul Universităţii Tehnice "Gheorghe Asachi" din Iaşi, nodul de comunicaţii Data Center, în prezenţa reprezentanţilor ambelor părţi. Recepţia calitativă la beneficiar se va face în termen de maxim 24 ore de la livrarea produselor. Recepţia cantitativă şi calitativă va fi consemnată într-un proces verbal de recepţie semnat de ambele părţi.

Dreptul achizitorului de a inspecta, de a testa şi, dacă este necesar, a respinge, nu va fi limitat sau amânat datorită faptului că produsele au fost inspectate sau testate de furnizor, cu sau fără participarea unui reprezentant al achizitorului, anterior livrării acestora la destinaţie.

d) Condiţiile şi termenele de plată:

Plata se va face anual, prin O.P., în contul de Trezorerie indicat de către operatorul economic, în baza facturii fiscale. Preţul contractului nu se actualizează.

LOT1 (lot unic) – Serviciu de mentenanta, drept de utilizare, update software antivirus pentru 3 ani

Sursa de finanţare: **Finanţare de bază**

Nr.crt.	Codul de clasificare CPV	Produs / caracteristici	UM	Cant. (buc)
1.	72260000-5	Serviciu de mentenanta, drept de utilizare, update software antivirus	Buc.	1

Nr. crt.	**Specificaţii tehnice**	
1.	Serviciu de mentenanta, drept de utilizare, update software antivirus	
	Conţinut serviciu	Cheie de licenţiere ce asigură drept de utilizare, mentenanţă şi update software antivirus pe o perioadă de 3 ani, pentru: • minim 2900 staţii de lucru • minim 20 servere fizice • minim 50 servere de tip maşină virtuală
	Caracteristici generale	Produsul reprezintă o platforma integrata pentru managementul securitatii, gandita ca o solutie modulara si contine urmatoarele module: • O consola de management care asigura functionalitati de administrare. • Protectie statii si servere fizice/virtuale. • Protectie si securitate pentru telefoanele mobile de tip smartphone cu sistem de operare iOS sau Android (prin licentiere distincta). • Protectie si securitate pentru serverele email Microsoft Exchange (prin licentiere distincta).
	Consola de management	**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.

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. Produsul suporta licentierea per procesor fizic (socket). In felul acesta numarul masinilor virtuale poate varia oricand, ele fiind protejate.
6. Solutia va include un modul de update server prin care se asigura actualizarea de produs si a semnaturilor.
7. Solutia va pemite activarea/dezactivarea actualizarilor de produs/semnaturi.
8. Solutia permite stabilirea actualizarii automate a consolei de management prin stabilirea recurentei zilnice, saptamanale sau lunare, dar si prin stabilirea intervalului orar in care acesta se va actualiza. De asemenea, permite si trimiterea unei alerte de nefunctionalitate, cu 30 de minute inainte de actualizare.
9. Pentru o mai buna urmarire a actualizarilor consolei de management, solutia permite vizualizarea unui jurnal de modificari in care sunt precizate istoric:
    a. versiunea consolei de management
    b. data versiunii
    c. functii noi si imbunatatiri
    d. probleme rezolvate
    e. probleme cunoscute
10. 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).
11. Solutia va permite integrarea cu un server Syslog pentru raportarea evenimentelor antimalware.
12. Solutia va permite instalarea serviciului de SMNP prin care se pot raporta statusul masinilor din cadrul componentei de management.
13. Solutia permite creare unei copii de siguranta a bazei de date a consolei de administrare, la cerere sau programata, putand fi stocata local, pe un server FTP sau in retea.

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.

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.
13. Solutia permite descoperirea tuturor aplicatiilor instalate pe toate statiile si serverele din reatea, prin rularea unui task din consola de administrare.

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)

Rapoarte:

1. Solutia va contine rapoarte care prezinta statusul masinilor client 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.
5. Solutia include un generator de rapoarte care ofera posibilitatea de a investiga o problema de securitate pe baza mai multor criterii, mentinand informatiile concise si ordonate corespunzator. Astfel, solutia include interogari precum: starea terminalului, evenimente terminal, evenimente Exchange.
6. Interogarea legata de starea terminalului include informatii precum:
   a. tip masina
   b. infrastructura retelei careia ii apartine terminalul
   c. datele agentului de securitate
   d. starea modulelor de protectie
   e. rolurile terminalelor.
7. Interogarea legata de evenimente terminal include informatii precum:
   a. calculatorul tinta pe care a avut loc evenimentul
   b. tipul starea si configuratia agentului de securitate instalat
   c. starea modulelor si rolurilor de protectie instalate pe agentul de securitate
   d. denunmirea si alocarea politicii
   e. utilizatorul autentificat in timpul evenimentului
   f. evenimente (site-uri blocate, aplicatii blocate, detectiile etc)
8. Interogarea legata de evenimente Exchange include informatii precum:
   a. Directia traficului e-mail
   b. Evenimente de securitate (detectarea programelor de tip malware sau a fisierelor atasate)
   c. Masurile implementate in fiecare situatie (curatarea, stergerea, inlocuirea sau carantinarea fisierului, stergerea sau respingerea e-mail-ului)

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.

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.

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.

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. Solutia dispune un server de actualizare (update) care face posibila stabilirea componentelor ce vor fi descarcate automat de pe internet, fara interventia

		administratorului. Astfel, administratorul va putea descarca pachetele pentru protectia statiilor si serverelor pe care ruleaza sistemul de operare Windows, Linux, Mac sau, poate descarca pachetele pentru modul de scanare centralizata in mediile de virtualizare VMware, Hyper-V sau Citrix. 6. In cadrul serverului de actualizare, pentru o mai buna urmarire a actualizarilor pachetele pentru protectia statiilor si serverelor sau a pachetelor pentru modul de scanare centralizata, se va putea vizualiza un jurnal de modificari in care sunt precizate istoric: a. versiunea pachetului b. data versiunii c. functii noi si imbunatatiri d. probleme rezolvate e. probleme cunoscute 7. Solutia permite testarea noilor versiuni de pachete de instalare ale clientului antimalware, inainte de a fi instalate pe toate statiile si serverele din retea, evitand posibile probleme ce pot afecta serverele sau statiile critice. Astfel, serverul de actualizare include 2 tipuri de actualizari de produs: a. Ciclu rapid, gandit pentru un mediu de test in cadrul retelei b. Ciclu lent, gandit pentru restul retelei (productie, servere critice etc) 8. Solutia permite stabilirea zonelor de test si critice din cadrul retelei prin intermediul politicilor din consola de management. **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.
	Protecție stații de lucru și servere fizice/virtuale	**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. Pentru o mai buna protectie a statiilor si serverelor, solutia include un vaccin anti-ransomware. Acest vaccin asigura protectia impotriva tuturor amenintarilor cunoscute de tip ransomware, prin imunizarea statiilor si serverelor, chiar daca sunt infectate si prin blocarea procesului de criptare. 3. Vaccinul anti-ransomware primeste actualizari de la producator, odata cu actualizarea semnaturilor produsului Antimalware. 4. Pentru o mai buna protectie a statiilor si serverelor, solutia include protectie impotriva atacurilor zero-day de tip exploit (atacuri directionate). **Cerinte de sistem:** • Sisteme de operare pentru statii de lucru: Windows 10, Windows 8, Windows 7, Windows Vista (SP1), Windows XP (SP3), Mac OS X Sierra (10.12.x), 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) • 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) **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. **Caracteristici si functionalitati principale ale modulului antimalware:** 1. Solutia permite administratorului sa stabileasca actiunea luata de produsul Antimalware la detectarea unei amenintari noi. Astfel administratorul va putea alege intre urmatoarele actiuni: a. Actiune imiplicita pentru fisiere infectate: - interzice accesul - dezinfecteaza - stergere - muta fisierele in carantina - nicio actiune b. Actiune alternativa pentru fisierele infectate: - interzice accesul - dezinfecteaza - stergere - muta fisierele in carantina c. Actiune imiplicita pentru fisierele suspecte: - interzice accesul - stergere - muta fisierele in carantina - nicio actiune d. Actiune alternativa pentru fisierele suspecte: - interzice accesul - stergere - muta fisierele in carantina 2. Scanarea automata in timp real va putea fi setata sa nu scaneze arhive sau fisiere care depasesc o anumita dimensiune, marimea fisierelor putand fi definita de administratorul solutiei, 3. Definirea pana la 16 nivele de profunzime pentru scanarea in arhive. 4. 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. 5. 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 ce depasesc o anumita cantitate de date, configurabila de catrre administrator. 6. Scanarea automata a emailurilor la nivelul statiei de lucru pentru POP3/SMTP. 7. Configurarea cailor ce urmeaza a fi scanate la cerere. 8. 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. 9. 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. 10. Posibilitatea de configura scanarile programate sa se execute cu prioritate redusa

11. 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.
12. Administratorul poate personaliza şi motoarele de scanare, având posibilitatea de a alege între mai multe tehnologii de scanare:
    - Scanare locală, când scanarea se efectuează pe staţia de lucru locală. Modul de scanare locală este potrivit pentru maşinile puternice, având toate semnăturile şi motoarele stocate local.
    - Scanarea hibrid cu motoare light (Cloud public), cu o amprentă medie, folosind scanarea în cloud şi, parţial, 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)
13. 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.
14. Pentru o protectie sporita, solutia antimalware trebuie sa poata scana paginile HTTP.
15. Pentru o mai buna gestionare a antimalware instalat pe statii, produsul va include optiunea de setare a unei parole pentru protectia la dezinstalare.
16. Pentru siguranta utilizatorului, clientul va include un modul de antiphishing.
17. Solutia ofera protectie in timp real pe masinile cu sistem de operare Linux in conformitate cu versiunea de kernel instalata.
18. 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.

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.

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.

Protectia datelor:

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

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).

Controlul aplicatiilor:

1. Pentru o mai buna inventariere si administrare, solutia va include o sectiune in consola de administrare unde se vor regasi toate aplicatiile descoperite in retea, grupate dupa: nume, versiune, descoperit la, gasit pe.
2. Pentru o mai buna inventariere si administrare, solutia va include o sectiune in consola de administrare unde se vor regasi toate procesele negrupate descoperite in retea, grupate

		dupa: nume, versiune, nume produs, versiune produs, editor/autor, descoperit la, gasit pe. 3. Pentru prevenirea infectarii statiilor si serverelor dar si pentru a permite aplicatiilor descoperite in retea sa se poata actualiza, solutia permite definirea unor programe de actualizare (Updater) care vor fi lasate sa actualizeze diferite aplicatii instalate pe statii sau servere. 4. Solutia include optiunea de a permite sau a bloca rularea anumitor aplicatii sau procese definite de administrator (inclusiv subprocese) dupa: a. Cale fisier: local, CD-ROM, portabil sau retea b. Hash **c.** Certificat **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. **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 disponibila local pe masina client. 3. Administratorul va putea suprascrie din consola setarile aplicate de utilizatorii Power User. **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.
Mentenanță și support tehnic		Pe toată durata contractului

Nota:

1. Ofertanții vor atașa propunerii tehnice fișele tehnice ale produselor de la producător.

2. Ofertanții vor pune la dispoziția beneficiarului, cel puțin două nume, adrese și numere de telefon pentru asistenta tehnică.

3. Autoritatea contractantă își rezervă dreptul de a verifica datele tehnice prezentate de către ofertanți. În cazul unor neconcordanțe sau a prezentării unor date false, autoritatea contractantă are dreptul de a elimina oferta respectivă. Caracteristicile prezentate în propunerea tehnică și nerealizate în exploatare, vor determina suportarea de către furnizor a contravalorii eventualelor daune cauzate autorității contractante.

Întocmit,
Direcția Informatizare și Comunicații Digitale,
Director,
ing. mat. Marius Constantin Șutu