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

SPECIFICAŢII TEHNICE F4.1

În cazul unei discrepanţe sau al unui conflict cu cerințele din secțiunea 2. Fișa de date a achiziției (FDA), prevederile din FDA vor prevala asupra prevederilor de mai jos.

Numărul procedurii de achiziţie *nr. ocds-b3wdp1-MD-1646123927520 din 09 martie 2022*
Denumirea procedurii de achiziţie: *Licențe antivirus pentru anul 2022*

Cod CPV	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	8
	Bunuri/ servicii						
	Lotul 1:						
48200000-0	Software antivirus pentru protecția stațiilor de lucru (PC, NoteBook, tabletă)	BitDefender GravityZone Ultra	România	BitDefender	Conform anexei	**Tip:** *Soluția de protecție și securitate (BitDefender GravityZone Ultra).* 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").	

Digitally signed by Celonenco Vitalie
Date: 2022.03.08 21:10:53 EET
Reason: MoldSign Signature
Location: Moldova

48200000-0	Software antivirus pentru protecția stațiilor de lucru (PC, NoteBook, tabletă)	BitDefender GravityZone Ultra	România	BitDefender	Conform anexei	**<u>Caracteristici generale ale produsului:</u>** 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: • Protecție stații (PC, NoteBook) și servere fizice și virtualizate; • Protecție și securitate pentru dispozitive de tip tabletă cu sistem de operare iOS sau Android; • Protecție și securitate pentru serverele email Microsoft Exchange; • Serviciu de corelare și răspuns la evenimente de tip EDR („endpoint detection and response"). **Consola de management:** Pachetul de instalare va fi livrat ca o mașină virtuală, care conține toate rolurile sau serviciile necesare. Consola nu va necesita o licență suplimentară pentru sistemul de operare. Imaginea de tip template poată a fi importa în: 1. VMware vSphere; 2. Citrix XenServer; 3. Microsoft Hyper-V; 4. KVM; 5. Nutanix. *Consola de management* va fi livrată cu o baza de date inclusă, non-relațională fără a fi nevoie de licențe adiționale. **Cerințe generale produs:** *<u>Soluția:</u>* 1. include un unul sau mai multe module de update server prin	

						care să asigure actualizarea componentelor și a semnăturilor; 2. permite activarea/dezactivarea actualizărilor automate de produs/semnături și a consolei de management; 3. transmite alerte de ne funcționalitate, cu 30 de minute înainte de actualizare; 4. permite vizualizarea unui jurnal de modificări în care sunt precizate istoric: versiunea consolei de management, data versiunii, funcții noi și îmbunătățiri, probleme rezolvate, probleme cunoscute; 5. afișează notificările și alertele existente, să alerteze administratorul în cazul unor probleme majore (configurabile): licențiere, detecție virusi, actualizări de produs disponibile); 6. permite integrarea cu un server Syslog pentru raportarea evenimentelor antivirus; 7. permite instalarea serviciului de SMNP pentru raportarea statusului mașinilor din cadrul componentei de management; 8. permite crearea unei copii de siguranță a bazei de date a consolei de administrare, la cerere sau programat, stocata local, pe un server FTP sau în rețea. **Protecție stații și servere fizice si virtualizate – caracteristici minime:** Soluția antivirus: - permite instalarea personalizată a modulelor; - include un „vaccin" anti-ransomware, cu actualizări de la producător, pentru protecția	

						împotriva tuturor amenințărilor cunoscute de tip ransomware, prin imunizarea stațiilor și serverelor, chiar daca sunt infectate și blocarea procesului de criptare; - include protecție împotriva atacurilor zero-day de tip exploit (atacuri direcționate); - include modul avansat de securitate – HyperDetect, bazat pe tehnologii de tip „machine learning tunabil" proiectat special pentru a detecta atacuri avansate și activitati suspecte în faza pre-executie; - include modul avansat de securitate pentru protecție împotriva: atacurilor direcționate (Targeted Attack - APT), fisierelor suspecte și traficului la nivel de rețea suspect, exploit-urilor, ransomware și grayware. Fiecărui tip de amenințare menționat, i se vor putea stabili, independent, un nivel de protecție dorit: permisiv, normal, agresiv includere în sandbox, ce va putea trimite manual sau automat fișiere, unde vor putea fi „detonate" pentru o analiză în profunzime; - include două variante de analiza a sandbox-ului: doar monitorizare sau blocare cu două tipuri de acțiuni de remediere: implicită și de siguranța. Pentru acțiunea implicită: doar raportare, dezinfecție, ștergere și transmitere în carantină. Pentru acțiunea de siguranța: ștergere sau permutare în carantină; - include modul de detectare, corelare si răspuns la evenimente de tip EDR („endpoint detection and response") capabil sa identifice	

						amenințări avansate sau atacuri in curs de desfășurare; **Protecție și securitate pentru serverele de mail Microsoft Exchange(2019, 2016, 2013 cu rol de Edge Transport sau Mailbox):** Soluția de protecție a serverelor de Exchange: - oferă protecție antivirus, antispam (inclusiv antiphishing), precum și filtrare de atașamente și conținut, prin integrarea cu serverul Microsoft Exchange cu posibilitatea de scanarea antivirus la cerere a bazelor de date Exchange; - asigură scanarea atașamentelor și a conținutului mesajelor în timp real, fără a afecta vizibil performanța serverului de mail; - asigură actualizarea antivirus automat la un interval de maxim 1 ora, precum si la cerere; - include, pe lîngă detecția pe baza de semnături, scanarea euristică comportamentală pentru a proteja sistemul de virușii necunoscuți prin detectarea codurilor; - oferă opțiuni multiple de acțiune la identificarea unui atașament virusat (dezinfectare, ștergere, mutare în carantină); - oferă protecție anti-spyware (cu bază de semnături actualizabilă) pentru a preveni furtul de date confidențiale; - oferă protecție antispam (cu o bază de semnături actualizabilă. Modulul antispam va trebui să includă un filtru URL cu o baza de adrese URL cunoscute a fi folosite în	

						mesaje spam, precum și un filtru de caractere pentru detectarea automata a mesajelor scrise cu caractere chirilice sau asiatice; - oferă filtru RBL care să identifice spam-ul prin sincronizarea cu anumite baze de date online care conțin liste de servere de mail cunoscute ca fiind la originea acestui tip de mesaje; - oferă un serviciu/filtru online pentru îmbunătățirea protecției împotriva valurilor de spam nou apărute; - oferă posibilitatea de a defini politici de filtrare antivirus, antispam, a conținutului sau atașamentelor pentru diferite grupuri sau utilizatori; - asigură actualizarea produsului va fi configurabilă și se va putea realiza de pe internet, direct sau printr-un proxy, sau din cadrul rețelei de pe un server de actualizare propriu; - oferă statistici atît referitoare la scanarea antivirus cît și la scanarea antispam; - se integrează în cadrul consolei de management unitar al soluției antivirus în consola centrală unică.	

Semnat:_____ Numele, Prenumele: **Vitalie CELONENCO** În calitate de: **Administrator**

Ofertantul: **„RTS ONE" S.R.L.** Adresa: **mun. Chișinău, str. Mit. Bănulescu-Bodoni 59/B of. 815**