ANUNȚ DE PARTICIPARE

Achiziționarea pachetelor software aferente securității informaționale

1. **Denumirea autorității contractante:** Banca Națională a Moldovei
2. **IDNO:** 79592
3. **Adresa:** bd. Grigore Vieru 1
4. **Numărul de telefon:** 022 822 237 / 022 822 338
5. **Adresa de e-mail și de internet a autorității contractante:** achizitii.contracte@bnm.md, **www.bnm.md**
6. **Adresa de e-mail sau de internet de la care se va putea obține accesul la documentația de atribuire:** documentația de atribuire este anexată în cadrul procedurii în SIA „RSAP" M-Tender
7. **Cumpărătorul/Beneficiarul invită operatorii economici interesați, care îi pot satisface necesitățile, să participe la procedura de achiziție** a pachetelor software aferente securității informaționale:

Nr. d/o	Cod CPV	Denumirea bunurilor	Unitatea de măsură	Cantitatea	Specificarea tehnică deplină solicitată	Valoarea estimată, fără TVA, MDL
Lotul 1: Soluție de protecție, securitate, patch management și disk encryption pentru locurile de muncă						
1.1	48760000-3	Soluție de protecție, securitate, patch management și disk encryption pentru locurile de muncă	buc	1	*Tip: Subscriere anuală pentru soluția de protecție și securitate, pentru 580 locuri de muncă (PC/laptop/VDI) și 750 căsuțe poștale pentru perioada 12.01.2021-12.01.2022).* *Cantitate: Este responsabilitatea Ofertantului de a determina modelul de licențiere luând în calcul:* *- 580 locuri de muncă (PC/laptop, VDI) , 750 căsuțe poștale,* *- Patch management pentru 200 locuri de muncă,* *- Disk Encryption management pentru 100 locuri de muncă.* *Produsul antivirus oferit trebuie să ocupe locurile de top în testele internaționale independente cu renume mondial în domeniu (certificări „AV-TEST", „VIRUS BULLETIN'S", „REAL-WORLD PROTECTION", „MALWARE PROTECTION")* ***Caracteristici generale ale produsului:***	

					Produsul va 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.* • *Protecție și securitate pentru telefoanele mobile de tip smartphone cu sistem de operare iOS sau Android.* • *Protecție și securitate pentru serverele email Microsoft Exchange.* ***<u>Consola de management:</u>*** *Pachetul de instalare să fie 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 să poată a fi importa în:* 1. *VMware vSphere* 2. *Citrix XenServer* 3. *Microsoft Hyper-V* 4. *KVM.* *Consola de management să fie livrată cu o baza de date inclusă, non-relațională.* *Soluția trebuie să:* • *fie scalabilă, astfel ca oricare dintre roluri sau servicii să poată fi instalate separat sau împreună pe aceeași sau mai multe VDI-uri.* • *asigure următoarele roluri: server cu baza de date, server de comunicație, server de actualizare, server de web.* • *asigure posibilitatea de a instala serviciile de scanare centralizată pentru mediile virtuale VMware și Citrix prin task din consola de management.*	

					• *includă un modul load balancer pentru performanța și redundanță* • *includă mecanisme de configurare a disponibilității pentru serverul cu baze de date (clustering).* ***<u>Cerințe generale produs:</u>*** *Soluția trebuie să:* 1. *includă un unul sau mai multe module de update server prin care să asigure actualizarea componentelor și a semnăturilor.* 2. *permită activarea/dezactivarea actualizărilor automate de produs/semnături și a consolei de management.* 3. *transmită alerte de ne funcționalitate, cu 30 de minute înainte de actualizare.* 4. *permită vizualizarea unui jurnal de modificări în care sunt precizate istoric: versiunea consolei de management, data versiunii, funcții noi si îmbunătățiri, probleme rezolvate, probleme cunoscute* 5. *afișeze notificările și alertele existente, să alerteze administratorul în cazul unor probleme majore (configurabile): licențiere, detecție viruși, actualizări de produs disponibile).* 6. *permită integrarea cu un server Syslog pentru raportarea evenimentelor antivirus.* 7. *permită instalarea serviciului de SMNP pentru raportarea statusului mașinilor din cadrul componentei de management.* 8. *permită 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. ***<u>Inventarierea rețelei – managementul securității</u>*** *Produsul trebuie să:* - *se integreze cu domenii Active Directory multiple, VMware vCenter, Citrix Xen și să importe inventarul acestor platforme.* - *permită descoperirea mașinilor din Microsoft Hyper-V, Red Hat VM, Oracle VM, KVM.* - *permită descoperirea stațiilor fizice neintegrate în Active Directory (Workgroup) cu ajutorul Network discovery.* - *ofere opțiuni de căutare, sortare și filtrare după numele sistemului, sistem de operare si adresa IP.* - *permită instalarea la distanță sau manual a clienților antivirus pe mașini fizice și virtuale.* - *permită selectarea modulelor componente atunci când se creează pachetul clientului care se instalează pe mașinile fizice/virtuale.* - *permită lansarea de task-uri de scanare, actualizare, instalare, dezinstalare la distanță pentru clientul antivirus.* - *ofere posibilitatea de repornire a mașinilor fizice de la distanță.* - *ofere informații detaliate despre fiecare task inițiat și afișarea statutului lui.* - *permită configurarea centralizată a clienților antivirus prin intermediul politicilor.* - *ofere în consola de management informații detaliate ale obiectelor*	

					din consola: Nume, IP, Sistem de operare, Grup, Politica atribuită, Ultimele actualizare, Versiunea produsului, Versiunea de semnături. - *permită descoperirea tuturor aplicațiilor instalate pe toate stațiile și serverele din rețea.* ***<u>Politici:</u>*** *Produsul trebuie să:* - *permită configurarea setărilor clientului antivirus prin intermediul unei singure politici ce conține setări pentru toate module* - *conțină opțiuni specifice de activare/dezactivare și configurare a funcționalităților precum scanarea antivirus la cerere, firewall, controlul accesului la Internet, controlul aplicațiilor, scanarea traficului web, controlul dispozitivelor, power user.* - *permită aplicarea politicilor pe mașini client, grupuri de mașini, pool-uri de resurse (VMware), domeniu, unități organizaționale sau useri de active directoy.* - *poată fi schimbată automat în funcție de: User-ul logat, IP sau clasa de IP, Gateway-ul alocat, DNS serverul alocat, Clientul este/nu este în accesai rețea cu infrastructura de management, Tipul rețelei (lan, wireless).* ***<u>Monitorizare și raportare:</u>*** *Produsul trebuie să:* - *permită setarea de opțiuni specifice pentru afișarea rapoartelor existente.*	

					- *deține un panou central care să afișeze statutul modulelor și rapoartele lor pentru perioadele de timp specificate.* - *conține rapoarte care prezinta statusul mașinilor clienților, al actualizărilor, fișierelor malware detectate, aplicațiile blocate, site-urilor web blocate.* - *trimită rapoarte către un număr nelimitat de adrese de email.* - *permită vizualizarea rapoartelor curente programate de administrator.* - *permită exportarea rapoartelor în format .pdf si detaliile ca format .csv.* - *includă un generator de rapoarte care să ofere posibilitatea de a investiga o problema de securitate pe baza mai multor criterii, menținând informațiile concise si ordonate corespunzător, să includă interogări precum: starea terminalului, evenimente terminal, evenimente Exchange.* - *ofere interogări legate de starea terminalului precum: tip mașină, infrastructură rețelei căreia aparține, datele agentului de securitate, starea modulelor de protecție, rolurile terminalelor.* - *ofere interogări legate de evenimente precum: calculatorul ținta pe care a avut loc evenimentul, tipul starea și configurația agentului de securitate instalat, starea modulelor și rolurilor de protecție instalate pe*	

					agentul de securitate, denumirea și alocarea politicii, utilizatorul autentificat în timpul evenimentului, evenimente (site-uri blocate, aplicații blocate, detecțiile etc) - *ofere interogări de evenimente Exchange precum: direcția traficului e-mail, evenimente de securitate (detectarea programelor de tip malware sau a fișierelor atașate), măsurile implementate în fiecare situație (curățarea, ștergerea, înlocuirea sau carantinarea fișierului, ștergerea sau respingerea e-mail-ului)* ***<u>Carantină:</u>*** - *Produsul trebuie să permită restaurarea fișierelor din carantină în locația originală sau într-o cale configurabilă.* - *Locația, fișierele și administrarea Carantinei trebuie să fie efectuată central din consola de management.* ***<u>Utilizatori:</u>*** - *Administrarea este necesar să fie efectuată pe bază de roluri multiple predefinite : Administrator companie, Administrator rețea, Reporter și alte roluri configurabile detaliat cu posibilitatea de selectare a serviciilor și obiectelor pentru care un utilizator poate face modificări.* - *Utilizatorii să poată fi importați din Microsoft Active Directory sau creați în consola de management.* - *Să fie posibilă deconectarea automată a*	

					oricărui tip de utilizator după un anumit timp. ***<u>Log-uri:</u>*** - *Soluția trebuie să permită înregistrarea acțiunilor utilizatorilor și să ofere informații detaliate pentru fiecare acțiune a unui utilizator cu posibilitatea de filtrare.* ***<u>Protecție stații și servere fizice si virtualizate – caracteristici minime:</u>*** *Soluția antivirus trebuie să:* - *permită instalarea personalizată a modulelor,* - *includă 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.* - *includă protecție împotriva atacurilor zero-day de tip exploit (atacuri direcționate).* - *includă module avansate de securitate, proiectate special pentru a detecta atacuri avansate și activități suspecte în faza pre-execuție, pentru protecție împotriva: atacurilor direcționate (Targeted Attack - APT), fișierelor suspecte și traficului la nivel de rețea suspect, exploit-urilor, ransomware și grayware cu posibilitatea de stabilire a nivelului de protecție dorit: permisiv, normal, agresiv cu posibilitatea extinderii nivelului de raportare*	

					pentru a include nivelurile superioare. - *includă un sandbox în cloud-ul producătorului, ce va putea trimite manual sau automat fișiere, unde vor putea fi „detonate” pentru o analiză în profunzime.* - *includă 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* ***<u>Cerințe de sistem:</u>*** - *Sisteme de operare pentru stații de lucru: Windows 7 și mai recent, Mac OS X 10.10. și mai recent, Red Hat Enterprise Linux / CentOS 6 și mai recent, Oracle Linux 6.3 și mai recent, Ubuntu 14.04 și mai recent, SUSE Linux Enterprise Server 11 și mai recent, OpenSUSE 42 și mai recent, Fedora 25 și mai recent, Debian 8.0 și mai recent.* - *Sisteme de operare Windows pentru servere: Windows Server 2008/2008 R2/2012/2012 R2/2016/2019.* ***<u>Administrare și instalare remote:</u>*** - *Pachetele de instalare trebuie să fie configurabile cu modulele necesare: firewall, content control, device control, power user.* - *Să existe posibilitatea de instalare manuală, sau automată la distanță, direct din consola de management.* - *Consola trebuie să includă o secțiune, „Audit”, unde se*	

					vor păstra toate acțiunile întreprinse de administratori și utilizatori ai consolei, cu informații detaliate: logare, editare, creare, delogare, permutare etc. - *Produsul trebuie să ofere posibilitatea de a crea pachetele de instalare de tip web installer sau kit full.* - *Produsul trebuie să permită selectarea clientului care va realiza descoperirea stațiilor din rețea, altele decît cele integrate în domen.* ***<u>Caracteristici și funcționalități principale ale modulului antivirus</u>*** *Produsul trebuie sa permită:* - *stabilirea acțiunilor întreprinse de modulul antivirus la detectarea unei amenințări noi. Astfel administratorul va putea alege între următoarele acțiuni:* 1. *implicită pentru fișiere infectate: interzice accesul, dezinfectează, ștergere, mută fișierele în carantină, nici o acțiune.* 2. *alternativă pentru fișierele infectate: interzice accesul, dezinfectează, ștergere, permutare fișiere în carantină.* 3. *acțiune implicită pentru fișierele suspecte: interzice accesul, ștergere, mută fișierele în carantină, nici o acțiune.* 4. *acțiune alternativă pentru fișierele suspecte: interzice accesul, ștergere, mută fișierele în carantină.*	

					- *scanarea automată în timp real cu setarea excepțiilor, definirea unor liste de excludere de la scanarea în timp real și la cerere a anumitor directoare, discuri, fișiere, extensii sau procese, să nu scaneze arhive sau fișiere mai mari de « x » MB, definirea nivelelor de profunzime pentru scanarea în arhive.* - *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 semnătura nu a fost lansata încă.* - *scanarea oricărui suport de stocare a informației (CD-uri, harduri externe, unități partajate etc).* - *scanarea automată a emailurilor la nivelul stației de lucru pentru POP3/SMTP.* - *configurarea căilor ce urmează a fi scanate la cerere.* - *cu ajutorul unei baze de date complete cu semnături de spyware și a euristicii de detecție a acestui tip de programe, produsul va trebui să ofere protecție anti-spyware.* - *setarea priorităților scanărilor programate.* - *configurarea scanării în cloud sau pe mașina de scanare instalată în rețea și parțial scanarea locală pentru stațiile ce nu au suficiente resurse hardware* - *administratorului să personalizeze și motoarele de scanare, având posibilitatea de a alege*	

					între mai multe tehnologii de scanare: scanare locală, scanarea hibrid cu motoare light, scanarea centralizată în Cloud-ul privat, scanare centralizată cu fallback pe scanare locală, scanare centralizată cu fallback* pe scanare hibrid.* - *setarea a tipurilor de detecție: bazate pe semnături, bazate de comportamentul fișierelor și bazatte pe monitorizarea proceselor.* - *scanarea paginilor web.* - *setarea a unei parole pentru protecția la dezinstalare.* - *modul de antiphishing.* - *protecție în timp real pe mașinile cu sistem de operare Linux in conformitate cu versiunea de kernel instalată.* - *instalarea clientului pe mașinile virtuale parte a unui pool doar pe mașina de tip template, după care se recompune pool-ul de mașini virtuale.* ***Firewall:*** - *sa ofere posibilitatea de a configura reguli de firewall pentru aplicații sau conectivitate.* - *modulul să poată fi instalat/dezinstalat la cerere.* - *să permită definirea de rețele de încredere pentru mașina destinație.* ***Protecția datelor:*** - *Produsul trebuie să permite blocarea datelor confidențiale (pin-ul cardului, cont bancar etc) transmise prin HTTP sau SMTP prin crearea unor reguli specifice.* ***Controlul conținutului:*** *Produsul trebuie să ofere un modul integrat dedicat*	

					controlului accesului la Internet cu următoarele particularități: blocarea accesului la Internet pentru anumite mașini client sau grupuri de mașini, blocarea accesului la Internet pe intervale orare, blocarea paginilor de internet care conțin anumite cuvinte cheie, controlul accesului numai la anumite pagini de internet specificate de administrator, blocarea accesului la anumite aplicații definite de administrator, restricționarea accesului pe anumite pagini de internet după anumite categorii prestabilite (ex: online dating, violenta, pornografie etc). ***<u>Controlul aplicațiilor:</u>*** *Pentru administrare și inventariere eficientă produsul trebuie să dețină un modul care va oferi posibilitatea de a:* - *efectua descoperirea aplicațiilor utilizate pe stațiile utilizatorilor grupate după: nume, versiune, descoperit la, găsit pe.* - *regăsi toate procesele descoperite în rețea, grupate după: nume, versiune, nume produs, versiune produs, editor/autor, descoperit la, găsit pe.* - *bloca rularea anumitor aplicații sau procese definite de administrator (inclusiv subprocese) după: cale fișier: local, CD-ROM, portabil sau rețea, hash , certificat.* ***<u>Controlul dispozitivelor:</u>*** *Produsul trebuie să conțină un modul pentru controlul dispozitivelor care:* - *poate fi instalat/dezinstalat*	

					conform setărilor stabilite. - *permite controlul următoarelor tipuri de dispozitive: Bluetooth Devices, CDROM Devices, Floppy Disk Drives, Security Policies 153, IEEE 1284.4, IEEE 1394, Imaging Devices, Modems, Tape Drives, Windows Portable, COM/LPT Ports, SCSI Raid, Printers, Network Adapters, Wireless Network Adapters, Internal and External Storage.* - *permite configurarea de reguli prin care se vor defini permisiunile pentru dispozitivele conectate la mașina client.* - *permite configurarea de excluderi pentru diferite tipuri de dispozitive pentru care s-au configurat reguli.* ***Power User:*** *Produsul trebuie să conțină un modul pentru setări specifice – power user care să:* - *poată fi instalat/dezinstalat în funcție de preferința administratorului.* - *permită posibilitatea de a acorda utilizatorilor drepturi de Power User, pentru a putea accesa și modifica setările clientului antivirus dintr-o consola disponibilă local pe mașina client.* - *permită administratorului soluției să suprascrie din consola setările aplicate de utilizatorii Power User.* ***Actualizare:*** *Produsul trebuie să ofere posibilitatea de efectuare a actualizărilor:*	

					- *la nivel de stație în mod silențios (fără avertizări).* - *folosind unul sau mai multe servere de actualizare.* - *pentru locațiile la distanță prin intermediul unui client antivirus care are și rol de server de actualizare.* ***<u>Protecție și securitate pentru telefoane mobile de tip smartphone:</u>*** *Produsul trebuie să ofere client de protecție pentru dispozitive mobile cu platforma Android (de la v. 2.2) și iOS (de la v 5.)* *Clientul mobil trebuie să:* - *permită asocierea unui dispozitiv cu un utilizator din Active Directory.* - *ofere posibilitatea instalării prin trimiterea unui email către utilizator cu detaliile de instalare.* - *permită activarea dispozitivului mobil în consola de management prin scanarea unui cod QR.* - *asigure disponibilitatea pachetele de instalare pe Apple App Store si Google Play.* - *să poată întreprinde următoarele acțiuni: blocarea dispozitivului; deblocarea dispozitivului; ștergerea datelor si revenirea la setările din fabrica; localizarea dispozitivului; scanarea dispozitivului(doar pentru cele cu sistem de operare Android); criptarea memoriei dispozitivului(doar pentru cele cu sistem de operare Android).* - *consola va permite raportarea dispozitivelor: active, inactive, deconectate, cu sistemul de operare modificat astfel încât utilizatorul sa aibă acces total asupra lui*	

					(rooted or jailbroken devices). - *întreprindă automat acțiuni în cazul în care un dispozitiv nu este conform cu setările dorite: Ignorare; Blocarea accesului; Blocarea dispozitivului; Ștergerea datelor si revenirea la setările din fabrica; Ștergerea dispozitivului din consola.* - *ofere posibilitatea de a impune blocarea dispozitivelor cu ajutorul unei parole cu complexitate și perioada de expirare configurabilă, posibilitate de autoblocare a dispozitivului după un număr de minute definite de administrator.* - *ofere posibilitate de a genera mai multe profiluri care vor stabili reguli de securitate pentru conectivitatea la Wi-Fi sau VPN (numai pentru sistemul de operare iOS) dar și unele legate de accesul la anumite pagini de internet. precum: permiterea, blocarea sau programarea pentru anumite zile si intervale orare a accesului la anumite pagini de internet; crearea unor excepții pentru blocarea sau permiterea accesului către anumite pagini de internet.* - *includă posibilitatea de configurare profilurile acces pagini de internet pentru sistemul de operare iOS cu opțiuni de activare sau dezactivare a: utilizarii browser-ului Safari; opțiunii de*	

					completare automata a informațiilor; alertării utilizatorului în cazul accesării unor pagini frauduloase; Javascript; Pop-up-urilor; Cookie-uri. ***<u>Protecție și securitate pentru serverele de mail Microsoft Exchange</u>*** *Soluția de protecție a serverelor de Exchange trebuie să:* - *ofere 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.* - *asigure scanarea atașamentelor și a conținutului mesajelor în timp real, fără a afecta vizibil performanța serverului de mail.* - *asigure actualizarea antivirus automat la un interval de maxim 1 ora, precum si la cerere.* - *includă, pe lîngă detecția pe baza de semnături, scanarea euristică comportamentală pentru a proteja sistemul de virușii necunoscuți prin detectarea codurilor.* - *ofere opțiuni multiple de acțiune la identificarea unui atașament virusat (dezinfectare, ștergere, mutare în carantină).* - *ofere protecție anti-spyware (cu bază de semnături actualizabilă) pentru a preveni furtul de date confidențiale.* - *ofere 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. - *ofere 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.* - *ofere un serviciu/filtru online pentru îmbunătățirea protecției împotriva valurilor de spam nou apărute.* - *ofere posibilitatea de a defini politici de filtrare antivirus, antispam, a conținutului sau atașamentelor pentru diferite grupuri sau utilizatori.* - *asigure 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.* - *ofere statistici atît referitoare la scanarea antivirus cît și la scanarea antispam.* - *se integreze în cadrul consolei de management unitar al soluției antivirus în consola centrală unică.* ***<u>Patch management:</u>*** *Soluție pentru managementul actualizării aplicațiilor exploatate* pentru 200 stații de lucru: Bitdefender GravityZone Patch Managemnt sau echivalentul.*	

					Soluția trebuie să acopere următoarele funcționalități minime: - *Integrarea clientului de patch managemnt cu clientul Antivirus, ca un modul separat.* - *Administrarea produsului trebuie să fie realizată din aceeași consolă de management ca și soluția de protecție antivirus pentru mediul fizic (stații și servere), mediul virtual (VDI-uri si servere virtuale), căsuțe de email Exchange si dispozitive mobile (Android si iOS).* - *Abilitatea de a funcționa în mod automat cu următoarele presetări:* a. *Programarea evaluării pentru patch-ul lipsă* b. *Programarea instalării automate, în baza categoriei de patch-uri (securitate / non-securitate)* c. *Posibilitatea de a amâna repornirea, dacă instalarea patch-ului o cere.* - *Opțiunea de a iniția scanarea, descoperirea și instalarea de patch-uri la cerere.* - *Posibilitatea de a vedea toate patch-urile care lipsesc din infrastructură și agregarea lor într-un inventar de patch-uri.* - *Vizibilitatea de patch-uri instalate și a celor lipsă pe stațiile de lucru.* - *Informații despre patch-uri instalate și motivul sau cauza instalării nereușite .* - *Posibilități de a instala rapid patch-uri lipsă.*	

					- *Posibilitatea de a stopa instalarea unuia sau a mai multor patch-uri/update-uri.* - *Notificarea periodică privind statul infrastructurii, patch-uri instalate, patch-uri lipsă* - *Stocarea locală a patch-urilor primite.* **- (7-Zip, Adobe: Acrobat/Bridge/Creative Cloud/Distiller/Dreamweaver/ Flash/Photoshop/Reader, Apache, Apache Tomcat, Apple: iCloud/iTunes/Mobile Device Support/QuickTime/Safari/Software Update, WebEx: Meeting Center/Productivity Tools, CitrixȘ Receiver/Single Sign-On/Delivery Controller/GoToMeeting/Online Plugin/Provisioning Services/Virtual Delivery Agent/XenApp/XenDesktop, FileZilla, Foxit: PhantomPDF/Reader, Gimp, TightVNC, Google: Chrome Browser for enterprise/Drive/Picasa, Greenshot, KeePass, LibreOffice, ImgBurn, Microsoft: .NET/Azure/DirectX/Dynamics /Exchange Server/Exchange System Manager/Forefront/Internet Explorer/Internet Information Server/Lync/Lync Server/Office/Outlook/Power BI Desktop/Report Viewer/Search/Services for Unix/Sharepoint/Skype/Silverlight/System Center Operations Manager/System Center Virtual Machine Manager/SQL Server/Systems Management Server/Virtual Machine/Virtual PC/Virtual Server/Visual Basic/Visual C++/Windows/Windows*	

					Defender/WSUS/Windows Mail/Kerberos, Firefox, Thunderbird, Notepad++, GeForce Experience, Opera, Oracle: OpenOffice/VM VirtualBox, Recuva, Prezi Desktop, RealVNC, PuTTY, Java, TeamViewer, PDF-Xchange, UltraVNC, VLC, VMware: Horizon View Client/Player/Tools/Workstation, WinSCP,Wireshark,Xmind) ***Disk Encryption*** *Soluție pentru managementul criptării discurilor pentru 100 calculatoare portabile: GravityZone Full DiskEncryption sau echivalentul.* *Soluția trebuie să acopere următoarele funcționalități minime:* *- Administrarea produsului trebuie să fie realizată din aceeași consolă de management ca și soluția de protecție antivirus pentru mediul fizic (stații și servere), mediul virtual (VDI-uri si servere virtuale), căsuțe de email Exchange si dispozitive mobile (Android si iOS).* *- Clientul pentru disk encryption nu trebuie să fie ca un modul separat în cadrul clientului Antivirus.* *- produsul trebuie să folosească mecanismul nativ de criptare al sistemului de operare: BitLocker pentru Windows si FileVault pentru Mac OSX.* *- Produsul trebuie să crypteze hard diskurile stațiilor de lucru integral.* *- Produsul trebuie să impună autentificarea utilizatorului înainte de startarea sistemei de operare (pre-boot authentication).* *- Produsul trebuie să păstreze cheile de criptare pe același*	

					server de management al protecției antivirus, managementul cheilor utilizate să fie efectuat din aceeași consolă comună, inclusiv recuperarea rapidă a cheilor la solicitarea autorizată. *- Produsul trebuie să ofere un raport complet asupra stării de criptare a dispozitivelor inclusiv: numele stației, IP-ul stației, sistemul de operare, ID-ul volumului/partiției, numele partiției, starea criptării partiției, tipul partiției: boot, non-boot, mărimea partiției în GB, ID-ul cheii de recuperare.* *- Produsul trebuie să asigure criptarea pentru Următoarele OS: Windows 7 Enterprise (with TPM); Windows 8.1 Pro/ Enterprise; Windows 10 Pro/ Enterprise; WindowsServer 2008 R2 (withTPM); WindowsServer 2012/2012 R2, WindowsServer 2016, OSX 10.9/ 10.10 / 10.11/ 10.12* ***Alte cerințe:*** *<u>Perioada de suport și menținere de la producător:</u>* *1. Pentru soluția ofertată se solicită a fi 12 luni pentru perioada 12.01.2021-12.01.2022.* *2. Producătorul trebuie să ofere suport 24/24, prin e-mail sau conectare de la distanță.* *<u>Notă</u>: Lucrările de instalare, configurare, punerea în funcțiune a soluției trebuie să fie executate de Ofertant, iar costul acestora trebuie să fie incluse în ofertă.* ***Termen de livrare:** obligatoriu în perioada 01.12.2020 - 25.12.2020, care include și timpul lucrărilor de instalare, configurare și punerea în funcțiune a soluției.*	
Valoarea estimată, lei, fără TVA, lot 1:						**214 050,83**

Lotul 2: Menținerea licențelor McAfee						
2.1	72268000-1	Servicii de asigurare a accesului la suport anual Business Support, sau echivalentul, pentru licențe McAfee Total Protection for Data Loss Prevention Software, pentru 400 licențe	buc	1	***Tip:*** *Serviciile de asigurare a accesului la suport anual Business Support, sau echivalentul, de la producătorul licențelor McAfee, sunt necesar să fie oferite în baza prelungirii termenului de prestare a serviciilor respective pentru perioada 14.12.2020-13.12.2021 pentru licențele McAfee Total Protection for Data Loss Prevention Software exploatate în cadrul Sistemului Informațional al BNM pentru 400 utilizatori și vor include:* *- prezentarea de către Prestator a unui document confirmativ parvenit de la compania producător, sau* *- publicarea informației confirmative pe site-ul producătorului.* ***Cerințe față de serviciile de suport:*** *- Daily product updates (.DATs, engines, etc.)* *- Product upgrades* *- Malware alerts with remediation analysis* *- Malware analysis service* *- Malware trend podcasts and blogs* *- Chat, web, and phone support with remote desktop control* *- 24/7 phone support (normally under 5 minutes to expert), unlimited number of calls to McAfee Technical Support* *- Automatic diagnostic and remediation tools* *- Online product test environments.* *Termen de prestare: obligatoriu în perioada 01.11.2020 - 14.12.2020 inclusiv.*	
2.2	48219100-7	Subscriere anuală pentru licența McAfee Web Protection, inclusiv 1 an de suport anual Business Support, sau echivalentul,	buc	1	***Tip: S****ubscriere anuale pentru perioada de la 07.11.2020 până la 06.11.2021 pentru licența pentru 400 utilizatori McAfee Web Protection exploatată în cadrul Sistemului Informațional al BNM, cu un an de suport de tipul Business*	

		pentru 400 utilizatori			*Support inclus, sau echivalentul* ***Cantitate:*** *1 licență pentru 400 utilizatori.* ***Cerințe față de serviciile de suport:*** *Daily product updates (.DATs, engines, etc.)* *Product upgrades* *Malware alerts with remediation analysis* *Malware analysis service* *Malware trend podcasts and blogs Chat, web, and phone support with remote desktop control 24/7 phone support (normally under 5 minutes to expert), unlimited number of calls to McAfee Technical Support Automatic diagnostic and remediation tools* *Online product test environments.* *Termen de livrare: obligatoriu în perioada 01.10.2020 - 07.11.2020 inclusiv.*	
Valoarea estimată, lei, fără TVA, lot 2:						**408 284,17**
Lotul 3: Menținerea soluției IBM Qradar						
3.1	72267000-4	Servicii de asigurare a accesului la menținerea anuală a instrumentului IBM Security Qradar	buc	1	***Tip:*** *Serviciile de asigurare a accesului la suport anual de la producătorul licențelor de tip Annual Software Subscription & Support Renewal 12 Months, sau echivalentul, pentru perioada 01.11.2020 - 31.10.2021, a instrumentului exploatat în cadrul Sistemului Informațional al BNM cu următoarea componență:* • *IBM Security QRadar SIEM All-in-One Virtual 3190 Install (licență de bază) – 1 buc.* *IBM Security QRadar Virtual SIEM Event Capacity Increase of 100 EPS Install (pachete adiționale) – 9 buc.* ***Termen de prestare:*** *Confirmarea prestării serviciilor trebuie să fie prezentată obligatoriu în perioada 01.10.2020 - 30.10.2020 inclusiv, și va include:*	

					- furnizarea de către Prestator a unui document confirmativ parvenit de la compania producător, sau *- publicarea informației confirmative pe site-ul producătorului.*	
3.2	72267000-4	Servicii de asigurare a accesului la menținerea anuală a modulului IBM Security QRadar Vulnerability Manager	buc	1	***Tip:*** *Serviciile de asigurare a accesului la suport anual de la producătorul licențelor de tip Annual Software Subscription & Support Renewal 12 Months, sau echivalentul, a modulului IBM Security QRadar Vulnerability Manager, trebuie să fie egalată cu perioada de suport pentru Instrumentul IBM Security Qradar indicat la prima poziție, până la 31.10.2021, cu următoarea componență:* • *IBM QRadar Software Node Install License - 1 licență pentru consola de roluri de software* • *IBM Security QRadar Vulnerability Manager Software 60XX Install License – 1 licență pentru scanarea la vulnerabilități a 256 resurse informaționale (assets) și managementul de configurare standard a 50 de resurse* ***Termen de prestare:*** *Confirmarea prestării serviciilor trebuie să fie prezentată obligator în perioada 01.10.2020 - 30.10.2020 inclusiv, și va include:* *- furnizarea de către Prestator a unui document confirmativ parvenit de la compania producător, sau* *- publicarea informației confirmative pe site-ul producătorului.*	
Valoarea estimată, lei, fără TVA, lot 3:						**155 443,34**
Lotul 4: ***Soluție integrată pentru gestionarea aplicațiilor și dispozitivelor mobile***						
4.1	48730000-4	Soluție integrată pentru gestionarea aplicațiilor și dispozitivelor mobile, cu 12 luni	buc	1	***Tip:*** *Licență pentru soluția integrată pentru gestionarea aplicațiilor și dispozitivelor mobile pentru 50 utilizatori, cu 12 luni suport standard de la*	

		suport standard de la Producător inclus			*Producător inclus, care sa cuprindă tehnologii moderne pentru gestionarea aplicațiilor și dispozitivelor mobile cu un grad de protecție ridicat.* ***Cantitate:*** *Este responsabilitatea Ofertantului de a determina modelul de licențiere luând în calcul asigurarea cu licență pentru 50 utilizatori cu posibilitatea asignării până la 5 dispozitive per utilizator precum și posibilitatea extinderii ulterioare a numărului de licențe.* ***Nota:*** *Ofertantul va veni cu o soluție care va acoperi partea de software necesară pentru întreaga soluție cu respectarea cerințelor specificate mai jos:* ***<u>Cerințe tehnice și specifice:</u>*** *Sistemul propus trebuie să fie o soluție inovatoare, care să asigure următoarele cerințe:* ***1. Cerințe pentru Securitatea datelor corporative:*** • *Controlul securizat al accesului la datele corporative;* • *Autentificare bifactorială la datele corporative;* • *Prevenirea pierderilor de date (DLP);* • *Posibilitatea de implementare a politicilor de criptare (dispozitiv, SD);* • *Posibilitatea de securizare și control pentru E-mail și DLP:* - *Control asupra atașamentelor email;* - *Control asupra datelor inserate sau copiate;* • *Posibilitatea de securizare și control al browser-ului mobil;* • *Posibilitatea de ștergere condiționată a datelor corporative de pe dispozitivele mobile;* • *Posibilitatea de a lucra offline (nu necesită o conexiune permanentă la*	

					server pentru identificarea și eliminarea amenințărilor pe dispozitive); • *Partajarea datelor corporative de cele personale(BYOD);* • *Posibilitatea de creare a canalului VPN securizat per aplicație (inclusiv Windows);* ***2.Cerințe pentru Managementul Aplicațiilor:*** • *Identificarea aplicațiilor mobile instalate și posibilitatea de distribuție a aplicațiilor noi;* • *Posibilitatea de categorizare a aplicațiilor mobile;* • *Posibilitatea de creare a listelor admise/interzise de aplicații mobile;* • *Posibilitatea de creare a restricțiilor pentru rețele wifi* • *Managementul aplicațiilor mobile (magazine intern de aplicații mobile);* • *Publicare și livrare centralizată sigură a aplicațiilor mobile;* • *Containerizarea aplicațiilor mobile;* ***3. Cerințe pentru Managementul dispozitivelor;*** • *Posibilitatea de încadrare a dispozitivelor mobile personale, în mediul corporativ (BYOD);* • *Posibilitatea utilizatorilor de auto-înrolare a dispozitivelor mobile (self-service) în sistem;* • *Posibilitatea de integrare a soluției cu infrastructura existentă a întreprinderii;* - *Active Directory;* - *Aplicații interne a companiei (aplicații Web, Mobile);* - *FileServer;* - *SIEM;*	

					• *Managementul conținutului dispozitivului mobil;* • *Managementul dispozitivelor mobile;* • *Posibilitatea de creare a modului de lucru KIOSK;* • *Geo-localizarea dispozitivelor mobile;* • *Suport pentru o gamă extinsă de platforme:* - *Windows 10 Desktop;* - *MacOS;* - *Android;* - *iOS;* • *Sistemul trebuie să ofere funcții avansate de gestionare pentru PC-urile Windows 10 precum:* - *personalizarea aspectului sistemului;* - *executarea scripturilor PowerShell (.ps1);* - *executarea de scripturi pentru modificarea registrului (.reg);* - *setarea BitLocker pentru criptarea discului;* - *gestionarea drepturilor utilizatorului;* - *setarea accesului la funcțiile Windows (meniul de setări);* - *instalarea oricărui GPO prin registru;* - *gestionarea sistemului de fișiere;* - *instalarea de drivere;* - *instalarea aplicațiilor LOB;* - *instalarea pachetelor software;* - *dezinstalarea software-ului preinstalat;* - *gestionarea imprimantei, etc.;* ***4. Cerințe pentru Serverul de administrare:*** • *Instalarea componentelor serverului soluției nu trebuie să necesite preinstalarea unui sistem de operare separat și a unei baze de date separate, precum și a licențelor lor separate*	

					• *Posibilitatea de a instala componente suplimentare de server:* - *pentru a asigura funcționarea sistemului cu disponibilitate ridicată (high availability)* - *posibilitatea utilizării în scopuri de testare înainte de a adăuga orice funcționalitate în mediul de lucru* • *Soluția trebuie să asigure extinderea cu ușurință a dispozitivelor gestionate* • *Posibilitatea de update a soluției direct din consola de administrare, fără implicarea directă a producătorului* • *Android Enterprise suport pentru dispozitivele BYOD* ***5.Certificări conform standar delor internaționale:*** • *FIPS 140-2;* • *ISO/IEC 27001:2013;* • *Common Criteria Certification;* *Cerința de certificare poate fi demonstrata prin prezentarea copiei certificatului, sau referință pe saitul producătorului.* ***Alte cerințe obligatorii:*** *<u>Perioada de suport și menținere de la producător:</u>* *3. Pentru soluția ofertată se solicită a fi pentru o perioadă de 12 luni din data acceptanței soluției.* *4. Producătorul trebuie să ofere:* *- suport 24/24, prin e-mail sau conectare de la distanță,* *- asigurarea accesului la update-uri si Baza de cunoștințe (Knowledge Base + Product Updates)* *<u>Notă</u>: Lucrările de instalare, configurare (inclusiv configurarea politicilor inițiale), punerea în funcțiune a soluției precum și transferul*	

					de cunoștințe trebuie să fie executate de Ofertant, iar costul acestora trebuie să fie incluse în ofertă. ***Termen de livrare:*** *30 de zile lucrătoare din data intrării în vigoare a contractului care include și timpul lucrărilor de instalare, configurare și punerea în funcțiune a soluției.*	
Valoarea estimată, lei, fără TVA, lot 4:						**136 048,34**
Valoarea estimată totală, lei fără TVA						**913 826,68**

8. **Admiterea sau interzicerea ofertelor alternative: nu se admite.**

9. **Termenii și condițiile de prestare:** *Toate bunurile/serviciile vor fi livrate și/sau prestate de către Vânzător/Prestator la sediul Cumpărătorului/Beneficiarului în termenele indicate pe fiecare lot în parte. Vânzătorul/Prestatorul va asigura livrarea bunurilor și/sau prestarea serviciilor în corespundere cu toate cerințele înaintate.*

10. **Termenul de valabilitate a contractului:** *31.12.2020 (după caz).*

11. **Contract de achiziție rezervat atelierelor protejate sau că acesta poate fi executat numai în cadrul unor programe de angajare protejată (după caz): Nu**

12. **Scurta descriere a criteriilor privind eligibilitatea operatorilor economici care pot determina eliminarea acestora și a criteriilor de selecție; nivelul minim (nivelurile minime) al (ale) cerințelor eventual impuse; se menționează informațiile solicitate (DUAE, documentație):**

Nr. d/o	Descrierea criteriului/cerinței	Mod de demonstrare a îndeplinirii criteriului/cerinței:	Nivelul minim/ Obligativitatea
1	Formularul ofertei	*Original confirmat prin semnătura electronică – conform formularului F3.1. din documentația de atribuire*	Da
2	Garanție pentru ofertă	***Forma garanției:*** *a) Garanția pentru ofertă prin transfer la contul autorității contractante, conform următoarelor date bancare:* *Beneficiarul plății: Banca Națională a Moldovei* *Denumirea Băncii: Banca Națională a Moldovei* *Codul fiscal: 79592* *IBAN: MD12NB000000000004914852* *Contul bancar: NBMDMD2X* *<u>cu nota</u> "Pentru garanția pentru ofertă la procedura de achiziție prin LD"* ***sau,*** *b) Oferta va fi însoțită de o Garanție pentru ofertă (emisă de o bancă) conform formularului F3.2 din secțiunea a 3-a – Formulare pentru depunerea ofertei din documentația de atribuire*	Da
3	Garanția de bună execuție	***Forma garanției de bună execuție:*** *a. Garanția de bună execuție prin transfer la contul autorității contractante, conform următoarelor date bancare:* *Beneficiarul plății: Banca Națională a Moldovei* *Denumirea Băncii: Banca Națională a Moldovei*	Da *(se va prezenta de către ofertantul câștigător la încheierea contractului)*

		Codul fiscal: 79592 *IBAN: MD65NB00000000004914771* *Contul bancar: NBMDMD2X* *cu nota "Pentru garanția de bună executare a contractului la procedura de achiziție prin LD"* ***sau*** *b. Garanția de bună execuție emisă de o bancă conform formularului F3.3 din documentația de atribuire.*	
4	Specificații tehnice	*Original confirmat prin semnătura electronică – conform formularului F4.1. din documentația de atribuire*	Da
5	Specificații de preț	*Original confirmat prin semnătura electronică – conform formularului F4.2. din documentația de atribuire*	Da
6	Formularul DUAE	*Original confirmat prin semnătura electronică*	Da
7	Măsuri de identificare a clientului, de monitorizare a activităților şi tranzacțiilor, conform procedurilor interne ale Băncii Naționale a Moldovei cu privire la prevenirea și combaterea spălării banilor și finanțării terorismului.	*Chestionar pentru Furnizor/Prestator – Varianta scanată de pe original sau original/copie confirmată prin semnătura electronică – conform formularului F3.4. din documentația de atribuire*	Da (la solicitare)
8	Certificatul de înregistrare a întreprinderii/Extrasul din Registrul de stat al persoanelor juridice, emis de către Camera Înregistrării de Stat / I.P. „Agenția Servicii Publice" sau organul împuternicit conform țării de reşedință a ofertantului	*Varianta scanată de pe original confirmată prin semnătura electronică*	Da (la solicitare)
9	Certificat de atribuire a contului bancar eliberat de banca deținătoare de cont după data punerii în aplicare a codurilor IBAN	*Varianta scanată de pe original confirmată prin semnătura electronică*	Da (la solicitare)
10	Raport financiar	*Copia ultimului raport financiar pentru anul 2019, semnat de reprezentatul companiei de audit, de contabilul certificat sau avizate de către Biroul Național de Statistică al Republicii Moldova –copii certificate conform cu originalul confirmată prin semnătura electronică a Ofertantului*	Da (la solicitare)

11	Demonstrarea experienței operatorului economic în domeniul de activitate aferent obiectului contractului ce urmează a fi atribuit	*Ofertantul trebuie să posede o experiență specifică în prestarea serviciilor și/sau livrarea bunurilor similare de cel puțin 1 an în domeniu, reputație bună, să fie dotat cu tehnică necesară şi să dispună de competențe profesionale, echipament şi alte resurse, inclusiv servicii post-vânzare, precum şi competențe manageriale, experiență specifică, personal calificat necesar pentru realizarea contractului şi alte capacități necesare pentru a executa contractul de achiziție publică la calitatea solicitată, pe toată perioada de valabilitate. Pentru demonstrarea îndeplinirii acestor cerințe operatorul economic completează capitolele aferente în DUAE și Declarația privind lista principalelor prestări servicii și/sau livrări de bunuri similare în ultimii ani (F.3.5) cu nominalizarea cel puțin a 2 (două) contracte în baza căruia se întrunesc cerințele stabilite. În scopul verificării și confirmării informațiilor declarate, Ofertantul trebuie să fie dispus la solicitare să prezinte documente suport ca copie (extras) ale respectivului/ respectivelor contract/ contracte, astfel încât autoritatea contractantă să poată identifica natura serviciilor prestate și/sau bunurilor livrate, valoarea acestora și prețul.*	Da (la solicitare)
12	Demonstrarea accesului la personalul necesar pentru îndeplinirea corespunzătoare a obiectului contractului ce urmează a fi atribuit (personalul de specialitate care va avea un rol esențial în îndeplinirea acestuia)	*Cerințe suplimentare pentru lotul 1, 4:* *- Ofertantul trebuie să aibă cel puțin o referință de instalare pentru soluția propusă.* *- Ofertantul trebuie să prezinte dovezi că poate pune la dispoziția Beneficiarului pentru executarea contractului de achiziție publică specialiști calificați certificați de către Producătorul soluției care vor fi responsabili pentru instalarea/configurarea soluției ofertate în conformitate cu cerințele stabilite de Beneficiar (să fie anexate certificatele corespunzătoare).*	Da (la solicitare)
13	Actul care atestă dreptul de livrare a bunurilor/prestare a serviciilor	*Copia certificatului ce atestă relația Ofertantului cu Producătorul sau copia certificatului de partener autorizat al producătorului sau autorizației de livrare/prestare - Varianta scanată de pe original confirmată prin semnătura electronică*	Da (la solicitare)

IMPORTANT: ***În conformitate cu Legea privind achizițiile publice nr.131 din 03.07.2015 și anume, art.65 alin. (4), prezentarea ofertei presupune în mod obligatoriu depunerea „ofertei tehnice (F4.1), ofertei financiare (F4.2), formularului DUAE și garanția pentru ofertă”.***

13. **Criteriul de evaluare aplicat pentru adjudecarea contractului:** *Prețul cel mai scăzut, fără TVA.*

Evaluarea va fi efectuată pe fiecare lot separat, cu corespunderea cerințelor față de ofertant şi corespunderea tuturor cerințelor tehnice minime obligatorii privind obiectul achiziției.

14. **Termenul limită de depunere/deschidere a ofertelor:**

- **până la ora: 14:00**
- **pe data: 07.09.2020**

15. **Adresa la care trebuie transmise ofertele sau cererile de participare:**

Ofertele vor fi depuse electronic prin intermediul SIA „RSAP" M-Tender.

16. **Termenul de valabilitate a ofertelor: 60 zile calendaristice**

17. **Locul deschiderii ofertelor:** *SIA „RSAP" M-TENDER.*

Ofertele întârziate vor fi respinse

18. **Limba sau limbile în care trebuie redactate ofertele sau cererile de participare:** *limba română.*

19. **Alte informații relevante: *nu sunt***

20. **Denumirea și adresa organismului competent de soluționare a contestațiilor:**
Agenția Națională pentru Soluționarea Contestațiilor
Adresa: mun. Chișinău, bd. Ștefan cel Mare și Sfânt nr.124 (et.4), MD 2001;
Tel/Fax/email: 022-820 652, 022 820-651, contestatii@ansc.md

21. **Data publicării anunțului de intenție sau, după caz, precizarea că nu a fost publicat un astfel de anunț:** *Buletin nr.4 din 28.01.2020.*

22. **Data transmiterii spre publicare a anunțului de participare: 10.08.2020**

Conducătorul grupului de lucru: Aureliu CINCILEI *(semnat electronic)*