Anexa nr.22
la Documentația standard pentru procedura de achiziție, cu nr. de identificare în SIA RSAP Mtender: ocds-b3wdp1-MD-1768565493760

SPECIFICAȚII TEHNICE

Numărul procedurii de achiziție: MTender ID: **ocds-b3wdp1-MD-1768565493760**
Obiectul achiziției: **Licența Antivirus pentru anul 2026**

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 referinţă
1	*2*	*3*	*4*	*5*	*6*	*7*
Licența Antivirus	Bitdefender GravityZone Business Security	România	Bitdefender	**CARACTERISTICI GENERALE ALE PRODUSULUI** Produsul („solutia") reprezinta o platforma integrata pentru managementul securitatii, gandita ca o solutie modulara. Produsul contine urmatoarele module: *A. Consola de management care asigura functionalitati de administrare.* *B. Protectie antimalware pentru statii fizice, laptop-uri si servere.* **A. CONSOLA DE MANAGEMENT** 1. Cerințe generale: 1.1. Interfața consolei de management va fi in limba romana. 1.2. Interfața clientului de securitate, care se instaleaza pe statii si servere, va fi in limba romana. 1.3. Manualul de instalare a produsului va fi in limba romana.	**Tip:** Subscriere anuală pentru soluția de protecție și securitate pentru 370 entități pentru perioada de 12 luni. **Cantitate:** Se oferă soluția Bitdefender GravityZone, cu urmatorul model de licentiere: *- GravityZone Business Security 370 entități (PC/laptop/VDI/Server).* 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"). **CARACTERISTICI GENERALE ALE PRODUSULUI** Soluția reprezintă o platformă integrată pentru managementul securității, gândita ca o soluție modulară. Produsul va conține următoarele module, toate cu posibilitatea de a fi gestionate și administrate dintr-o singură consolă de management: *A. Consola de management care asigura funcționalități de administrare.* *B. Protecție antimalware pentru stații fizice, laptop-uri și servere.* **A. CONSOLA DE MANAGEMENT** 1. Cerințe generale: 1.1. Interfața consolei de management este în limba română. 1.2. Interfața clientului de securitate, care se instalează pe stații și servere, este în limba română. 1.3. Manualul de instalare a produsului este în limba română.	

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
				1.4. Manualul de administrare a produsului va fi in limba romana. 1.5. Soluția va permite activarea/dezactivarea actualizarilor de produs/semnaturi. 1.6. Actualizări automate a consolei de management facute de catre producatorul solutiei, fara a fi necesara intervenția utilizatorului. 1.7. Notificările – prezente in interfața, notificarile necitite sunt evidentiate, trimise catre una sau mai multe adrese de email, alerteaza administratorul in cazul unor probleme majore: licentiere, detectie virusi, actualizari de produs disponibile). 1.8. Consola de management este accesibila de oriunde in lume (este bazata pe un serviciu cloud de tip Software-as-a-Service), fara a fi nevoie de setari suplimentare din partea utilizatorului. 1.9. Consola de management este accesibila atat de pe statii de lucru cat si de pe dispozitive mobile (smartphone, tableta). **2. Panou de monitorizare si raportare (Dashboard):** 2.1. Rapoartele din panoul de monitorizare vor putea fi configurate specificand numele raportului, tipul raportului, tinta raportului, optiuni specifice pentru orice tip de raport (de exemplu pentru raportul de actualizare - care este intervalul dupa care o stație este considerata neactualizata). 2.2. Panoul central conține rapoarte pentru toate modulele suportate. 2.3. Rapoartele din panoul central de comanda permit: adaugarea altor rapoarte, ștergerea lor si rearanjarea. **3. Inventarierea rețelei – managementul securitatii:** 3.1. Solutia se va integra cu domeniul Active Directory si va putea importa inventarul. 3.2. Se permite descoperirea statiilor statii fizice neintegrate in Active Directory (Workgroup) cu ajutorul Network discovery. 3.3. Solutia va oferi 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. 3.4. Solutia va permite crearea unui pachet unic pentru toate sistemele de operare, de statii sau servere. Astfel, administratorul va putea descarca	1.4. Manualul de administrare a produsului este în limba română. 1.5. Soluția permite activarea/ dezactivarea actualizărilor de produs/semnături. 1.6. Actualizări automate a consolei de management făcute de către producătorul soluției, fără a fi necesară intervenția utilizatorului. 1.7. 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 viruși, actualizări de produs disponibile). 1.8. Consola de management este accesibilă de oriunde în lume (este bazată pe un serviciu cloud de tip Software-as-a-Service), fără a fi nevoie de setări suplimentare din partea utilizatorului. 1.9. Consola de management este accesibilă atât de pe stații de lucru cât și de pe dispozitive mobile (smartphone, tableta). **2. Panou de monitorizare si raportare (Dashboard):** 2.1. Rapoartele din panoul de monitorizare se pot configura 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). 2.2. Panoul central conține rapoarte pentru toate modulele suportate. 2.3. Rapoartele din panoul central de comanda permit: adăugarea altor rapoarte, ștergerea lor și rearanjarea. **3. Inventarierea rețelei – managementul securității:** 3.1. Soluția se integrează cu domeniul Active Directory si poate importa inventarul. 3.2. Soluția permite descoperirea stațiilor fizice neintegrate în Active Directory (Workgroup) cu ajutorul Network Discovery. 3.3. Soluția oferă opțiuni de căutare, sortare și filtrare după numele sistemului, sistem de operare, adresa IP, politica aplicata, ultima dată când s-a conectat (online si/sau offline) și FQDN. 3.4. Soluția permite crearea unui pachet unic pentru toate sistemele de operare, de stații sau servere. Astfel, administratorul poate descarcă 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
				pachetele pentru protectia statiilor si serverelor pe care ruleaza sistemul de operare Windows, Linux, Mac. 3.5. Solutia va permite instalarea la distanta sau manual a clientilor antimalware pe masini fizice/virtuale. 3.6. Solutia va permite selectarea modulelor componente atunci cand se creaza pachetul clientului care se instalează pe mașinile fizice/virtuale. 3.7. Solutia va permite lansarea de task-uri de scanare, actualizare, instalare, dezinstalarea la distanta pentru clientul antimalware. 3.8. Solutia va oferi posibilitatea de repornire a masinilor fizice de la distanta. 3.9. Solutia va oferi informatii detaliate despre fiecare task si se fiseaza daca task-ul s-a finalizat sau nu cu succes. 3.10. Solutia va permite configurarea centralizata a clientilor antimalware prin intermediul politicilor 3.11. Se vor oferi in consola de management informatii detaliate ale obiectelor din consola: Nume, IP, Sistem de operare, Grup, Politica atribuita, Ultimele actualizare, Versiunea produsului, Versiunea de semnaturi. **4. Politici:** 4.1. Solutia va permite configurarea setarilor antimalware prin intermediul politicilor din consola de management. 4.2. Politica va contine optiuni specifice de activare/dezactivare si configurarea functionalitatilor precum scanarea antimalware la cerere, firewall, controlul accesului la Internet, controlul aplicatiilor, scanarea traficului web,controlul dispozitivelor, power user. 4.3. Solutia permite aplicarea politicilor pe masini client, grupuri de masini, domeniu, unitati organizationale. 4.4. Politica sa poate fi schimbata automat in functie de: a) IP sau clasa de IP al statiei b) Gateway-ul alocat c) DNS serverul alocat d) WINS serverul alocat e) Sufix DNS pentru conexiunea dhcp	pentru protecția stațiilor și serverelor pe care rulează sistemul de operare Windows, Linux, Mac. 3.5. Soluția permite instalarea la distanță sau manual a clienților antimalware pe mașini fizice/virtuale. 3.6. Soluția permite selectarea modulelor componente atunci când se creează pachetul clientului care se instalează pe mașinile fizice/virtuale. 3.7. Soluția permite lansarea de task-uri de scanare, actualizare, instalare, dezinstalarea la distanță pentru clientul antimalware. 3.8. Soluția oferă posibilitatea de repornire a mașinilor fizice de la distanță. 3.9. Soluția oferă informații detaliate despre fiecare task și se fișează dacă task-ul s-a finalizat sau nu cu succes. 3.10. Soluția permite configurarea centralizată a clienților antimalware prin intermediul politicilor 3.11. 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. **4. Politici:** 4.1. Soluția permite configurarea setărilor antimalware prin intermediul politicilor din consola de management. 4.2. 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. 4.3. Soluția permite aplicarea politicilor pe mașini client, grupuri de mașini, domeniu, unități organizaționale. 4.4. 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	

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
				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) **5. Rapoarte:** 5.1. Solutia va contine rapoarte care prezinta statusul masinilor clientil din punct de vedere al actualizarilor, fisierelor malware detectate, aplicatiile blocate, site-urilor web blocate. 5.2. Rapoartele programate pot fi trimise catre un numar nelimitat de adrese de email (nu este nevoie sa aiba un cont in consola de management). 5.3. Solutia va permite vizualizarea rapoartelor curente programate de administrator. 5.4. Solutia va permite exportarea rapoartelor in format .pdf si detaliile ca format .csv. **6. Carantina:** 6.1. Solutia va permite restaurarea fisierelor carantinate in locatia originala sau intr-o cale configurabila cu optiunea de excludere automata a fisierului restaurat. 6.2. Carantina va fi locala, pe fiecare statia administrata si va fi administrata, fie local, fie din consola de management. **7. Utilizatori:** 7.1. Administrarea se va putea face pe baza de roluri. 7.2. 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. 7.3. Utilizatorii pot fi importati din Microsoft Active Directory sau creati in consola de management. 7.4. Se va permite configurarea detaliata a drepturilor administrative, permitand selectarea serviciilor si obiectelor pentru care un utilizator poate face modificari. 7.5. Se va permite deconectarea automata a oricarui tip de utilizator dupa un anumit timp pentru o protectie sporita a datelor afisate in consola de administrare. Acest interval se poate personaliza de administratorul solutiei.	f) Clientul este/nu este in aceeași rețea cu infrastructura de management (stația de lucru poate soluționa implicit numele gazdei) g) Tipul rețelei (lan, wireless) **5. Rapoarte:** 5.1. Soluția conține rapoarte care prezintă statusul mașinilor clienți din punct de vedere al actualizărilor, fișierelor malware detectate, aplicațiile blocate, site-urilor web blocate. 5.2. Rapoartele programate pot fi trimise către un număr nelimitat de adrese de email (nu este nevoie sa aibă un cont in consola de management). 5.3. Soluția permite vizualizarea rapoartelor curente programate de administrator. 5.4. Soluția permite exportarea rapoartelor in format .pdf si detaliile ca format .csv. **6. Carantina:** 6.1. Soluția permite restaurarea fișierelor carantinate în locația originală sau într-o cale configurabilă cu opțiunea de excludere automată a fișierului restaurat. 6.2. Carantina va fi locală, pe fiecare stația administrata și va fi administrată, fie local, fie din consola de management. **7. Utilizatori:** 7.1. Administrarea se poate face pe baza de roluri. 7.2. 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 si generează rapoarte. 7.3. Utilizatorii pot fi importați din Microsoft Active Directory sau creați în consola de management. 7.4. Soluția permite configurarea detaliată a drepturilor administrative, permițând selectarea serviciilor și obiectelor pentru care un utilizator poate face modificări. 7.5. Soluția permite deconectarea automată a oricărui tip de utilizator după un anumit timp pentru o protecție sporita a datelor afișate in consola de administrare. Acest interval se poate personaliza de administratorul soluției.	

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*
				8. Log-uri: 8.1. Inregistrarea actiunilor utilizatorilor. 8.2. Se vor oferi informatii detaliate pentru fiecare actiune a unui utilizator. 8.3. Se va permite filtrarea actiunilor utilizator dupa numele utilizatorului, actiune. **9. Actualizare:** 9.1. Se permite definirea de locatii de actualizare multiple. 9.2. Se permite activarea/dezactivarea actualizarilor de produs si semnaturi. 9.3. Orice client antivirus sa poata fi configurat sa livreze update-urile catre alt client antivirus 9.4. 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, solutia include 2 tipuri de actualizari de produs: a) Ciclu rapid, gandit pentru un mediu de test in cadrul retelei b) Ciclu lent, gandit pentru restul retelei (productie, servere critice etc) 9.5. Solutia permite stabilirea zonelor de test si critice din cadrul retelei prin intermediul politicilor din consola de management. **B. PROTECȚIE STAȚII ȘI SERVERE FIZICE** 1. Caracteristici generale minimale si eliminatorii: 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). 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. 1.3. Vaccinul anti-ransomware primeste actualizari de la producator, odata cu actualizarea semnaturilor produsului Antimalware.	**8. Log-uri:** 8.1. Înregistrarea acțiunilor utilizatorilor. 8.2. Se vor oferi informații detaliate pentru fiecare acțiune a unui utilizator. 8.3. Soluția permite filtrarea acțiunilor utilizator după numele utilizatorului, acțiune. **9. Actualizare:** 9.1. Soluția permite definirea de locații de actualizare multiple. 9.2. Soluția permite activarea/dezactivarea actualizărilor de produs si semnături. 9.3. Orice client antivirus poate fi configurat să livreze update-urile către alt client antivirus 9.4. Soluția permite testarea noilor versiuni de pachete de instalare ale clientului antimalware, înainte de a fi instalate pe toate stațiile si serverele din rețea, evitând posibile probleme ce pot afecta serverele sau stațiile critice. Astfel, soluția include 2 tipuri de actualizări de produs: c) Ciclu rapid, gândit pentru un mediu de test in cadrul rețelei d) Ciclu lent, gândit pentru restul rețelei (producție, servere critice etc) 9.5. Soluția permite stabilirea zonelor de test si critice din cadrul rețelei prin intermediul politicilor din consola de management. **B. PROTECȚIE STAȚII ȘI SERVERE FIZICE** 1. Caracteristici generale minimale si eliminatorii: 1.1. Pentru reducerea la minim a consumului de resurse, soluția antimalware trebuie permite instalarea personalizata a modulelor deținute (de exemplu, sa permită instalarea soluției antimalware fără modulul de control al accesului web, modul de control al dispozitivelor sau modulul firewall). 1.2. Pentru o mai buna protecție a stațiilor si serverelor, soluția include un vaccin anti-ransomware. Acest vaccin asigura protecția împotriva tuturor amenințărilor cunoscute de tip ransomware, prin imunizarea stațiilor si serverelor, chiar daca sunt infectate si prin blocarea procesului de criptare. 1.3. Vaccinul anti-ransomware primește actualizări de la producător, odată cu actualizarea semnăturilor produsului Antimalware.	

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
				1.4. 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). 1.5. Pentru o mai buna protectie a a statiilor si serverelor, solutia include un modul integrat de tip ERA (Endpoint Risk Analytics – Analiza de risc a endpoint-ului) capabil sa identifice si remedieze in mod automatizat sau manual un numar mare de riscuri existente la nivel de retea sau sistem de operare ce pot afecta functionalitatea si nivelul de securizare al endpoint-ului **2. Cerinte de sistem:** - Sisteme de operare pentru statii de lucru: Windows11, Windows 10, Windows 8/8.1, Windows 7, Mac OS Monterey 12.x, macOS BIG SUR 11.x, macOS Catalina 10.15, Mac OS X Mojave (10.14), Mac OS High Sierra (10.13), Mac OS Sierra (10.12), - Sisteme de operare embedded: Windows 10 IOT Enterprise, Windows Embedded 8.1 Industry, Windows Embedded 8 Standard, Windows Embedded Standard 7,Windows Embedded POS Ready 7 Windows Embedded POSReady 7, Windows Embedded Enterprise 7 - Sisteme de operare pentru servere: Windows Server 2022, Windows Server 2019, Windows Server 2019 CORE, Windows Server 2016 , Windows Server 2016 (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 7.x, 8.x,9.x, CentOS 7.x, 8.x, Ubuntu 16.04 sau mai recent, SUSE Linux Enterprise Server 12SP4,5, SUSE LINUX Exnterprise15 SP2,SP3, OpenSUSE LEAP 15-2-15.3., Fedora 31 sau mai recent, AWS Bottlerocket 2020.03, Amazon Linux v2, Google COS Milestones 77,81,85, Azure Mariner 2, AlmaLinux 8,9.x, Rocky Linux 8.x, Cloud Linux 7,8.x, Pardus 21, Linux Mint 20.3, Miracle 8.4. **3. Administrare si instalare remote:** 3.1. Inainte de instalare, administratorul va putea particulariza pachetele de instalare cu modulele	1.4. Pentru o mai buna protecție a stațiilor și serverelor, soluția include protecție împotriva atacurilor zero-day de tip exploit avansate (atacuri direcționate) bazata pe tehnologii de învățare automata (machine learning). 1.5. Pentru o mai buna protecție a a stațiilor si serverelor, soluția include un modul integrat de tip ERA (Endpoint Risk Analytics – Analiza de risc a endpoint-ului) capabil sa identifice si remedieze in mod automatizat sau manual un număr mare de riscuri existente la nivel de rețea sau sistem de operare ce pot afecta funcționalitatea si nivelul de securizare al endpoint-ului **2. Cerințe de sistem:** - Sisteme de operare pentru stații de lucru: Windows11, Windows 10, Windows 8/8.1, Windows 7, Mac OS Monterey 12.x, macOS BIG SUR 11.x, macOS Catalina 10.15, Mac OS X Mojave (10.14), Mac OS High Sierra (10.13), Mac OS Sierra (10.12), - Sisteme de operare embedded: Windows 10 IOT Enterprise, Windows Embedded 8.1 Industry, Windows Embedded 8 Standard, Windows Embedded Standard 7,Windows Embedded POS Ready 7 Windows Embedded POSReady 7, Windows Embedded Enterprise 7 - Sisteme de operare pentru servere: Windows Server 2022, Windows Server 2019, Windows Server 2019 CORE, Windows Server 2016 , Windows Server 2016 (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 7.x, 8.x,9.x, CentOS 7.x, 8.x, Ubuntu 16.04 sau mai recent, SUSE Linux Enterprise Server 12SP4,5, SUSE LINUX Exnterprise15 SP2,SP3, OpenSUSE LEAP 15-2-15.3., Fedora 31 sau mai recent, AWS Bottlerocket 2020.03, Amazon Linux v2, Google COS Milestones 77,81,85, Azure Mariner 2, AlmaLinux 8,9.x, Rocky Linux 8.x, Cloud Linux 7,8.x, Pardus 21, Linux Mint 20.3, Miracle 8.4. **3. Administrare și instalare remote:** 3.1. Înainte de instalare, administratorul poate particulariza pachetele de instalare cu 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
				dorite: firewall, content control, device control, power user. 3.2. Instalarea se va putea face in mai multe moduri: a) prin descarcarea directa a pachetului pe statia pe care se va face instalarea; b) prin instalarea la distanta, direct din consola de management c) trimiterea pe email (oricate adrese) a pachetului de instalare pentru Windows, Linux, Mac. 3.3. Instalarea clientilor la distanta in alte locatii decat cele in care este instalata consola de management se va face prin intermediul unui client existent in locatiile respective de tip relay pentru a minimiza traficul in WAN. 3.4. In consola vor fi disponibile informatii despre fiecare statie: numele statiei, IP, sistem de operare, module instalate, politica aplicata, informatii despre actualizari etc. 3.5. Din consola se va putea trimite o singura politica pentru configurarea integrala a clientului de pe statii/servere. 3.6. Consola va include o sectiune, „Audit", unde se vor mentiona toate actiunile intreprinse fie de administratori fie de reporteri, cu informatii detaliate: logare, editare, creare, delogare, mutare etc. 3.7. Posibilitatea creari unui singur pachet de instalare, utilizabil atat pentru sistemele de operare pe 32 de biti cat si pentru cele pe 64 de biti. 3.8. Posibilitatea creari unui singur pachet de instalare, utilizabil pentru statii (fizice si/sau virtuale), servere (fizice si/sau virtuale). 3.9. Posibilitatea de a crea pachetele de instalare de tip web installer sau kit full. 3.10. Administratorul va putea crea grupuri sau chiar subgrupuri, unde va putea muta statiile/serverele din retea pentru cele care nu sunt integrate domeniu. 3.11. Permite selectarea clientului care va realiza descoperirea statiilor din retea, altele decat cele integrate in domeniu. **4. Caracteristici si functionalitati principale ale modulului antimalware:**	dorite: firewall, content control, device control, power user. 3.2. Instalarea se poate efectua în mai multe moduri: d) prin descărcarea directa a pachetului pe stația pe care se va face instalarea; e) prin instalarea la distanță, direct din consola de management f) trimiterea pe email (oricâte adrese) a pachetului de instalare pentru Windows, Linux, Mac. 3.3. Instalarea clienților la distanță în alte locații decât cele in care este instalata consola de management se va face prin intermediul unui client existent in locațiile respective de tip relay pentru a minimiza traficul in WAN. 3.4. În consola vor fi disponibile informații despre fiecare stație: numele stației, IP, sistem de operare, module instalate, politica aplicata, informații despre actualizări etc. 3.5. Din consola se poate trimite o singură politică pentru configurarea integrală a clientului de pe stații/servere. 3.6. Consola include o secțiune, „Audit", unde se menționează toate acțiunile întreprinse fie de administratori fie de reporteri, cu informații detaliate: logare, editare, creare, delogare, mutare etc. 3.7. Soluția oferă posibilitatea creări unui singur pachet de instalare, utilizabil atât pentru sistemele de operare pe 32 de biți cat si pentru cele pe 64 de biți. 3.8. Soluția oferă posibilitatea creări unui singur pachet de instalare, utilizabil pentru stații (fizice si/sau virtuale), servere (fizice si/sau virtuale). 3.9. Soluția oferă posibilitatea de a crea pachetele de instalare de tip web installer sau kit full. 3.10. Administratorul poate crea grupuri sau chiar subgrupuri, unde va putea muta stațiile/serverele din rețea pentru cele care nu sunt integrate domeniu. 3.11. Soluția permite selectarea clientului care va realiza descoperirea stațiilor din rețea, altele decât cele integrate in domeniu. **4. Caracteristici si funcționalități principale ale modulului antimalware:**	

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
				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: 4.1.1. Actiune imiplicita pentru fisiere infectate: i. interzice accesul ii. dezinfecteaza iii. stergere iv. muta fisierele in carantina v. nicio actiune 4.1.2. Actiune alternativa pentru fisierele infectate: i. interzice accesul ii. dezinfecteaza iii. stergere iv. muta fisierele in carantina 4.1.3. Actiune imiplicita pentru fisierele suspecte: i. interzice accesul ii. stergere iii. muta fisierele in carantina iv. nicio actiune 4.1.4. Actiune alternativa pentru fisierele suspecte: i. interzice accesul ii. stergere iii. muta fisierele in carantina 4.2. Scanarea automata in timp real va putea fi setata sa nu scaneze arhive sau fisiere mai mari de « x » MB, marimea fisierelor putand fi definita de administratorul solutiei, 4.3. Definirea pana la 16 nivele de profunzime pentru scanarea in arhive. 4.4. Scanarea euristica comportamentala prin simularea unui calculator virtual in interiorul caruia sunt rulate aplicatii cu potential periculos protejand sistemul de virusii necunoscuti prin detectarea codurilor periculoase a caror semnatura nu a fost lansata inca. 4.5. Scanarea oricarui suport de stocare a informatiei (CD-uri, harduri externe, unitati partajate etc). De asemenea, se va putea anula scanarea in cazul in care sunt detectate unitati care au informatii stocate mai mult de « x » MB.	4.1. Soluția permite administratorului să stabilească acțiunea luata de produsul Antimalware la detectarea unei amenințări noi. Astfel administratorul va putea alege intre următoarele acțiuni: 4.1.1. Acțiune implicită pentru fișiere infectate: vi. interzice accesul vii. dezinfectează viii. ștergere ix. muta fișierele in carantina x. nicio acțiune 4.1.2. Acțiune alternativa pentru fișierele infectate: v. interzice accesul vi. dezinfectează vii. ștergere viii. muta fișierele in carantina 4.1.3. Acțiune implicită pentru fișierele suspecte: v. interzice accesul vi. ștergere vii. muta fișierele in carantina viii. nicio acțiune 4.1.4. Acțiune alternativa pentru fișierele suspecte: iv. interzice accesul v. ștergere vi. muta fișierele in carantina 4.2. Soluția permite scanarea automată în timp real care poate fi setată să nu scaneze arhive sau fișiere mai mari de « x » MB, mărimea fișierelor putând fi definita de administratorul soluției, 4.3. Soluția permite definirea până la 16 nivele de profunzime pentru scanarea in arhive. 4.4. Soluția permite scanarea euristica comportamentala prin simularea unui calculator virtual in interiorul căruia sunt rulate aplicații cu potențial periculos protejând sistemul de virușii necunoscuți prin detectarea codurilor periculoase a căror semnătura nu a fost lansata încă. 4.5. Soluția permite scanarea oricărui suport de stocare a informației (CD-uri, harduri externe, unități partajate etc). De asemenea, se va putea anula scanarea in cazul in care sunt detectate unități care au informații stocate mai mult de « x » MB. 4.6. Soluția permite scanarea automată a emailurilor la nivelul stației de lucru pentru POP3/SMTP.	

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
				4.6. Scanarea automata a emailurilor la nivelul statiei de lucru pentru POP3/SMTP. 4.7. Configurarea cailor ce urmeaza a fi scanate la cerere. 4.8. Clientii antimalware pentru workstation sa permita definirea unor liste de excludere de la scanarea in timp real si la cerere a anumitor directoare, discuri, fisiere, extensii sau procese. 4.9. Cu ajutorul unei baze de date complete cu semnaturi de spyware si a euristicii de detectie a acestui tip de programe, produsul va trebui sa ofere protectie anti-spyware. 4.10. Posibilitatea de configura scanarile programate sa se execute cu prioritate redusa 4.11. Produsul antimalware poate fi configurat sa foloseasca scanarea in cloud, si partial scanarea locala. 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. 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. 4.14. Pentru o protectie sporita, solutia antimalware trebuie sa poata scana paginile HTTP. 4.15. Pentru o mai buna gestionare a antimalware instalat pe statii, produsul va include optiunea de setare a unei parole pentru protectia la dezinstalare. 4.16. Pentru siguranta utilizatorului, clientul va include un modul de antiphishing.	4.7. În cadrul soluției poate fi configurată căile ce urmează a fi scanate la cerere. 4.8. Pentru clienții antimalware pentru workstation soluția permite definirea unor liste de excludere de la scanarea in timp real si la cerere a anumitor directoare, discuri, fișiere, extensii sau procese. 4.9. Cu ajutorul unei baze de date complete cu semnături de spyware si a euristicii de detecție a acestui tip de programe, produsul va trebui sa ofere protecție anti-spyware. 4.10. Soluția oferă posibilitatea de a configura scanările programate să se execute cu prioritate redusa 4.11. Produsul antimalware poate fi configurat sa folosească scanarea in cloud, si parțial scanarea locală. 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. 4.13. Pentru o protecție sporita, soluția antimalware oferă 3 tipuri de detecție: bazată pe semnături, bazata de comportamentul fișierelor si bazata pe monitorizarea proceselor. 4.14. Pentru o protecție sporită, soluția antimalware trebuie poate scana paginile HTTP. 4.15. Pentru o mai buna gestionare a antimalware instalat pe stații, soluția include opțiunea de setare a unei parole pentru protecția la dezinstalare. 4.16. Pentru siguranța utilizatorului, clientul are un modul de antiphishing. 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*
				4.17. Solutia ofera protectie in timp real pe masinile cu sistem de operare Linux in conformitate cu versiunea de kernel instalata. **5. Anti-Exploit-Avansat:** 5.1. Posibilitatea de a opri atacurile avansate de tip „zero-day" efectuate prin intermediul unor exploit-uri evazive 5.2. Depistarea in timp real a celor mai recente exploit-uri ce pot vulnerabiliza un sistem de operare. 5.3. Protejarea aplicatiilor utilizate frecvent si a celor de tip „sistem" cum ar fi browserele, aplicatiile de tip office sau reader, procesele critice aferente sistemelor de operare. **6. Firewall:** 6.1. Posibilitatea de a configura reguli de firewall pentru aplicatii sau conectivitate. 6.2. Modulul poate fi instalat/dezinstalat in functie de preferinta administratorului. 6.3. Posibilitatea de a defini retele de incredere pentru masina destinatie. 6.4. Abilitatea de a detecta scanarea de porturi. 6.5. Posibilitatea de a seta diferite profiluri de rețea ((Home/Office, Trusted, Public, Untrusted sau Let the Windows decide) 6.6. Abilitatea de a crea reguli personalizate bazate pe aplicație și/sau conexiune **7. Carantina:** 7.1. Produsul antimalware sa permita trimiterea automata a fisierelor din carantina catre laboratoarele antimalware ale producatorului. 7.2. Trimiterea continutului carantinei va putea fi expediat in mod automat, la un interval definit de administrator. 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. 7.4. Posibilitatea de a restaura un fisier din carantina in locatia lui originala. 7.5. Modulul de carantina va permite rescanarea obiectelor dupa fiecare actualizare de semnaturi. **8. Protectia datelor:**	**5. Anti-Exploit-Avansat:** 5.1. Soluția oferă posibilitatea de a opri atacurile avansate de tip „zero-day" efectuate prin intermediul unor exploit-uri evazive 5.2. Soluția poate depista în timp real a celor mai recente exploit-uri ce pot vulnerabiliza un sistem de operare. 5.3. Protejarea aplicațiilor utilizate frecvent si a celor de tip „sistem" cum ar fi browserele, aplicațiile de tip office sau reader, procesele critice aferente sistemelor de operare. **6. Firewall:** 6.1. Soluția oferă posibilitatea de a configura reguli de firewall pentru aplicații sau conectivitate. 6.2. Modulul poate fi instalat/dezinstalat in funcție de preferință administratorului. 6.3. Soluția oferă posibilitatea de a defini rețele de încredere pentru mașina destinație. 6.4. Soluția oferă abilitatea de a detecta scanarea de porturi. 6.5. Soluția oferă posibilitatea de a seta diferite profiluri de rețea ((Home/Office, Trusted, Public, Untrusted sau Let the Windows decide) 6.6. Soluția oferă abilitatea de a crea reguli personalizate bazate pe aplicație și/sau conexiune **7. Carantina:** 7.1. Produsul antimalware permite trimiterea automată a fișierelor din carantina către laboratoarele antimalware ale producătorului. 7.2. Soluția poate trimite conținutul carantinei care poate fi expediat în mod automat, la un interval definit de administrator. 7.3. Produsul antimalware permite ștergerea automată a fișierelor carantinate mai vechi de o anumita perioadă, pentru a nu încarcă inutil spațiul de stocare. 7.4. Soluția oferă posibilitatea de a restaura un fișier din carantina in locația lui originala. 7.5. Modulul de carantină permite rescanarea obiectelor după fiecare actualizare de semnături. **8. Protectia datelor:**	

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
				8.1. Produsul permite blocarea datelor confidentiale (pin-ul cardului, cont bancar etc) transmise prin HTTP sau SMTP prin crearea unor reguli specifice. **9. Controlul continutului:** 9.1. Consola va avea integrat un modul dedicat controlului accesului la Internet cu urmatoarele particularitati: a) Permite blocarea accesului la Internet pentru anumite masini client sau grupuri de masini. b) Permite blocarea accesului la Internet pe intervale orare. c) Permite blocarea paginilor de internet care contin anumite cuvinte cheie. d) Permite controlul accesului numai la anumite pagini de internet specificate de administrator; e) Permite blocarea accesului la anumite aplicatii definite de administrator; f) Permite restrictionarea accesului pe anumite pagini de internet dupa anumite categorii prestabilite (ex: online dating, violenta, pornografie etc). **10. Controlul dispozitivelor:** 10.1. Modulul poate fi instalat/dezinstalat in functie de preferinta administratorului. 10.2. Modulul va permite controlul urmatoarelor tipuri de dispozitive: a) Bluetooth Devices b) CDROM Devices c) Floppy Disk Drives d) Security Policies 153 e) IEEE 1284.4 f) IEEE 1394 g) Imaging Devices h) Modems i) Tape Drives j) Windows Portable k) COM/LPT Ports l) SCSI Raid m) Printers n) Network Adapters o) Wireless Network Adapters p) Internal and External Storage	8.1. Produsul permite blocarea datelor confidențiale (pin-ul cardului, cont bancar etc) transmise prin HTTP sau SMTP prin crearea unor reguli specifice. **9. Controlul conținutului:** 9.1. În Consolă poate fi integrat un modul dedicat controlului accesului la Internet cu următoarele particularități: g) Permite blocarea accesului la Internet pentru anumite mașini client sau grupuri de mașini. h) Permite blocarea accesului la Internet pe intervale orare. i) Permite blocarea paginilor de internet care conțin anumite cuvinte cheie. j) Permite controlul accesului numai la anumite pagini de internet specificate de administrator; k) Permite blocarea accesului la anumite aplicații definite de administrator; l) Permite restricționarea accesului pe anumite pagini de internet după anumite categorii prestabilite (ex: online dating, violenta, pornografie etc). **10. Controlul dispozitivelor:** 10.1. Modulul poate fi instalat/dezinstalat in funcție de preferință administratorului. 10.2. Modulul permite controlul următoarelor tipuri de dispozitive: q) Bluetooth Devices r) CDROM Devices s) Floppy Disk Drives t) Security Policies 153 u) IEEE 1284.4 v) IEEE 1394 w) Imaging Devices x) Modems y) Tape Drives z) Windows Portable aa) COM/LPT Ports bb) SCSI Raid cc) Printers dd) Network Adapters ee) Wireless Network Adapters ff) Internal and External Storage	

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*
				10.3. Modulul va permite configurarea de reguli prin care se vor defini permisiunile pentru dispozitivele conectate la masina client. 10.4. Modulul va permite configurarea de excluderi pentru diferite tipuri de dispozitive pentru care s-au configurat reguli. **11. Power User:** 11.1. Modulul poate fi instalat/dezinstalat in functie de preferinta administratorului. 11.2. Modulul permite posibilitatea de a acorda utilizatorilor drepturi de Power User. Utilizatorii vor putea accesa si modifica setarile clientului antimalware dintr-o consola dispobibila local pe masina client. 11.3. Modificarile efectuate din modulul Power User vor fi active local, pe masina pe care s-au facut respectivele modificari. 11.4. Administratorul va putea suprascrie din consola setarile aplicate de utilizatorii Power User. **12. Actualizare:** 12.1. Posibilitatea efectuarii actualizarii la nivel de statie in mod silentios (fara avertizare). 12.2. Sistem de actualizare cascadat folosind unul sau mai multe servere de actualizare (cascadate). 12.3. Actualizarea pentru locatiile remote prin intermediul unui client antimalware care are si rol de server de actualizare.	10.3. Modulul permite configurarea de reguli prin care se vor defini permisiunile pentru dispozitivele conectate la mașina client. 10.4. Modulul permite configurarea de excluderi pentru diferite tipuri de dispozitive pentru care s-au configurat reguli. **11. Power User:** 11.1. Modulul poate fi instalat/dezinstalat in funcție de preferință administratorului. 11.2. Modulul permite posibilitatea de a acorda utilizatorilor drepturi de Power User. Utilizatorii vor putea accesa si modifica setările clientului antimalware dintr-o consola disponibilă local pe mașina client. 11.3. Modificările efectuate din modulul Power User sunt active local, pe mașina pe care s-au făcut respectivele modificări. 11.4. Administratorul poate suprascrie din consolă setările aplicate de utilizatorii Power User. **12. Actualizare:** 12.1. Soluția oferă posibilitatea efectuării actualizării la nivel de stație in mod silențios (fără avertizare). 12.2. Sistem de actualizare cascadat folosind unul sau mai multe servere de actualizare (cascadate). 12.3. Actualizarea pentru locațiile remote prin intermediul unui client antimalware care are si rol de server de actualizare. **Alte cerințe oferite:** Perioada de suport și menținere de la producător: 1. Soluția ofertată se va livra pentru 12 luni; 2. Producătorul oferă suport 24/24, prin e-mail sau conectare de la distanță.	
TOTAL						

Semnat electronic: Digitally signed by Celonenco Vitalie
Date: 2026.01.27 01:18:39 EET
Reason: MoldSign Signature
Location: Moldova
MOLDOVA EUROPEANĂ

Numele, Prenumele: **CELONENCO Vitalie**
În calitate de: **Administrator**
Ofertantul: **„RTS ONE" S.R.L.**
Adresa: **mun.Chișinău, str.Mitropolit Gavriil Bănulescu-Bodoni, 59/B, of.804**