Anexa nr. 22
la Documentația standard
nr.115 din 15.09.2021

Specificații tehnice

Numărul procedurii de achiziție: MTender ID: **ocds-b3wdp1-MD-1700468736540 din 28 noiembrie 2023**

Obiectul achiziției: **Programa Antivirus**

Denumirea bunurilor	Modelul articolului	Țara de origine	Producă-torul	Specificarea tehnică deplină solicitată de către autoritatea contractantă	Specificarea tehnică deplină propusă de către ofertant	Standarde de referință
1	*2*	*3*	*4*	*5*	*6*	*7*
Lotul 1: Programa Antivirus	Bitdefender GravityZone Business Security Premium	România	Bitdefender	**Specificații pentru soluție de protecție si securitate antivirus pentru protectia infrastructurii:** Se solicita achizitia a unei soluții corporative de tip anti-malware, care sa ofere protecțiea, securitatea si scanarea vulnerabilităților a 450 de stații de lucru, servere fizice si virtualizate, cutii postale pentru o perioadă de 24 luni. Produsul (solutia) sa reprezinte o platforma integrata pentru managementul securitatii, gandita ca o solutie modulara. Produsul sa contina urmatoarele module: 1. O consola de management care asigura functionalitati de administrare. 2. Protectie statii si servere fizice/virtuale. 3. Protectie si securitate pentru serverele email Microsoft Exchange Produsul antivirus oferit trebuie să ocupe locurile de top în testele internaționale independente cu renume mondial în domeniu (certificări „AV-TEST", „VIRUS BULLETIN'S", „REAL-WORLD PROTECTION", „MALWARE PROTECTION"). **1. CONSOLA DE MANAGEMENT:** **1.1. Instalare și configurare** 1.1.1. Pachetul de instalare necesar să fie livrat ca o masina virtuala bazata pe sistem de operare Linux securizat care contine toate rolurile sau serviciile necesare. Consola nu va necesita o licenta suplimentara pentru sistemul de operare. Imaginea de tip template se va putea importa in:	**Caracateristici principale:** Se oferă soluția Bitdefender GravityZone, cu urmatorul model de licentiere: - *Bitdefender GravityZone Business Security Premium* pentru 450 stații de lucru, servere fizice si virtualizate, cutii postale, pentru o perioadă de 24 luni. Soluția propusă reprezintă o platforma integrată pentru managementul securitatii, gândită ca o soluție modulară. Produsul conține urmatoarele module: 1. O consola de management care asigură funcționalități de administrare. 2. Protecție stații și servere fizice/virtuale. 3. Protecție și securitate pentru serverele email Microsoft Exchange Produsul antivirus oferit ocupă locurile de top în testele internaționale independente cu renume mondial în domeniu (certificări „AV-TEST", „VIRUS BULLETIN'S", „REAL-WORLD PROTECTION", „MALWARE PROTECTION"). **1. CONSOLA DE MANAGEMENT:** **1.1. Instalare și configurare** 1.1.1. Pachetul de instalare va fi livrat ca o mașină virtuala bazată pe sistem de operare Linux securizat care conține toate rolurile sau serviciile necesare. Consola nu necesită o licență suplimentară pentru sistemul de operare. Imaginea de tip template poate importa în:	

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
1	*2*	*3*	*4*	*5*	*6*	*7*
				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 sa fie 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 sa fie 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 trebuie sa fie cel putin similare cu: Server cu baza de date, Server de comunicatie, Server de actualizare, Server de Web. 1.1.5. Solutia necesar să includă adițional 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 să fie 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 se fie 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. Interfata consolei de management să fie în limba romana.	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 va fi livrată cu o bază de date inclusa care este de tip non-relațională, pentru o funcționare cât mai rapidă, fără a fi nevoie de licențe adiționale. 1.1.3. Soluția propusă este scalabilă, astfel că oricare dintre roluri sau servicii pot fi instalate separat pe mai multe mașini virtuale sau pe aceeași mașină virtuală. 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 propusă include adițional și un modul de balansare (load balancer) pentru cazurile în care mai multe mașini virtuale ale componentei de management sunt instalate cu același rol (pentru Load Balancing și performanță/redundanță). 1.1.6. Soluția include un mecanism de configurare a disponibilității pentru Serverul cu baze de date (clustering pentru redundanță). Astfel, baza de date se poate instala de mai multe ori, pe mai multe mașini virtuale. 1.1.7. Masinile de scanare pentru mediile virtuale VsMware și Citrix sunt posibil de instalat la distanță prin task din consola de management, iar pentru alte platforme se poate descarcă separat din interfața web a produsului. **1.2. Cerinte generale:** 1.2.1. Interfata consolei de management este și în limba romana.	

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
1	2	3	4	5	6	7
				1.2.2. Interfata clientului de securitate, care se instaleaza pe statii si servere, să fie în limba romana. 1.2.3. Manualul de instalare a produsului să fie în limba romana. 1.2.4. Manualul de administrare a produsului să fie în limba romana. 1.2.5. Solutia să includă 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 să permită 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 să permita 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 – prezente in interfata, notificarile necitite să fie 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 sa permite integrarea cu un server Syslog pentru raportarea evenimentelor antimalware. 1.2.11. Solutia sa permite instalarea serviciului de SMNP prin care se pot raporta statusul masinilor din cadrul componentei de management.	1.2.2. Interfata clientului de securitate, care se instaleaza pe statii si servere, este în limba română. 1.2.3. Manualul de instalare a produsului este în limba română. 1.2.4. Manualul de administrare a produsului este în limba română. 1.2.5. Solutia include un modul de update server prin care asigură actualizarea de produs și a semnăturilor. 1.2.6. Soluția permite activarea/dezactivarea actualizărilor de produs/semnături. 1.2.7. Soluția permite stabilirea actualizării automate a consolei de management prin stabilirea recurentei zilnice, săptămânale sau lunare, dar si prin stabilirea intervalului orar în care acesta va fi actualizat. De asemenea, permite și trimiterea unei alerte de ne funcționalitate, cu 30 de minute înainte de actualizare. 1.2.8. Pentru o mai bună urmărire a actualizărilor consolei de management, soluția permite vizualizarea unui jurnal de modificări în care sunt precizate istoric: a) versiunea consolei de management b) data versiunii c) funcții noi și îmbunătățiri d) probleme rezolvate e) probleme cunoscute 1.2.9. Notificările – prezente în interfața, notificările necitite sunt evidențiate, pot fi trimise către una sau mai multe adrese de email, cu alertarea administratorul în cazul unor probleme majore: licențiere, detecție viruși, actualizări de produs disponibile). 1.2.10. Soluția permite integrarea cu un server Syslog pentru raportarea evenimentelor antimalware. 1.2.11. Solutia permite instalarea serviciului de SMNP prin care raportează statusul mașinilor din cadrul componentei de management.	

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
1	*2*	*3*	*4*	*5*	*6*	*7*
				1.2.12. Solutia sa 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 sa fie 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 necesar sa fie posibil 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 sa contina rapoarte pentru toate modulele suportate. 1.3.3. Rapoartele din panoul central de comanda sa permita: adaugarea altor rapoarte, stergerea lor si rearanjarea. **1.4. Inventarierea retelei – managementul securitatii:** 1.4.1. Solutia sa fie integrata cu domenii Active Directory multiple, VMware vCenter Server, Citrix Xen Server, Nutanix Prism Element si importa inventarul acestor platforme. 1.4.2. Sa permita descoperirea statiilor statii fizice neintegrate in Active Directory (Workgroup) cu ajutorul Network discovery. 1.4.3. 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. 1.4.4. Solutia sa permite crearea unui pachet unic pentru toate sistemele de operare, de statii sau servere. Astfel, administratorul sa poata descarca pachetele pentru protectia	1.2.12. Soluția permite creare unei copii de siguranță a bazei de date a consolei de administrare, la cerere sau programată, care poate fi stocată local, pe un server FTP sau în rețea. 1.2.13. Consola de management este accesibilă atât de pe stații de lucru cât și de pe dispozitive mobile (smartphone, tableta). **1.3. Panou de monitorizare și raportare (Dashboard):** 1.3.1. Rapoartele din panoul de monitorizare pot 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 considerată neactualizată). 1.3.2. Panoul central conține rapoarte pentru toate modulele suportate. 1.3.3. Rapoartele din panoul central de comanda permit: adăugarea altor rapoarte, ștergerea lor și rearanjarea. **1.4. Inventarierea rețelei – managementul securității:** 1.4.1. Soluția poate fi integrată cu domenii Active Directory multiple, VMware vCenter Server, Citrix Xen Server, Nutanix Prism Element si importa inventarul acestor platforme. 1.4.2. Soluția propusă permite descoperirea stațiilor stații fizice neintegrate în Active Directory (Workgroup) cu ajutorul Network discovery. 1.4.3. Soluția oferă opțiuni de căutare, sortare și filtrare după numele sistemului, sistem de operare, adresa IP, politica aplicata, ultima data când s-a conectat (online si/sau offline) si FQDN. 1.4.4. Soluția propusă permite crearea unui pachet unic pentru toate sistemele de operare, de stații sau servere. Astfel, administratorul poate descărca pachetele	

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
1	2	3	4	5	6	7
				statiilor si 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. Sa permita descoperirea masinilor din Microsoft Hyper-V, Red Hat VM, Oracle VM, KVM. 1.4.7. Solutia sa permita instalarea la distanta sau manual a clientilor antimalware pe masini fizice/virtuale. 1.4.8. Solutia sa permita selectarea modulelor componente atunci cand se creaza pachetul clientului care se instalează pe mașinile fizice/virtuale. 1.4.9. Solutia sa permita lansarea de task-uri de scanare, actualizare, instalare, dezinstalarea la distanta pentru clientul antimalware. 1.4.10. Solutia sa ofere posibilitatea de repornire a masinilor fizice de la distanta. 1.4.11. Solutia sa ofere informatii detaliate despre fiecare task si sa fiseaze daca task-ul s-a finalizat sau nu cu succes. 1.4.12. Solutia sa permita configurarea centralizata a clientilor antimalware prin intermediul politicilor. 1.4.13. Sa fie ofert 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 sa permita 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 sa permita configurarea setarilor clientului antimalware prin intermediul unei singure politici ce contine setari pentru toate module.	pentru protecția stațiilor și serverelor pe care rulează sistemul de operare Windows, Linux, Mac. 1.4.5. Pentru integrarea cu Active Directory, se poate defini intervalul (în ore) de sincronizare și forța sincronizarea. 1.4.6. Soluția permite descoperirea mașinilor din Microsoft Hyper-V, Red Hat VM, Oracle VM, KVM. 1.4.7. Soluția permite instalarea la distanță sau manual a clienților antimalware pe mașini fizice/virtuale. 1.4.8. Soluția permite selectarea modulelor componente atunci când se creează pachetul clientului care se instalează pe mașinile fizice/virtuale. 1.4.9. Soluția permite lansarea de task-uri de scanare, actualizare, instalare, dezinstalarea la distanță pentru clientul antimalware. 1.4.10. Soluția oferă posibilitatea de repornire a mașinilor fizice de la distanță. 1.4.11. Soluția oferă informații detaliate despre fiecare task și fișează daca task-ul s-a finalizat sau nu cu succes. 1.4.12. Soluția permite configurarea centralizată a clienților antimalware prin intermediul politicilor. 1.4.13. Soluția oferă 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. 1.4.14. Soluția permite descoperirea tuturor aplicațiilor instalate pe toate stațiile și serverele din rețea, prin rularea unui task din consola de administrare. **1.5. Politici:** 1.5.1. Soluția permite configurarea setărilor clientului antimalware prin intermediul unei singure politici ce conține setări pentru toate modulele.	

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
1	*2*	*3*	*4*	*5*	*6*	*7*
				1.5.2. Politica sa contina 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 sa permita 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 sa poata 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 sa contina 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 sa fie 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 sa permita vizualizarea rapoartelor curente programate de administrator. 1.6.4. Solutia sa permita exportarea rapoartelor in format .pdf si detaliile ca format .csv.	1.5.2. Politica conține opțiuni specifice de activare/dezactivare și configurarea funcționalităților precum scanarea antimalware la cerere, firewall, controlul accesului la Internet, controlul aplicațiilor, scanarea traficului web, controlul dispozitivelor, power user. 1.5.3. Soluția permite aplicarea politicilor pe mașini client, grupuri de mașini, pool-uri de resourse (VMware), domeniu, unități organizaționale, grupuri de securitate sau useri de active directoy. 1.5.4. Politica poate fi schimbată automat în funcție de: a) IP sau clasa de IP al stației 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 (stația de lucru poate soluționa 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. Soluția conține rapoarte care prezintă statusul mașinilor clienților din punct de vedere al actualizărilor, fișierelor malware detectate, aplicațiile blocate, site-urilor web blocate. 1.6.2. Rapoartele programate sunt posibil de trimis către un număr nelimitat de adrese de email (nu este nevoie să dețină un cont în consola de management). 1.6.3. Soluția permite vizualizarea rapoartelor curente programate de administrator. 1.6.4. Soluția permite exportarea rapoartelor în format .pdf și detaliile ca format .csv.	

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
1	*2*	*3*	*4*	*5*	*6*	*7*
				1.6.5. Solutia sa includa 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 sa 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 sa includa 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 sa includa 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:**	1.6.5. Soluția include un generator de rapoarte care oferă posibilitatea de a investiga o problemă de securitate pe baza mai multor criterii, menținând informațiile concise și ordonate corespunzător. Astfel, soluția include interogări precum: starea terminalului, evenimente terminal, evenimente Exchange. 1.6.6. Interogarea legata de starea terminalului include informații precum: a) tip mașină b) infrastructura rețelei căreia îi aparține terminalul c) datele agentului de securitate d) starea modulelor de protecție e) rolurile terminalelor. 1.6.7. Interogarea legată de evenimente terminal include informații precum: a) calculatorul țintă pe care a avut loc evenimentul b) tipul starea și configurația agentului de securitate instalat c) starea modulelor și rolurilor de protecție instalate pe agentul de securitate d) denumirea și alocarea politicii e) utilizatorul autentificat în timpul evenimentului f) evenimente (site-uri blocate, aplicații blocate, detecțiile etc) 1.6.8. Interogarea legată de evenimente Exchange include informații precum: a) Direcția traficului e-mail b) Evenimente de securitate (detectarea programelor de tip malware sau a fișierelor atașate) c) Măsurile implementate în fiecare situație (curățarea, ștergerea, înlocuirea sau carantinarea fișierului, ștergerea sau respingerea e-mail-ului) **1.7. Carantina:**	

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
1	*2*	*3*	*4*	*5*	*6*	*7*
				1.7.1. Solutia sa permita 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 sa fie 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 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. Sa fie oferite informatii detaliate pentru fiecare actiune a unui utilizator. 1.9.3. Sa permita filtrarea actiunilor utilizator dupa numele utilizatorului, actiune. **1.10. Actualizare:**	1.7.1. Soluția permite restaurarea fișierelor carantinate în locația originală sau într-o cale configurabilă. 1.7.2. Carantina este locală, pe fiecare stație administrată ș poate fi administrată, fie local, fie din consola de management 1.7.3. Soluția permite descărcarea fișierelor carantinate doar pentru mașinile virtuale protejate prin modulul mediilor virtuale integrat cu VMware vShield. **1.8. Utilizatori:** 1.8.1. Administrarea este posibil de făcut pe baza de roluri. 1.8.2. Roluri multiple predefinite: Administrator companie, Administrator rețea, Reporter sau rol personalizat: d) Administrator companie: administrează arhitectura consolei de management; e) Administrator rețea: administrează serviciile de securitate; f) Reporter: monitorizează și generează rapoarte. 1.8.3. Utilizatorii sunt posibil de importat din Microsoft Active Directory sau crearea în consola de management. 1.8.4. Soluția permite configurarea detaliată a drepturilor administrative, permițând selectarea serviciilor și obiectelor pentru care un utilizator poate face modificări. 1.8.5. Soluția permite deconectarea automată a oricărui tip de utilizator după un anumit timp pentru o protecție sporita a datelor afișate în consola de administrare. Acest interval poate fi personalizat de administratorul soluției. **1.9. Log-uri:** 1.9.1. Înregistrarea acțiunilor utilizatorilor. 1.9.2. Soluția oferă informații detaliate pentru fiecare acțiune a unui utilizator. 1.9.3. Soluția permite filtrarea acțiunilor utilizator după numele utilizatorului, acțiune. **1.10. Actualizare:**	

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
1	2	3	4	5	6	7
				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	1.10.1. Soluția permite definirea de locații de actualizări multiple. 1.10.2. Soluția permite activarea/dezactivarea actualizărilor de produs și semnături. 1.10.3. Soluția permite actualizarea produsului într-o rețea fără acces la Internet. 1.10.4. Orice client antivirus poate fi configurat să livreze update-urile către alt client antivirus 1.10.5. Soluția dispune de un server de actualizare (update) care face posibilă stabilirea componentelor ce vor fi descărcate automat de pe internet, fără intervenția administratorului. Astfel, administratorul poate 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. 1.10.6. În cadrul serverului de actualizare, pentru o mai buna urmărire a actualizărilor pachetele pentru protecția stațiilor și serverelor sau a pachetelor pentru modul de scanare centralizată, există posibilitatea de vizualizare a unui jurnal de modificări în care sunt precizate istoric: a) versiunea pachetului b) data versiunii c) funcții noi și îmbunătățiri d) probleme rezolvate e) probleme cunoscute 1.10.7. Soluția permite testarea noilor versiuni de pachete de instalare ale clientului antimalware, 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: a) Ciclu rapid, gândit pentru un mediu de test în cadrul rețelei	

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
1	2	3	4	5	6	7
				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. <u>PROTECTIE STATII SI SERVERE FIZICE SAU VIRTUALE</u>** **2.1. Caracteristici generale minimale si eliminatorii:** 2.1.1. Pentru reducerea la minim a consumului de resurse, solutia antimalware trebuie sa permita instalarea personalizata a modulelor detinute (de exemplu, sa permita instalarea solutiei antimalware fara modulul de control al accesului web, modul de control al dispozitivilelor sau modulul firewall). 2.1.2. Pentru o mai buna protectie a statiilor si serverelor, solutia sa includa 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 sa primesta actualizari de la producator, odata cu	b) Ciclu lent, gândit pentru restul rețelei (producție, servere critice etc) 1.10.8. Soluția permite stabilirea zonelor de test și critice din cadrul rețelei prin intermediul politicilor din consola de management. **1.11. Certificate:** 1.11.1. Accesul la consola de management se face doar prin HTTPS. 1.11.2. Serverul web, din consola centrală de management permite importarea de certificate digitale eliberate de o autoritate de certificare autorizată sau proprie organizației. 1.11.3. Soluția permite afișarea în consola de management informații despre certificate: nume, autoritatea emitenta, data eliberării și data expirării certificatelor eliberate. **2. <u>PROTECȚIE STAȚII ȘI SERVERE FIZICE SAU VIRTUALE</u>** **2.1. Caracteristici generale minimale și eliminatorii:** 2.1.1. Pentru reducerea la minim a consumului de resurse, soluția antimalware permite instalarea personalizată a modulelor deținute (de exemplu, permite instalarea soluției antimalware fără modulul de control al accesului web, modul de control al dispozitivelor sau modulul firewall). 2.1.2. Pentru o mai buna protecție a stațiilor și serverelor, soluția include un vaccin anti-ransomware. Acest vaccin asigură protecția împotriva tuturor amenințărilor cunoscute de tip ransomware, prin imunizarea stațiilor și serverelor, chiar dacă sunt infectate și prin blocarea procesului de criptare. 2.1.3. Vaccinul anti-ransomware primește actualizări de la producător, odată cu	

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
1	2	3	4	5	6	7
				actualizarea semnaturilor produsului Antimalware. 2.1.4. Pentru o mai buna protectie a statiilor si serverelor, solutia sa includa 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 sa includa 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 sa protejeze 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 sa fie cu 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 sa includa un sandbox in cloud-ul public al producatorului acesteia.	actualizarea semnăturilor produsului Antimalware. 2.1.4. Pentru o mai buna protecție a stațiilor și serverelor, soluția include protecție împotriva atacurilor zero-day de tip exploit avansate (atacuri direcționate) bazate pe tehnologii de învățare automată (machine learning). 2.1.5. Pentru o mai bună protecție a stațiilor și serverelor, soluția include un modul avansat de securitate – HyperDetect, bazat pe tehnologii de tip „machine learning tunabil", proiectat special pentru a detecta atacuri avansate și activități suspecte în faza pre-execuție. 2.1.6. Acest modul avansat de securitate protejează împotrivă: atacurilor direcționate (Targeted Attack - APT), fișierelor suspecte și traficului la nivel de rețea suspect, exploit-urilor, ransomware și grayware. Fiecărui tip de amenințare menționat, i se poate stabili, independent, un nivel de protecție dorit: permisiv, normal, agresiv. 2.1.7. Modulul avansat de securitate are posibilitatea de a raporta, bloca accesul, dezinfecta, șterge sau muta in carantina pentru fiecare din categoriile descrise. Astfel, administratorul poate decide dacă dorește întâi monitorizare sau dorește si blocarea amenințărilor. Aceste acțiuni menționate, pot fi stabilite independent, pentru fișiere sau pentru traficul din rețea, cu posibilitatea extinderii nivelului de raportare pentru a include nivelurile superioare (pot fi raportate amenințările care ar fi fost detectate daca nivelul de protecție era stabilit mai agresiv). 2.1.8. Pentru a oferi un nivel adițional de protecție a stațiilor și serverelor, soluția include un sandbox în cloud-ul public al producătorului acesteia.	

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
1	2	3	4	5	6	7
				2.1.9. Modulul de Sandbox sa poata 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 sa includa 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 sa includa 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 sa includa 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 sa poata 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, sa poata fi detectate corect chiar daca sunt incluse in arhive de tipul: : 7z, ACE, ALZip, ARJ, BZip2,	2.1.9. Modulul de Sandbox poate trimite automat fișiere în Sandbox-ul din cloud-ul producătorului unde pot fi „detonate" pentru o analiza in profunzime. 2.1.10. Modulul de Sandbox include 2 variante de analiză: doar monitorizare sau blocare. În modul monitorizare utilizatorul poate accesa fișierul dorit, pe când în modul blocare, utilizatorului i se va bloca rularea fișierului pana când Sandbox-ul din cloud-ul producătorului va da verdictul. 2.1.11. Modulul de Sandbox include doua tipuri de acțiuni de remediere: implicita și de siguranță. Pentru acțiunea implicită se poate stabili: doar raportare, dezinfecție, ștergere și carantinare. Pentru acțiunea de siguranță se poate stabili: ștergere sau carantinare. 2.1.12. Modulul de Sandbox include si posibilitatea de trimitere manuala a fișierelor în Sandbox-ul din cloud-ul producătorului. Astfel, daca administratorul suspectează un fișier ca fiind malițios, îl poate trimite manual in Sandbox pentru a fi „detonat" și a afla verdictul. Va putea trimite mai multe fișiere de odată, cu posibilitate de a specifica daca vor fi „detonate" individual sau toate în același timp. 2.1.13. Modulul de Sandbox poate suporta „detonarea" următoarelor tipuri de fișiere: Batch, CHM, DLL, EML, Flash SWF, HTML, HTML/script, HTML (Unicode), JAR (archive), JS, LNK, MHTML (doc), MHTML (ppt), MHTML (xls), Microsoft Excel, Microsoft PowerPoint, Microsoft Word, MZ/PE files (executable), PDF, PEF (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,	

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
1	2	3	4	5	6	7
				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 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;	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 stații 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 și instalare remote:** 2.3.1. Înainte 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 în mai multe moduri: a) prin descărcarea directa a pachetului pe statia pe care se va face instalarea;	

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
1	2	3	4	5	6	7
				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 sa fie disponibile informatii despre fiecare statie: numele statiei, IP, sistem de operare, module instalate, politica aplicata, informatii despre actualizari etc. 2.3.5. Din consola sa fie posibila trimite o singura politica pentru configurarea integrala a clientului de pe statii/servere. 2.3.6. Consola sa includa 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. Sa fie 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. Sa fie posibilitatea creari unui singur pachet de instalare, utilizabil pentru statii (fizice si/sau virtuale), servere (fizice si/sau virtuale), exchange. 2.3.9. Sa fie posibilitatea de a crea pachetele de instalare de tip web installer sau kit full. 2.3.10. Administratorul sa poata crea grupuri sau chiar subgrupuri, unde va putea muta statiile/serverele din retea pentru cele care nu sunt integrate domeniu. 2.3.11. Sa permita selectarea clientului care va realiza descoperirea statiilor din retea, altele decat cele integrate in domeniu. 2.3.12. Sa permita raportarea statiilor care sunt protejate respectiv neprotejate de catre solutie	b) prin instalarea la distanta, direct din consola de management 2.3.3. Instalarea clienților la distanta in alte locații decât cele în care este instalata consola de management să fie făcută prin intermediul unui alt client antivirus existent în locațiile respective pentru a minimiza traficul in WAN. 2.3.4. În consola sunt disponibile informații despre fiecare stație: numele stației, IP, sistem de operare, module instalate, politica aplicata, informații despre actualizări etc. 2.3.5. Din consola este posibilă de a trimite o singură politica pentru configurarea integrală a clientului de pe stații/servere. 2.3.6. Consola 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. 2.3.7. Soluția propusă oferă posibilitatea creări unui singur pachet de instalare, utilizabil atât pentru sistemele de operare pe 32 de biti cat si pentru cele pe 64 de biti. 2.3.8. Soluția propusă oferă posibilitatea creări unui singur pachet de instalare, utilizabil pentru stații (fizice si/sau virtuale), servere (fizice si/sau virtuale), exchange. 2.3.9. Soluția propusă 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 va putea muta stațiile/serverele din rețea pentru cele care nu sunt integrate domeniu. 2.3.11. Soluția permite selectarea clientului care va realiza descoperirea stațiilor din rețea, altele decât cele integrate in domeniu. 2.3.12. Soluția permite raportarea stațiilor care sunt protejate respectiv neprotejate de către soluție	

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
1	2	3	4	5	6	7
				2.4. Caracteristici si functionalitati principale ale modulului antimalware: 2.4.1. Solutia sa permita 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 - ștergere - 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 sa 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. Posibilitatea definirea pana la 16 nivele de profunzime pentru scanarea in arhive. 2.4.4. Posibilitatea scanarea euristica comportamentala prin simularea unui calculator virtual in interiorul caruia sunt rulate aplicatii cu potential periculos	**2.4. Caracteristici și funcționalități principale ale modulului antimalware:** 2.4.1. Soluția permite administratorului să stabilească acțiunea luată de produsul Antimalware la detectarea unei amenințări noi. Astfel administratorul poate alege între următoarele acțiuni: a) Acțiune implicită pentru fișiere infectate: - interzice accesul - dezinfectează - ștergere - muta fișierele in carantina - nicio acțiune b) Acțiune alternativă pentru fișierele infectate: - interzice accesul - dezinfectează - ștergere - mută fișierele în carantină c) Acțiune implicită pentru fișierele suspecte: - interzice accesul - ștergere - muta fisierele in carantina - nicio actiune d) Acțiune alternativa pentru fișierele suspecte: - interzice accesul - ștergere - muta fișierele in carantina 2.4.2. Scanarea automata in timp real poate fi setata sa nu scaneze arhive sau fișiere mai mari de « x » MB, mărimea fișierelor putând fi definita de administratorul soluției, 2.4.3. Soluția propusă oferă posibilitatea de definire pana la 16 nivele de profunzime pentru scanarea în arhive. 2.4.4. Soluția propusă oferă posibilitatea de scanare euristica comportamentală prin simularea unui calculator virtual în interiorul căruia sunt rulate aplicații cu	

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
1	2	3	4	5	6	7
				protejand sistemul de virusii necunoscuti prin detectarea codurilor periculoase a caror semnatura nu a fost lansata inca. 2.4.5. Sa fie posibil 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. fie posibilitati de scanarea automata a emailurilor la nivelul statiei de lucru pentru POP3/SMTP. 2.4.7. Sa fie posibilitati de configurarea cailor ce urmeaza a fi scanate la cerere. 2.4.8. Clientii antimalware pentru workstation sa poata permita 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 trebui sa ofere protectie anti-spyware. 2.4.10. Sa fie posibilitatea de a configura scanarile programate sa se execute cu prioritate redusa 2.4.11. Produsul antimalware sa poata 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 sa poata 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	potențial periculos protejând sistemul de virușii necunoscuți prin detectarea codurilor periculoase a căror semnătură nu a fost lansata încă. 2.4.5. Prin intermediul soluției propuse este posibil scanarea oricărui suport de stocare a informației (CD-uri, harduri externe, unități partajate etc). De asemenea, poate anula scanarea în cazul în care sunt detectate unități care au informații stocate mai mult de « x » MB. 2.4.6. Soluția propusă oferă posibilitatea de scanarea automată a emailurilor la nivelul stației de lucru pentru POP3/SMTP. 2.4.7. Soluția propusă oferă posibilități de configurarea cailor ce urmează 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 și la cerere a anumitor directoare, discuri, fișiere, extensii sau procese. 2.4.9. Cu ajutorul unei baze de date complete cu semnături de spyware si a euristicii de detecție a acestui tip de programe, produsul oferă protecție anti-spyware. 2.4.10. Produsul oferă posibilitatea de a configura scanările programate sa se execute cu prioritate redusa 2.4.11. Produsul antimalware poate fi configurat sa folosească scanarea în cloud, și parțial scanarea locala. Pentru stațiile ce nu au suficiente resurse hardware, scanarea sa se poate face cu o mașină de scanare instalata în rețea. 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	

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
1	2	3	4	5	6	7
				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 trebuie sa aiba 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 trebuie sa poata scana paginile HTTP. 2.4.15. Pentru o mai buna gestionare a antimalware instalat pe statii, produsul sa includa optiunea de setare a unei parole pentru protectia la dezinstalare. 2.4.16. Pentru siguranta utilizatorului, clientul sa includa un modul de antiphishing. 2.4.17. Solutia sa ofera protectie in timp real pe masinile cu sistem de operare Linux in conformitate cu versiunea de kernel instalata.	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 protecție sporita, soluția antimalware are 3 tipuri de detecție: bazata pe semnaturi, bazata de comportamentul fisierelor si bazata pe monitorizarea proceselor. 2.4.14. Pentru o protecție sporita, soluția antimalware poate scana paginile HTTP. 2.4.15. Pentru o mai buna gestionare a antimalware instalat pe stații, produsul include opțiunea de setare a unei parole pentru protecția la dezinstalare. 2.4.16. Pentru siguranța utilizatorului, clientul include un modul de antiphishing. 2.4.17. Soluția oferă protecție in timp real pe mașinile cu sistem de operare Linux in conformitate cu versiunea de kernel instalata.	

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
1	*2*	*3*	*4*	*5*	*6*	*7*
				2.4.18. Solutia sa poata 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 sa ofere 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 sa ofere 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 sa ofere 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. Sa fie posibilitatea de a opri atacurile avansate de tip „zero-day" efectuate prin intermediul unor exploit-uri evazive. 2.5.2. Sa depisteze in timp real a celor mai recente exploit-uri ce pot vulnerabiliza un sistem de operare. 2.5.3. Sa fiu protejate 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.	2.4.18. Soluția poate detecta atacuri de tip „file-less" incluzând pe cele ce folosesc utilitare aferente sistemelor de operare de tip interpretor de script (powershell). Soluția nu blocheze în mod uzual scripturi pentru a proteja împotriva acestor tipuri de atacuri. 2.4.19. Soluția oferă un modul adițional 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 și alte categorii de malware sofisticat înainte de faza de execuție. 2.4.20. Soluția oferă posibilitatea de restaurare a fișierelor modificate de un proces suspicios/necunoscut cu comportament de ransomware, odată ce soluția determină ca procesul este maliții os. 2.4.21. Soluția oferă protecție împotriva atacurilor ransomware inițiate la distanta, de pe alte stații de lucru (de exemplu: încercarea de atac ransomware pe un share de pe o stație 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 este capabilă de a depista în timp real a celor mai recente exploit-uri ce pot vulnerabiliza un sistem de operare. 2.5.3. Soluția protejează aplicațiile utilizate frecvent si a celor de tip „sistem" cum ar fi browserele, aplicațiile de tip Office sau reader, procesele critice aferente sistemelor de operare.	

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
1	*2*	*3*	*4*	*5*	*6*	*7*
				2.6. Firewall: 2.6.1. Sa fie posibilitatea de a configura reguli de firewall pentru aplicatii sau conectivitate. 2.6.2. Modulul sa poata fi instalat/dezinstalat in functie de preferinta administratorului. 2.6.3. Sa fie posibilitatea de a defini retele de incredere pentru masini destinate. 2.6.4. Sa fie abilitatea de a detecta scanarea de porturi. 2.6.5. Sa fie posibilitatea de a seta diferite profiluri de rețea ((Home/Office, Trusted, Public, Untrusted sau Let the Windows decide) 2.6.6. Sa fie abilitatea de a crea reguli personalizate bazate pe aplicație și/sau conexiune **2.7. Carantina:** 2.7.1. Produsul antimalware sa permita trimiterea automata a fisierelor din carantina catre laboratoarele antimalware ale producatorului. 2.7.2. Trimiterea continutului carantinei sa fie posibil de expediat in mod automat, la un interval definit de administrator. 2.7.3. Produsul antimalware sa permita stergerea automata a fisierelor carantinate mai vechi de o anumita perioada, pentru a nu incarca inutil spatiul de stocare. 2.7.4. Sa fie posibilitatea de a restaura un fisier din carantina in locatia lui originala. 2.7.5. Modulul de carantina sa permita rescanarea obiectelor dupa fiecare actualizare de semnaturi. **2.8. Protectia datelor:** 2.8.1. Produsul permite blocarea datelor confidentiale (pin-ul cardului, cont	**2.6. Firewall:** 2.6.1. Soluția oferă posibilitatea de a configura reguli de firewall pentru aplicații sau conectivitate. 2.6.2. Modulul poate fi instalat/dezinstalat in funcție de preferință administratorului. 2.6.3. Soluția oferă posibilitatea de a defini rețele de încredere pentru mașini 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 fișierelor din carantina către laboratoarele antimalware ale producătorului. 2.7.2. Trimiterea conținutului carantinei este posibil de expediat in mod automat, la un interval definit de administrator. 2.7.3. Produsul antimalware permite ștergerea automata a fișierelor carantinate mai vechi de o anumita perioada, pentru a nu încărca inutil spațiul de stocare. 2.7.4. Produsul are posibilitatea de a restaura un fișier din carantina in locația lui originala. 2.7.5. Modulul de carantina permite rescanarea obiectelor după fiecare actualizare de semnături. **2.8. Protecția datelor:** 2.8.1. Produsul permite blocarea datelor confidențiale (pin-ul cardului, cont	

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
1	*2*	*3*	*4*	*5*	*6*	*7*
				bancar etc) transmise prin HTTP sau SMTP prin crearea unor reguli specifice. **2.9. Controlul continutului:** 2.9.1. Consola sa detina 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 sa includa 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 sa includa 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.	bancar etc) transmise prin HTTP sau SMTP prin crearea unor reguli specifice. **2.9. Controlul conținutului:** 2.9.1. Consola deține integrat un modul dedicat controlului accesului la Internet cu următoarele particularități: a) Permite blocarea accesului la Internet pentru anumite mașini client sau grupuri de mașini. b) Permite blocarea accesului la Internet pe intervale orare. c) Permite blocarea paginilor de internet care conțin anumite cuvinte cheie. d) Permite controlul accesului numai la anumite pagini de internet specificate de administrator; e) Permite blocarea accesului la anumite aplicații definite de administrator; f) Permite restricționarea accesului pe anumite pagini de internet după anumite categorii prestabilite (ex: online dating, violenta, pornografie etc). **2.10. Controlul aplicațiilor:** 2.10.1. Pentru o mai buna inventariere si administrare, solutia include o secțiune în consola de administrare unde se vor regăsi toate aplicațiile descoperite in rețea, grupate după: nume, versiune, descoperit la, găsit pe. 2.10.2. Pentru o mai buna inventariere si administrare, soluția include o secțiune în consola de administrare unde sa se regăsească toate procesele negrupate descoperite în rețea, grupate după: nume, versiune, nume produs, versiune produs, editor/autor, descoperit la, găsit pe.	

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
1	*2*	*3*	*4*	*5*	*6*	*7*
				2.10.3. Pentru prevenirea infectarii statiilor si serverelor dar si pentru a permite aplicatiilor descoperite in retea sa se poata actualiza, solutia sa permita definirea unor programe de actualizare (Updater) care vor fi lasate sa actualizeze diferite aplicatii instalate pe statii sau servere. 2.10.4. 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 2.10.5. Acest modul sa poata 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 sa poata fi instalat/dezinstalat in functie de preferinta administratorului. 2.11.2. Modulul sa permita 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	2.10.3. Pentru prevenirea infectării stațiilor si serverelor dar si pentru a permite aplicațiilor descoperite în rețea se poate actualiza, soluția permite definirea unor programe de actualizare (Update) care vor fi lăsate sa actualizeze diferite aplicații instalate pe stații sau servere. 2.10.4. Soluția include opțiunea de a permite sau a bloca rularea anumitor aplicații sau procese definite de administrator (inclusiv sub procese) după: a. Cale fișier: local, CD-ROM, portabil sau rețea b. Hash c. Certificat 2.10.5. Acest modul poate funcționa în modul Whitelisting (prin care se blochează accesul la toate aplicațiile cu excepția celor menționate în lista alba) sau Blacklisting (prin care sa se blocheaze doar accesul la aplicațiile menționate in lista neagra). **2.11. Controlul dispozitivelor:** 2.11.1. Modulul poate fi instalat/dezinstalat in funcție de preferința administratorului. 2.11.2. Modulul permite controlul următoarelor 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	

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
1	2	3	4	5	6	7
				l. SCSI Raid m. Printers n. Network Adapters o. Wireless Network Adapters p. Internal and External Storage 2.11.3. Modulul sa permita configurarea de reguli prin care se vor defini permisiunile pentru dispozitivele conectate la masina client. 2.11.4. Modulul sa permita configurarea de excluderi pentru diferite tipuri de dispozitive pentru care s-au configurat reguli. 2.11.5. Modulul sa permita 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 sa permita 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 sa poata „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	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 mașină 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 poate limita accesul dispozitivelor externe la „read only" sau limita doar accesul la porturile USB ale endpoint-ului permițând orice alt tip de dispozitiv ce nu folosește acest tip de port/interfață. 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 funcție de preferința administratorului. 2.12.2. Modulul sa permite posibilitatea de a acorda utilizatorilor drepturi de Power User. Utilizatorii pot accesa si modifica setările clientului antimalware dintr-o consola disponibilă local pe mașina client.	

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
1	2	3	4	5	6	7
				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. Sa fie posibilitatea efectuarii actualizarii la nivel de statie in mod silentios (fara avertizare). 2.13.2. Deținerea sistem de actualizare cascadat folosind unul sau mai multe servere de actualizare (cascadate). Actualizarea pentru locatiile remote prin intermediul unui client antimalware care va avea si rol de server de actualizare. **3. <u>PROTECTIE SI SECURITATE PENTRU SERVERELE EMAIL MICROSOFT EXCHANGE</u>** **3.1. 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 3.1.1. Produsul sa ofere 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. 3.1.2. Produsul sa asigure scanarea atasamentelor si a continutului mesajelor in timp real, fara a afecta vizibil performanta serverului de mail.	2.12.3. Administratorul poate suprascrie din consola setările aplicate de utilizatorii Power User. **2.13. Actualizare:** 2.13.1. Soluția propusă oferă posibilitatea efectuării actualizării la nivel de stație în mod silențios (fără avertizare). 2.13.2. Deținerea sistem de actualizare cascadat folosind unul sau mai multe servere de actualizare (cascadate). Actualizarea pentru locatiile remote prin intermediul unui client antimalware care va avea si rol de server de actualizare. **3. <u>PROTECȚIE ȘI SECURITATE PENTRU SERVERELE EMAIL MICROSOFT EXCHANGE</u>** **3.1. 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 3.1.1. Produsul oferă protecție antimalware, antispam (inclusiv antiphishing), precum si filtrare de atașamente si conținut, prin integrarea cu serverul Microsoft Exchange. De asemenea, va permite scanarea antimalware la cerere a bazelor de date Exchange. 3.1.2. Produsul asigură scanarea atașamentelor si a conținutului mesajelor in timp real, fără a afecta vizibil performanta serverului de mail.	

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
1	*2*	*3*	*4*	*5*	*6*	*7*
				3.1.3. Actualizarea antimalware trebuie sa poata fi facuta automat la un interval de maxim 1 ora, precum si la cerere. 3.1.4. In afara de detectia pe baza de semnaturi, modulul de protectie antimalware va trebui sa includa si scanare euristica comportamentala, prin simularea unui calculator virtual in interiorul caruia sunt rulate si analizate aplicatii cu potential periculos, pentru a proteja sistemul de virusii necunoscuti prin detectarea codurilor periculoase a caror semnatura nu a fost lansata inca. 3.1.5. Produsul sa ofere optiuni multiple de actiune la identificarea unui atasament virusat (dezinfectare, stergere, mutare in carantina). 3.1.6. 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. 3.1.7. Produsul sa ofere protectie antispam, cu o baza de semnaturi actualizabila prin internet. 3.1.8. Modulul antispam trebui sa includa un filtru URL cu o baza de adrese URL cunoscute a fi folosite in mesaje spam, precum si un filtru de caractere pentru detectarea automata a mesajelor scrise cu caractere chirilice sau asiatice. 3.1.9. Produsul trebui sa ofere filtru RBL care sa identifice spam-ul prin sincronizarea cu anumite baze de date online care contin liste de servere de mail cunoscute ca fiind la originea acestui tip de mesaje. 3.1.10. Produsul trebui sa ofere un serviciu/filtru online pentru imbunatatirea protectiei impotriva valurilor de spam nou aparute.	3.1.3. Actualizarea antimalware poate fi făcută automat la un interval de maxim 1 ora, precum si la cerere. 3.1.4. In afara de detecția pe baza de semnături, modulul de protecție antimalware include și scanare euristica comportamentala, prin simularea unui calculator virtual in interiorul căruia sunt rulate si analizate aplicații cu potențial periculos, pentru a proteja sistemul de virușii necunoscuți prin detectarea codurilor periculoase a căror semnătură nu a fost lansata încă. 3.1.5. Produsul oferă opțiuni multiple de acțiune la identificarea unui atașament virusat (dezinfectare, ștergere, mutare în carantina). 3.1.6. Cu ajutorul unei baze de date complete cu semnături de spyware si a euristicii de detectie a acestui tip de programe, produsul oferă protecție anti-spyware pentru a preveni furtul de date confidențiale. 3.1.7. Produsul oferă protecție antispam, cu o baza de semnături actualizabila prin internet. 3.1.8. Modulul anti spam include un filtru URL cu o baza de adrese URL cunoscute a fi folosite in mesaje spam, precum și un filtru de caractere pentru detectarea automată a mesajelor scrise cu caractere chirilice sau asiatice. 3.1.9. Produsul oferă filtru RBL care identifică 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. 3.1.10. Produsul oferă un serviciu/filtru online pentru îmbunătățirea protecției împotriva valurilor de spam nou apărute.	

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
1	*2*	*3*	*4*	*5*	*6*	*7*
				3.1.11. Produsul sa ofere posibilitatea de a defini politici de filtrare antimalware, antispam, a continutului sau atasamentelor pentru diferite grupuri sau utilizatori. 3.1.12. Actualizarea produsului sa fie 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. 3.1.13. Produsul trebui sa ofere statistici atat referitoare la scanarea antivirus cat si la scanarea antispam. Produsul sa se integreze 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. **4. <u>ALTE CERINȚE OBLIGATORII:</u>** - Pentru soluția ofertată se solicită suport local și de la producător pentru 24 luni. - Producătorul trebuie să ofere suport 24/7, prin e-mail sau conectare de la distanță, inclusiv suport local. - Lucrările de instalare, configurare, punerea în funcţiune a soluției trebuie să fie executate de ofertant, iar costul acestora trebuie să fie incluse în oferta comerciala. - Se va oferi manual de instalare si administrare a produsului ofertat in limba romana si engleza. - Prezentarea a minim 2 certificate tehnice a persoanelor certificate pe produsul ofertat. - Ofertantul va prezenta Autorizarea de la producător care atestă dreptul de a livra bunuri/lucrări/servicii pe produsul ofertat.	3.1.11. Produsul oferă posibilitatea de a defini politici de filtrare antimalware, antispam, a conținutului sau atașamentelor pentru diferite grupuri sau utilizatori. 3.1.12. Actualizarea produsului poate fi configurabilă și să poate realiza de pe internet, direct sau printr-un proxy, sau din cadrul retelei de pe un server de actualizare propriu. 3.1.13. Produsul oferă statistici atât referitoare la scanarea antivirus cat si la scanarea anti spam. Produsul se integrează în cadrul consolei de management unitar al solutiei antivirus. Pentru ușurința accesului la setările produsului din diferite medii de operare, produsul are consola de administrare web. **4. <u>ALTE CERINȚE OBLIGATORII:</u>** - Soluția ofertată vine cu suport local și de la producător pentru 24 luni. - Producătorul oferă suport 24/7, prin e-mail sau conectare de la distanță, inclusiv suport local. - Lucrările de instalare, configurare, punerea în funcțiune a soluției este executată de ofertant, iar costul acestora este inclus în oferta comerciala. - Se va oferi manual de instalare si administrare a produsului ofertat in limba romana si engleza. - Prezentarea a minim 2 certificate tehnice a persoanelor certificate pe produsul ofertat (atașate la prezenta propunere tehnică). - Ofertantul va prezenta Autorizarea de la producător care atestă dreptul de a livra bunuri/lucrări/servicii pe produsul ofertat (atașate la prezenta propunere tehnică)..	

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
1	*2*	*3*	*4*	*5*	*6*	*7*
				- Ofertantul va pune la dispoziție cel puțin o persoana certificata in calitate de auditor intern pentru sistemul de management al securității informațiilor conform ISO/IEC 27001:2018 in cazul apariție problemelor de securitate; - Ofertantul va prezenta minim 3 referințe de implementare pe piața locală in ultimii 2 ani a soluției ofertate de aceeasi complexitate si volum de statii/echipamente. Termen de livrare: 10 zile lucrătoare de la data semnării contractului, care include și timpul lucrărilor de instalare, configurare și punerea în funcțiune a soluției.	- În calitate de Ofertant vă punem la dispoziție cel puțin o persoană certificată în calitate de auditor intern pentru sistemul de management al securității informațiilor conform ISO/IEC 27001:2018 în cazul apariție problemelor de securitate; - În calitate de Ofertant vă prezentăm (atașate la prezenta propunere tehnică) minim 3 referințe de implementare pe piața locală în ultimii 2 ani a soluției ofertate de aceeași complexitate si volum de stații/echipamente. Termen de livrare: 10 zile lucrătoare de la data semnării contractului, care include și timpul lucrărilor de instalare, configurare și punerea în funcțiune a soluției.	
TOTAL						

Semnat electronic:

Digitally signed by Celonenco Vitalie
Date: 2023.11.28 07:13:34 EET
Reason: MoldSign Signature
Location: Moldova

Numele, Prenumele: **CELONENCO Vitalie**
Ofertantul: **„RTS ONE" S.R.L.**

În calitate de: **Administrator**
Adresa: **mun.Chișinău, str.Mitropolit Gavriil Bănulescu-Bodoni, 59/B, of.804**