"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-1669281555537**

SPECIFICAȚII TEHNICE

Numărul procedurii de achiziție: MTender ID: ocds-b3wdp1-MD-1669281555537
Denumirea procedurii de achiziție: **Licențe antivirus**

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
1. Licențe antivirus pentru Servere fizice (Hosts) 2. Licențe antivirus	Bitdefender GravityZone Business Security Premium, 530	Romania	Bitdefender	**CARACTERISTICI GENERALE ALE PRODUSULUI** Produsul este o platforma integrata pentru managementul securității, gândita ca o soluție modulara.	**CARACTERISTICI GENERALE ALE PRODUSULUI** Produsul **Bitdefender GravityZone Business Security Premium, pentru 530 dispozitive, 12 luni suport** - este o platforma integrata pentru managementul securității, gândita ca o soluție	

pentru Virtual machine's (Linux, Windows 2008 R2, Windows 2012 R2, Windows Server 2019) 3. Licențe antivirus pentru Stații de lucru/laptop (platforma Linux, Windows)/utilizatori Microsoft Exchange Server 2019 (Windows server 2019, VM)/ căsuțe poștale	dispozitive, 12 luni suport			Produsul conține următoarele module: A. O consola de management care asigura funcționalități de administrare; B. Protecție stații și servere fizice/virtuale; C. Protecție și securitate pentru telefoanele mobile de tip smartphone; D. Protecție și securitate pentru serverele email Microsoft Exchange. E. Integrare SIEM. A. CONSOLA DE MANAGEMENT 1. Instalare și configurare: 1.1. Pachetul de instalare se poate instala pe mașina virtuala care sa opereze pe unul din hypervizori de mai jos : 1.1.1. VMware vSphere 1.1.2. Citrix XenServer 1.1.3. Microsoft Hyper-V 1.1.4. Oracle VM.	modulara. Produsul conține următoarele module: A. O consola de management care asigura functionalitati de administrare. B. Protectie statii si servere fizice/virtuale. C. Protectie si securitate pentru telefoanele mobile de tip smartphone cu sistem de operare iOS sau Android. D. Protectie si securitate pentru serverele email Microsoft Exchange E. Integrare SIEM. Produsul antivirus ofertat ocupă locurile de top în testele internaționale independente cu renume mondial în domeniu (certificări AV-TEST, AV-Comparatives, etc.) 1. CONSOLA DE MANAGEMENT 1.1 Instalare si configurare: 1.1.1 Pachetul de instalare este 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. Pachetul de instalare se poate instala pe mașina virtuala care sa opereze pe unul din hypervizori de mai jos : 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 este livrata cu o baza de date inclusa care este de tip non-	

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

				1.2. Soluția va fi scalabila, astfel ca oricare dintre roluri sau servicii pot fi instalate separat pe mai multe mașini virtuale sau pe aceeași mașina virtuala. 1.3. Rolurile principale trebuie să fie cel puțin similare cu: Server cu baza de date, Server de comunicație, Server de actualizare, Server de Web. 2. Cerințe generale: 2.1. Interfața consolei de management va fi în prezenta în limbile de circulație internaționala 2.2. Interfața clientului de securitate, care se instalează pe stații și servere, va fi în prezenta în limbile de circulație internaționala.	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. 1.1.4 Rolurile principale sunt similare cu: Server cu baza de date, Server de comunicatie, Server de actualizare, Server de Web. 1.1.5 Solutia 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 se va putea instala de mai multe ori, pe mai multe masini virtuale. 1.1.7 Masinile de scanare pentru mediile virtuale VsMware si Citrix este posibil instalare 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 Interfața consolei de management este prezenta în limbile de circulație internaționala (Engleza, romana, rusa, etc.) 1.2.2 Interfața clientului de securitate, care se instalează pe stații și servere, va fi în prezenta	

				2.3. Manualul de instalare a produsului va fi în prezenta în limbile de circulație internaționala 2.4. Manualul de administrare a produsului va fi în prezenta în limbile de circulație internaționala. 2.5. Soluția va include un modul de update server prin care se asigura actualizarea de produs și a semnăturilor. 2.6. Soluția va permite activarea/dezactivarea actualizărilor de produs/semnături. 2.7. Soluția permite stabilirea actualizării automate a consolei de management prin stabilirea recurentei zilnice, săptămânale sau lunare, dar și prin stabilirea intervalului orar în care acesta se va actualiza. De asemenea, permite și trimiterea unei alerte de ne funcționalitate, cu 30 de minute înainte de actualizare. 2.8. Pentru o mai buna urmărire a actualizărilor consolei de management, soluția permite vizualizarea unui jurnal de modificări în care sunt precizate istoric: 2.8.1. versiunea consolei de management 2.8.2. data versiunii 2.8.3. funcții noi și îmbunătățiri 2.8.4. probleme rezolvate 2.8.5. probleme cunoscute 2.9. Notificările – prezente în interfața, notificările necitite sunt evidențiate, trimise către una sau mai multe adrese de email, alertează administratorul în cazul unor probleme majore: licențiere, detecție virusi, actualizări de produs disponibile).	în limbile de circulație internaționala. (Engleza, romana, rusa, etc.) 1.2.3 Manualul de instalare a produsului este prezentat in limbile engleza, roamana, rusa. 1.2.4 Manualul de administrare a produsului este prezentat in limbile engleza, roamana, rusa. 1.2.5 Solutia include un modul de update server prin care să asigure actualizarea de produs si a semnaturilor. 1.2.6 Solutia pemite 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, să permită 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 b. data versiunii c. functii noi si imbunatatiri d. probleme rezolvate e. probleme cunoscute 1.2.9 Notificarile – sunt prezente in interfata, notificarile 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).	

				2.10. Soluția va permite integrarea cu un server Syslog pentru raportarea evenimentelor anti malware. 2.11. Soluția va permite instalarea serviciului de SMNP prin care se pot raporta statusul mașinilor din cadrul componentei de management. 2.12. Soluția permite creare unei copii de siguranța a bazei de date a consolei de administrare, la cerere sau programata,. 2.13. Endpoint Risk Management și Analytics 2.14. Introduceți zero configurațiile greșite, aplicațiile vulnerabile, riscurile comportamentului utilizatorilor, dispozitivele și utilizatorii individuali și remediați configurările greșite sau vulnerabilitățile corecțiilor. 3. Panou de monitorizare și raportare (Dashboard): 3.1. Rapoartele din panoul de monitorizare vor putea fi configurate specificând numele raportului, tipul raportului, ținta raportului, opțiuni specifice pentru orice tip de raport (de exemplu pentru raportul de actualizare - care este intervalul după care o stație este considerata neactualizata). 3.2. Panoul central conține rapoarte pentru toate modulele suportate. 3.3. Rapoartele din panoul central de comanda permit: adăugarea altor rapoarte, ștergerea lor și rearanjarea. 3.4.O platformă integrată de protecție a punctelor finale, gestionarea riscurilor și	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 Endpoint Risk Management și Analytics 1.2.14 Solutia permite introducerea zero configurațiilor greșite, aplicațiile vulnerabile, riscurile comportamentului utilizatorilor, dispozitivele și utilizatorii individuali și remediați configurările greșite sau vulnerabilitățile corecțiilor. 1.2.15 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 este posibil sa fie 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 contine rapoarte pentru toate modulele suportate. 1.3.3 Rapoartele din panoul central de comanda permite: adaugarea altor rapoarte, stergerea lor si rearanjarea. 1.3.4. O platformă integrată de protecție a punctelor finale, gestionarea riscurilor și	

				criminalistică pentru atacuri. Îmbunătățit cu analiza riscului comportamentului utilizatorului. 3.5. Modul include analiza cauzei rădăcină, vizualizarea lanțului de atac și acțiuni de remediere legate de amenințările detectate și blocate de tehnologiile de prevenire ca exemplu, Antimalware (Exploit Defense, PowerShell Defense, HyperDetect etc.), Sandbox și Network -Apărarea atacului. 3.6. Analiza securității traficului în rețea (NTSA) detectează atacurile avansate în timp real, oferă contextul amenințărilor și declanșează un răspuns autonom la incidente. NTSA folosește o combinație de învățare automată și analize de comportament cu informații de la Aanti Virus intelligence intelligence - format din cel puțin 400-500 de milioane de senzori la nivel global - pentru a detecta amenințările pentru toate entitățile, gestionate sau neadministrate, pentru traficul de rețea criptat sau necriptat. 4. Inventarierea rețelei – managementul securității: 4.1. Soluția se va integra cu domenii Active Directory multiple, VMware vCenter, Citrix Xen și importa inventarul acestor platforme. 4.2. Pentru integrarea cu Active Directory, se va putea defini și intervalul (în ore) de sincronizare și forța sincronizarea. 4.3. Se permite descoperirea mașinilor din Microsoft Hyper-V, Red Hat VM, Oracle VM, KVM.	criminalistică pentru atacuri. Îmbunătățit cu analiza riscului comportamentului utilizatorului. 1.3.5. Modul include analiza cauzei rădăcină, vizualizarea lanțului de atac și acțiuni de remediere legate de amenințările detectate și blocate de tehnologiile de prevenire ca exemplu, Antimalware (Exploit Defense, PowerShell Defense, HyperDetect etc.), Sandbox și Network -Apărarea atacului. 1.3.6. Analiza securității traficului în rețea (NTSA) detectează atacurile avansate în timp real, oferă contextul amenințărilor și declanșează un răspuns autonom la incidente. NTSA folosește o combinație de învățare automată și analize de comportament cu informații de la Aanti Virus intelligence intelligence - format din cel puțin 400-500 de milioane de senzori la nivel global - pentru a detecta amenințările pentru toate entitățile, gestionate sau neadministrate, pentru traficul de rețea criptat sau necriptat. 1.4 Inventarierea retelei – managementul securitatii: 1.4.1. Solutia se integreaza cu domenii Active Directory multiple, VMware vCenter Server, Citrix Xen Server, Nutanix Prism Element si importa inventarul acestor platforme. 1.4.2. Pentru integrarea cu Active Directory, se poate defini și intervalul (în ore) de sincronizare și forța sincronizarea. 1.4.3 Solutia permite descoperirea masinilor din Microsoft Hyper-V, Red Hat VM, Oracle VM, KVM .	

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

				4.4. Se permite descoperirea stațiilor stații fizice neintegrate în Active Directory (Workgroup) cu ajutorul Network discovery. 4.5.Soluția va oferi opțiuni de căutare, sortare și filtrare după numele sistemului, sistem de operare și adresa IP. 4.6. Soluția va permite instalarea la distanta sau manual a clienților anti malware pe mașini fizice/virtuale. 4.7. Soluția va permite selectarea modulelor componente atunci când se creează pachetul clientului care se instalează pe mașinile fizice/virtuale. 4.8. Soluția va permite lansarea de task-uri de scanare, actualizare, instalare,dezinstalarea la distanta pentru clientul anti malware. 4.9. Soluția va oferi posibilitatea de repornire a mașinilor fizice de la distanta. 4.10. Soluția va oferi informații detaliate despre fiecare task și va afișa daca task-ul s-a finalizat sau nu cu succes. 4.11. Soluția va permite configurarea centralizata a clienților anti malware prin intermediul politicilor 4.12. Se vor oferi în consola de management informații detaliate ale obiectelor din consola: Nume, IP, Sistem de operare, Grup, Politica atribuita, Ultimele actualizare, Versiunea produsului, Versiunea de semnături. 4.13. Soluția permite descoperirea tuturor aplicațiilor instalate pe toate stațiile și serverele din rețea, prin rularea unui task din consola de administrare.	1.4.4. Se permite descoperirea stațiilor stații fizice neintegrate în Active Directory (Workgroup) cu ajutorul Network discovery. 1.4.5. Solutia sa ofere 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 1.4.6. Solutia permite instalarea la distanta sau manual a clientilor antimalware pe masini fizice/virtuale. 1.4.7. Solutia permite selectarea modulelor componente atunci cand se creaza pachetul clientului care se instalează pe mașinile fizice/virtuale. 1.4.8.Solutia permite lansarea de task-uri de scanare, actualizare, instalare, dezinstalarea la distanta pentru clientul antimalware. 1.4.9.Solutia ofera posibilitatea de repornire a masinilor fizice de la distanta. 1.4.10. Solutia ofera informatii detaliate despre fiecare task si sa fiseaze daca task-ul s-a finalizat sau nu cu succes. 1.4.11.Solutia permite configurarea centralizata a clientilor antimalware prin intermediul politicilor. 1.4.12. Se ofera 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. 1.4.13. Solutia permite descoperirea tuturor aplicatiilor instalate pe toate statiile si serverele din reatea, prin rularea unui task din consola de administrare. 1.4.14. Solutia permite crearea unui pachet unic pentru toate sistemele de operare, de statii sau servere. Astfel, administratorul sa poata descarca pachetele pentru protectia statiilor si	

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

				5. Politici: 5.1. Soluția va permite configurarea setărilor clientului anti malware prin intermediul unei singure politici ce conține setări pentru toate module 5.2. Politica va conține opțiuni specifice de activare/dezactivare și configurarea funcționalităților precum scanarea anti malware la cerere, firewall, controlul accesului la Internet, controlul aplicațiilor, scanarea traficului web, controlul dispozitivelor, power user. 5.3. Solutia va permite crearea unei politici dedicate sau configurații care pot fi lansate în mod automat fara interventia administratorului în cazul în care numărul de incidente malware depășește un prag definit (de exemplu, in timpul unui " atac de virus ")Soluția permite aplicarea politicilor pe mașini client, grupuri de mașini, pool-uri de resurse (VMware), domeniu, unități organizaționale sau useri de active directory. 5.4.Politica să poate fi schimbata automat în funcție de: 5.4.1. User-ul logat pe stație 5.4.2. IP sau clasa de IP al stației 5.4.3. Gateway-ul alocat	serverelor pe care ruleaza sistemul de operare Windows, Linux, Mac. 1.4.5 Pentru integrarea cu Active Directory, se poata defini intervalul (in ore) de sincronizare si forta sincronizarea. 1.4.6 Solutia ofea 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 1.5 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 olutia va permite crearea unei politici dedicate sau configurații care pot fi lansate în mod automat fara interventia administratorului în cazul în care numărul de incidente malware depășește un prag definit (de exemplu, in timpul unui " atac de virus ") 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. User-ul logat pe stație b. IP sau clasa de IP al statiei c. Gateway-ul alocat	

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

				5.4.4. DNS serverul alocat 5.4.5. Clientul este/nu este în aceeași rețea cu infrastructura de management 5.4.6. Tipul rețelei (lan, wireless) 6. Rapoarte: 6.1. Soluția va conține rapoarte care prezinta statutul mașinilor clienților din punct de vedere al actualizărilor, fișierelor malware detectate, aplicațiile blocate, site-urilor web blocate. 6.2. Rapoartele programate pot fi trimise către un număr nelimitat de adrese de email (nu este nevoie să aibă un cont în consola de management). 6.3. Soluția va permite vizualizarea rapoartelor curente programate de administrator. 6.4. Soluția va permite exportarea rapoartelor în format .pdf și detaliile ca format .csv. 6.5. Soluția include un generator de rapoarte care oferă posibilitatea de a investiga o problema de securitate pe baza mai multor criterii, menținând informațiile concise și ordonate corespunzător. Astfel, soluția include interogări precum: starea terminalului, evenimente terminal, evenimente Exchange. 6.6. Interogarea legata de starea terminalului include informații precum: 6.6.1. tip mașină 6.6.2. infrastructura rețelei căreia ii aparține terminalul 6.6.3. datele agentului de securitate	d. DNS serverul alocat e. WINS serverul alocat f. Sufix DNS pentru conexiunea dhcp g. Clientul este/nu este in acceasi retea cu infrastructura de management (statia de lucru poate solutiona implicit numele gazdei) h. Tipul retelei (lan, wireless) 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 este posibil 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 include interogari precum: starea terminalului, evenimente terminal, evenimente Exchange. 1.6.6 Interogarea legata de starea terminalului include informatii precum: a. tip masina b. infrastructura retelei careia ii apartine terminalul c. datele agentului de securitate	

				6.6.4. starea modulelor de protecție 6.6.5. rolurile terminalelor. 6.7.Interogarea legata de evenimente terminal include informații precum: 6.7.1. calculatorul țința pe care a avut loc evenimentul 6.7.2. tipul starea și configurația agentului de securitate instalat 6.7.3. starea modulelor și rolurilor de protecție instalate pe agentul de securitate 6.7.4. denumirea și alocarea politicii 6.7.5. utilizatorul autentificat în timpul evenimentului 6.7.6. evenimente (site-uri blocate, aplicații blocate, detecțiile etc) 6.8.Interogarea legata de evenimente Exchange include informații precum: 6.8.1. Direcția traficului e-mail 6.8.2. Evenimente de securitate (detectarea programelor de tip malware sau a fișierelor atașate) 6.8.3. Masurile implementate în fiecare situație (curățarea, ștergerea, înlocuirea sau punerea în carantină a fișierului, ștergerea sau respingerea e-mail-ului) 7. Carantina: 7.1. Soluția va permite restaurarea fișierelor din carantină în locația originala sau într-o cale configurabila. 7.2.Carantina va fi locala, pe fiecare stația administrata și va fi administrata, fie local, fie din consola de management 7.3.Permite descărcarea fișierelor din carantină doar pentru mașinile virtuale protejate prin modulul mediilor virtuale integrat cu VMware vShield. 8. Utilizatori:	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:	

				8.1. Administrarea se va putea face pe baza de roluri. 8.2. Roluri multiple predefinite: Administrator companie, Administrator rețea, Reporter sau rol personalizat. 8.3. Administrator companie: administrează arhitectura consolei de management; 8.4. Administrator rețea: administrează serviciile de securitate; 8.5. Reporter: monitorizează și generează rapoarte. 8.6. Utilizatorii pot fi importați din Microsoft Active Directory sau creați în consola de management. 8.7. Se va permite configurarea detaliata a drepturilor administrative, permițând selectarea serviciilor și obiectelor pentru care un utilizator poate face modificări. 9. Log-uri: 9.1. Înregistrarea acțiunilor utilizatorilor. 9.2.Se vor oferi informații detaliate pentru fiecare acțiune a unui utilizator. 9.3.Se va permite filtrarea acțiunilor utilizator după numele utilizatorului, acțiune. 10. Actualizare: 10.1. Se permite definirea de locații de actualizare multiple. 10.2. Se permite activarea/dezactivarea actualizărilor de produs și semnături. 10.3. Se permite actualizarea produsului într-o rețea fără acces la Internet.	1.8.1 Administrarea este posibil 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 este posibil de importat din Microsoft Active Directory sau crearea in consola de management. 1.8.4 Este permisa configurarea detaliata a drepturilor administrative, permitand selectarea serviciilor si obiectelor pentru care un utilizator poate face modificari. 1.8.5 Soluția 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 sa se poata personaliza de administratorul solutiei. 1.9 Log-uri: 1.9.1 Inregistrarea actiunilor utilizatorilor. 1.9.2 Sunt oferite informatii detaliate pentru fiecare actiune a unui utilizator. 1.9.3 Permite filtrarea actiunilor utilizator dupa numele utilizatorului, actiune. 1.10 Actualizare: 1.10.1 Permite definirea de locatii de actualizare multiple. 1.10.2 Permite activarea/dezactivarea actualizarilor de produs si semnaturi. 1.10.3 Permite actualizarea produsului intr-o retea fara acces la Internet.	

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

				10.4. Orice client antivirus să poată fi configurat să livreze update-urile către alt client antivirus 10.5. Soluția dispune un server de actualizare (update) care face posibila stabilirea componentelor ce vor fi descărcate automat de pe internet, fără intervenția administratorului. Astfel, administratorul va putea descarcă pachetele pentru protecția stațiilor și serverelor pe care rulează sistemul de operare Windows, Linux, Mac sau, poate descarcă pachetele pentru modul de scanare centralizata în mediile de virtualizare VMware, Hyper-V sau Citrix. 10.6. In cadrul serverului de actualizare, pentru o mai buna urmărire a actualizărilor pachetele pentru protecția stațiilor și serverelor sau a pachetelor pentru modul de scanare centralizata, se va putea vizualiza un jurnal de modificări în care sunt precizate istoric: 10.6.1. versiunea pachetului 10.6.2. data versiunii 10.6.3. funcții noi și îmbunătățiri 10.6.4. probleme rezolvate 10.6.5. probleme cunoscute 10.7. Soluția permite testarea noilor versiuni de pachete de instalare ale clientului anti malware, înainte de a fi instalate pe toate stațiile și serverele din rețea, evitând posibile probleme ce pot afecta serverele sau stațiile critice. Astfel, serverul de actualizare include 2 tipuri de actualizări de produs:	1.10.4 Orice client antivirus poate fi configurat sa livreze update-urile catre alt client antivirus 1.10.5 Solutia dispune de 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, este posibil de vizualizat 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 1.10.7 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 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)	

				11. Certificate: 11.1. Accesul la consola de management să se facă doar prin HTTPS. 11.2. Serverul web, din consola centrala de management trebuie să permită importarea de certificate digitale eliberate de o autoritate de certificare autorizata sau proprie organizației. 11.3. Soluția permite afișarea în consola de management informații despre certificate: nume, autoritatea emitenta, data eliberării și data expirării certificatelor eliberate. **B. PROTECȚIE STAȚII și SERVERE FIZICE/VIRTUALE** 1. Caracteristici generale minimale și eliminatorii: 1.1. Pentru reducerea la minim a consumului de resurse, soluția anti malware trebuie să permită instalarea personalizata a modulelor deținute (de exemplu, să permită instalarea soluției anti malware fără modulul de control al accesului web, modul de control al dispozitivelor sau modulul firewall). 1.2. Pentru o mai buna protecție a stațiilor și serverelor, soluția include un vaccin anti-ransomware. Acest vaccin asigura protecția împotriva tuturor amenințărilor cunoscute de tip ransomware, prin imunizarea stațiilor și serverelor, chiar daca sunt infectate și prin blocarea procesului de criptare.	1.10.8 Solutia permite 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 permite importarea de certificate digitale eliberate de o autoritate de certificare autorizata sau proprie organizatiei. 1.11.3 Solutia permite 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	

				1.3. Pentru o mai buna protecție a stațiilor și serverelor, soluția include protecție împotriva atacurilor zero-day de tip exploit (atacuri direcționate).	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 protejeaza 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 va putea stabili, independent, un nivel de protectie dorit: permisiv, normal, agresiv. 2.1.7 Modulul avansat de securitate este posibilitatea de a raporta, bloca accesul, dezinfecta, sterge sau muta in carantina pentru fiecare din categoriile descrise. Astfel, administratorul sa poata decide daca doreste intai monitorizare sau doreste si blocarea amenintarilor. Aceste actiuni mentionate, sa 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 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 sa poata 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 va putea stabili: doar raportare, dezinfectie, stergere si carantinare. Pentru actiunea de siguranta se va putea 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.	

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

					2.1.14 Fisierele mentionate anterior, poate 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. Cerințe de sistem: 2.1. Sisteme de operare pentru stații de lucru: Windows 10, Windows 8, Windows 7, 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)	2.2 Cerinte de sistem: • Sisteme de operare pentru statii de lucru: Windows 11, 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	
				2.2. 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,	• 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	
				2.3. 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 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.	
				2.4. Sisteme de operare MAC: Mac OS X El Capitan (10.11.x), Mac OS X Yosemite (10.10.5),	• Sisteme de operare MAC: Mac OS X El Capitan (10.11.x), Mac OS X Yosemite (10.10.5), Mac OS X	

				Mac OS X Mavericks (10.9.5), Mac OS X Mountain Lion (10.8.5) 3. Administrare și instalare remote: 3.1. Înainte de instalare, administratorul va putea particulariza pachetele de instalare cu modulele dorite: firewall, content control, device control, 3.2. Instalarea se va putea face în mai multe moduri: 3.3. prin descărcarea directa a pachetului pe stația pe care se va face instalarea; 3.4. prin instalarea la distanta, direct din consola de management 3.5. Instalarea clienților la distanta în alte locații decât cele în care este instalata consola de management se va face prin intermediul unui alt client antivirus existent în locațiile respective pentru a minimiza traficul în WAN. 3.6. In consola vor fi disponibile informații despre fiecare stație: numele stației, IP, sistem de operare, module instalate, politica aplicata, informații despre actualizări etc. 3.7. Din consola se va putea trimite o singura politica pentru configurarea integrala a clientului de pe stații/servere. 3.8. Consola va include o secțiune, „Audit", unde se vor menționa toate acțiunile întreprinse fie de administratori fie de reporteri, cu informații detaliate: logare, editare, creare, delogare, mutare etc. 3.9. Posibilitatea creării unui singur pachet de instalare, utilizabil atât pentru sistemele de operare pe 32 de biți cat și pentru cele pe 64 de biți. 3.10. Posibilitatea creării unui singur pachet de instalare, utilizabil pentru stații (fizice si/sau virtuale), servere (fizice si/sau virtuale),.	Mavericks (10.9.5), Mac OS X Mountain Lion (10.8.5) 2.3 Administrare si instalare remote: 2.3.1 Inainte de instalare, administratorul sa poata particulariza pachetele de instalare cu modulele dorite: firewall, content control, device control, power user. 2.3.2 Instalarea sa 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 poate fi facuta prin intermediul unui alt client antivirus existent in locatiile respective pentru a minimiza traficul in WAN. 2.3.4 In consola sunt disponibile informatii despre fiecare statie: numele statiei, IP, sistem de operare, module instalate, politica aplicata, informatii despre actualizari etc. 2.3.5 Din consola este posibil pentru a 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 Este posibil crearea 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 Este posibil crearea unui singur pachet de instalare, utilizabil pentru statii (fizice si/sau virtuale), servere (fizice si/sau virtuale), exchange.	

				3.11. Administratorul va putea crea grupuri sau chiar subgrupuri, unde va putea muta stațiile/serverele din rețea pentru cele care nu sunt integrate domeniu. 3.12. Permite selectarea clientului care va realiza descoperirea stațiilor din rețea, altele decât cele integrate în domeniu. 4. Caracteristici și funcționalități principale ale modulului anti malware: 4.1. Soluția permite administratorului să stabilească acțiunea luata de produsul Anti malware la detectarea unei amenințări noi. Astfel administratorul va putea alege intre următoarele acțiuni: 4.1.1. Acțiune implicită pentru fișiere infectate: 4.1.1.1. interzice accesul 4.1.1.2. dezinfectează 4.1.1.3. ștergere 4.1.1.4. muta fișierele în carantina 4.1.1.5. nicio acțiune 4.1.2. Acțiune alternativa pentru fișierele infectate: 4.1.2.1. interzice accesul 4.1.2.2. dezinfectează 4.1.2.3. ștergere 4.1.2.4. muta fișierele în carantina 4.1.3. Acțiune implicită pentru fișierele suspecte: 4.1.3.1. interzice accesul 4.1.3.2. ștergere 4.1.3.3. muta fișierele în carantina 4.1.3.4. nicio acțiune 4.1.4. Acțiune alternativa pentru fișierele suspecte:	2.3.9 Sa fie 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 va putea muta statiile/serverele din retea pentru cele care nu sunt integrate domeniu. 2.3.11 Permite selectarea clientului care va realiza descoperirea statiilor din retea, altele decat cele integrate in domeniu. 2.3.12 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 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:	

				4.1.4.1. interzice accesul 4.1.4.2. ștergere 4.1.4.3. muta fișierele în carantina 4.2.Scanarea automata în timp real va putea fi setata să nu scaneze arhive sau fișiere mai mari de « x » MB, mărimea fișierelor putând fi definita de administratorul soluției, 4.3.Definirea pana la 16 nivele de profunzime pentru scanarea în arhive. 4.4. Scanarea euristica comportamentala prin simularea unui calculator virtual în interiorul căruia sunt rulate aplicații cu potențial periculos protejând sistemul de virușii necunoscuți prin detectarea codurilor periculoase a căror semnătură nu a fost lansata încă. 4.5.Scanarea oricărui suport de stocare a informației (CD-uri, harduri externe, unități partajate etc). De asemenea, se va putea anula scanarea în cazul în care sunt detectate unități care au informații stocate mai mult de « x » MB. 4.6. Scanarea automata a emailurilor la nivelul stației de lucru pentru POP3/SMTP. 4.7. Configurarea cailor ce urmează a fi scanate la cerere. 4.8. Clienții anti malware pentru stațiile de lucru să permită definirea unor liste de excludere de la scanarea în timp real și la cerere a anumitor directoare, discuri, fișiere, extensii sau procese. 4.9. Cu ajutorul unei baze de date complete cu semnături de spyware și a euristicii de detecție a acestui tip de programe, produsul va trebui să ofere protecție anti-spyware. 4.10. Posibilitatea de configura scanările programate să se execute cu prioritate redusa	- interzice accesul - stergere - muta fisierele in carantina 2.4.2 Scanarea automata in timp real poate fi setata sa nu scaneze arhive sau fisiere mai mari de « x » MB, marimea fisierelor putand fi definita de administratorul solutiei, 2.4.3 Este posibila definirea pana la 16 nivele de profunzime pentru scanarea in arhive. 2.4.4 Este posibila 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. 2.4.5 Este posibila scanarea oricarui suport de stocare a informatiei (CD-uri, harduri externe, unitati partajate etc). De asemenea, sa poata anula scanarea in cazul in care sunt detectate unitati care au informatii stocate mai mult de « x » MB. 2.4.6 Este posibil de scanare automata a emailurilor la nivelul statiei de lucru pentru POP3/SMTP. 2.4.7 Este posibil de configurarat caile ce urmeaza a fi scanate la cerere. 2.4.8 Clientii antimalware pentru workstation 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 ofera protectie anti-spyware. 2.4.10 Este posibil de a configura scanarile programate sa se execute cu prioritate redusa	

				4.11. Produsul anti malware poate fi configurat să folosească scanarea în cloud, și parțial scanarea locala. Pentru stațiile ce nu au suficiente resurse hardware, scanarea se poate face cu o mașina de scanare instalata în rețea. 4.12. Administratorul poate personaliza și motoarele de scanare, având posibilitatea de a alege între mai multe tehnologii de scanare: 4.12.1. 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. 4.12.2. 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. 4.13. Pentru o protecție sporita, soluția anti malware trebuie să aibă 3 tipuri de detecție: bazata pe semnături, bazata de comportamentul fișierelor și bazata pe monitorizarea proceselor.	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 sa 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 include 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.	

				4.14. Pentru o protecție sporita, soluția anti malware trebuie să poată scana paginile HTTP. 4.15. Pentru o mai buna gestionare a anti malware instalat pe stații, produsul va include opțiunea de setare a unei parole pentru protecția la dezinstalare. 4.16. Pentru siguranța utilizatorului, clientul va include un modul de antiphishing. 4.17. Soluția oferă protecție în timp real pe mașinile cu sistem de operare Linux în conformitate cu versiunea de kernel instalata. 4.18. Pe mașinile virtuale parte a unui pool instalarea clientului anti malware se face doar	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 sa nu blocheze in mod uzual scripturi pentru a proteja impotriva acestor tipuri de atacuri. 2.4.19 Solutia ofera 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 ofera 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 ofera 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). 2.4.22. Pe mașinile virtuale parte a unui pool instalarea clientului anti malware se face doar pe mașina de tip template, după care se recompune pool-ul de mașini virtuale. 2.5 Anti-Exploit-Avansat:	

				pe mașina de tip template, după care se recompune pool-ul de mașini virtuale. 5. Firewall: 5.1. Posibilitatea de a configura reguli de firewall pentru aplicații sau conectivitate. 5.2. Modulul poate fi instalat/dezinstalat în funcție de preferința administratorului. 5.3. Posibilitatea de a defini rețele de încredere pentru mașina destinație. 6. Carantina: 6.1. Produsul anti malware să permită trimiterea automata a fișierelor din carantina către laboratoarele anti malware ale producătorului. 6.2. Trimiterea conținutului carantinei va putea fi expediat în mod automat, la un interval definit de administrator.	2.5.1 Este posibil de a opri atacurile avansate de tip „zero-day" efectuate prin intermediul unor exploit-uri evazive. 2.5.2 Solutia depisteza in timp real cele mai recente exploit-uri ce pot vulnerabiliza un sistem de operare. 2.5.3 Solutie ofera protectie pentru 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 Este posibil 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 Este posibil de a defini retele de incredere pentru masini destinate. 2.6.4 Este posibil de a detecta scanarea de porturi. 2.6.5 Este posibil de a seta diferite profiluri de rețea ((Home/Office, Trusted, Public, Untrusted sau Let the Windows decide) 2.6.6 Solutia este capabila 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.	

				6.3. Produsul anti malware să permită ștergerea automata a fișierelor din carantină mai vechi de o anumita perioada, pentru a nu încărca inutil spațiul de stocare. 6.4. Posibilitatea de a restaura un fișier din carantina în locația lui originala. 6.5. Modulul de carantina va permite re-scanarea obiectelor după fiecare actualizare de semnături. 7. Controlul conținutului: 7.1. Consola va avea integrat un modul dedicat controlului accesului la Internet cu următoarele particularități: 7.1.1. Permite blocarea accesului la Internet pentru anumite mașini client sau grupuri de mașini. 7.1.2. Permite blocarea accesului la Internet pe intervale orare. 7.1.3. Permite blocarea paginilor de internet care conțin anumite cuvinte cheie. 7.1.4. Permite controlul accesului numai la anumite pagini de internet specificate de administrator; 7.1.5. Permite blocarea accesului la anumite aplicații definite de administrator; 7.1.6. Permite restricționarea accesului pe anumite pagini de internet după anumite categorii prestabilite (ex: online dating, violenta, pornografie etc). 8. Controlul aplicațiilor:	2.7.4 Este posibil de a restaura un fisier din carantina in locatia lui originala. 2.7.5 Modulul de carantina permite 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	

				8.1. Pentru o mai buna inventariere și administrare, soluția va include o secțiune în consola de administrare unde se vor regăsi toate aplicațiile descoperite în rețea, grupate după: nume, versiune, descoperit la, găsit pe. 8.2.Produsul trebuie sa permită administratorului sa identifice toate încercările utilizatorului de pornire a aplicației si sa reglementeze lansarea aplicațiilor prin intermediul regulilor de control pentru pornirea aplicațiilor 8.3.produsul trebuie sa permită administratorului sa creeze reguli pentru pornirea aplicațiilor, stabilind multiple condiții cum ar fi: - calea către florerul ce conține fișierul executabil al aplicației - metadata (denumirea originala a fișierului executabil al unei aplicații, numele fișierului executabil al unei aplicații aflate pe un dispozitiv drive, versiunea fișierului executabil al aplicației, numele aplicației si producătorul aplicației) - MD5 hash al fișierului executabil al aplicației. - aplicația aparține unei categorii predefinite, care este actualizata constant de producător 8.4. Pentru o mai buna inventariere și administrare, soluția va include o secțiune în consola de administrare unde se vor regăsi toate procesele negrupate descoperite în rețea, grupate după: nume, versiune, nume produs, versiune produs, editor/autor, descoperit la, găsit pe. 8.5.Pentru prevenirea infectării stațiilor și serverelor dar și pentru a permite aplicațiilor descoperite în rețea să se poată actualiza, soluția permite definirea unor programe de actualizare (Updater) care vor fi lăsate să	toate aplicatiile descoperite in retea, grupate dupa: nume, versiune, descoperit la, gasit pe. 2.10.2 Produsul permite administratorului sa identifice toate încercările utilizatorului de pornire a aplicației si sa reglementeze lansarea aplicațiilor prin intermediul regulilor de control pentru pornirea aplicațiilor 2.10.3 produsul permite administratorului sa creeze reguli pentru pornirea aplicațiilor, stabilind multiple condiții cum ar fi: - calea către florerul ce conține fișierul executabil al aplicației - metadata (denumirea originala a fișierului executabil al unei aplicații, numele fișierului executabil al unei aplicații aflate pe un dispozitiv drive, versiunea fișierului executabil al aplicației, numele aplicației si producătorul aplicației) - MD5 hash al fișierului executabil al aplicației. - aplicația aparține unei categorii predefinite, care este actualizata constant de producător 2.10.4 Pentru o mai buna inventariere și administrare, soluția include o secțiune în consola de administrare unde se vor regăsi toate procesele negrupate descoperite în rețea, grupate după: nume, versiune, nume produs, versiune produs, editor/autor, descoperit la, găsit pe. 2.10.5 Pentru prevenirea infectării stațiilor și serverelor dar și pentru a permite aplicațiilor descoperite în rețea să se poată actualiza, soluția permite definirea unor programe de actualizare (Updater) care vor fi lăsate să actualizeze diferite aplicații instalate pe stații sau servere.	

				actualizeze diferite aplicații instalate pe stații sau servere. 8.6.Produsul trebuie sa permită implementarea politicilor negare implicit pentru pornirea aplicațiilor 9. Controlul dispozitivelor: 9.1. Modulul poate fi instalat/dezinstalat în funcție de preferința administratorului. 9.2.Modulul va permite controlul următoarelor tipuri de dispozitive: 9.2.1. Bluetooth Devices 9.2.2. CDROM Devices 9.2.3. USB 9.2.4. Floppy Disk Drives 9.2.5. Security Policies 153 9.2.6. IEEE 1284.4 9.2.7. IEEE 1394 9.2.8. Imaging Devices 9.2.9. Modems 9.2.10. Tape Drives 9.2.11. Windows Portable 9.2.12. COM/LPT Ports 9.2.13. SCSI Raid 9.2.14. Printers 9.2.15. Network Adapters	2.10.6 Produsul permite implementarea politicilor negare implicit pentru pornirea aplicațiilor 2.10.7 Solutia sa includa 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 2.10.8 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. USB d. Floppy Disk Drives e. Security Policies 153 f. IEEE 1284.4 g. IEEE 1394 h. Imaging Devices i. Modems j. Tape Drives k. Windows Portable l. COM/LPT Ports m. SCSI Raid n. Printers o. Network Adapters p. Wireless Network Adapters q. Internal and External Storage	

				9.2.16. Wireless Network Adapters 9.2.17. Internal and External Storage 9.3. Modulul va permite configurarea de reguli prin care se vor defini permisiunile pentru dispozitivele conectate la mașina client. 9.4. Modulul va permite configurarea de excluderi pentru diferite tipuri de dispozitive pentru care s-au configurat reguli. 10. Actualizare:	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 poate fi instalat/dezinstalat in functie de preferinta administratorului. 2.12.2 Modulul permite 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 poate suprascrie din consola setarile aplicate de utilizatorii Power User. 2.13 Actualizare: 2.13.1 Este posibil efectuarea actualizarii la nivel de statie in mod silentios (fara avertizare).	

				10.1. Posibilitatea efectuării actualizării la nivel de stație în mod silențios (fără avertizare). 10.2. Sistem de actualizare cascadat folosind unul sau mai multe servere de actualizare (cascadate). 10.3. Actualizarea pentru locațiile remote prin intermediul unui client anti malware care are și rol de server de actualizare. **C. PROTECȚIE și SECURITATE PENTRU TELEFOANELE MOBILE DE TIP SMARTPHONE** 1. Cerințe minime de sistem: 1.1. Telefoane și tablete cu sistem de operare iOS 9+, iPadOS 13+: Apple iPhone și tablete iPad 1.2. Telefoane și tablet cu sistem de operare Android 4+ 2. Caracteristici: 2.1. Permite asocierea unui dispozitiv cu un utilizator din Active Directory. 2.2. Instalarea se face prin trimiterea unui email către utilizator cu detaliile de instalare. 2.3. Activarea dispozitivului mobil în consola de management să se facă prin scanarea unui cod QR. 2.4. Pachetele de instalare se vor putea descarcă de pe Apple App Store și Google Play. 2.5. Se vor putea întreprinde următoarele acțiuni: 2.5.1. Blocarea dispozitivului; 2.5.2. Deblocarea dispozitivului; 2.5.3. Ștergerea datelor și revenirea la setările din fabrica; 2.5.4. Localizarea dispozitivului; 2.5.5. Scanarea dispozitivului(doar pentru cele cu sistem de operare Android);	2.13.2 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 care 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 și tablete cu sistem de operare iOS 9+, iPadOS 13+: Apple iPhone și tablete iPad • Telefoane și tablet cu sistem de operare Android 4+ 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 pot descarca de pe Apple App Store si Google Play. 3.2.5 Se poate 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).	

				2.5.6. Criptarea memoriei dispozitivului(doar pentru cele cu sistem de operare Android). 2.6.Consola va permite raportarea dispozitivelor: active, inactive, deconectate, cu sistemul de operare modificat astfel încât utilizatorul să aibă acces total asupra lui (rooted or jailbroken devices). 3. Setări de securitate: 3.1. In cazul în care un dispozitiv nu este conform cu setările dorite, se vor putea întreprinde automat acțiunile: 3.1.1. Ignorare; 3.1.2. Blocarea accesului; 3.1.3. Blocarea dispozitivului; 3.1.4. Ștergerea datelor și revenirea la setările din fabrica; 3.1.5. Ștergerea dispozitivului din consola. 3.2.Se va putea impune blocarea dispozitivelor cu ajutorul unei parole. Aceasta parola va putea fi configurata să conțină: 3.2.1. Parola simpla sau complexa (în funcție de cerințele sistemului de operare); 3.2.2. Numere și litere; 3.2.3. O lungime minima definita de administrator; 3.2.4. Un număr minim de caractere speciale, definit de administrator; 3.2.5. Perioada de expirare a parolei. Perioada va putea fi definita de administrator; 3.2.6. Configurarea restricției refolosirii parolei; 3.2.7. Numărul de introduceri incorecte a parolei, de către utilizator;	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, sa fie posibil 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.	

				3.2.8. Perioada de autoblocare a dispozitivului după un număr de minute definite de administrator. 3.3. Se vor putea genera mai multe profiluri care vor stabili reguli de securitate pentru conectivitatea la Wi-Fi sau VPN (numai pentru sistemul de operare iOS) dar și unele legate de accesul la anumite pagini de internet. 3.4. Profilurile de Wi-Fi vor conține următoarele opțiuni: 3.4.1. Generale – se definește SSID precum și tipul securității rețelei; 3.4.2. Setări TCP/IP – atât pentru protocolul IPv4 dar și pentru IPv6; 3.4.3. Setări de proxy – dezactivat, automat sau configurat manual. 3.5. Profilurile acces pagini de internet pentru sistemul de operare Android includ opțiuni precum: 3.5.1. Permiterea, blocarea sau programarea pentru anumite zile și intervale orare a accesului la anumite pagini de internet; 3.5.2. Crearea unor excepții pentru blocarea sau permiterea accesului către anumite pagini de internet. 3.6. Profilurile acces pagini de internet pentru sistemul de operare iOS includ opțiuni de activare sau dezactivare a: 3.6.1. Utilizării browser-ului Safari; 3.6.2. Opțiunii de completare automata a informațiilor; 3.6.3. Alertării utilizatorului în cazul accesării unor pagini frauduloase; 3.6.4. Java script; 3.6.5. Pop-up-urilor; 3.6.6. Cookie-uri.	3.3.3 Se poate 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 – se defineste SSID precum si tipul securitatii retelei; b. Setari TCP/IP – atat pentru protocolul IPv4 dar si pentru IPv6; c. Setari de proxy – dezactivat, automat sau configurat manual. 3.3.5 Profilurile acces pagini de internet pentru sistemul de operare Android sa includa 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 sa inlcuda 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**	

				D. PROTECȚIE și SECURITATE PENTRU SERVERELE EMAIL MICROSOFT EXCHANGE 1.1. Produsul va oferi protecție anti malware, anti spam (inclusiv anti phishing), precum și filtrare de atașamente și conținut, prin integrarea cu serverul Microsoft Exchange. De asemenea, va permite scanarea anti malware la cerere a bazelor de date Exchange. 1.2. Produsul va asigura scanarea atașamentelor și a conținutului mesajelor în timp real, fără a afecta vizibil performanta serverului de mail. 1.3. Actualizarea anti malware trebuie să poată fi făcută automat la un interval de maxim 1 ora, precum și la cerere. 1.4. In afara de detecția pe baza de semnături, modulul de protecție anti malware va trebui să includă și scanare euristica comportamentala, prin simularea unui calculator virtual în interiorul căruia sunt rulate și analizate aplicații cu potențial periculos, pentru a proteja sistemul de virușii necunoscuți prin detectarea codurilor periculoase a căror semnătură nu a fost lansata încă. 1.5. Produsul va oferi opțiuni multiple de acțiune la identificarea unui atașament virusat (dezinfectare, ștergere, mutare în carantina). 1.6. Cu ajutorul unei baze de date complete cu semnături de spyware și a euristicii de detecție a acestui tip de programe, produsul va oferi protecție anti-spyware pentru a preveni furtul de date confidențiale. 1.7. Produsul va oferi protecție anti spam, cu o baza de semnături actualizabila prin internet. 1.8. Modulul anti spam va trebui să includă un filtru URL cu o baza de adrese URL cunoscute	4.1.1 Produsul ofera 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 asigura scanarea atasamentelor si a continutului mesajelor in timp real, fara a afecta vizibil performanta serverului de mail. 4.1.3 Actualizarea antimalware poate 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 ofera 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 va oferi protectie anti-spyware pentru a preveni furtul de date confidentiale. 4.1.7 Produsul ofera protectie antispam, cu o baza de semnaturi actualizabila prin internet. 4.1.8 Modulul antispam include un filtru URL cu o baza de adrese URL cunoscute a fi folosite in mesaje spam, precum si un filtru de caractere	

				a fi folosite în mesaje spam, precum și un filtru de caractere pentru detectarea automata a mesajelor scrise cu caractere chirilice sau asiatice. 1.9. Produsul va trebui 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. 1.10. Produsul va trebui să ofere un serviciu/filtru online pentru îmbunătățirea protecției împotriva valurilor de spam nou apărute. 1.11. Produsul va oferi posibilitatea de a defini politici de filtrare anti malware, anti spam, a conținutului sau atașamentelor pentru diferite grupuri sau utilizatori. 1.12. Actualizarea produsului va fi configurabila și se va putea realiza de pe internet, direct sau printr-un proxy, sau din cadrul rețelei de pe un server de actualizare propriu. 1.13. Produsul va trebui să ofere statistici atât referitoare la scanarea antivirus cat și la scanarea anti spam. 1.14. Produsul se va integra în cadrul consolei de management unitar al soluției antivirus. Pentru ușurința accesului la setările produsului din diferite medii de operare, produsul va avea consola de administrare web. **E. CERINȚE FAȚĂ DE SERVICIILE DE IMPLEMENTARE și CONFIGURARE** 1.1. Ofertantul selectat va livra și instala licențele pentru soluția ofertată 1.2. Ofertantul selectat va efectua pregătirea mediului de instalare pentru soluția propusă, după care va asigura implementarea inițială a	pentru detectarea automata a mesajelor scrise cu caractere chirilice sau asiatice. 4.1.9 Produsul ofera 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 ofera un serviciu/filtru online pentru imbunatatirea protectiei impotriva valurilor de spam nou aparute. 4.1.11 Produsul ofera 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 sa se putea realiza de pe internet, direct sau printr-un proxy, sau din cadrul retelei de pe un server de actualizare propriu. 4.1.13 Produsul ofera statistici atat referitoare la scanarea antivirus cat si la scanarea antispam. 4.1.14 Produsul se integreaza 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. **5. CERINȚE FAȚĂ DE SERVICIILE DE IMPLEMENTARE și CONFIGURARE** 5.1. În calitate de ofertant selectat vom livra și instala licențele pentru soluția ofertată 5.2. În calitate de ofertant selectat vom efectua pregătirea mediului de instalare pentru soluția propusă, după care va asigura implementarea	

				soluției aplicative în mediul de producție și mediul de testare. 1.3. Ofertantul selectat va efectua configurarea inițială a soluției, atât pentru mediul de producție, cât și mediul de testare. Prin configurare inițială se înțelege setarea tuturor parametrilor aplicabili în corespundere cu cerințele (clientului), inclusiv configurarea și instalarea soluției ofertate, setarea politicilor și testarea înainte de a fi pusa în producție. 1.4. În baza rezultatelor de la etapa de design, Ofertantul selectat va implementa toate configurările/customizările agreate darea în exploatare a soluției. 1.5. Ofertantul va asigura integrarea soluției cu cel puțin următoarele aplicații terțe: 1.5.1. Integrarea cu Active Directory – pentru a asigura autentificarea utilizatorilor în cadrul soluției prin AD; 1.5.2. Integrarea cu platforma mobila (telefoane, tablete) – pentru securizarea perimetrului mobile. 1.6. Ofertantul selectat va efectua instalarea soluției ofertate în întreaga infrastructură a Secretariatului Parlamentului inclusiv la toți utilizatorii finali (instalarea se va considera încheiată în momentul când toți utilizatorii vor avea instalat agentul și calculatorul va primi cel puțin o actualizare a bazelor și a agentului) 1.7. La sfârșitul etapei, Ofertantul va face o demonstrație a soluției și a modulelor care au fost acoperite, fapt care va servi drept unul din criteriile de acceptanță ale etapei de implementare. 1.8. După acceptanța finală a soluției, va fi activată în mod automat opțiunea de garanție	inițială a soluției aplicative în mediul de producție și mediul de testare. 5.3. În calitate de ofertant selectat vom efectua configurarea inițială a soluției, atât pentru mediul de producție, cât și mediul de testare. Prin configurare inițială se înțelege setarea tuturor parametrilor aplicabili în corespundere cu cerințele (clientului), inclusiv configurarea și instalarea soluției ofertate, setarea politicilor și testarea înainte de a fi pusa în producție. 5.4. În baza rezultatelor de la etapa de design, în calitate de ofertant selectat vom implementa toate configurările/customizările agreate darea în exploatare a soluției. 5.5. În calitate de ofertant vom asigura integrarea soluției cu cel puțin următoarele aplicații terțe: 5.5.1. Integrarea cu Active Directory – pentru a asigura autentificarea utilizatorilor în cadrul soluției prin AD; 5.5.2. Integrarea cu platforma mobila (telefoane, tablete) – pentru securizarea perimetrului mobile. 5.6. În calitate de ofertant selectat vom efectua instalarea soluției ofertate în întreaga infrastructură a Secretariatului Parlamentului inclusiv la toți utilizatorii finali (instalarea se va considera încheiată în momentul când toți utilizatorii vor avea instalat agentul și calculatorul va primi cel puțin o actualizare a bazelor și a agentului) 5.7. La sfârșitul etapei, vom efectua o demonstrație a soluției și a modulelor care au fost acoperite, fapt care va servi drept unul din criteriile de acceptanță ale etapei de implementare. 5.8. După acceptanța finală a soluției, va fi activată în mod automat opțiunea de garanție	

				post-implementare și suport. Perioada de garanție post-implementare și suport va fi de 1 an calendaristic de la data activării acestei opțiuni. 1.9. Serviciile de garanție post-implementare și suport se referă la serviciile oferite de către Ofertantul selectat adițional la serviciile de mentenanță și suport a licențelor, oferite direct de către producătorul licențelor. 1.10. Serviciile de garanție post-implementare și suport, vor include următoarele componente: 1.10.1. Gestionarea serviciului de actualizare a serverelor la ultimele actualizări oferite de producător; 1.10.2. Gestionarea incidentelor de securitate apărute pe perioada suportului activ; 1.10.3. Solicitărilor de schimbare a politicilor de securitate; 1.10.4. Solicitări de analiza și corecție a politicilor de securitate în cadrul companiei implementate. **F. Cerințele fata de serviciile de instruire** 1.1. În cadrul proiectului, Ofertantul va organiza sesiuni de instruire și transfer de cunoștințe pentru grupurile țintă în vederea formării setului de cunoștințe necesar pentru a permite echipei instruite să preia menținerea și configurarea ulterioară a soluției, în conformitate cu necesitățile utilizatorilor 1.2. Instruirea se va organiza pentru diferite grupuri țintă la sediul Cumpărătorului sau online. 1.2.1. Analist - 1 persoană 1.2.2. Administrator - 5 persoane,	post-implementare și suport. Perioada de garanție post-implementare și suport va fi de 1 an calendaristic de la data activării acestei opțiuni. 5.9.Serviciile de garanție post-implementare și suport se referă la serviciile oferite de către „RTS ONE" S.R.L. selectat adițional la serviciile de mentenanță și suport a licențelor, oferite direct de către producătorul licențelor. 5.10. Serviciile de garanție post-implementare și suport, vor include următoarele componente: – Gestionarea serviciului de actualizare a serverelor la ultimele actualizări oferite de producător; – Gestionarea incidentelor de securitate apărute pe perioada suportului activ; – Solicitărilor de schimbare a politicilor de securitate; – Solicitări de analiza și corecție a politicilor de securitate în cadrul companiei implementate. **6. CERINȚELE FATA DE SERVICIILE DE INSTRUIRE** 6.1. În cadrul proiectului, „RTS ONE" S.R.L. va organiza sesiuni de instruire și transfer de cunoștințe pentru grupurile țintă în vederea formării setului de cunoștințe necesar pentru a permite echipei instruite să preia menținerea și configurarea ulterioară a soluției, în conformitate cu necesitățile utilizatorilor 6.2.Instruirea se va organiza pentru diferite grupuri țintă la sediul Cumpărătorului sau online. 6.2.1. Analist - 1 persoană 6.2.2. Administrator - 5 persoane,	

				1.3. În acest sens, ca parte a ofertei, Ofertantul va prezenta ca parte a ofertei, un plan de instruire, în care se va indica ce tipuri de instruiri va efectua Ofertantul, pentru ce categorie de utilizatori, precum și cuprinsul/agenda acestor instruiri. 1.4. În afara instruirilor ce țin de utilizarea soluției, Ofertantul trebuie să efectueze și sesiuni de instruire pentru echipa de menținere din partea Cumpărătorului, în scopul asigurării unui nivel adecvat de cunoștințe și competențe, pentru a putea utiliza eficient instrumentele de configurare și dezvoltare disponibile în cadrul soluției. 1.5. În cadrul serviciilor de implementare, pentru a asigura transferul necesar de cunoștințe către echipa Cumpărătorului, Ofertantul va fi de acord ca cel puțin o persoană să asiste la lucrările de parametrizare/configurare, stabilite de comun acord de către Părți. 1.6. Ofertantul selectat la etapa de încheiere a contractului, va trebui să elaboreze și să convină cu Cumpărătorul următoarele elemente ale componentei de instruire: 1.6.1. Strategia Ofertantului cu privire la instruire și programul de formare; 1.6.2. Structura și componența pachetului de cursuri pentru formare și a manualelor de studiu pentru fiecare categorie de utilizator; 1.6.3. Metodologia și procedurile de evaluare și control al eficienței și suficienței sesiunilor de instruire. 1.7. În cadrul sesiunilor de instruire, Ofertantul va pune la dispoziția Cumpărătorului întreg setul de documentație al soluției, care să cuprindă cel puțin următoarele componente: **G. Licențe:**	6.3.În acest sens, ca parte a ofertei, RTS ONE" S.R.L. va prezenta ca parte a ofertei, un plan de instruire, în care se va indica ce tipuri de instruiri va efectua RTS ONE" S.R.L. , pentru ce categorie de utilizatori, precum și cuprinsul/agenda acestor instruiri. 6.4. În afara instruirilor ce țin de utilizarea soluției, RTS ONE" S.R.L. va efectua și sesiuni de instruire pentru echipa de menținere din partea Cumpărătorului, în scopul asigurării unui nivel adecvat de cunoștințe și competențe, pentru a putea utiliza eficient instrumentele de configurare și dezvoltare disponibile în cadrul soluției. 6.5.În cadrul serviciilor de implementare, pentru a asigura transferul necesar de cunoștințe către echipa Cumpărătorului, RTS ONE" S.R.L. va fi de acord ca cel puțin o persoană să asiste la lucrările de parametrizare/configurare, stabilite de comun acord de către Părți. 6.6.RTS ONE" S.R.L. selectat la etapa de încheiere a contractului, va trebui să elaboreze și să convină cu Cumpărătorul următoarele elemente ale componentei de instruire: – Strategia Ofertantului cu privire la instruire și programul de formare; – Structura și componența pachetului de cursuri pentru formare și a manualelor de studiu pentru fiecare categorie de utilizator; – Metodologia și procedurile de evaluare și control al eficienței și suficienței sesiunilor de instruire.. 6.7.În cadrul sesiunilor de instruire, RTS ONE" S.R.L. va pune la dispoziția Cumpărătorului întreg setul de documentație al soluției, care să cuprindă cel puțin următoarele componente **7. LICENȚE:**	

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

				1.1. Desktopuri/ Căsuțe de email – 500 1.2. Mașini virtuale – 20 1.3. Servere – 10 **H. Cerințe minime de calificare a ofertanților:** 1.1. Disponibilitatea interfeței administratorului și a agentului soluției ofertate în limbele circulație internațională ; 1.2. Producătorul trebuie să ofere suport tehnic 24/7, inclusiv în limbele circulație internațională prin e-mail sau telefon; 1.3. Suport tehnic local 24/7 în limbele circulație internațională din partea partenerului local; 1.4. Autorizarea de la Producător a partenerului vis-a-vis de dreptul de vânzare a produselor pe teritoriul R. Moldova; 1.5. Autorizarea de la Producător a partenerului vis-a-vis de dreptul de a oferi suport tehnic pe teritoriul R. Moldova; 1.6. Prezentarea documentelor confirmative a minim 2 specialiști certificați pe soluția propusa.	7.1. Desktopuri/ Căsuțe de email – 500 7.2.Servere/ Mașini virtuale – 30 **8. CERINȚE MINIME DE CALIFICARE A OFERTANȚILOR:** 8.1. Disponibilitatea interfeței administratorului și a agentului soluției ofertate în limbele circulație internațională ; 8.2.Producătorul va oferi suport tehnic 24/7, inclusiv în limbele circulație internațională prin e-mail sau telefon; 8.3.Suport tehnic local 24/7 în limbele circulație internațională din partea partenerului local; 8.4. Autorizarea de la Producător a partenerului vis-a-vis de dreptul de vânzare a produselor pe teritoriul R. Moldova; 8.5.Autorizarea de la Producător a partenerului vis-a-vis de dreptul de a oferi suport tehnic pe teritoriul R. Moldova; 8.6.Prezentarea documentelor confirmative a minim 2 specialiști certificați pe soluția propusa.	
TOTAL						

Semnat:

Numele, Prenumele: **CELONENCO Vitalie**

În calitate de: **Administrator**

Ofertantul: **„RTS ONE" S.R.L.**

Digitally signed by Celonenco Vitalie
Date: 2022.12.05 18:06:04 EET
Reason: MoldSign Signature
Location: Moldova

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