"RTS ONE" S.R.L.
https://rts.md
(+373) 22 101 777
office@rts.one
str. Mitropolit
G. Bănulescu-Bodoni
59/B, of. 815

Anexa nr. 22
la Documentația standard pentru procedura
de achiziție, cu nr. de identificare în SIA RSAP
Mtender: **ocds-b3wdp1-MD-1661254155757**

SPECIFICAȚII TEHNICE

Numărul procedurii de achiziție: MTender ID: **ocds-b3wdp1-MD-1661254155757**
Denumirea procedurii de achiziție: **Servicii de asigurarea protecției și securității cibernetice**

Denumirea bunurilor	**Modelul articolului**	**Ţara de origine**	**Producă-torul**	**Specificarea tehnică deplină solicitată de către autoritatea contractantă**	**Specificarea tehnică deplină propusă de către ofertant**	**Standarde de referinţă**
2	3	4		5	6	7
Lot 1 Servicii de asigurarea protecției și securității cibernetice	Bitdefender GravityZone Business Security Premium (Elite)	Romania	Romania	Conform Anunțului de participare, pct.8 – Specificații tehnice	**Produsul este o platformă de management al securității endpoin-urilor, gândită ca o soluție modulară și scalabilă.** **Termenul de valabilitate a serviciilor SW Subscription & Support Renewal antivirus software sunt valabile pentru 36 luni.** **1. CONSOLA DE MANAGEMENT** ***1.1. Instalare si configurare:***	

					1.1.1. Pachetul de instalare necesar va fi livrat ca o masina virtuala bazata pe sistem de operare Linux securizat care contine toate rolurile sau serviciile necesare. Consola nu necesita o licenta suplimentara pentru sistemul de operare. Imaginea de tip template se va putea importa in: a. VMware vSphere, View, Horizon b. Citrix XenServer, XenApp, Xen Desktop c. Microsoft Hyper-V d. Red Hat Enterprise Virtualization e. KVM sau „Kernel-based Virtual Machine" f. Oracle VM. g. Nutanix h. Alte platforme de virtualizare, la cerere 1.1.2. Consola de management necesar va fi livrat 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. 1.1.3. Solutia este scalabila, astfel ca oricare dintre roluri sau servicii pot fi instalate separat pe mai multe masini virtuale sau pe aceeasi masina virtuala.R 1.1.4. Rolurile principale sunt cel putin similare cu: Server cu baza de date, Server de comunicatie, Server de actualizare, Server de Web. 1.1.5. Solutia propusă 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). 1.1.6. În solutia este inclus un mecanism de configurare a disponibilitatii pentru Serverul cu baze de date (clustering pentru redundanta). Astfel, baza de date poate fi instala de mai multe ori, pe mai multe masini virtuale. 1.1.7. Masinile de scanare pentru mediile virtuale VsMware si Citrix sunt posibil de instalat la distanta prin task din consola de management, iar pentru alte platforme se descarca separat din interfata web a produsului. ***1.2. Cerinte generale:*** 1.2.1. Interfata consolei de management este și în limba romana. 1.2.2. Interfata clientului de securitate, care se instaleaza pe statii si servere, este în limba romana. 1.2.3. Manualul de instalare a produsului este în limba romana. 1.2.4. Manualul de administrare a produsului este în limba romana.	

					1.2.5. Solutia include un modul de update server prin care să asigure actualizarea de produs si a semnaturilor. 1.2.6. Solutia să pemită activarea/dezactivarea actualizarilor de produs/semnaturi. 1.2.7. 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 fie actualizat. De asemenea, permite si trimiterea unei alerte de nefunctionalitate, cu 30 de minute inainte de actualizare. 1.2.8. 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 a) versiunea consolei de management b) data versiunii c) functii noi si imbunatatiri d) probleme rezolvate e) probleme cunoscute 1.2.9. Notificarile – prezente in interfata, notificarile necitite sunt evidentiate, trimise catre una sau mai multe adrese de email, cu alertarea administratorul in cazul unor probleme majore: licentiere, detectie virusi, actualizari de produs disponibile). 1.2.10. Solutia permite integrarea cu un server Syslog pentru raportarea evenimentelor antimalware. 1.2.11. Solutia permite instalarea serviciului de SMNP prin care se pot raporta statusul masinilor din cadrul componentei de management. 1.2.12. 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. 1.2.13. Consola de management este accesibila atat de pe statii de lucru cat si de pe dispozitive mobile (smartphone, tableta). ***1.3. Panou de monitorizare si raportare (Dashboard):*** 1.3.1. Rapoartele din panoul de monitorizare sunt posibil de 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). 1.3.2. Panoul central necesar contine rapoarte pentru toate modulele suportate. 1.3.3. Rapoartele din panoul central de comanda permit: adaugarea altor rapoarte, stergerea lor si rearanjarea. ***1.4. Inventarierea retelei – managementul securitatii:*** 1.4.1. Solutia poate fi integrata cu domenii Active Directory multiple, VMware vCenter Server, Citrix Xen Server, Nutanix Prism Element si importa inventarul acestor platforme. 1.4.2. Soluția permite descoperirea statiilor statii fizice neintegrate in Active Directory (Workgroup) cu ajutorul Network discovery. 1.4.3. Solutia oferă optiuni de cautare, sortare si filtrare dupa numele sistemului, sistem de operare, adresa IP, politica aplicata, ultima data cand s-a conectat (online si/sau offline) si FQDN. 1.4.4. Solutia permite crearea unui pachet unic pentru toate sistemele de operare, de statii sau servere. Astfel, administratorul poate descarca pachetele pentru protectia statiilor si serverelor pe care ruleaza sistemul de operare Windows, Linux, Mac. 1.4.5. Pentru integrarea cu Active Directory, soluția poata defini intervalul (in ore) de sincronizare si forta sincronizarea. 1.4.6. Soluția permita descoperirea masinilor din Microsoft Hyper-V, Red Hat VM, Oracle VM, KVM. 1.4.7. Solutia permite instalarea la distanta sau manual a clientilor antimalware pe masini fizice/virtuale. 1.4.8. Solutia permite selectarea modulelor componente atunci cand se creaza pachetul clientului care se instalează pe mașinile fizice/virtuale. 1.4.9. Solutia permite lansarea de task-uri de scanare, actualizare, instalare, dezinstalarea la distanta pentru clientul antimalware. 1.4.10. Solutia oferă posibilitatea de repornire a masinilor fizice de la distanta. 1.4.11. Solutia oferă informatii detaliate despre fiecare task si sa fiseaze daca task-ul s-a finalizat sau nu cu succes. 1.4.12. Solutia permite configurarea centralizata a clientilor antimalware prin intermediul politicilor.	

					1.4.13. Soluția oferă 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. 1.4.14. Solutia permite descoperirea tuturor aplicatiilor instalate pe toate statiile si serverele din reatea, prin rularea unui task din consola de administrare. ***1.5. Politici:*** 1.5.1. Solutia permite configurarea setarilor clientului antimalware prin intermediul unei singure politici ce contine setari pentru toate module. 1.5.2. Politica 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. 1.5.3. Solutia permite aplicarea politicilor pe masini client, grupuri de masini, pool-uri de resourse (VMware), domeniu, unitati organizationale, grupuri de securitate sau useri de active directoy. 1.5.4. Politica poate fi schimbata automat in functie de: a) IP sau clasa de IP al statiei b) Gateway-ul alocat c) DNS serverul alocat d) WINS serverul alocat e) Sufix DNS pentru conexiunea dhcp f) Clientul este/nu este in acceasi retea cu infrastructura de management (statia de lucru poate solutiona implicit numele gazdei) g) Tipul retelei (lan, wireless) h) User-ul logat pe statie i) Etichete definite pe masini virtuale in cloud (disponibile doar prin integrare Amazon EC2 sau MS Azure)	

					1.6. Rapoarte: 1.6.1. Solutia contine rapoarte care prezinta statusul masinilor clientilor din punct de vedere al actualizarilor, fisierelor malware detectate, aplicatiile blocate, site-urilor web blocate. 1.6.2. Rapoartele programate permit trimiterea catre un numar nelimitat de adrese de email (nu este nevoie sa detina un cont in consola de management). 1.6.3. Solutia permite vizualizarea rapoartelor curente programate de administrator. 1.6.4. Solutia permite exportarea rapoartelor in format .pdf si detaliile ca format .csv. 1.6.5. 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 sa includa interogari precum: starea terminalului, evenimente terminal, evenimente Exchange. 1.6.6. Interogarea legata de starea terminalului includa 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. 1.6.7. 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) 1.6.8. 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) ***1.7. Carantina:*** 1.7.1. Solutia permite restaurarea fisierelor carantinate in locatia originala sau intr-o cale configurabila. 1.7.2. Carantina va fi locala, pe fiecare statia administrata si va fi administrata, fie local, fie din consola de magement 1.7.3. Permite descarcarea fisierelor carantinate doar pentru masinile virtuale protejate prin modulul mediilor virtuale integrat cu VMware vShield. ***1.8. Utilizatori:*** 1.8.1. Administrarea este posibila de facut pe baza de roluri. 1.8.2. 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. 1.8.3. Utilizatorii sa fie posibil de importat din Microsoft Active Directory sau crearea in consola de management. 1.8.4. Sa fie permis configurarea detaliata a drepturilor administrative, permitand selectarea serviciilor si obiectelor pentru care un utilizator poate face modificari. 1.8.5. Se fie permis deconectarea automata a oricarui tip de utilizator dupa un anumit timp pentru o protectie sporita a datelor afisate in consola de administrare. Acest interval sa se poata personaliza de administratorul solutiei.	

					1.9. Log-uri: 1.9.1. Inregistrarea actiunilor utilizatorilor. 1.9.2. Soluția oferă informatii detaliate pentru fiecare actiune a unui utilizator. 1.9.3. Sa permita filtrarea actiunilor utilizator dupa numele utilizatorului, actiune. ***1.10. Actualizare:*** 1.10.1. Sa permita definirea de locatii de actualizare multiple. 1.10.2. Sa permita activarea/dezactivarea actualizarilor de produs si semnaturi. 1.10.3. Sa permita actualizarea produsului intr-o retea fara acces la Internet. 1.10.4. Orice client antivirus sa poata fi configurat sa livreze update-urile catre alt client antivirus 1.10.5. Solutia sa dispuna un server de actualizare (update) care va 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. 1.10.6. 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 fie posibilitatea de vizualizare unui 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 1.10.7. Solutia sa permita 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 sa includa 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) 1.10.8. Solutia sa permita stabilirea zonelor de test si critice din cadrul retelei prin intermediul politicilor din consola de management. ***1.11. Certificate:*** 1.11.1. Accesul la consola de management sa se faca doar prin HTTPS. 1.11.2. Serverul web, din consola centrala de management trebuie sa permita importarea de certificate digitale eliberate de o autoritate de certificare autorizata sau proprie organizatiei. 1.11.3. Solutia sa permita afisarea in consola de management informatii despre certificate: nume, autoritatea emitenta, data eliberarii si data expirarii certificatelor eliberate. **2. PROTECTIE STATII SI SERVERE FIZICE SAU VIRTUALE** ***2.1. Caracteristici generale minimale si eliminatorii:*** 2.1.1. Pentru reducerea la minim a consumului de resurse, solutia antimalware permite 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). 2.1.2. 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. 2.1.3. Vaccinul anti-ransomware primeste actualizari de la producator, odata cu actualizarea semnaturilor produsului Antimalware. 2.1.4. Pentru o mai buna protectie a statiilor si serverelor, solutia include protectie impotriva atacurilor zero-day de tip exploit avansate (atacuri directionate) bazata pe tehnologii de invatare automata (machine learning). 2.1.5. Pentru o mai buna protectie a statiilor si serverelor, solutia include un modul avansat de securitate – HyperDetect, bazat pe tehnologii de tip „machine learning tunabil", proiectat special	

					pentru a detecta atacuri avansate si activitati suspecte in faza pre-executie. 2.1.6. Acest modul avansat de securitate protejează impotriva: atacurilor directionate (Targeted Attack - APT), fisierelor suspecte si traficului la nivel de retea suspect, exploit-urilor, ransomware si grayware. Fiecarui tip de amenintare mentionat, i se poate stabili, independent, un nivel de protectie dorit: permisiv, normal, agresiv. 2.1.7. Modulul avansat de securitate are posibilitatea de a raporta, bloca accesul, dezinfecta, sterge sau muta in carantina pentru fiecare din categoriile descrise. Astfel, administratorul poate decide daca doreste intai monitorizare sau doreste si blocarea amenintarilor. Aceste actiuni mentionate, pot fi stabilite independent, pentru fisiere sau pentru traficul din retea, cu posibilitatea extinderii nivelului de raportare pentru a include nivelurile superioare (vor putea fi raportate amenintarile care ar fi fost detectate daca nivelul de protectie era stabilit mai agresiv). 2.1.8. Pentru a oferi un nivel aditional de protectie a statiilor si serverelor, solutia include un sandbox in cloud-ul public al producatorului acesteia. 2.1.9. Modulul de Sandbox poate trimite automat fisiere in Sandbox-ul din cloud-ul producatorului unde vor putea fi „detonate" pentru o analiza in profunzime. 2.1.10. Modulul de Sandbox include doua variante de analiza: doar monitorizare sau blocare. In modul monitorizare utilizatorul poate accesa fisierul dorit, pe cand in modul blocare, utilizatorului i se va bloca rularea fisierului pana cand Sandbox-ul din cloud-ul producatorului va da verdictul. 2.1.11. Modulul de Sandbox include doua tipuri de actiuni remediere: implicita si de siguranta. Pentru actiunea implicita se poate stabili: doar raportare, dezinfectie, stergere si carantinare. Pentru actiunea de siguranta se poate stabili: stergere sau carantinare. 2.1.12. Modulul de Sandbox include si posibilitatea de trimitere manuala a fisierelor in Sandbox-ul din cloud-ul producatorului. Astfel, daca administratorul suspecteaza un fisier ca fiind malitios, il poate trimite manual in Sandbox pentru a fi „detonat" si a afla verdictul. Va putea trimite mai multe fisiere de odata, cu posibilitate de a specifica daca vor fi „detonate" individual sau toate in acelasi timp.	

					2.1.13. Modulul de Sandbox poate suporta „detonarea" urmatoarelor tipuri de fisiere: 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 (executable), PIF (executable), RTF, SCR, URL (binary), VBE, VBS, WSF, WSH, WSH-VBS, XHTML. 2.1.14. Fisierele mentionate anterior, pot fi detectate corect chiar daca sunt incluse in arhive de tipul: : 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. ***2.2. Cerinte de sistem:*** – Sisteme de operare pentru statii de lucru: Windows 10, Windows 8/8.1, Windows 7, MAC OS X Catalina (10.15.x), Mac OS X Mojave (10.14.x), Mac OS X High Sierra (10.13.x), Mac OS X Sierra (10.12.x), Mac OS X El Capitan (10.11.x) – Sisteme de operare embedded: Windows 10 IoT Enterprise, Windows Embedded 8.1 Industry, Windows Embedded 8 Standard, Windows Embedded Standard 7, Windows Embedded POSReady 7, Windows Embedded Enterprise 7 – Sisteme de operare pentru servere: Windows Server 2019, Windows Server 2016 (inc Core), Windows Server 2012 R2, Windows Server 2012, Windows Small Business Server (SBS) 2011, Windows Server 2008 R2 – Sisteme de operare Linux: Red Hat Enterprise Linux / CentOS 6 sau mai recent, Ubuntu 14.04 LTS sau mai recent, SUSE Linux Enterprise Server 11 SP4 sau mai recent, OpenSUSE LEAP 42.x sau mai recent, Fedora 25 sau mai recent, Debian 8.0 sau mai recent, Oracle Linux 6.3 sau mai recent, Amazon Linux AMI 2016.09 sau mai recent. ***2.3. Administrare si instalare remote:*** 2.3.1. Inainte de instalare, administratorul poate particulariza pachetele de instalare cu modulele dorite: firewall, content control, device control, power user. 2.3.2.Instalarea se poate 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	

					2.3.3. Instalarea clientilor la distanta in alte locatii decat cele in care este instalata consola de management sa fie facuta prin intermediul unui alt client antivirus existent in locatiile respective pentru a minimiza traficul in WAN. 2.3.4. In consola este disponibilă informatii despre fiecare statie: numele statiei, IP, sistem de operare, module instalate, politica aplicata, informatii despre actualizari etc. 2.3.5. Din consola este posibila trimite o singura politica pentru configurarea integrala a clientului de pe statii/servere. 2.3.6. Consola 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. 2.3.7. Soluția oferă 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. 2.3.8. Soluția oferă posibilitatea creari unui singur pachet de instalare, utilizabil pentru statii (fizice si/sau virtuale), servere (fizice si/sau virtuale), exchange. 2.3.9. Soluția oferă posibilitatea de a crea pachetele de instalare de tip web installer sau kit full. 2.3.10. Administratorul poate crea grupuri sau chiar subgrupuri, unde poate muta statiile/serverele din retea pentru cele care nu sunt integrate domeniu. 2.3.11. Soluția permite selectarea clientului care realizează descoperirea statiilor din retea, altele decat cele integrate in domeniu. 2.3.12. Soluția permite raportarea statiilor care sunt protejate respectiv neprotejate de catre solutie ***2.4. Caracteristici si functionalitati principale ale modulului antimalware:*** 2.4.1. Solutia permite administratorului sa stabileasca actiunea luata de produsul Antimalware la detectarea unei amenintari noi. Astfel administratorul poate 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 2.4.2. Scanarea automata in timp real poata fi setata sa nu scaneze arhive sau fisiere mai mari de « x » MB, marimea fisierelor putand fi definita de administratorul solutiei, 2.4.3. Soluția oferă posibilitatea de definire pana la 16 nivele de profunzime pentru scanarea in arhive. 2.4.4. Soluția oferă posibilitatea de scanare 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. 2.4.5. Soluția oferă posibilitatea de scanare a oricarui suport de stocare a informatiei (CD-uri, harduri externe, unitati partajate etc). De asemenea, poate anula scanarea in cazul in care sunt detectate unitati care au informatii stocate mai mult de « x » MB. 2.4.6. Soluția oferă posibilitatea de scanare automata a emailurilor la nivelul statiei de lucru pentru POP3/SMTP. 2.4.7. Soluția oferă posibilitatea de configurarea cailor ce urmeaza a fi scanate la cerere. 2.4.8. Clientii antimalware pentru workstation pot permite definirea unor liste de excludere de la scanarea in timp real si la cerere a anumitor directoare, discuri, fisiere, extensii sau procese.	

					2.4.9. Cu ajutorul unei baze de date complete cu semnaturi de spyware si a euristicii de detectie a acestui tip de programe, produsul oferă protectie anti-spyware. 2.4.10. Soluția oferă posibilitatea de a configura scanarile programate sa fie executate cu prioritate redusa 2.4.11. 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. 2.4.12. 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 va stoca local nicio semnătură, iar scanarea va fi 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) 2.4.13. Pentru o protectie sporita, solutia antimalware are 3 tipuri de detectie: bazata pe semnaturi, bazata de comportamentul fisierelor si bazata pe monitorizarea proceselor. 2.4.14. Pentru o protectie sporita, solutia antimalware poate scana paginile HTTP. 2.4.15. Pentru o mai buna gestionare a antimalware instalat pe statii, produsul include optiunea de setare a unei parole pentru protectia la dezinstalare.	

					2.4.16. Pentru siguranta utilizatorului, clientul include un modul de antiphishing. 2.4.17. Solutia ofera protectie in timp real pe masinile cu sistem de operare Linux in conformitate cu versiunea de kernel instalata. 2.4.18. Solutia poate detecta atacuri de tip „file-less" incluzand pe cele ce folosesc utilitare aferente sistemelor de operare de tip interpretor de script (powershell). Solutia poate sa nu blocheze in mod uzual scripturi pentru a proteja impotriva acestor tipuri de atacuri. 2.4.19. Solutia oferă un modul aditional de securitate bazat pe algoritmi tunabili de machine learning respectiv algoritmi euristici agresivi capabili sa detecteze si blocheze atacuri de tip persistent sau targetat precum si alte categorii de malware sofisticat inainte de faza de executie. 2.4.20. Solutia oferă posibilitatea de restaurare a fisierelor modificate de un proces suspicios/necunoscut cu comportament de ransomware, odata ce solutia determina ca procesul este malitios. 2.4.21. Solutia oferă protectie importriva atacurilor ransomware initiate la distanta, de pe alte statii de lucru (de exemplu: incercarea de atac ransomware pe un share de pe o statie de lucru care are acces la share). ***2.5. Anti-Exploit-Avansat:*** 2.5.1. Soluția oferă posibilitatea de a opri atacurile avansate de tip „zero-day" efectuate prin intermediul unor exploit-uri evazive. 2.5.2. Soluția poate depista in timp real a celor mai recente exploit-uri ce pot vulnerabiliza un sistem de operare. 2.5.3. Soluția oferă posibilitatea de protejare a aplicatiile utilizate frecvent si a celor de tip „sistem" cum ar fi browserele, aplicatiile de tip office sau reader, procesele critice aferente sistemelor de operare. ***2.6. Firewall:*** 2.6.1. Soluția oferă posibilitatea de a configura reguli de firewall pentru aplicatii sau conectivitate. 2.6.2. Modulul poate fi instalat/dezinstalat in functie de preferinta administratorului.	

					2.6.3. Soluția oferă posibilitatea de a defini retele de incredere pentru masini destinate. 2.6.4. Soluția are abilitatea de a detecta scanarea de porturi. 2.6.5. Soluția oferă posibilitatea de a seta diferite profiluri de rețea ((Home/Office, Trusted, Public, Untrusted sau Let the Windows decide) 2.6.6. Soluția are abilitatea de a crea reguli personalizate bazate pe aplicație și/sau conexiune ***2.7. Carantina:*** 2.7.1. Produsul antimalware permite trimiterea automata a fisierelor din carantina catre laboratoarele antimalware ale producatorului. 2.7.2.Trimiterea continutului carantinei este posibil de expediat in mod automat, la un interval definit de administrator. 2.7.3.Produsul antimalware permite stergerea automata a fisierelor carantinate mai vechi de o anumita perioada, pentru a nu incarca inutil spatiul de stocare. 2.7.4. Soluția oferă posibilitatea de a restaura un fisier din carantina in locatia lui originala. 2.7.5.Modulul de carantina permita rescanarea obiectelor dupa fiecare actualizare de semnaturi. ***2.8. Protectia datelor:*** 2.8.1. Produsul permite blocarea datelor confidentiale (pin-ul cardului, cont bancar etc) transmise prin HTTP sau SMTP prin crearea unor reguli specifice. ***2.9. Controlul continutului:*** 2.9.1. Consola detine 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). ***2.10. Controlul aplicatiilor:*** 2.10.1. Pentru o mai buna inventariere si administrare, solutia include o sectiune in consola de administrare unde se vor regasi toate aplicatiile descoperite in retea, grupate dupa: nume, versiune, descoperit la, gasit pe. 2.10.2. Pentru o mai buna inventariere si administrare, solutia include o sectiune in consola de administrare unde sa se regaseasca toate procesele negrupate descoperite in retea, grupate dupa: nume, versiune, nume produs, versiune produs, editor/autor, descoperit la, gasit pe. 2.10.3. 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. 2.10.4. 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 2.10.5. Acest modul poate functiona in modul Whitelisting (prin care se blocheaza accesul la toate applicatiile cu exceptia celor mentionate in lista alba) sau Blacklisting (prin care sa se blocheaze doar accesul la aplicatiile mentionate in lista neagra). ***2.11. Controlul dispozitivelor:*** 2.11.1. Modulul poate fi instalat/dezinstalat in functie de preferinta administratorului. 2.11.2. Modulul 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 2.11.3. Modulul permite configurarea de reguli prin care se vor defini permisiunile pentru dispozitivele conectate la masina client. 2.11.4. Modulul permite configurarea de excluderi pentru diferite tipuri de dispozitive pentru care s-au configurat reguli. 2.11.5. Modulul permite configurarea de reguli prin care se vor defini permisiunile pentru dispozitivele conectate la masina client cum ar fi: permis/blocat/custom respectiv sa poata limita accesul dispozitivelor externe la „read only" sau limita doar accesul la porturile USB ale endpoint-ului permitand orice alt tip de dispozitiv ce nu foloseste acest tip de port/interfata. 2.11.6. Modulul permite configurarea de excluderi pentru diferite tipuri de dispozitive pentru care s-au configurat reguli pe baza a Product/Device/Hardware ID. 2.11.7. Modulul poate „descoperi" noi dispozitive si raporta prezenta acestora in consola de management. ***2.12. Power User:*** 2.12.1. Modulul sa poata fi instalat/dezinstalat in functie de preferinta administratorului. 2.12.2. Modulul sa permita posibilitatea de a acorda utilizatorilor drepturi de Power User. Utilizatorii sa pata accesa si modifica setarile clientului antimalware dintr-o consola dispobibila local pe masina client.	

					2.12.3. Administratorul va putea suprascrie din consola setarile aplicate de utilizatorii Power User. ***2.13. Actualizare:*** 2.13.1. Soluția oferă posibilitatea efectuarii actualizarii la nivel de statie in mod silentios (fara avertizare). 2.13.2. Soluția detine un sistem de actualizare cascadat folosind unul sau mai multe servere de actualizare (cascadate). 2.13.3. Actualizarea pentru locatiile remote prin intermediul unui client antimalware va avea si rol de server de actualizare. **3. PROTECTIE SI SECURITATE PENTRU TELEFOANELE MOBILE DE TIP SMARTPHONE** ***3.1. Cerinte minime de sistem:*** – Telefoane cu sistem de operare iOS 8.1 sau mai nou: Apple iPhone si tablete iPad – Telefoane sau tablete cu sistem de operare Android 4.0.3 sau mai nou ***3.2. Caracteristici:*** 3.2.1 Permite asocierea unui dispozitiv cu un utilizator din Active Directory. 3.2.2 Instalarea se face prin trimiterea unui email catre utilizator cu detaliile de instalare. 3.2.3 Activarea dispozitivului mobil in consola de management se face prin scanarea unui cod QR. 3.2.4 Pachetele de instalare se poate descarca de pe Apple App Store si Google Play. 3.2.5 Se pot 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). 3.2.6 Consola permite raportarea dispozitivelor: active, inactive, deconectate, cu sistemul de operare modificat astfel incat utilizatorul sa aiba acces total asupra lui (rooted or jailbroken devices). ***3.3. Setari de securitate:*** 3.3.1. In cazul in care un dispozitiv nu este conform cu setarile dorite, există posibilitatea de intreprins automat actiunile: a. Ignorare; b. Blocarea accesului; c. Blocarea dispozitivului; d. Stergerea datelor si revenirea la setarile din fabrica; e. Stergerea dispozitivului din consola. 3.3.2. Se poate impune blocarea dispozitivelor cu ajutorul unei parole. Aceasta parola sa poata 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. 3.3.3. Sa se poata 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. 3.3.4. Profilurile de Wi-Fi sa contina urmatoarele optiuni:	

					a. Generale – 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. 3.3.5. Profilurile acces pagini de internet pentru sistemul de operare Android include 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. 3.3.6. Profilurile acces pagini de internet pentru sistemul de operare iOS inlcude 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. **4. PROTECTIE SI SECURITATE PENTRU SERVERELE EMAIL MICROSOFT EXCHANGE** ***4.1. Cerinte minime de sistem:*** – Exchange server 2019, 2016, 2013 cu rol de Edge Transport sau Mailbox – Exchange server 2010, 2007 cu rol de Edge Transport, Hub Transport sau Mailbox – Microsoft Windows Server 2008R2 sau mai nou 4.1.1. Produsul oferă 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. 4.1.2. Produsul asigură scanarea atasamentelor si a continutului mesajelor in timp real, fara a afecta vizibil performanta serverului de mail. 4.1.3. Actualizarea antimalware poata fi facuta automat la un interval de maxim 1 ora, precum si la cerere. 4.1.4. In afara de detectia pe baza de semnaturi, modulul de protectie antimalware include 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. 4.1.5. Produsul oferă optiuni multiple de actiune la identificarea unui atasament virusat (dezinfectare, stergere, mutare in carantina). 4.1.6. Cu ajutorul unei baze de date complete cu semnaturi de spyware si a euristicii de detectie a acestui tip de programe, produsul oferă protectie anti-spyware pentru a preveni furtul de date confidentiale. 4.1.7. Produsul oferă protectie antispam, cu o baza de semnaturi actualizabila prin internet. 4.1.8. Modulul antispam trebui include 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. 4.1.9. Produsul oferă 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. 4.1.10. Produsul oferă un serviciu/filtru online pentru imbunatatirea protectiei impotriva valurilor de spam nou aparute.	

"RTS ONE" S.R.L.
https://rts.md
(+373) 22 101 777
office@rts.one
str. Mitropolit G. Bănulescu-Bodoni 59/B, of. 815

					4.1.11. Produsul oferă posibilitatea de a defini politici de filtrare antimalware, antispam, a continutului sau atasamentelor pentru diferite grupuri sau utilizatori. 4.1.12. Actualizarea produsului este configurabila si se poate realiza de pe internet, direct sau printr-un proxy, sau din cadrul retelei de pe un server de actualizare propriu. 4.1.13. Produsul oferă statistici atat referitoare la scanarea antivirus cat si la scanarea antispam. 4.1.14. Produsul se integrează in cadrul consolei de management unitar al solutiei antivirus. Pentru usurinta accesului la setarile produsului din diferite medii de operare, produsul va avea consola de administrare web. **Lucrările de instalare, configurare, punerea în funcțiune a soluției vor fi efectuate de către compania „RTS ONE" S.R.L. , iar costul este inclus în conformitate cu Oferta comercială** *(Specificații de preț, Anexa nr.23)*	
TOTAL						

Semnat:

Digitally signed by Celonenco Vitalie
Date: 2022.09.02 09:12:37 EEST
Reason: MoldSign Signature
Location: Moldova

Numele, Prenumele: **CELONENCO Vitalie**

În calitate de: **Administrator**

Ofertantul: **„RTS ONE" S.R.L.**

Adresa: **mun.Chișinău, str.Mitropolit Gavriil Bănulescu-Bodoni, 59/B, of.815**