Anexa nr.2 la Anunțul de participare

Specificații tehnice

Numărul procedurii de achiziție: **ocds-b3wdp1-MD-1733743670453**
Obiectul achiziției: **Licențe 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*
Licențe antivirus	Bitdefender GravityZone Business Security Enterprise	România	Bitdefender	Conform Anunțului de participare, pct.12 – Specificații Antivirus (Anexa)	**Cantitate:** - **220 entități (PC/laptop/VDI/Server) din acest volum minim 75 destinate pentru servere;** 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 conține următoarele module, toate cu posibilitatea de a fi gestionate și administrate dintr-o singură consolă de management: • Protecție stații și servere fizice și virtualizate; • Posibilitatea de a adaugă protecție și securitate pentru telefoanele mobile de tip smartphone cu sistem de operare iOS sau Android; • Serviciu de corelare și răspuns la evenimente de tip EDR („endpoint detection and response"). **Consola de management:** **1. Instalare si configurare:** 1. Mașinile de scanare (pentru tipul de scanare centralizata) pentru mediile	

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*
					virtuale se descarcă din interfața web a produsului. **2. Cerinte generale:** 1. Interfața consolei de management este și in limba romana. 2. Interfața clientului de securitate, se instalează pe stații și servere, este în limba romana. 3. Manualul de instalare a produsului este în limba romana. 4. Manualul de administrare a produsului este în limba romana. 5. Soluția permite activarea/ dezactivarea actualizărilor de produs/ semnături. 6. Actualizări automate a consolei de management făcute de către producătorul soluției, fără intervenția utilizatorului. 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). 8. Consola de management este accesibila de oriunde în lume (soluție de tip Cloud), fără a fi nevoie de setări suplimentare din partea utilizatorului. 9. Consola de management este accesibila atât de pe stații de lucru cât și de pe dispozitive mobile (smartphone, tableta). **3. Panou de monitorizare și raportare (Dashboard):**	

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. 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). 2. Panoul central conține rapoarte pentru toate modulele suportate. 3. Rapoartele din panoul central de comanda permit: adăugarea altor rapoarte, ștergerea lor și rearanjarea. **4. Inventarierea retelei – managementul securitatii:** 1. Soluția se poate integra cu domeniul Active Directory și poate importa inventarul. 2. Permite descoperirea stațiilor fizice neintegrate în Active Directory (Workgroup) cu ajutorul Network discovery. 3. Solutia 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) si FQDN. 4. Solutia permite crearea unui pachet unic pentru toate sistemele de operare, de statii sau servere. Astfel, administratorul poate descarca pachetele pentru protectia statiilor și serverelor pe care rulează sistemul de operare Windows, Linux, Mac. 5. Soluția permite instalarea la distanță sau manual a clienților antimalware pe mașini fizice/virtuale.	

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
					6. Soluția permite selectarea modulelor componente atunci când se creează pachetul clientului care se instalează pe mașinile fizice/virtuale. 7. Soluția permite lansarea de task-uri de scanare, actualizare, instalare, dezinstalarea la distanta pentru clientul antimalware. 8. Soluția oferă posibilitatea de repornire a mașinilor fizice de la distanță. 9. Soluția oferă informatii detaliate despre fiecare task și se afișează daca task-ul s-a finalizat sau nu cu succes. 10. Soluția permite configurarea centralizată a clienților antimalware prin intermediul politicilor 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. **5. Politici:** 1. Soluția permite configurarea setărilor clientului antimalware prin intermediul unei singure politici ce conține setări pentru toate module 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. 3. Soluția permite aplicarea politicilor pe mașini client, grupuri de mașini, domeniu, unități organizaționale.	

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. 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) **6. Rapoarte:** 1. Soluția conține rapoarte care prezinta statusul mașinilor clienților din punct de vedere al actualizărilor, fișierelor malware detectate, aplicațiile blocate, site-urilor web blocate. 2. Rapoartele programate pot fi trimise către un număr nelimitat de adrese de email (nu este nevoie sa aibă un cont în consola de management). 3. Soluția permite vizualizarea rapoartelor curente programate de administrator. 4. Soluția permite exportarea rapoartelor în format .pdf și detaliile ca format .csv. sau arhiva. 5. Soluția include un generator de rapoarte care oferă posibilitatea de a investiga o problema de securitate pe baza mai multor criterii, menținând informațiile concise și ordonate corespunzător. Astfel, soluția include interogări precum:	

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
					starea terminalului, evenimente terminal, etc. 6. Interogarea legată 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. 7. Interogarea legată de evenimente terminal include informații precum: a. calculatorul ținta pe care a avut loc evenimentul b. tipul starea ți 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 in timpul evenimentului f. evenimente (site-uri blocate, aplicații blocate, detecțiile etc) **7. Carantina:** 1. Soluția permite restaurarea fișierelor carantinate în locația originală sau într-o cale configurabila. 2. Carantina este locală, pe fiecare stație administrată și poate fi administrată, fie local, fie din consola de management. **8. Utilizatori:**	

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. Administrarea se poate face pe baza de roluri. 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. 3. Utilizatorii pot fi importați din Microsoft Active Directory sau creați in consola de management. 4. Soluția permite configurarea detaliată a drepturilor administrative, permițând selectarea serviciilor și obiectelor pentru care un utilizator poate face modificări. 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 poate fi personalizată de administratorul soluției. **9. Log-uri:** 1. Înregistrarea acțiunilor utilizatorilor. 2. Soluția oferă informații detaliate pentru fiecare acțiune a unui utilizator. 3. Soluția permite filtrarea acțiunilor utilizator după numele utilizatorului, acțiune. **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. Soluția permite definirea de locații de actualizare multiple. 2. Soluția permite activarea/ dezactivarea actualizărilor de produs și semnături. 3. Orice client antivirus poate fi configurat sa livreze update-urile către alt client antivirus 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 critice. Astfel, serverul de actualizare 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) 5. Soluția permite stabilirea zonelor de test si critice din cadrul rețelei prin intermediul politicilor din consola de management. **B. PROTECTIE STATII ȘI SERVERE FIZICE/VIRTUALE** **1. Caracteristici generale minimale și eliminatorii:** 1. Pentru reducerea la minim a consumului de resurse, soluția antimalware permite instalarea personalizată a modulelor deținute (de exemplu, să permită instalarea soluției antimalware fără modulul de control al accesului web, modul de control al dispozitivelor sau modulul firewall).	

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. Pentru o mai buna protecție a stațiilor și serverelor, soluția include un vaccin anti-ransomware. Acest vaccin asigura protecția împotriva tuturor amenințărilor cunoscute de tip ransomware, prin imunizarea stațiilor și serverelor, chiar dacă sunt infectate și prin blocarea procesului de criptare. 3. Vaccinul anti-ransomware primește actualizări de la producător, odată cu actualizarea semnăturilor produsului Antimalware. 4. Pentru o mai buna protecție a stațiilor și serverelor, soluția include protecție împotriva atacurilor zero-day de tip exploit avansate (atacuri direcționate) bazată pe tehnologii de învățare automata (machine learning). 5. Pentru o mai buna 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 rețea sau sistem de operare ce pot afecta funcționalitatea și nivelul de securizare al endpoint-ului 6. Pentru o mai buna 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 in faza pre-execuție. 7. Acest modul avansat de securitate va proteja împotriva: atacurilor	

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*
					direcționate (Targeted Attack - APT), fișierelor suspecte și traficului la nivel de rețea suspect, exploit-urilor, ransomware si grayware. Fiecărui tip de amenințare menționat, i se vor putea stabili, independent, un nivel de protecție dorit: permisiv, normal, agresiv. 8. Modulul avansat de securitate are posibilitatea de a raporta, bloca accesul, dezinfecta, șterge sau muta în carantina pentru fiecare din categoriile descrise. Astfel, administratorul va putea decide daca dorește întâi monitorizare sau dorește și blocarea amenințărilor. Aceste acțiuni menționate, vor putea fi stabilite independent, pentru fișiere sau pentru traficul din rețea, cu posibilitatea extinderii nivelului de raportare pentru a include nivelurile superioare (vor putea fi raportate amenințările care ar fi fost detectate dacă nivelul de protecție era stabilit mai agresiv). 9. Pentru a oferi un nivel adițional de protecție a stațiilor și serverelor, soluția include un sandbox în cloud-ul public al producătorului acesteia. 10. Modulul de Sandbox poate trimite automat fișiere în Sandbox-ul din cloud-ul producătorului unde vor putea fi „detonate" pentru o analiza în profunzime. 11. Modulul de Sandbox include două variante de analiza: doar monitorizare sau blocare. In modul monitorizare utilizatorul va putea accesa fișierul dorit, pe când în modul blocare, utilizatorului i se va bloca rularea fișierului până când	

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*
					Sandbox-ul din cloud-ul producătorului va da verdictul. 12. Modulul de Sandbox include două tipuri de acțiuni remediere: implicită 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. 13. Modulul de Sandbox include și posibilitatea de trimitere manuală a fișierelor în Sandbox-ul din cloud-ul producătorului. Astfel, dacă administratorul suspectează un fișier ca fiind maliții̧os, îl poate trimite manual in Sandbox pentru a fi „detonat" și a afla verdictul. Soluția poate trimite mai multe fișiere de odată, cu posibilitate de a specifica dacă vor fi „detonate" individual sau toate în același timp. 14. Modulul de Sandbox suportă „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. 15. Fișierele menționate anterior, pot fi detectate corect chiar dacă sunt incluse în arhive de tipul: : 7z, ACE, ALZip, ARJ, BZip2, cpio, GZip, LHA, Linux TAR, LZMA Compressed Archive, MS Cabinet, MSI, PKZIP,	

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
					RAR, Unix Z, ZIP, ZIP (multivolume), ZOO, XZ. 16. Modul de detectare, corelare și răspuns la evenimente de tip EDR („endpoint detection and response") capabil să identifice amenințări avansate sau atacuri în curs de desfășurare. 17. Soluția cuprinde colectare de date și evenimente despre hardware si software aferent fiecărei stații de lucru aducând informații detaliate referitoare la incidentele detectate, o hartă detaliată a acestora precum și acțiuni de remediere automate și integrare cu modulele de Sandbox și modulul avansat de securitate - – HyperDetect. Din punct de vedere funcțional modulul EDR cuprinde 2 componente distincte: senzorul ce colectează și procesează datele respectiv partea de analiza de securitate care are ca obiect interpretarea acestora. 18. Modulul EDR are capacitatea de a evalua activitatea tipică a unui endpoint din perspectiva securității acestuia conform tehnicilor de atac MITRE („baselining") și poate raporta orice deviație de la acest comportament sub forma unui incident. 19. Modulul EDR permite filtrarea incidentelor din interfața grafică în funcție intervalul de timp, pe baza unui scor de încredere („confidence score"), indicatori de atac, tehnici de atac (ATT&CK) respectiv sistem de operare afectat cât și după IP, nume fișier, nume stație.	

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*
					20. Modulul permite vizualizarea detaliată a incidentelor incluzând detalii specifice fiecărui nod afectat după cum urmează: tabul „rezumat" generează o harta de principiu a incidentului, tabul „timeline" detaliază incidentul în funcție de amprenta de timp a fiecăreia acțiuni aferente incidentului, respectiv butonul „acționează" care poate genera un set de masuri specifice fiecărui element din harta incidentului (kill, carantina – la nivel de nod, investigați – virus total, sandbox, google – la nivel de fișier, adăugare în lista de blocare – la nivel de rețea sau instalare patch – la nivel de nod). 21. Modulul poate bloca fișiere și/sau procese folosind valori hash de tip MD5/SHA256 direct din pagina aferenta incidentului sau importate folosind un fișier CSV. 22. Modulul poate excepta fișiere non-malițioase de la acțiunea de investigare sau poate genera/adaugă un set de fișiere malițioase într-o listă neagră pentru a preveni mișcarea laterală a fișierelor/ proceselor malițioase. 23. Modulul permite deschiderea unei conexiuni remote către un endpoint potențial infectat pentru a permite o investigare rapida a gazdei, colecta date despre atac respectiv remedia în timp real brește de securitate eliminând astfel posibile incertitudini privitoare la comportamentul potențial malițios al unor fișiere/procese, reducând timpul de remediere (downtime) în cazul 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
					care un atac a avut succes și stația țintă trebuie reconfigurată/ reinstalată, permite executarea unor comenzi în linia de comanda care se execută cu privilegii de kernel ce permit eliminarea în timp real a unor amenințări sau colectarea de date privitoare la atacul în desfășurare. 24. Pentru o mai buna protecție, produsul permite vizualizarea incidentelor extinse din cadrul tehnologiei XDR (Extended Incidents), care creează prin corelarea evenimentelor de pe mai multe stații din rețeaua clientului. **2. Cerințe 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	

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
					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:** 1. Inainte de instalare, administratorul poate particulariza pachetele de instalare cu modulele dorite: firewall, content control, device control, power user. 2. Instalarea se face în mai multe moduri: a. prin descarcarea directă a pachetului pe statia pe care se va face instalarea; b. prin instalarea la distanță, direct din consola de management c. trimiterea pe email (oricâte adrese) a linkului cu pachetul de instalare pentru Windows, Linux, Mac. 3. Instalarea clienților la distanță în alte locații decât cele în care este instalată consola de management se va face prin intermediul unui alt client antivirus existent în locațiile	

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*
					respective pentru a minimiza traficul in WAN. 4. În consolă sunt disponibile informații despre fiecare stație: numele stației, IP, sistem de operare, module instalate, politica aplicată, informații despre actualizări etc. 5. Din consola se poate trimite o singură politică pentru configurarea integrală a clientului de pe stații/servere. 6. Consola include o secțiune, „Audit", unde se vor menționa toate acțiunile intreprinse fie de administratori fie de reporteri, cu informații detaliate: logare, editare, creare, delogare, mutare etc. 7. Posibilitatea creării unui singur pachet de instalare, utilizabil atât pentru sistemele de operare pe 32 de biti cât și pentru cele pe 64 de biți. 8. Posibilitatea creări unui singur pachet de instalare, utilizabil pentru stații (fizice și/sau virtuale), servere (fizice și/sau virtuale). 9. Posibilitatea de a crea pachetele de instalare de tip web installer sau kit full. 10. Administratorul poate crea grupuri sau chiar subgrupuri, unde poate muta stațiile/serverele din rețea pentru cele care nu sunt integrate domeniu. 11. Permite selectarea clientului care va realiza descoperirea stațiilor din rețea, altele decât cele integrate în domeniu. **4. Caracteristici și 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
					1. Solutia permite administratorului să stabilească acțiunea luată de produsul Antimalware la detectarea unei amenințări noi. Astfel, administratorul va putea alege între următoarele acțiuni: a) Acțiune implicita pentru fișiere infectate: 1. interzice accesul 2. dezinfecteaza 3. stergere 4. muta fisierele in carantina 5. nicio actiune b) Acțiune alternativă pentru fișierele infectate: 1. interzice accesul 2. dezinfecteaza 3. stergere 4. muta fisierele in carantina c) Acțiune implicită pentru fișierele suspecte: 1. interzice accesul 2. stergere 3. muta fisierele in carantina 4. nicio actiune d) Acțiune alternativă pentru fișierele suspecte: 1. interzice accesul 2. stergere 3. muta fisierele in carantina 2. Scanarea automată în timp real poate fi setată să nu scaneze arhive sau fisiere mai mari de « x » MB, marimea fițierelor putând fi definită 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*
					3. Definirea până la 16 nivele de profunzime pentru scanarea în arhive. 4. Scanarea euristică comportamentală prin simularea unui calculator virtual în interiorul căruia sunt rulate aplicații cu potențial periculos protejând sistemul de virușii necunoscuți prin detectarea codurilor periculoase a căror semnatura nu a fost lansată încă. 5. Scanarea oricarui suport de stocare a informației (CD-uri, harduri externe, unitati partajate etc). De asemenea, se poate anula scanarea în cazul în care sunt detectate unități care au informații stocate mai mult de « x » MB. 6. Scanarea automată a emailurilor la nivelul stației de lucru pentru POP3 (incoming)/SMTP(outgoing). 7. Configurarea căilor ce urmeaza a fi scanate la cerere. 8. Clienții antimalware pentru workstation permite definirea unor liste de excludere de la scanarea în timp real și la cerere a anumitor directoare, discuri, fișiere, extensii sau procese. 9. Cu ajutorul unei baze de date complete cu semnături de spyware și a euristicii de detectie a acestui tip de programe, produsul oferă protecție anti-spyware. 10. Abilitatea de a detecta atacuri fără fișiere, inclusiv cele care folosesc instrumente legitime ale sistemului de operare, cum ar fi Powershell sau interpreții de script. Soluția	

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
					blochează global scripturile pentru a realiza acest lucru. 11. Oferă tehnologia Anti-Ransomware. 12. Posibilitatea de configura scanarile programate să se execute cu prioritate redusă. 13. Produsul antimalware poate fi configurat să folosească scanarea în cloud, și parțial scanarea locală. Pentru stațiile ce nu au suficiente resurse hardware, scanarea se poate face cu o mașina de scanare instalată în rețea (scanare centralizată). 14. Administratorul poate personaliza și motoarele de scanare, având posibilitatea de a alege între mai multe tehnologii de scanare: • Scanare locală, când scanarea se efectuează pe stația de lucru locală. Modul de scanare locală este potrivit pentru mașinile puternice, având toate semnăturile și motoarele stocate local. • Scanarea hibrid cu motoare light (Cloud public), cu o amprentă medie, folosind scanarea în cloud și, parțial, semnături locale. Acest mod de scanare oferă avantajul unui consum mai bun de resurse, fără să implice scanarea locală. • Scanarea centralizată în Cloud-ul privat, cu o amprentă redusă, necesitând un server de securitate pentru scanare. În acest caz, nu se stochează local nicio semnătură, iar scanarea este transferată către serverul de securitate. • Scanare centralizată (Scanare în cloud privat cu server de	

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
					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) 15. Pentru o protectie sporita, solutia antimalware are 3 tipuri de detecție: bazată pe semnături, bazată de comportamentul fișierelor și bazată pe monitorizarea proceselor. 16. Pentru o protecție sporită, soluția antimalware poate scana paginile HTTP. 17. Pentru o mai buna gestionare a antimalware instalat pe stații, produsul include opțiunea de setare a unei parole pentru protecția la dezinstalare. 18. Pentru siguranța utilizatorului, clientul include un modul de antiphishing. 19. Soluția oferă protecție în timp real pe mașinile cu sistem de operare Linux în conformitate cu versiunea de kernel instalată. **5. Anti-Exploit-Avansat:** 1. Posibilitatea de a opri atacurile avansate de tip „zero-day" efectuate prin intermediul unor exploit-uri evazive 2. Depistarea în timp real a celor mai recente exploit-uri ce pot vulnerabiliza un sistem de operare. 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.	

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*
					6. Firewall: 1. Posibilitatea de a configura reguli de firewall pentru aplicații sau conectivitate. 2. Modulul poate fi instalat/ dezinstalat în funcție de preferința administratorului. 3. Posibilitatea de a defini rețele de încredere pentru mașină destinație. 4. Abilitatea de a detecta scanarea de porturi. 5. Posibilitatea de a seta diferite profiluri de rețea ((Home/Office, Trusted, Public, Untrusted sau Let the Windows decide) 6. Abilitatea de a crea reguli personalizate bazate pe aplicație și/sau conexiune **7. Carantina:** 1. Produsul antimalware permite trimiterea automată a fișierelor din carantina către laboratoarele antimalware ale producătorului. 2. Trimiterea conținutului carantinei poate fi expediat în mod automat, la un interval definit de administrator. 3. Produsul antimalware permite ștergerea automată a fișierelor carantinate mai vechi de o anumita perioada, pentru a nu încărca inutil spațiul de stocare. 4. Posibilitatea de a restaura un fișier din carantina în locația lui originală.	

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
					5. Modulul de carantină permite rescanarea obiectelor după fiecare actualizare de semnături. **8. Protectia datelor:** 1. Produsul permite blocarea datelor confidențiale (pin-ul cardului, cont bancar etc) transmise prin HTTP sau SMTP prin crearea unor reguli specifice. **9. Controlul continutului:** 1. Consola are integrat un modul dedicat controlului accesului la Internet cu urmatoarele particularitati: 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). **10. Controlul dispozitivelor:**	

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. Modulul poate fi instalat/dezinstalat în funcție de preferința administratorului. 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 l. SCSI Raid m. Printers n. Network Adapters o. Wireless Network Adapters p. Internal and External Storage 3. Modulul permite configurarea de reguli prin care se definesc permisiunile pentru dispozitivele conectate la mașina client. 4. Modulul permite configurarea de excluderi pentru diferite tipuri de dispozitive pentru care s-au configurat reguli. **11. Power User:** 1. Modulul poate fi instalat/dezinstalat in functie de preferinta administratorului. 2. Modulul permite posibilitatea de a acorda utilizatorilor drepturi de	

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
					Power User. Utilizatorii vor putea accesa si modifica setarile clientului antimalware dintr-o consola disponibila local pe masina client. 3. Modificarile efectuate din modulul Power User vor fi active local, pe masina pe care s-au facut respectivele modificari. 4. Administratorul poate suprascrie din consola setările aplicate de utilizatorii Power User. **12. Actualizare:** 1. Posibilitatea efectuării actualizării la nivel de stație în mod silențios (fără avertizare). 2. Sistem de actualizare cascadat folosind unul sau mai multe servere de actualizare (cascadate). 3. Actualizarea pentru locațiile remote prin intermediul unui client antimalware care are si rol de server de actualizare. 4. Abilitatea de a împiedica punctele finale să iasă pe internet pentru a descrca actualizări. **13. Protecție Anti-manipulare:** 1. Protecția anti-manipulare permite detecția driverelor vulnerabile pe dispozitivele conectate (endpointuri) și când sunt efectuate încercări avansate de atac pentru a dezactiva agentul de securitate, ceea ce poate duce la compromiterea integrității produsului. 2. Modulul permite detectarea de drivere vulnerabile pe dispozitivele	

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
					conectate care pot fi exploatate de atacatori, reprezentând amenințări la adresa integrității produsului. Tehnologia este compatibilă cu sistemele de operare Windows și Linux. 3. Soluția este capabilă să protejeze împotriva Amenințărilor noi sau erorilor umane neintenționate ce ar putea fi proiectate pentru a permite acces neautorizat la kernel, ducând la compromiterea integrității poate detecta când funcțiile de tip callback ale agentului de securitate au fost eliminate sau dezactivate în mod malițios. **Alte cerințe:** • Perioada de suport și menținere de la producător: • Pentru soluția ofertată se solicită a fi 12 luni pentru perioada 12.01.2024-12.01.2025; • Producătorul oferă suport 24/24, prin e-mail sau conectare de la distanță. Notă: Lucrările de instalare, configurare, punerea în funcțiune a soluției este executată de Ofertant, iar costul acestora sunt incluse în ofertă.	
TOTAL						

Semnat:

Digitally signed by Celonenco Vitalie
Date: 2024.12.16 19:12:20 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**