



„RTS ONE” S.R.L.



1018600009979



(+373) 22 101 777



office@rts.one



http://rts.md



str. Mitropolit G. Bănulescu-Bodoni, 59/B, of.804



Anexa nr.22
la Documentația standard nr.
ocds-b3wdp1-MD-1702456303378
din 13 decembrie 2023

Specificații tehnice

Numărul procedurii de achiziție: MTender ID: **ocds-b3wdp1-MD-1702456303378** din 13 decembrie 2023

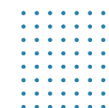
Obiectul achiziției: **Licența Antivirus pentru anul 2024**

Denumirea bunurilor	Modelul articolului	Țara de origine	Producătorul	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
Licența Antivirus	Bitdefender GravityZone Business Security	România	Bitdefender	CARACTERISTICI GENERALE ALE PRODUSULUI Produsul („soluția”) reprezintă o platformă integrată pentru managementul securității, gândită ca o soluție modulară. Produsul conține următoarele module: A. <i>Consola de management care asigură funcționalități de administrare.</i> B. <i>Protecție antimalware pentru stații fizice, laptop-uri și servere.</i> A. CONSOLA DE MANAGEMENT 1. Cerințe generale: 1.1. Interfața consolei de management va fi în limba română.	Tip: Subscriere anuală pentru soluția de protecție și securitate pentru 350 entități pentru perioada de 12 luni. Cantitate: Se oferă soluția Bitdefender GravityZone, cu urmatorul model de licențiere: - <i>GravityZone Business Security 350 entități (PC/laptop/VDI/Server).</i> 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, gândită 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. <i>Consola de management care asigură funcționalități de administrare.</i> B. <i>Protecție antimalware pentru stații fizice, laptop-uri și servere.</i> A. CONSOLA DE MANAGEMENT 1. Cerințe generale: 1.1. Interfața consolei de management este în limba română.	



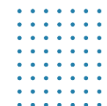
Denumirea bunurilor	Modelul articolului	Țara de origine	Producătorul	Specificarea tehnică deplină solicitată de către autoritatea contractantă	Specificarea tehnică deplină propusă de către ofertant	Standarde de referință
1	2	3	4	5	6	7
				1.2. Interfața clientului de securitate, care se instalează pe stații și servere, va fi în limba română. 1.3. Manualul de instalare a produsului va fi în limba română. 1.4. Manualul de administrare a produsului va fi în limba română. 1.5. Soluția va 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 virusi, 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 și raportare (Dashboard): 2.1. Rapoartele din panoul de monitorizare vor putea fi configurate specificând numele raportului, tipul raportului, ținta raportului, opțiuni specifice pentru orice tip de raport (de exemplu pentru raportul de actualizare - care este intervalul după care o stație este considerată neactualizată). 2.2. Panoul central conține rapoarte pentru toate modulele suportate. 2.3. Rapoartele din panoul central de comandă permit: adăugarea altor rapoarte, ștergerea lor și rearanjarea. 3. Inventarierea rețelei - managementul securității:	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. 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 virusi, 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 și 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 considerată neactualizată). 2.2. Panoul central conține rapoarte pentru toate modulele suportate. 2.3. Rapoartele din panoul central de comandă permit: adăugarea altor rapoarte, ștergerea lor și rearanjarea. 3. Inventarierea rețelei - managementul securității:	

Denumirea bunurilor	Modelul articolului	Țara de origine	Producătorul	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
				3.1. Soluția se va integra cu domeniul Active Directory și va putea importa inventarul. 3.2. Se permite descoperirea stațiilor fizice neintegrate în Active Directory (Workgroup) cu ajutorul Network discovery. 3.3. Soluția va oferi opțiuni de căutare, sortare și filtrare după numele sistemului, sistem de operare, adresa IP, politica aplicată, ultima dată când s-a conectat (online și/sau offline) și FQDN. 3.4. Soluția va permite crearea unui pachet unic pentru toate sistemele de operare, de stații sau servere. Astfel, administratorul va putea descărca pachetele pentru protecția stațiilor și serverelor pe care rulează sistemul de operare Windows, Linux, Mac. 3.5. Soluția va permite instalarea la distanță sau manual a clienților antimalware pe mașini fizice/virtuale. 3.6. Soluția va permite selectarea modulelor componente atunci când se creează pachetul clientului care se instalează pe mașinile fizice/virtuale. 3.7. Soluția va permite lansarea de task-uri de scanare, actualizare, instalare, deinstalarea la distanță pentru clientul antimalware. 3.8. Soluția va oferi posibilitatea de repornire a mașinilor fizice de la distanță. 3.9. Soluția va oferi informații detaliate despre fiecare task și se fișează dacă task-ul s-a finalizat sau nu cu succes. 3.10. Soluția va permite configurarea centralizată a clienților antimalware prin intermediul politicilor 3.11. Se vor oferi în consola de management informații detaliate ale obiectelor din consola: Nume, IP, Sistem de operare, Grup, Politica atribuită, Ultimele actualizări, Versiunea produsului, Versiunea de semnături. 4. Politici: 4.1. Soluția va permite configurarea setărilor antimalware prin intermediul politicilor din consola de management.	3.1. Soluția se integrează cu domeniul Active Directory și 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 aplicată, ultima dată când s-a conectat (online și/sau offline) și FQDN. 3.4. Soluția permite crearea unui pachet unic pentru toate sistemele de operare, de stații sau servere. Astfel, administratorul poate descărca pachetele 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, deinstalarea 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 atribuită, Ultimele actualizări, Versiunea produsului, Versiunea de semnături. 4. Politici: 4.1. Soluția permite configurarea setărilor antimalware prin intermediul politicilor din consola de management.	



Denumirea bunurilor	Modelul articolului	Țara de origine	Producătorul	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
				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 f) Clientul este/nu este in aceeasi 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 clientii 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.	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 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 administrată și va fi administrată, fie local, fie din consola de management.	

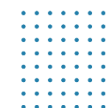




Denumirea bunurilor	Modelul articolului	Țara de origine	Producătorul	Specificarea tehnică deplină solicitată de către autoritatea contractantă	Specificarea tehnică deplină propusă de către ofertant	Standarde de referință
1	2	3	4	5	6	7
				7. Utilizatori: 7.1. Administrarea se va putea face pe baza de roluri. 7.2. Roluri multiple predefinite: Administrator companie, Administrator rețea, Reporter sau rol personalizat. a) Administrator companie: administrează arhitectura consolei de management; b) Administrator rețea: administrează serviciile de securitate; c) Reporter: monitorizează și generează rapoarte. 7.3. Utilizatorii pot fi importati din Microsoft Active Directory sau creați în consola de management. 7.4. Se va permite configurarea detaliată a drepturilor administrative, permițând selectarea serviciilor și obiectelor pentru care un utilizator poate face modificări. 7.5. Se va permite deconectarea automată a oricărui tip de utilizator după un anumit timp pentru o protecție sporită a datelor afișate în consola de administrare. Acest interval se poate personaliza de administratorul soluției. 8. Log-uri: 8.1. Înregistrarea acțiunilor utilizatorilor. 8.2. Se vor oferi informații detaliate pentru fiecare acțiune a unui utilizator. 8.3. Se va permite filtrarea acțiunilor utilizator după numele utilizatorului, acțiune. 9. Actualizare: 9.1. Se permite definirea de locații de actualizare multiple. 9.2. Se permite activarea/dezactivarea actualizărilor de produs și semnături. 9.3. Orice client antivirus să poată 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 și serverele din rețea, evitând posibile probleme ce pot afecta serverele sau stațiile	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 și 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 sporită a datelor afișate în consola de administrare. Acest interval se poate personaliza de administratorul soluției. 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 și 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 și serverele din rețea, evitând posibile probleme ce pot afecta serverele sau stațiile	



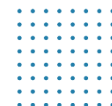
Denumirea bunurilor	Modelul articolului	Țara de origine	Producătorul	Specificarea tehnică deplină solicitată de către autoritatea contractantă	Specificarea tehnică deplină propusă de către ofertant	Standarde de referință
1	2	3	4	5	6	7
				critice. Astfel, soluția include 2 tipuri de actualizări de produs: a) Ciclu rapid, gândit pentru un mediu de test în cadrul rețelei b) Ciclu lent, gândit pentru restul rețelei (producție, servere critice etc) 9.5. Soluția permite stabilirea zonelor de test și critice din cadrul rețelei prin intermediul politicilor din consola de management. B. PROTECȚIE STAȚII ȘI SERVERE FIZICE 1. Caracteristici generale minimale și eliminatorii: 1.1. Pentru reducerea la minim a consumului de resurse, soluția antimalware trebuie să permită instalarea personalizată a modulelor deținute (de exemplu, să permită instalarea soluției antimalware fără modulul de control al accesului web, modulul de control al dispozitivelor sau modulul firewall). 1.2. Pentru o mai bună 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. 1.3. Vaccinul anti-ransomware primește actualizări de la producător, odată cu actualizarea semnăturilor produsului Antimalware. 1.4. Pentru o mai bună protecție a stațiilor și serverelor, soluția include protecție împotriva atacurilor zero-day de tip exploit avansate (atacuri direcționate) bazată pe tehnologii de învățare automată (machine learning). 1.5. Pentru o mai bună protecție a stațiilor și serverelor, soluția include un modul integrat de tip ERA (Endpoint Risk Analytics – Analiza de risc a endpoint-ului) capabil să identifice și remedieze în mod automatizat sau manual un număr mare de riscuri existente la nivel de	critice. Astfel, soluția include 2 tipuri de actualizări de produs: c) Ciclu rapid, gândit pentru un mediu de test în cadrul rețelei d) Ciclu lent, gândit pentru restul rețelei (producție, servere critice etc) 9.5. Soluția permite stabilirea zonelor de test și critice din cadrul rețelei prin intermediul politicilor din consola de management. B. PROTECȚIE STAȚII ȘI SERVERE FIZICE 1. Caracteristici generale minimale și eliminatorii: 1.1. Pentru reducerea la minim a consumului de resurse, soluția antimalware trebuie să permită instalarea personalizată a modulelor deținute (de exemplu, să permită instalarea soluției antimalware fără modulul de control al accesului web, modulul de control al dispozitivelor sau modulul firewall). 1.2. Pentru o mai bună 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. 1.3. Vaccinul anti-ransomware primește actualizări de la producător, odată cu actualizarea semnăturilor produsului Antimalware. 1.4. Pentru o mai bună protecție a stațiilor și serverelor, soluția include protecție împotriva atacurilor zero-day de tip exploit avansate (atacuri direcționate) bazată pe tehnologii de învățare automată (machine learning). 1.5. Pentru o mai bună protecție a stațiilor și serverelor, soluția include un modul integrat de tip ERA (Endpoint Risk Analytics – Analiza de risc a endpoint-ului) capabil să identifice și remedieze în mod automatizat sau manual un număr mare de riscuri existente la nivel de	



Denumirea bunurilor	Modelul articolului	Țara de origine	Producătorul	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
				rețea sau sistem de operare ce pot afecta funcționalitatea și nivelul de securizare al endpoint-ului 2. Cerințe de sistem: - Sisteme de operare pentru stații de lucru: Windows 11, 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 Enterprise Server 15 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 va putea particulariza pachetele de instalare cu modulele dorite: firewall, content control, device control, power user. 3.2. Instalarea se va putea face în mai multe moduri:	rețea sau sistem de operare ce pot afecta funcționalitatea și nivelul de securizare al endpoint-ului 2. Cerințe de sistem: - Sisteme de operare pentru stații de lucru: Windows 11, 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 Enterprise Server 15 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 dorite: firewall, content control, device control, power user. 3.2. Instalarea se poate efectua în mai multe moduri:	



Denumirea bunurilor	Modelul articolului	Țara de origine	Producătorul	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
				a) prin descărcarea directă a pachetului pe stația pe care se va face instalarea; b) prin instalarea la distanță, direct din consola de management c) trimiterea pe email (oricate adrese) a pachetului de instalare pentru Windows, Linux, Mac. 3.3. Instalarea clienților la distanță în alte locații decât cele în care este instalată consola de management se va face prin intermediul unui client existent în locațiile respective de tip relay pentru a minimiza traficul în WAN. 3.4. În consola vor fi disponibile informații despre fiecare stație: numele stației, IP, sistem de operare, module instalate, politica aplicată, informații despre actualizări etc. 3.5. Din consola se va putea trimite o singură politică pentru configurarea integrală a clientului de pe stații/serve. 3.6. Consola va include o secțiune, „Audit”, unde se vor menționa toate acțiunile întreprinse fie de administratori fie de reporteri, cu informații detaliate: logare, editare, creare, delogare, mutare etc. 3.7. Posibilitatea creării unui singur pachet de instalare, utilizabil atât pentru sistemele de operare pe 32 de biți cât și pentru cele pe 64 de biți. 3.8. Posibilitatea creării unui singur pachet de instalare, utilizabil pentru stații (fizice și/sau virtuale), serve (fizice și/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 stațiile/servele din rețea pentru cele care nu sunt integrate în domeniu. 3.11. Permite selectarea clientului care va realiza descoperirea stațiilor din rețea, altele decât cele integrate în domeniu.	d) prin descărcarea directă a pachetului pe stația pe care se va face instalarea; e) prin instalarea la distanță, direct din consola de management f) trimiterea pe email (oricate adrese) a pachetului de instalare pentru Windows, Linux, Mac. 3.3. Instalarea clienților la distanță în alte locații decât cele în care este instalată consola de management se va face prin intermediul unui client existent în locațiile respective de tip relay pentru a minimiza traficul în WAN. 3.4. În consola vor fi disponibile informații despre fiecare stație: numele stației, IP, sistem de operare, module instalate, politica aplicată, informații despre actualizări etc. 3.5. Din consola se poate trimite o singură politică pentru configurarea integrală a clientului de pe stații/serve. 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 creării unui singur pachet de instalare, utilizabil atât pentru sistemele de operare pe 32 de biți cât și pentru cele pe 64 de biți. 3.8. Soluția oferă posibilitatea creării unui singur pachet de instalare, utilizabil pentru stații (fizice și/sau virtuale), serve (fizice și/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/servele din rețea pentru cele care nu sunt integrate în domeniu. 3.11. Soluția permite selectarea clientului care va realiza descoperirea stațiilor din rețea, altele decât cele integrate în domeniu.	

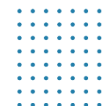


Denumirea bunurilor	Modelul articolului	Țara de origine	Producătorul	Specificarea tehnică deplină solicitată de către autoritatea contractantă	Specificarea tehnică deplină propusă de către ofertant	Standarde de referință
1	2	3	4	5	6	7
				4. Caracteristici si functionalitati principale ale modului antimalware: 4.1. Soluția 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 implicita 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 implicita 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	4. Caracteristici si funcționalități principale ale modului antimalware: 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	



Denumirea bunurilor	Modelul articolului	Țara de origine	Producătorul	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
				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. 4.6. 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 semnături 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.	sistemul de virusii necunoscuți prin detectarea codurilor periculoase a căror semnatura 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. 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 în 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.	

Denumirea bunurilor	Modelul articolului	Țara de origine	Producătorul	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
				4.13. Pentru o protecție sporită, soluția antimalware trebuie să aibă 3 tipuri de detecție: bazată pe semnături, bazată de comportamentul fișierelor și bazată pe monitorizarea proceselor. 4.14. Pentru o protecție sporită, soluția antimalware trebuie să poată scana paginile HTTP. 4.15. Pentru o mai bună gestionare a antimalware instalat pe stații, produsul va include opțiunea de setare a unei parole pentru protecția la dezinstalare. 4.16. Pentru siguranța utilizatorului, clientul va include un modul de antiphishing. 4.17. Soluția oferă protecție în timp real pe mașinile cu sistem de operare Linux în conformitate cu versiunea de kernel instalată. 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 în timp real a celor mai recente exploit-uri ce pot vulnerabiliza un sistem de operare. 5.3. Protejarea aplicațiilor utilizate frecvent și 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. Posibilitatea de a configura reguli de firewall pentru aplicații sau conectivitate. 6.2. Modulul poate fi instalat/dezinstalat în funcție de preferința administratorului. 6.3. Posibilitatea de a defini rețele de încredere pentru mașina destinație. 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	4.13. Pentru o protecție sporită, soluția antimalware oferă 3 tipuri de detecție: bazată pe semnături, bazată de comportamentul fișierelor și bazată pe monitorizarea proceselor. 4.14. Pentru o protecție sporită, soluția antimalware trebuie să poată scana paginile HTTP. 4.15. Pentru o mai bună 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 în timp real pe mașinile cu sistem de operare Linux în conformitate cu versiunea de kernel instalată. 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 și 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 în 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)	



Denumirea bunurilor	Modelul articolului	Țara de origine	Producătorul	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
				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 semnături. 8. Protectia datelor: 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;	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 anumită perioadă, pentru a nu încărca inutil spațiul de stocare. 7.4. Soluția oferă posibilitatea de a restaura un fișier din carantina în locația lui originala. 7.5. Modulul de carantină permite rescanarea obiectelor după fiecare actualizare de semnături. 8. Protectia datelor: 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 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;	





Denumirea bunurilor	Modelul articolului	Țara de origine	Producătorul	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
				f) Permite restricționarea accesului pe anumite pagini de internet după anumite categorii prestabilite (ex: online dating, violența, pornografie etc). 10. Controlul dispozitivelor: 10.1. Modulul poate fi instalat/dezinstalat în funcție de preferința administratorului. 10.2. Modulul va 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 l) SCSI Raid m) Printers n) Network Adapters o) Wireless Network Adapters p) Internal and External Storage 10.3. Modulul va permite configurarea de reguli prin care se vor defini permisiunile pentru dispozitivele conectate la mașina 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 în funcție de preferința administratorului. 11.2. Modulul permite posibilitatea de a acorda utilizatorilor drepturi de Power User. Utilizatorii vor putea accesa și modifica setările clientului antimalware dintr-o consolă disponibilă local pe mașina client. 11.3. Modificările efectuate din modulul Power User vor fi active local, pe mașina pe care s-au făcut respectivele modificări.	l) Permite restricționarea accesului pe anumite pagini de internet după anumite categorii prestabilite (ex: online dating, violența, pornografie etc). 10. Controlul dispozitivelor: 10.1. Modulul poate fi instalat/dezinstalat în 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 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 în funcție de preferință administratorului. 11.2. Modulul permite posibilitatea de a acorda utilizatorilor drepturi de Power User. Utilizatorii vor putea accesa și modifica setările clientului antimalware dintr-o consolă 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.	





„RTS ONE” S.R.L.



1018600009979



(+373) 22 101 777



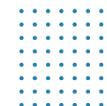
office@rts.one



http://rts.md



str. Mitropolit G. Bănulescu-Bodoni, 59/B, of.804



Denumirea bunurilor	Modelul articolului	Țara de origine	Producătorul	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
				11.4. Administratorul va putea suprascrise din consola setările aplicate de utilizatorii Power User. 12. Actualizare: 12.1. Posibilitatea efectuării actualizării la nivel de stație în 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 și rol de server de actualizare.	11.4. Administratorul poate suprascrise din consolă setările aplicate de utilizatorii Power User. 12. Actualizare: 12.1. Soluția oferă posibilitatea efectuării actualizării la nivel de stație în 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 și rol de server de actualizare. Alte cerințe: <u>Perioada de suport și mentinere de la producător:</u> 1. Soluția oferată se va livra pentru 12 luni; 2. Producătorul oferă suport 24/24, prin e-mail sau conectare de la distanță.	
TOTAL						

Semnat electronic:

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**