Specificaţii tehnice (F4.1)

[Acest tabel va fi completat de către ofertant în coloanele 3, 4, 5, 7, iar de către autoritatea contractantă – în coloanele 1, 2, 6, 8]

Numărul procedurii de achiziţie - conform SIA RSAP din ocds-b3wdp1-MD-1582647627015 din 25.02.2020

Denumirea procedurii de achiziţie: **Pachete software şi sisteme informatice, Pachete software antivirus conform necesităţilor Armatei Naţionale**

Cod CPV	Denumirea bunurilor solicitate	Modelul articolu-lui	Ţara de origine	Produ-cătorul	Specificarea tehnică deplină solicitată de către autoritatea contractantă	Specificarea tehnică deplină propusă de către ofertant	Standarde de referinţă
1	2	3	4	5	6	7	8
48000000-8	Pachete software antivirus	Bitdefender	România	România	**Soluție de protecție și securitate antivirus pentru protecția infrastructurii:** Se solicită achiziția unei soluții corporative antivirus de protecție și securitate pentru o perioadă de 36 luni: - **760** sisteme IT (stații de lucru fizice/virtualizate și servere fizice/virtualizate); - **760** licențe pentru managementul patch-urilor; - **10** licențe pentru dispozitive mobile; - **70** licențe pentru criptare a hardisk-urilor; - peste 1000 căsuțe poștale de tip Exchange. **1.1. Cerințe tehnice funcționale minim solicitate:** - Soluția va asigura protecție pentru stații de lucru și servere cu următoarele SO: ✓ Windows XP (SP3), 7, Vista (SP1), 8.1, 10, Mac OS X 10.12.x, 10.11.x, 10.10.x ,10.9.x, 10.8.x; ✓ Windows Server 2003/2008/2008 R2/2012/2012 R2/2016, 2019. ✓ Red Hat Enterprise Linux / CentOS 5.6 sau mai recent, Oracle Linux 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, Debian 5.0 sau mai recent. - Soluția va oferi unul sau mai multe module de update server care va asigura actualizarea componentelor și a semnăturilor;	Conform Cerințelor tehnice a Autorității contractante	ISO 9001 ISO 27001

Digitally signed by Cioclea Victor
Date: 2020.04.09 09:31:38 EEST
Reason: MoldSign Signature
Location: Moldova

					- Va permite activarea și dezactivarea actualizărilor automate de produs și semnături, precum și a consolei de management; - Va transmite alerte de nefuncționalitate, cu minim 30 de minute înainte de actualizare pentru a avea un timp de reacție în cazul unei defecțiuni a acesteia; - Va oferi un istoric cu toate modificările realizate față de soluție precum: versiunea consolei de management, data versiunii, funcții noi și îmbunătățiri, probleme soluționate, probleme cunoscute și alte funcționalități; - Va oferi posibilitatea de a primi notificări despre alertele existente, să notifice administratorul în cazul unor probleme critice (cu posibilitate de a fi configurabile la necesitate) precum: licențiere, detecție viruși, actualizări de produs disponibile și altele ce țin de funcționarea corectă a produsului, etc.; - Va oferi posibilitatea de integrare cu un server Syslog pentru raportarea evenimentelor antivirus și preluarea acestora de către o soluție de tip SIEM; - Soluția va înregistra evenimentele în baza activităților/acțiunilor create de utilizatorii finali și va putea oferi informații detaliate pentru fiecare acțiune în parte, inclusiv cu posibilitatea de filtrare a acestora; - Va oferi posibilitatea de instalare a protocolului SMNP pentru a putea remite rapoarte referitor la statutul mașinilor din cadrul consolei de management; - Va oferi obligatoriu posibilitatea de creare a copiei de siguranță a bazei de date a consolei de administrare, la cerere sau planificată, stocată local, fie pe un file server, FTP sau în rețea în scopul asigurării continuității activității și minimalizării riscului; - Soluția se va integra cu următoarele sisteme IT și servicii: AD, VMware vCenter, Citrix Xen, inclusiv cu importarea inventarului acestor platforme; - Să fie interoperabilă și să recunoască infrastructuri virtualizate ca: Microsoft Hyper-V, Red Hat VM, Oracle VM, KVM etc.; - Să ofere posibilitatea de descoperire a echipamentelor IT care nu pot fi sau nu au fost integrate în AD (prezente în Workgroup și/sau care nu sunt incluse în domen) prin intermediul Network discovery;		

					- Să ofere posibilități de căutare, sortare și filtrare după numele sistemului, SO și adresă IP; - Să ofere posibilitatea de instalare și configurare local sau la distanță a utilizatorilor antivirus pe sistemele IT (utilizatori finali, servere, inclsiv cele virtualizate); - Să ofere posibilitatea de selectare a modulelor componente atunci când se crează pachetul utilizatorului care se instalează pe echipamentele IT (fizice și virtualizate); - Să poată lansa operații de scanare, actualizare, instalare, dezinstalare la distanță pentru clientul antivirus. Să ofere posibilități de repornire a mașinilor fizice de la distanță; - Să ofere informații detaliate despre fiecare activitate inițiată (cu afișarea statutului); - Să includă configurarea centralizată a clienților antivirus prin politicile create (setate); - Să includă în consola de management urmatoarele informații despre sistemele IT precum: Nume, adresă IP, SO, Grup, Politica atribuită fiecărui utilizator sau grup, ultimele actualizări, Versiunea produsului inclusiv Versiunea de semnături; - Să ofere posibilitatea de găsire și afișare a tuturor aplicațiilor instalate pe toate echipamentele IT (stații și servere din rețea); - Să includă posibilitatea de creare și descărcare a unui pachet unic pentru toate SO (Windows, Linux, MacOS etc.), atât pentru echipamentele IT ale utilizatorilor, cât și pe servere (fizice și virtualizate); - Să includă activarea, dezactivarea, posibilitatea de configurare a funcționalităților precum: scanarea la cerere, firewall, controlul accesului la Internet, controlul aplicațiilor, scanarea traficului web, controlul dispozitivelor, dreptul autorizat (privilegiat) al utilizatorului; - Să includă posibilitatea de aplicare și setare a politicilor pe echipamentele IT ale clienților, grupurilor de mașini, domen, unități organizaționale sau utilizatori din AD; - Să includă posibilitatea de schimbare a unei politici sau a mai multor politici în funcție de: Utilizatorii logați, adrese sau clase IP, Gateway, server DNS alocat, clienți care fac parte sau nu din aceiași rețea cu infrastructura de management, Tipul rețelei (lan, wireless);		

					- În cazul fișierului care ajunge în carantină, soluția va oferi posibilitatea de restabilire a fișierului în locația de origine sau într-o altă locație pentru a putea fi modificat și configurat. De asemenea, administrarea carantinei trebuie să se poată realiza centralizat din consola de management (lucrul cu transformarea fișierelor și repoziționarea lor); - Administrarea, monitorizarea utilizatorilor să fie efectuată pe baza rolurilor atribuite și/sau implicite: admin (rețea, companie), reporter și alte roluri disponibile sau implicite care vor fi configurate cu posibilitatea de selectare a serviciilor și obiectelor pentru care un utilizator poate avea acces sau poate face modificări. Utilizatorii vor putea fi importați din AD sau adăugați (creați) manual prin intermediul consolei de management. De asemenea, va include funcționalitatea de deconectare automată a oricărui tip de utilizator (necătând la rolurile alocate) după o anumită perioadă de timp; - Să ofere posibilitatea de a primi și transmite actualizările prin setarea de locații, prin alocarea permisiunilor pentru a activa și dezactiva funcția de actualizări de produs (sistem) și semnături. Va include posibilitatea ca orice client antivirus să poată fi configurat cu proprietatea de a transmite actualizările necesare către alt client antivirus. Actualizările se vor putea realiza la nivel de stație în mod silențios (fără avertizări) sau fie folosind unul sau mai multe servere de actualizări și, de asemenea, pentru locațiile la distanță prin intermediul unui client antivirus care are și rol de server de actualizare; - Să includă posibilitatea de a testa noile versiuni de pachete de instalare ale clientului antivirus, înainte de a fi instalate pe toate echipamentele IT și serverele din infrastructura existentă, evitând careva probleme ce pot afecta anumite servere sau stații critice. Soluția propusă, prin intermediul serverului de actualizare, va oferi actualizarea de produs în două cicluri: ciclul rapid destinat unui mediu de testare în cadrul rețelei și ciclul lent - destinat pentru infrastructura de rețea (producție, servere critice etc.). De asemenea, soluția va include posibilitatea de stabilire a zonelor de testare și chiar a zonelor stabilite ca critice din cadrul infrastructurii de rețea prin intermediul politicilor setate (create și configurate) din consola de management;		

					- Să includă posibilitatea de a instala la necesitate module personalizate; - Soluția propusă va include o funcționalitate împotriva virușilor anti-ransomware (cu funcțional de criptare), cu actualizări de la producător pentru protecția împotriva amenințărilor cunoscute de tip ransomware, prin protecția stațiilor utilizatorilor și a serverelor (chiar dacă sunt infectate) și blocarea procesului de criptare. Pe lângă funcționalitatea anti-ransomware, soluția va oferi protecție împotriva atacurilor de tip zero-day (atacuri direcționate) și inclusiv va include module avansate de securitate, destinate pentru a detecta atacuri cibernetice avansate și activități suspecte în faza de pre-execuție, pentru protecție împotriva: atacurilor direcționate de tip APT (advanced persistent attack), fișierelor suspecte și traficului suspect la nivel de rețea, exploit-urilor, ransom-ware și gray-ware cu posibilitatea de stabilire a nivelului de protecție dorit: permisiv, normal, agresiv cu posibilitatea extinderii nivelului de raportare pentru a include nivelurile superioare; - Să includă un funcțional de tip sandbox în cloud-ul producătorului, ce va oferi posibilitatea de trimitere manuală și la alegere, inclusiv automat, fișiere, unde vor putea fi incluse pentru o analiză în profunzime. Acest funcțional de tip sandbox va include câteva posibilități de analiză precum: doar monitorizare sau blocare cu două tipuri de acțiuni de remediere: implicită și de siguranță. Pentru acțiunea implicită se va oferi minim posibilități de raportare, tratare, ștergere și transmitere în carantină. Pentru acțiunea de siguranță se va oferi minim posibilități de ștergere sau permutare în carantină. Legat de posibilitatea de trimitere manuală a fișierelor în sandbox-ul din cloud-ul producătorului, aceasta va trebui să fie realizată exclusiv prin oferirea dreptului administratorului de a realiza acest lucru în urmatoarele cazuri: dacă administratorul suspectează un fișier ca fiind maliții, îl poate trimite manual în sandbox pentru a fi analizat și a afla consecințele reale. Acesta va putea să trimită mai multe fișiere odată sau doar unul, cu posibilitate de a specifica dacă vor fi analizate individual sau toate în același timp. Acest modul va trebui să suporte analiza urmatoarelor tipuri de fișiere: Batch, CHM, DLL, EML, Flash SWF, HTML, HTML/script, HTML (Unicode), JAR		

					(archive), JS, LNK, MHTML (.doc), MHTML (ppt), MHTML (.xls), Microsoft Excel, Microsoft PowerPoint, Microsoft Word, MZ/PE files (executable), PDF, PEF (executabile), PIF (executabile), RTF, SCR, URL (binare), VBE, VBS, WSF, WSH, WSH-VBS, XHTML. Fișierele menționate, vor putea fi detectate corect chiar dacă sunt incluse în arhive de tip: 7z, ACE, ALZip, ARJ, BZip2, cpio, GZip, LHA, Linux TAR, LZMA Compressed Archive, MS Cabinet, MSI, PKZIP, RAR, Unix Z, ZIP, ZIP (multivolume), ZOO, XZ; - Să ofere posibilitatea de stabilire a acțiunilor întreprinse de modulul antivirus la detectarea unei amenințări noi prin oferirea posibilității administratorului de soluție de a lua minim următoarele acțiuni: 1. Implicită, pentru fișiere infectate: interzice accesul, tratare, ștergere, permutare fișiere în carantină, nici o acțiune; 2. Alternativă pentru fișierele infectate: interzice accesul, tratare, ștergere, permutare fișiere în carantină; 3. Acțiune implicită pentru fișierele suspecte: interzice accesul, ștergere, permutare fișiere în carantină, nici-o acțiune. 4. Acțiune alternativă pentru fișierele suspecte: interzice accesul, ștergere, permutare fișiere în carantină; - Să includă scanarea cu setare automată la moment (în timp real), cu posibilitatea de a configura excepții sau a exclude careva filtre sau setări și prin definirea unor liste de excludere de la scanare în timp real și la cerere a anumitor directoare, discuri, fișiere, extensii sau procese și să nu scaneze arhive sau fișiere mai mari de „x” MB, definirea nivelelor de profunzime pentru scanarea în arhive; - Să ofere funcțional de scanare euristică comportamentală prin simularea unui calculator virtual în interiorul căruia se rulează aplicații cu potențial periculos protejând sistemul de atacurile cibernetice necunoscute prin detectarea codurilor periculoase a căror semnătură nu a fost lansată încă. Pe lângă scanarea euristică, soluția va cuprinde minim următoarele funcționalități: scanarea oricărui suport de stocare a informației (CD-uri, hard-uri externe, unități partajate etc.) și scanarea automată a email-urilor la nivelul stației de lucru pentru protocoalele POP3/SMTP. Aceasta va include cel puțin cinsprezece nivele de profunzime pentru scanarea în arhive, să configureze căile ce urmează a fi scanate la cerere, să ofere protecție anti-spyware cu ajutorul		

					unei baze de date complete cu semnături de spyware și a euristicii de detecție a acestui tip de programe, să poată seta priorități pentru scanările programate, să poată configura scanarea în cloud sau pe mașina de scanare instalată în rețea și parțial scanarea locală pentru stațiile ce nu au suficiente resurse hardware; - Administratorul să aibă posibilitate de a personaliza, inclusiv motoarele de scanare, având posibilitate de alegere între mai multe tehnologii de scanare: scanare locală (de pe stația locală), scanare hibridă (utilizarea parțial a stației locale cu motoare ușoare de scanare pentru reducerea resurselor și scanarea centralizată în instrastructura instituției), scanare centralizată în cloud-ul privat al instituției (crearea unui server de securitate de scanare). Scanarea centralizată va include posibitatea de trecere pe scanare locală sau de trecere pe scanare hibridă; - Să ofere posibilitatea de a seta tipuri de detecție pe bază de semnături, pe bază de comportamentul fișierelor sau chiar pe baza monitorizării proceselor; - Să includă posibilități de scanare a paginilor web, cu posibilitatea de a seta o parolă pentru protecția la dezinstalare, funcțional de tip antiphishing, protecție în timp real pe mașinile cu sistem de operare Linux și/sau Windows în conformitate cu versiunea de kernel instalată și chiar instalarea clientului pe mașinile virtuale parte a unui grup doar pe mașina de tip model, după care se recompune grupa sau grupul de mașini virtualizate; - Să ofere posibilitatea de a seta reguli pentru funcționalul de firewall, pentru aplicații sau conectivitate. Modulul de firewall să poată fi instalat sau dezinstalat la necesitate. Acesta, inclusiv va permite definirea rețelelor de încredere pentru sistemul IT cu destinație; - Să ofere funcțional de blocare a datelor confidențiale ale utilizatorului, precum ar fi (pin-ul cardului, cont bancar și altele) transmise prin HTTP sau SMTP, prin crearea unor reguli specifice; - Să ofere un modul integrat dedicat controlului conținutului prin acces la Internet cu următoarele particularități: blocarea accesului la accesarea Internetului pentru anumite echipamente IT client sau grupuri de mașini, blocarea accesului la Internet pe intervale orare, blocarea		

					paginilor web care conțin anumite cuvinte cheie, controlul accesului numai la anumite pagini web specificate de administrator, blocarea accesului la anumite aplicații definite de administrator, restricționarea accesului pe anumite pagini web după anumite categorii prestabilite (ex: online dating, violență, pornografie etc. care fac parte din acest grup); - Să ofere funcțional de control al aplicațiilor pentru administrare și inventariere care va oferi posibilitatea de a efectua descoperirea aplicațiilor utilizate pe stațiile utilizatorilor grupate după: nume, versiune, descoperit la, găsit pe etc. Va include posibilitatea de a accesa toate procesele descoperite în timpul scanării rețelei, aranjate (filtrate) după: nume, nume produs, versiune produs, editor sau autor, descoperit la, găsit pe, etc. Va putea să blocheze rularea anumitor aplicații sau procese definite de administrator (inclusiv la nivel de subprocese) după: cale stocare fișier: local, CD-ROM, portabil sau rețea, hash, certificat etc.; - Să ofere funcțional de control al dispozitivelor externe cu următorul funcțional: de a instala sau dezinstala conform setărilor stabilite în baza cadrului legal intern al instituției, de a permite controlul următoarelor tipuri de dispozitive: Bluetooth Devices, CDROM Devices, Floppy Disk Drives, Security Policies 153, IEEE 1284.4, IEEE 1394, Imaging Devices, Modems, Tape Drives, Windows Portable, COM/LPT Ports, SCSI Raid, Printers, Network Adapters, Wireless Network Adapters, Internal and External Storage; de a permite configurarea de reguli prin care se vor defini permisiunile pentru dispozitivele conectate la mașina client, de a permite configurarea de excluderi pentru diferite tipuri de dispozitive pentru care s-au configurat reguli; - Să ofere funcțional de a acorda acces cu drepturi privilegiate, ca: instalarea, dezinstalarea la necesitatea administratorului sau al utilizatorului, acordarea utilizatorilor drepturi privilegiate pentru o anumită perioadă de timp, pentru a putea accesa și modifica setările clientului antivirus dintr-o consolă disponibilă local sau de a permite administratorului soluției să suprascrie din consolă setările aplicate de utilizatorii cu drept privilegiat; - Să ofere funcțional de control al dispozitivelor mobile diponibile pe platforma Android (de la versiunea 5 până la		

					cea actuală) și iOS (de la versiunea 5 până la cea actuală). Necesitatea acestui funcțional este necesar ca în cazul în care clientul va dori să protejeze inclusiv și terminalele mobile, aceasta să se poată realiza doar prin transfer de licență și nu prin achiziția unui alt modul. Drept urmare, acesta trebuie să ofere posibilități de asociere a unui dispozitiv cu un utilizator din AD, să ofere posibilitatea instalării prin trimiterea unui email către utilizator cu detalii de instalare, să permită activarea dispozitivului mobil în consola de management prin scanarea unui cod QR, să asigure disponibilitatea pachetelor de instalare de pe AppStore și GooglePlay, să poată întreprinde inclusiv acțiuni de blocare a dispozitivelor, de deblocare a dispozitivelor, de ștergere a datelor și revenire la setările din fabrică, de localizare a dispozitivelor, de scanare a dispozitivelor (cel putin pentru cele cu sistem de operare Android), de criptare a informației dispozitivelor (cel putin pentru cele cu sistem de operare Android). Funcționalul de control al dispozitivelor mobile va oferi raportarea dispozitivelor: active, inactive, deconectate, cu sistemul de operare modificat astfel încât utilizatorul sa aibă acces total asupra lui (rooted or jailbroken devices), va putea întreprinde automat acțiuni în cazul în care un dispozitiv nu este conform cu setările dorite precum: ignorarea; blocarea accesului, blocarea dispozitivului sau ștergerea datelor și revenirea la setările din fabrică și inclusiv ștergerea dispozitivului din consolă; - Să includă forțarea blocării dispozitivelor prin parole, respectând regulile privind complexitatea setată în baza politicilor stabilite, cu o perioadă de expirare setată, posibilitate de autoblocare a dispozitivelor după un număr de minute setat; - Să includă posibilitatea de a seta profiluri care vor stabili măsuri/reguli/filtre de securitate pentru a accesa rețelele fără fir sau cele tunelare dar și pentru a accesa careva pagini web prin: a permite, a bloca sau planifica pentru anumite zile și perioade orare a accesului la anumite pagini web; crea unele excepții pentru blocarea sau permiterea accesului către anumite pagini Internet. Va include posibilitatea de a seta profiluri de acces a paginilor web, de a permite sau de a bloca: utilizarea browsere-lor, opțiunea de completare automată a informațiilor, alertarea		

					utilizatorului în cazul accesării unor pagini frauduloase, Javascript, Pop-up-urilor, Cookie-uri etc.; - Să ofere funcțional de management al actualizării aplicațiilor. Acesta din urma trebuie să ofere un minim de funcțional precum: integrarea clientului de patch management cu clientul antivirus, ca un modul separat. Gestionarea produsului trebuie să fie realizată din aceeași consolă de management ca și soluția de securitate antivirus pentru infrastructura fizică și virtualizată (echipamente IT și servere), dar și pentru serverul de Exchange și dispozitivele mobile (Android și iOS) descrise mai sus. Posibilitatea funcționării în mod automat cu următoarele presetări: programarea evaluării pentru patch-ul lipsă, programarea instalării automate, în baza categoriei de patch-uri (securitate și non-securitate) și posibilitatea de a amâna repornirea, dacă instalarea patch-ului o cere. De asemenea, soluția va include opțiunea de scanare, descoperire și instalare de patch-uri la cerere, posibilitatea de a descoperi patch-urile lipsă din infrastructură și agregarea lor într-un inventar de patch-uri, de a oferi vizibilitatea de patch-uri instalate și a celor lipsă pe stațiile de lucru, informații despre patch-uri instalate și motivul sau cauza instalării nereușite, posibilități de a instala rapid patch-uri lipsă, posibilitatea de a stopa instalarea unuia sau a mai multor patch-uri/update-uri, inclusiv notificarea periodică privind statul infrastructurii, patch-uri instalate, patch-uri lipsă și stocarea locală a patch-urilor primite; - Să includă posibilitatea de cunoaștere a patch-iurilor necesare pentru minimum urmatoarele aplicatii: 7-Zip, Adobe: Acrobat / Bridge / Creative Cloud / Distiller / Dreamweaver / Flash / Photoshop / Reader, Apache, Apache Tomcat, Apple: iCloud / iTunes / Mobile Device Support / QuickTime / Safari / Software Update, WebEx: Meeting Center / Productivity Tools, Citrix Receiver / Single Sign-On / Delivery Controller / GoToMeeting / Online Plugin / Provisioning Services / Virtual Delivery Agent / XenApp / XenDesktop, FileZilla, Foxit: PhantomPDF / Reader, Gimp, TightVNC, Google: Chrome Browser for enterprise / Drive / Picasa, Greenshot, KeePass, LibreOffice, ImgBurn, Microsoft: .NET / Azure / DirectX / Dynamics / Exchange Server / Exchange System Manager / Forefront / Internet Explorer /		

					Internet Information Server /Lync / Lync Server / Office / Outlook / Power BI Desktop / Report Viewer / Search / Services for Unix / Sharepoint / Skype / Silverlight / System Center Operations Manager / System Center Virtual Machine Manager / SQL Server / Systems Management Server / Virtual Machine / Virtual PC / Virtual Server / Visual Basic / Visual C++ / Windows / Windows Defender / WSUS / Windows Mail /Kerberos, Firefox, Thunderbird, Notepad++, GeForce Experience, Opera, Oracle: OpenOffice / VM VirtualBox, Recuva, Prezi Desktop, RealVNC, PuTTY, Java, TeamViewer, PDF-Xchange, UltraVNC, VLC, VMware: Horizon View Client/Player/Tools/Workstation, WinSCP, Wireshark, Xmind); - Să ofere funcțional pentru managementul criptării discurilor pentru un numar de calculatoare (staționare și portabile) selectate. Aceasta va trebui sa ofere un minim de funcțional precum: să poată fi gestionată cu aceeași soluție propusă pentru protecția stațiilor de lucru și servere, mobile, mail și managementul patch-urilor, să folosească mecanismul nativ de criptare al SO: BitLocker pentru Windows și FileVault pentru Mac OSX, să cripteze discurile rigide ale stațiilor de lucru integral, să impună autentificarea utilizatorului înainte de startarea SO (autentificarea la pre-butare), să păstreze cheile de criptare pe acelaș server de management al protecției antivirus, managementul cheilor utilizate să fie efectuat din aceeași consolă, inclusiv recuperarea rapidă a cheilor la solicitarea autorizată, să ofere un raport complet asupra stării de criptare a dispozitivelor inclusiv: numele stației, IP-ul stației, SO, ID-ul volumului/partiției, numele partiției, starea criptării partiției, tipul partiției: boot, non-boot, mărimea partiției în GB, ID-ul cheii de recuperare, să asigure criptarea pentru următoarele SO: Windows 7 Enterprise (with TPM); Windows 8.1 Pro/ Enterprise; Windows 10 Pro/Enterprise; WinServer 2008 R2 (withTPM); WinServer 2012/2012 R2, WinServer 2016, OSX 10.9/ 10.10 / 10.11/ 10.12; I. Să ofere funcțional de protecție a serverului de mail de tip Exchange prin aceeași soluție propusă, inclusiv și management, fără achiziția unui modul adițional sau licență adițională. Funcționalul minim solicitat pentru protecția serverului de mail de tip Exchange ar trebui să ofere protecție antivirus, antispam (inclusiv antiphishing), precum și filtrare		

					de atașamente și conținut, să asigure scanarea atașamentelor și a conținutului mesajelor în timp real, fără a afecta vizibil performanța serverului de mail, să asigure actualizarea antivirus automat la un interval de maxim 1 oră, precum și la cerere, să includă, pe lângă detecția pe baza de semnături, scanarea euristică comportamentală pentru a proteja sistemul de viruși necunoscuți prin detectarea codurilor, să ofere opțiuni multiple de acțiune la identificarea unui atașament virusat (dezinfectare, ștergere, mutare în carantină), să ofere protecție anti-spyware (cu bază de semnături actualizabilă) pentru a preveni furtul de date confidențiale, să ofere protecție antispam (cu o bază de semnături actualizabilă. Modulul antispam pentru funcționalul solicitat va trebui să includă un filtru URL cu o bază de adrese URL cunoscute a fi folosite în mesaje spam, precum și un filtru de caractere pentru detectarea automată a mesajelor scrise cu caractere latine, chirilice, asiatice și altele, să ofere filtru RBL care să identifice spam-ul prin sincronizarea cu anumite baze de date online care conțin liste de servere de mail cunoscute ca fiind la originea acestui tip de mesaje, să ofere un serviciu/filtru online pentru îmbunătățirea protecției împotriva valurilor de spam nou apărute, să ofere posibilitatea de a defini politici de filtrare antivirus, antispam, a conținutului sau atașamentelor pentru diferite grupuri sau utilizatori, să asigure actualizarea produsului că va fi configurabilă și se va putea realiza din internet, direct sau printr-un proxy, sau din cadrul rețelei de pe un server de actualizare propriu, să ofere statistici atât referitoare la scanarea antivirus, cât și la scanarea antispam. **1.2. Cerintele tehnice vis-a-vis de administrarea solutiei:** - Soluția propusă va fi livrată ca o mașină virtuală preinstalată. Aceasta nu va necesita nici o licență suplimentară pentru sistemul de operare, iar imaginea (de tip template) va fi posibil de a fi importată pe urmatoarele platforme de virtualizare: VMware vSphere, Citrix XenServe, Microsoft Hyper-V, Red Hat Enterprise Virtualization, KVM, Oracle VM; - Administrarea se va face doar printr-o consolă de management pentru întreaga soluție cu funcționalul solicitat mai sus. Aceasta trebuie să fie oferită cu o bază de date inclusă care să ofere un funcțional de scalabilitate (să nu fie dependent de componentele de hardware, orice maşină poate fi îndepărtată sau adăugată fără eforturi operaţionale semnificative, oricare dintre roluri sau servicii să fie instalate		

					separat sau împreună pe aceeași sau mai multe VDI-uri), să poată asigura mai multe roluri precum: server cu bază de date, server de comunicație, server de actualizare, server de web, să asigure posibilitatea de a instala serviciile de scanare centralizată pentru mediile virtuale VMware și Citrix prin sarcina directă din consola de management, să poată oferi un modul de load balancy pentru performanță și redundanță, inclusiv mecanisme de configurare a disponibilității pentru serverul cu baze de date (clustering) și chiar posibilitatea de a fi accesată atât de pe stațiile de lucru cât și de pe dispozitivele mobile; - Pentru o administrare mai accesibilă și mai usoară, interfața consolei de administare și a clientului de securitate (instalată pe stațiile de lucru și servere) prioritate va avea cea propusă în limba română (preferențial), engleză, rusă (opțional); - Să ofere posibilitate de urmărire a actualizărilor consolei de administare vizualizând următoarele date: Versiunea consolei de management, Data versiunii, Funcții noi și Îmbunătățiri, Probleme rezolvate, Probleme cunoscute. **1.3. Cerinte vis-a-vis de functionalul de raportare:** - Să poată oferi funcțional de raportare cu capabilități de setare de opțiuni specifice pentru afișarea rapoartelor existente, să ofere un panou central care să afișeze statutul modulelor și rapoartele lor pentru perioadele de timp specificate, să conțină rapoarte care prezintă statutul mașinilor clienților, al actualizărilor, fișierelor malware detectate, aplicațiile blocate, paginilor web blocate, să trimită rapoarte către un număr nelimitat de adrese de email, să permită vizualizarea rapoartelor curente programate de administrator, să permită exportarea rapoartelor în format .pdf și detaliile ca format .csv., să includă un generator de rapoarte care să ofere posibilitatea de a investiga o problemă de securitate pe baza mai multor criterii, menținând informațiile concise și ordonate corespunzător, să includă interogări precum: starea terminalului, evenimente terminal, evenimente Exchange, să ofere interogări legate de starea terminalului precum: tip mașină, infrastructura rețelei căreia aparține, datele agentului de securitate, starea modulelor de protecție, rolurile terminalelor, să ofere interogări legate de		

					evenimente precum: calculatorul țintă pe care a avut loc evenimentul, tipul, starea și configurația agentului de securitate instalat, starea modulelor și rolurilor de protecție instalate pe agentul de securitate, denumirea și alocarea politicii, utilizatorul autentificat în timpul evenimentului, evenimente (site-uri blocate, aplicații blocate, detecțiile etc.), să ofere interogări de evenimente Exchange precum: direcția traficului e-mail, evenimente de securitate (detectarea programelor de tip malware sau a fișierelor atașate), măsurile implementate în fiecare situație (tratarea, ștergerea, înlocuirea sau trimiterea în carantină a fișierului, ștergerea sau blocarea e-mail-ului). **1.4. Alte cerințe obligatorii:** 1.Pentru soluția ofertată se solicită a fi 36 luni suport atât local, cât și de la producător; 2.Producătorul trebuie să ofere suport 24/7, prin e-mail sau conectare de la distanță, inclusiv suport local din partea partenerului; 3.Lucrările de instalare, configurare, punerea în funcţiune a soluției trebuie să fie executate de ofertant; 4.Prezentarea certificatelor de conformitate ISO 27001 și ISO 9001 ale ofertantului, valabile la data prezentării; 5.Prezentarea certificatelor de calificare pentru personalul implicat în livrarea, instalarea produsului, precum și instruirea personalului local (până la 5 persoane); 6.Manualul de instalare și administrare a produsului va fi în limba română (preferențial) și limba engleză (obligatoriu); 7.Autorizarea de la Producător vis-a-vis de dreptul de vânzare a produselor pe teritoriul Republicii Moldova (copia diplomei de partener autorizat- MAF); Termen de livrare (instalare): 30 zile lucrătoare de la data întregistrării contractului la trezoreria regională Chișinău.		
Total							

Semnat:_____

Numele, Prenumele: Victor Cioclea

În calitate de: Administrator

Ofertantul: S.C. „RTS ONE” S.R.L.

Adresa: mun. Chișinău, str. Mit. Bănulescu-Bodoni 59/B of. 815