

FIȘA DE DATE A ACHIZIȚIEI (FDA)

Următoarele date specifice referitoare la bunurile și la serviciile solicitate vor completa, suplimenta sau ajusta prevederile instrucțiunilor pentru ofertanți (IPO). În cazul unei discrepante sau al unui conflict, prevederile de mai jos vor prevala asupra prevederilor din IPO.

1. Dispoziții generale

Nr.	Rubrica	Datele Autorității Contractante/Organizatorului procedurii
1.1.	Autoritatea contractantă/Organizatorul procedurii, IDNO:	Agenția asigurare resurse și administrare patrimoniu a Ministerului Apărării 1006601001229
1.2.	Obiectul achiziției:	Pachete software și sisteme informatice, Pachete software antivirus conform necesităților Armatei Naționale.
1.3.	Numărul și tipul procedurii de achiziție:	Conform SIA RSAP
1.4.	Tipul obiectului de achiziție:	Licitație deschisă
1.5.	Codul CPV:	48000000-8
1.6.	Sursa alocațiilor bugetare/banilor publici și perioada bugetară:	Ministerul Finanțelor
1.7.	Administratorul alocațiilor bugetare:	Agenția asigurare resurse și administrare patrimoniu a Ministerului Apărării
1.8.	Partenerul de dezvoltare (după caz):	-
1.9.	Denumirea cumpărătorului, IDNO:	Agenția asigurare resurse și administrare patrimoniu a Ministerului Apărării
1.10.	Destinatarul bunurilor, IDNO:	Centrul comunicații și informatică
1.11.	Limba de comunicare:	De stat
1.12.	Locul/Modalitatea de transmitere a clarificărilor referitor la documentația de atribuire	Adresa: Prin SIA RSAP Tel: 022-25-22-09 25-23-57 25-23-00 Fax: 022 25 20 49 E-mail: vitalie.rohac@army.md Persoana de contact: ROHAC VITALIE
1.13.	Contract de achiziție rezervat atelierelor protejate	-
1.14.	Tipul contractului:	Vânzare-cumpărare
1.15.	Condiții speciale de care depinde îndeplinirea contractului(neobligatoriu):	-

2. Listă bunurilor și specificații tehnice:

Nr. d/o	Cod CPV	Denumirea bunurilor solicitate	U/M	Cantitatea	Specificarea tehnică deplină solicitată. Standarde de referință	Valoarea estimată fără TVA
1.	48000000-8	Pachete software și sisteme informatice	buc	1	OS Licenses: Microsoft Windows Server 2019 +50 call-uri. WinSvrSTDCore ENG LicSAPk OLP 16Lic A Gov CoreLic; WinSvrCAL 2019 ENG OLP A Gov DvcCAL - licențe permanente pentru 50 PC-uri. I. Cerințe minime de calificare a ofertanților: 1.1. Producătorul trebuie să ofere suport 24/7, prin e-	57500,00

					<p>mail sau conectare de la distanță, inclusiv suport local din partea partenerului.</p> <p>1.2. Prezentare a minim 2 certificate tehnice al ofertantului;</p> <p>1.3. Lucrările de instalare, configurare, punerea în funcțiune a soluției trebuie să fie executate de Ofertant, iar costul acestora trebuie să fie incluse în ofertă.</p> <p>1.4. Ofertantul trebuie sa fie certificat ISO 9001 și 27001. Prezentarea documentelor justificate este obligatorie.</p> <p>1.5. Prezentarea autorizării de la Producător (MAF);</p> <p>1.6. Autorizarea de la Producător a partenerului vis-a-vis de dreptul de a oferi suport tehnic pe teritoriul R. Moldova;</p> <p>Termen livrare: pînă la 30 zile de la data intrării în vigoare a contractului, care include și timpul lucrărilor de instalare, configurare și punerea în funcțiune a soluției.</p>	
2.	48000000-8	Pachete software antivirus	buc	1	<p>Soft Antivirus (Produsul Antivirus va acoperi următoarea infrastructură: PC-uri fizice și virtualizate, servere fizice și virtualizate, căsuțe poștale pe Exchange și mobile/tablete (Android & IOS), 760 licențe, pînă la 1140 căsuțe poștale pe Exchange; Patch Management pentru 760 dispozitive, 36 luni; Full Disk Encryption pentru 70 dispozitive, 36 luni)</p> <p>CARACTERISTICI GENERALE ALE PRODUSULUI</p> <p>Produsul este o platformă integrată pentru managementul securității, gândită ca o soluție modulară de protecție și securitate pentru 735 calculatoare, 5 servere fizice, 10 servere virtuale, 10 dispozitive mobile și peste 1000 căsuțe poștale pentru o perioadă de 36 luni. Produsul conține următoarele module:</p> <p>A. O consola de management care asigura funcționalități de administrare dintr-o singură consolă;</p> <p>B. Protecție stații și servere fizice/virtuale:</p> <ul style="list-style-type: none"> - Windows 10,8.1,7, Vista (SP1), XP (SP3), Mac OS X 10.12.x, 10.11.x, 10.10.x, 10.9.x, 10.8.x . - Windows Server 2003/2008/2008 R2/2012/2012 R2/2016/2019. - Red Hat Enterprise Linux / CentOS 5.6 sau mai recent, Oracle Linux 6 sau mai recent, Ubuntu 10.04 LTS sau mai recent, SUSE Linux Enterprise Server 11 sau mai recent, OpenSUSE 11 sau mai recent, Fedora 15 sau mai actual, Debian 5.0 sau mai recent. <p>C. Protecție și securitate pentru telefoanele mobile de tip smartphone cu sistem de operare iOS și Android;</p> <p>D. Protecție și securitate pentru serverele email Microsoft Exchange.</p> <p>E. Integrare SIEM.</p> <p>A. CONSOLA DE MANAGEMENT</p> <p>1. Instalare și configurare:</p> <p>1.1.Pachetul de instalare va fi livrat ca o mașină virtuală preinstalată care conține toate rolurile și serviciile necesare. Consola nu va necesita o licența suplimentară pentru sistemul de operare. Imaginea de tip template va putea fi importată în unul din următoarele sisteme de operare:</p> <ul style="list-style-type: none"> 1.1.1.Vmware vSphere 1.1.2.Microsoft Hyper-V 1.1.3.Red Hat Enterprise Virtualization 	775850,00

				<p>1.1.4.KVM</p> <p>1.1.5.Oracle VM etc.</p> <p>1.2. Consola de management se livrează cu o baza de date inclusă care este de tip non-relațională, pentru o funcționare cât mai rapidă, fără a fi nevoie de licențe adiționale.</p> <p>1.3. Soluția va fi scalabilă, astfel ca oricare dintre roluri sau servicii pot fi instalate separat pe mai multe mașini virtuale sau pe aceeași mașină virtuală.</p> <p>1.4. Rolurile principale trebuie să fie cel puțin similare cu: Serverul cu bază de date, Serverul de comunicație, Serverul de actualizare, Serverul de Web.</p> <p>1.5. Să asigure posibilitatea de a instala serviciile de scanare centralizată pentru mediile virtuale Vmware și Citrix prin task din consola de management.</p> <p>1.6. Soluția va include adițional și un modul de balansare (loadbalancer) pentru cazurile în care mai multe mașini virtuale ale componentei de management sunt instalate cu același rol (pentru LoadBalancing și performanță/redundanță).</p> <p>1.7. Soluția va include un mecanism de configurare a disponibilității pentru Serverul cu baze de date (clustering pentru redundanță). Astfel, baza de date se va putea instala de mai multe ori, pe mai multe mașini virtuale.</p> <p>1.8. Să includă posibilitatea de a fi accesată atât de pe stațiile de lucru cât și de pe dispozitivele mobile (tabletă, smartphone).</p> <p>2. Cerințe generale:</p> <p>2.1. Interfața consolei de management va fi cel puțin în două limbi (engleză și română).</p> <p>2.2. Interfața clientului de securitate, care se instalează pe stații și servere, va avea posibilitatea de a fi instalată cel puțin în două limbi (engleză și română).</p> <p>2.3. Manualul de instalare a produsului va fi în limba română și sau engleză.</p> <p>2.4. Manualul de administrare a produsului va fi în limba română și sau engleză.</p> <p>2.5. Soluția va include un modul de update server prin care se asigură actualizarea de produs și a semnăturilor.</p> <p>2.6. Soluția va permite activarea/dezactivarea actualizărilor de produs/semnături.</p> <p>2.7. Soluția va permite stabilirea actualizării automate a consolei de management prin stabilirea recurenței zilnice, săptămânale sau lunare, dar și prin stabilirea intervalului orar în care acesta se va actualiza. De asemenea, va permite și trimiterea unei alerte de ne funcționalitate, cu 30 de minute înainte de actualizare.</p> <p>2.8. Pentru o mai bună urmărire a actualizărilor consolei de management, soluția permite vizualizarea unui jurnal de modificări în care sunt precizate istoric:</p> <p>2.8.1. versiunea consolei de management</p> <p>2.8.2. data versiunii</p> <p>2.8.3. funcții noi și îmbunătățiri</p> <p>2.8.4. probleme rezolvate</p> <p>2.8.5. probleme cunoscute</p> <p>2.9. Notificările – prezente în interfață, notificările necitite sunt evidențiate, trimise către una sau mai multe adrese de email, alertează administratorul în cazul unor probleme majore: licențiere, detecție viruși, actualizări de produs disponibile.</p> <p>2.10. Soluția va permite integrarea cu un server Syslog pentru raportarea evenimentelor anti malware.</p> <p>2.11. Soluția va permite instalarea serviciului de</p>	
--	--	--	--	---	--

				<p>SMNP prin care se pot raporta statusul mașinilor din cadrul componentei de management.</p> <p>2.12. Soluția va permite crearea unei copii de siguranță a bazei de date a consolei de administrare, la cerere sau programată, putând fi stocată local, pe un server FTP sau în rețea.</p> <p>3. Panou de monitorizare și raportare (Dashboard):</p> <p>3.1. Rapoartele din panoul de monitorizare vor putea fi configurate specificând numele raportului, tipul raportului, ținta raportului, opțiuni specifice pentru orice tip de raport.</p> <p>3.2. Panoul central conține rapoarte pentru toate modulele suportate.</p> <p>3.3. Rapoartele din panoul central de comandă permit: adăugarea altor rapoarte, ștergerea lor și rearanjarea.</p> <p>4. Inventarierea rețelei – managementul securității:</p> <p>4.1. Soluția se va integra cu domenii Active Directory multiple, VmwarevCenter, Citrix Xen și importa inventarul acestor platforme.</p> <p>4.2. Pentru integrarea cu Active Directory, se va putea defini și intervalul (în ore) de sincronizare și forța sincronizarea.</p> <p>4.3. Se va permite descoperirea mașinilor din Microsoft Hyper-V, Red Hat VM, Oracle VM, KVM.</p> <p>4.4. Se va permite descoperirea stațiilor fizice neintegrate în Active Directory (Workgroup) cu ajutorul Network discovery.</p> <p>4.5. Soluția va oferi opțiuni de căutare, sortare și filtrare după numele sistemului, sistem de operare și adresa IP.</p> <p>4.6. Soluția va permite instalarea la distanță sau manual a clienților anti malware pe mașini fizice/virtuale.</p> <p>4.7. Soluția va permite selectarea modulelor componente, atunci când se creează pachetul clientului care se instalează pe mașinile fizice/virtuale.</p> <p>4.8. Soluția va permite lansarea de task-uri de scanare, actualizare, instalare, dezinstalarea la distanță pentru clientul anti malware.</p> <p>4.9. Soluția va oferi posibilitatea de repornire a mașinilor fizice de la distanță.</p> <p>4.10. Soluția va oferi informații detaliate despre fiecare task și va afișa dacă task-ul s-a finalizat sau nu cu succes.</p> <p>4.11. Soluția va permite configurarea centralizată a clienților anti malware prin intermediul politicilor.</p> <p>4.12. 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.</p> <p>4.13. Soluția permite descoperirea tuturor aplicațiilor instalate pe toate stațiile și serverele din rețea, prin rularea unui task din consola de administrare. Astfel, administratorul va putea descărca pachetele pentru protecția stațiilor și serverelor pe care rulează SO Windows, Linux și Mac.</p> <p>5. Politici:</p> <p>5.1. Soluția va permite configurarea setărilor clientului anti malware prin intermediul unei singure politici ce conține setări pentru toate modulele.</p> <p>5.2. Politica va conține opțiuni specifice de</p>
--	--	--	--	--

				<p>activare/dezactivare și configurarea funcționalităților precum scanarea anti malware la cerere, firewall, controlul accesului la Internet, controlul aplicațiilor, scanarea traficului web, controlul dispozitivelor, utilizator cu drepturi privilegiate (poweruser).</p> <p>5.3. Soluția va permite aplicarea politicilor pe mașini client, grupuri de mașini, pool-uri de resurse (VMware), domeniu, unități organizaționale sau utilizatori din Active Directory.</p> <p>5.4. Politica să poată fi schimbată automat în funcție de:</p> <p>5.4.1. User-ul logat pe stație</p> <p>5.4.2. IP sau clasa de IP al stației</p> <p>5.4.3. Gateway-ul alocat</p> <p>5.4.4. DNS serverul alocat</p> <p>5.4.5. Clientul este/nu este în aceeași rețea cu infrastructura de management</p> <p>5.4.6. Tipul rețelei (lan, wireless)</p> <p>6. Rapoarte:</p> <p>6.1. Soluția va permite generarea rapoartelor care prezintă statutul mașinilor clienților din punct de vedere al actualizărilor, fișierelor malware detectate, aplicațiile blocate, site-urilor web blocate.</p> <p>6.2. Rapoartele programate pot fi trimise către un număr nelimitat de adrese de email (nu este nevoie să aibă un cont în consola de management).</p> <p>6.3. Soluția va permite vizualizarea rapoartelor curente programate de administrator.</p> <p>6.4. Soluția va permite exportarea rapoartelor în format .pdf și detaliile ca format .csv.</p> <p>6.5. Soluția va 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.</p> <p>6.6. Interogarea legată de starea terminalului include informații precum:</p> <p>6.6.1. tip mașină</p> <p>6.6.2. infrastructura rețelei căreia îi aparține terminalul</p> <p>6.6.3. datele agentului de securitate</p> <p>6.6.4. starea modulelor de protecție</p> <p>6.6.5. rolurile terminalelor.</p> <p>6.7. Interogarea legată de evenimente terminal include informații precum:</p> <p>6.7.1. calculatorul țintă pe care a avut loc evenimentul</p> <p>6.7.2. tipul starea și configurația agentului de securitate instalat</p> <p>6.7.3. starea modulelor și rolurilor de protecție instalate pe agentul de securitate</p> <p>6.7.4. denumirea și alocarea politicii</p> <p>6.7.5. utilizatorul autentificat în timpul evenimentului</p> <p>6.7.6. evenimente (site-uri blocate, aplicații blocate, detecțiile etc.)</p> <p>6.8. Interogarea legată de evenimente Exchange include informații precum:</p> <p>6.8.1. Direcția traficului e-mail</p> <p>6.8.2. Evenimente de securitate (detectarea programelor de tip malware sau a fișierelor atașate)</p> <p>6.8.3. Măsurile implementate în fiecare situație (curățarea, ștergerea, înlocuirea sau punerea în carantină a fișierului, ștergerea sau respingerea e-mail-ului)</p> <p>7. Carantina:</p> <p>7.1. Soluția va permite restaurarea fișierelor din carantină în locația originală sau într-o cale configurabilă.</p> <p>7.2. Locația, fișierele și administrarea Carantinei</p>
--	--	--	--	--

				<p>trebuie să fie efectuată central din consola de management.</p> <p>7.3. Permite descărcarea fișierelor din carantină doar pentru mașinile virtuale protejate prin modulul mediilor virtuale integrat cu VMware vShield.</p> <p>8. Utilizatori:</p> <p>8.1. Administrarea se va putea face pe bază de roluri.</p> <p>8.2. Roluri multiple predefinite: Administrator companie, Administrator rețea, Reporter sau rol personalizat.</p> <p>8.3. Administrator companie: administrează arhitectura consolei de management;</p> <p>8.4. Administrator rețea: administrează serviciile de securitate;</p> <p>8.5. Reporter: monitorizează și generează rapoarte.</p> <p>8.6. Utilizatorii pot fi importați din Microsoft Active Directory sau creați în consola de management.</p> <p>8.7. Se va permite configurarea detaliată a drepturilor administrative, permițând selectarea serviciilor și obiectelor pentru care un utilizator poate face modificări.</p> <p>8.8. Se va permite deconectarea automată a oricărui tip de utilizator după un anumit timp.</p> <p>9. Log-uri:</p> <p>9.1. Înregistrarea acțiunilor utilizatorilor.</p> <p>9.2. Se vor oferi informații detaliate pentru fiecare acțiune a unui utilizator.</p> <p>9.3. Se va permite filtrarea acțiunilor utilizatorului după numele utilizatorului și după acțiune.</p> <p>10. Actualizare:</p> <p>10.1. Se permite definirea de locații de actualizare multiple.</p> <p>10.2. Se permite activarea/dezactivarea actualizărilor de produs și semnături.</p> <p>10.3. Se permite actualizarea produsului într-o rețea fără acces la Internet.</p> <p>10.4. Orice client antivirus să poată fi configurat să livreze update-urile către alt client antivirus</p> <p>10.5. Soluția va putea fi instalată pe un server de actualizare (update) care face posibilă stabilirea componentelor ce vor fi descărcate automat de pe internet, fără intervenția administratorului. Astfel, administratorul va putea descărca pachetele pentru protecția stațiilor și serverelor pe care rulează sistemul de operare Windows sau Linux sau poate descărca pachetele pentru modul de scanare centralizată în mediile de virtualizare VMwaresauHyper-V.</p> <p>10.6. În cadrul serverului de actualizare, pentru o mai bună urmărire a actualizărilor pachetele pentru protecția stațiilor și serverelor sau a pachetelor pentru modul de scanare centralizată, se va putea vizualiza un jurnal de modificări în care sunt precizate istoric:</p> <p>10.6.1. versiunea pachetului</p> <p>10.6.2. data versiunii</p> <p>10.6.3. funcții noi și îmbunătățiri</p> <p>10.6.4. probleme rezolvate</p> <p>10.6.5. probleme cunoscute</p> <p>10.7. Soluția permite testarea noilor versiuni de pachete de instalare ale clientului anti malware, 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:</p> <p>10.8. Ciclul rapid, gândit pentru un mediu de test în cadrul rețelei</p>	
--	--	--	--	---	--

				<p>10.9. Ciclu lent, gândit pentru restul rețelei (producție, servere critice etc.)</p> <p>10.10. Soluția permite stabilirea zonelor de test și critice din cadrul rețelei prin intermediul politicilor din consola de management.</p> <p>B. PROTECȚIE STAȚII și SERVERE FIZICE/VIRTUALE</p> <p>1. Caracteristici generale minimale și eliminatorii:</p> <p>1.1. Pentru reducerea la minim a consumului de resurse, soluția anti malware trebuie să permită instalarea personalizată a modulelor deținute (de exemplu, să permită instalarea soluției anti malware fără modulul de control al accesului web, modul de control al dispozitivelor sau modulul firewall).</p> <p>1.2. Pentru o mai buna 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.</p> <p>1.3. Vaccinul anti-ransomware primește actualizări de la producător, odată cu actualizarea semnăturilor produsului Anti malware.</p> <p>1.4. Pentru o mai buna protecție a stațiilor și serverelor, soluția include protecție împotriva atacurilor zero-day de tip exploit (atacuri direcționate).</p> <p>1.5. Include 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.</p> <p>1.6. Include un sandbox în cloud-ul producătorului, ce va putea trimite manual sau automat fișiere, unde vor putea fi „detonate” pentru o analiză în profunzime.</p> <p>1.7. Include două variante de analiza a sandbox-ului: doar monitorizare sau blocare cu două tipuri de acțiuni de remediere: implicită și de siguranță. Pentru acțiunea implicită: doar raportare, dezinfectie, ștergere și transmitere în carantină. Pentru acțiunea de siguranță: ștergere sau permutare în carantină.</p> <p>1.8. Modulul de Sandbox va include și posibilitatea de trimitere manuală a fișierelor în Sandbox-ul din cloud-ul producătorului. Astfel, dacă administratorul suspectează un fișier ca fiind malițios, îl poate trimite manual în Sandbox pentru a fi „detonat” și a afla verdictul. Va putea trimite mai multe fișiere de odată, cu posibilitate de a specifica dacă vor fi „detonate” individual sau toate în același timp. Acces modul va putea suporta „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. Aceste fișiere menționate anterior, vor putea fi detectate corect chiar dacă sunt incluse în arhive de tipul: 7z, ACE, ALZip, ARJ, BZip2, cpio, GZip,</p>
--	--	--	--	---

				<p>LHA, Linux TAR, LZMA Compressed Archive, MS Cabinet, MSI, PKZIP, RAR, Unix Z, ZIP, ZIP (multivolume), ZOO, XZ.</p> <p>2. Cerințe de sistem:</p> <p>2.1. Sisteme de operare pentru stații de lucru: Windows 10, Windows 8, Windows 7, Windows Vista (SP1), Windows XP (SP3) sau mai recent.</p> <p>2.2. Sisteme de operare embedded: Windows Embedded 8.1 Industry, Windows Embedded 8 Standard, Windows Embedded Standard 7, Windows Embedded POS Ready 7, Windows Embedded Enterprise 7, Windows Embedded POS Ready 2009, Windows Embedded Standard 2009, Windows XP Embedded with Service Pack 2, Windows XP Tablet PC Edition.</p> <p>2.3. Sisteme de operare pentru servere: Windows Server 2012 R2, Windows Server 2012, Windows Small Business Server (SBS) 2011, Windows Small Business Server (SBS) 2008, Windows Server 2008 R2, Windows Server 2008, Windows Small Business Server (SBS) 2003, Windows Server 2003 R2, Windows Server 2003 with Service Pack 1, Windows Home Server sau mai recent.</p> <p>2.4. Sisteme de operare Linux: Red Hat Enterprise Linux / CentOS 5.6 sau mai recent, Ubuntu 10.04 LTS sau mai recent, SUSE Linux Enterprise Server 11 sau mai recent, OpenSUSE 11 sau mai recent, Fedora 15 sau mai actual, Debian 5.0 sau mai recent.</p> <p>3. Administrare și instalare remote:</p> <p>3.1. Înainte de instalare, administratorul va putea particulariza pachetele de instalare cu modulele dorite: firewall, content control, device control, power user.</p> <p>3.2. Instalarea se va putea face în mai multe moduri:</p> <p>3.2.1. prin descărcarea directă a pachetului pe stația pe care se va face instalarea;</p> <p>3.2.2. prin instalarea la distanță, direct din consola de management.</p> <p>3.2.3. trimiterea pe email (oricare adrese) a pachetului de instalare pentru Windows, Linux, Mac.</p> <p>3.2.4. 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 respective pentru a minimiza traficul în WAN.</p> <p>3.2.5. 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.</p> <p>3.2.6. Din consola se va putea trimite o singură politică pentru configurarea integrală a clientului de pe stații/servere.</p> <p>3.2.7. Consola va include o secțiunea, unde se vor menționa toate acțiunile întreprinse fie de administratori, fie de reporteri, cu informații detaliate: logare, editare, creare, delogare, mutare etc.</p> <p>3.2.8. 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.</p> <p>3.2.9. Posibilitatea creării unui singur pachet de instalare, utilizabil pentru stații (fizice și/sau virtuale), servere (fizice și/sau virtuale), Exchange.</p> <p>3.2.10. Posibilitatea de a crea pachetele de instalare de tip web installer sau kit full.</p> <p>3.2.11. Administratorul va putea crea grupuri sau chiar subgrupuri, unde va putea muta stațiile/serverele</p>
--	--	--	--	---

				<p>din rețea pentru cele care nu sunt integrate în domeniu.</p> <p>3.2.12. Permite selectarea clientului care va efectua descoperirea stațiilor din rețea, altele decât cele integrate în domeniu.</p> <p>4. Caracteristici și funcționalități principale ale modulului anti malware:</p> <p>4.1. Soluția permite administratorului să stabilească acțiunea luată de produsul Anti malware la detectarea unei amenințări noi. Astfel, administratorul va putea alege între următoarele acțiuni:</p> <p>4.1.1. Acțiune implicită pentru fișiere infectate:</p> <p>4.1.1.1.interzice accesul</p> <p>4.1.1.2.dezinfectează</p> <p>4.1.1.3.ștergere</p> <p>4.1.1.4.mută fișierele în carantină</p> <p>4.1.1.5.nici o acțiune</p> <p>4.1.2. Acțiune alternativă pentru fișierele infectate:</p> <p>4.1.2.1.interzice accesul</p> <p>4.1.2.2.dezinfectează</p> <p>4.1.2.3.ștergere</p> <p>4.1.2.4.mută fișierele în carantină</p> <p>4.1.3. Acțiune implicită pentru fișierele suspecte:</p> <p>4.1.3.1.interzice accesul</p> <p>4.1.3.2.ștergere</p> <p>4.1.3.3.mută fișierele în carantină</p> <p>4.1.3.4.nici o acțiune</p> <p>4.1.4. Acțiune alternativa pentru fișierele suspecte:</p> <p>4.1.4.1.interzice accesul</p> <p>4.1.4.2.ștergere</p> <p>4.1.4.3.mută fișierele în carantină</p> <p>4.2. Scanarea automată în timp real va putea fi setată să nu scaneze arhive sau fișiere mai mari de « x » MB, mărimea fișierelor putând fi definită de administratorul soluției,</p> <p>4.3. Definirea nivelelor de profunzime pentru scanarea în arhive.</p> <p>4.4. Scanarea euristică comportamentală prin simularea unui calculator virtual în interiorul căruia sunt rulate aplicații cu potențial periculos, protejând sistemul de aplicații malițioase necunoscute prin detectarea codurilor periculoase a căror semnătură nu a fost lansată încă.</p> <p>4.5. Scanarea oricărui suport de stocare a informației (CD-uri, harduri externe, unități partajate etc). De asemenea, se va putea anula scanarea în cazul în care sunt detectate unități care au informații stocate mai mult de « x » MB.</p> <p>4.6. Scanarea automată a emailurilor la nivelul stației de lucru pentru POP3/SMTP.</p> <p>4.7. Definirea până la 16 nivele de profunzime pentru scanarea în arhive.</p> <p>4.8. Configurarea căilor ce urmează a fi scanate la cerere.</p> <p>4.9. Clienții anti malware pentru stațiile de lucru să permită definirea unor liste de excludere de la scanarea în timp real și la cerere a anumitor directoare, discuri, fișiere, extensii sau procese.</p> <p>4.10. 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.</p> <p>4.11. Posibilitatea de a configura scanările programate să se execute cu prioritate redusă</p> <p>4.12. Produsul anti malware poate fi configurat să folosească scanarea în cloud, și parțial scanarea locala. Pentru stațiile ce nu au suficiente resurse hardware,</p>	
--	--	--	--	---	--

				<p>scanarea se poate face cu o mașina de scanare instalată în rețea.</p> <p>4.13. Administratorul poate personaliza și motoarele de scanare, având posibilitatea de a alege între mai multe tehnologii de scanare:</p> <p>4.13.1. Configurarea scanării în cloud sau pe mașina de scanare instalată în rețea și parțial scanarea locală pentru stațiile ce nu au suficiente resurse hardware</p> <p>4.13.2. 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.</p> <p>4.13.3. Setarea tipurilor de detecție: bazate pe semnături, bazate de comportamentul fișierelor și bazate pe monitorizarea proceselor.</p> <p>4.13.4. Scanarea paginilor web.</p> <p>4.13.5. Setarea unei parole pentru protecție la dezințalare.</p> <p>4.13.6. Modul de antiphishing.</p> <p>4.13.7. Protecție în timp real pe mașinile cu sistem de operare Linux în conformitate cu versiunea de kernel instalată.</p> <p>4.13.8. Instalarea clientului pe mașinile virtuale parte a unui pool doar pe mașina de tip template, după care se recompune pool-ul de mașini virtuale.</p> <p>5. Firewall:</p> <p>5.1. Posibilitatea de a configura reguli de firewall pentru aplicații sau conectivitate.</p> <p>5.2. Modulul poate fi instalat/dezinstalat în funcție de preferința administratorului.</p> <p>5.3. Posibilitatea de a defini rețele de încredere pentru mașina destinație.</p> <p>6. Carantina:</p> <p>6.1. Produsul anti malware să permită trimiterea automata a fișierelor din carantină în locația originală sau într-o cale configurabilă.</p> <p>6.2. Trimiterea conținutului carantinei va putea fi expedit în mod automat, la un interval definit de administrator.</p> <p>6.3. Produsul anti malware să permită ștergerea automata a fișierelor din carantină mai vechi de o anumita perioada, pentru a nu încărca inutil spațiul de stocare.</p> <p>6.4. Posibilitatea de a restaura un fișier din carantină în locația lui originală.</p> <p>6.5. Modulul de carantină va permite re-scanarea obiectelor după fiecare actualizare de semnături.</p> <p>6.6. Locația, fișierele și administrarea Carantinei trebuie să fie efectuată central din consola de management.</p> <p>7. Protecția datelor:</p> <p>7.1. Produsul permite blocarea datelor confidențiale (pin-ul cardului, cont bancar etc.) transmise prin HTTP sau SMTP prin crearea unor reguli specifice.</p> <p>8. Controlul conținutului:</p> <p>8.1. Consola va avea integrat un modul dedicat controlului accesului la Internet cu următoarele particularități:</p> <p>8.1.1. Permite blocarea accesului la Internet pentru anumite mașini client sau grupuri de mașini.</p> <p>8.1.2. Permite blocarea accesului la Internet pe</p>
--	--	--	--	--

				<p>intervale orare.</p> <p>8.1.3. Permite blocarea paginilor de Internet care conțin anumite cuvinte cheie.</p> <p>8.1.4. Permite controlul accesului numai la anumite pagini de internet specificate de administrator;</p> <p>8.1.5. Permite blocarea accesului la anumite aplicații definite de administrator;</p> <p>8.1.6. Permite blocarea descărcării unor anumite tipuri de extensii de fișiere, definite de administrator (ex: .exe, .zip, .rar, .mp3 etc.)</p> <p>8.1.7. Permite restricționarea accesului pe anumite pagini de internet după anumite categorii prestabilite (ex: online dating, violență, pornografie etc.).</p> <p>9. Controlul aplicațiilor:</p> <p>9.1. Soluția va include o secțiune în consola de administrare unde se vor regăsi toate aplicațiile descoperite în rețea, grupate după: nume, versiune, descoperit la, găsit pe.</p> <p>9.2. Soluția va include o secțiune în consola de administrare unde se vor regăsi toate procesele negrupate descoperite în rețea, grupate după: nume, versiune, nume produs, versiune produs, editor/autor, descoperit la, găsit pe.</p> <p>9.3. Soluția include opțiunea de a permite sau a bloca rularea anumitor aplicații sau procese definite de administrator (inclusiv sub procese) după:</p> <p>9.3.1. Cale fișier: local, CD-ROM, portabil sau rețea;</p> <p>9.3.2. Hash;</p> <p>9.3.3. Certificat.</p> <p>10. Controlul dispozitivelor:</p> <p>10.1. Modulul poate fi instalat/dezinstalat în funcție de preferința administratorului.</p> <p>10.2. Modulul va permite controlul următoarelor tipuri de dispozitive:</p> <p>10.2.1. Bluetooth Devices</p> <p>10.2.2. CDROM Devices</p> <p>10.2.3. Floppy Disk Drives</p> <p>10.2.4. Security Policies 153</p> <p>10.2.5. IEEE1394, IEEE1284.4</p> <p>10.2.6. ImagingDevices</p> <p>10.2.7. Modems</p> <p>10.2.8. Tape Drives</p> <p>10.2.9. Windows Portable (including USB devices and ports)</p> <p>10.2.10. COM/LPT Ports</p> <p>10.2.11. SCSI Raid</p> <p>10.2.12. Printers</p> <p>10.2.13. NetworkAdapters</p> <p>10.2.14. Wireless NetworkAdapters</p> <p>10.2.15. InternalandExternalStorage</p> <p>10.3. Modulul va permite configurarea de reguli prin care se vor defini permisiunile pentru dispozitivele conectate la mașina client.</p> <p>10.4. Modulul va permite configurarea de excluderi pentru diferite tipuri de dispozitive pentru care s-au configurat reguli.</p> <p>11. Power User:</p> <p>11.1. Modulul poate fi instalat/dezinstalat în funcție de preferința administratorului.</p> <p>11.2. Modulul permite posibilitatea de a acorda utilizatorilor drepturi de Power User. Utilizatorii vor putea accesa și modifica setările clientului anti malware dintr-o consola disponibilă local pe mașina client.</p> <p>11.3. Administratorul va putea suprascrie din</p>
--	--	--	--	---

				<p>consola setările aplicate de utilizatorii Power User.</p> <p>12. Actualizare:</p> <p>12.1. Posibilitatea efectuării actualizării la nivel de stație în mod silențios (fără avertizări).</p> <p>12.2. Sistem de actualizare în trepte (cascadat) folosind unul sau mai multe servere de actualizare (cascadate).</p> <p>12.3. Actualizarea pentru locațiile remote prin intermediul unui client anti malware care are și rol de server de actualizare.</p> <p>C. PROTECȚIE ȘI SECURITATE PENTRU TELEFOANELE MOBILE DE TIP SMARTPHONE</p> <p>1. Cerințe minime de sistem:</p> <p>1.1. Produsul trebuie să ofere client de protecție pentru dispozitive mobile cu platforma Android (de la v. 2.2) și iOS (de la v 5.) sau mai recente</p> <p>2. Caracteristici:</p> <p>2.1. Permite asocierea unui dispozitiv cu un utilizator din Active Directory.</p> <p>2.2. Instalarea se face prin trimiterea unui email către utilizator cu detaliile de instalare.</p> <p>2.3. Activarea dispozitivului mobil în consola de management să se facă prin scanarea unui cod QR.</p> <p>2.4. Pachetele de instalare se vor putea descărca de pe Apple App Store și Google Play.</p> <p>2.5. Se vor putea întreprinde următoarele acțiuni:</p> <p>2.5.1. Blocarea dispozitivului;</p> <p>2.5.2. Deblocarea dispozitivului;</p> <p>2.5.3. Ștergerea datelor și revenirea la setările din fabrică;</p> <p>2.5.4. Localizarea dispozitivului;</p> <p>2.5.5. Scanarea dispozitivului (doar pentru cele cu sistem de operare Android);</p> <p>2.5.6. Criptarea memoriei dispozitivului (doar pentru cele cu sistem de operare Android);</p> <p>2.5.7. Consola va permite raportarea dispozitivelor: active, inactive, deconectate, cu sistemul de operare modificat astfel încât utilizatorul să aibă acces total asupra lui (rooted or jailbrokendevices).</p> <p>3. Setări de securitate:</p> <p>3.1. În cazul în care un dispozitiv nu este conform cu setările dorite, se vor putea întreprinde automat acțiunile:</p> <p>3.1.1. Ignorare;</p> <p>3.1.2. Blocarea accesului;</p> <p>3.1.3. Blocarea dispozitivului;</p> <p>3.1.4. Ștergerea datelor și revenirea la setările din fabrică;</p> <p>3.1.5. Ștergerea dispozitivului din consolă.</p> <p>3.2. Se va putea impune blocarea dispozitivelor cu ajutorul unei parole. Aceasta parolă va putea fi configurată să conțină:</p> <p>3.2.1. Parolă simplă sau complexă (în funcție de cerințele sistemului de operare);</p> <p>3.2.2. Numere și litere;</p> <p>3.2.3. O lungime minimă definită de administrator;</p> <p>3.2.4. Un număr minim de caractere speciale, definit de administrator;</p> <p>3.2.5. Perioada de expirare a parolei. Perioada va putea fi definită de administrator;</p> <p>3.2.6. Configurarea restricției refolosirii parolei;</p>	
--	--	--	--	--	--

				<p>3.2.7. Numărul de introduceri incorecte a parolei, de către utilizator;</p> <p>3.2.8. Perioada de autoblocare a dispozitivului după un număr de minute definite de administrator.</p> <p>3.3. Se vor putea 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.</p> <p>3.4. Profilurile de Wi-Fi vor conține următoarele opțiuni:</p> <p>3.4.1. Generale – se definește SSID precum și tipul securității rețelei;</p> <p>3.4.2. Setări TCP/IP – atât pentru protocolul IPv4, dar și pentru IPv6;</p> <p>3.4.3. Setări de proxy – dezactivat, automat sau configurat manual.</p> <p>3.5. Profilurile acces pagini de internet pentru sistemul de operare Android vor include opțiuni precum:</p> <p>3.5.1. Permitea, blocarea sau programarea pentru anumite zile și intervale orare a accesului la anumite pagini de internet;</p> <p>3.5.2. Crearea unor excepții pentru blocarea sau permiterea accesului către anumite pagini de internet.</p> <p>3.6. Profilurile acces pagini de internet pentru sistemul de operare iOS vor include opțiuni de activare sau dezactivare a:</p> <p>3.6.1. Utilizării browser-ului Safari;</p> <p>3.6.2. Opțiunii de completare automată a informațiilor;</p> <p>3.6.3. Alertării utilizatorului în cazul accesării unor pagini frauduloase;</p> <p>3.6.4. Java script;</p> <p>3.6.5. Pop-up-urilor;</p> <p>3.6.6. Cookie-uri.</p> <p>D. PROTECȚIE ȘI SECURITATE PENTRU SERVERELE DE MAIL MICROSOFT EXCHANGE</p> <p>1. Va consta în:</p> <p>1.1. Produsul va oferi protecție anti malware, anti spam (inclusiv antiphishing), precum și filtrare de atașamente și conținut, prin integrarea cu serverul Microsoft Exchange cu posibilitatea de scanare a antivirus la cererea bazelor de date Exchange.</p> <p>1.2. Produsul va asigura scanarea atașamentelor și a conținutului mesajelor în timp real, fără a afecta vizibil performanța serverului de mail.</p> <p>1.3. Actualizarea antivirus trebuie să poată fi făcută automat la un interval de maxim 1 oră, precum și la cerere.</p> <p>1.4. Modulul de protecție antivirus va trebui să includă și scanare euristica comportamentală, prin simularea unui calculator virtual în interiorul căruia sunt rulate și analizate aplicații cu potențial periculos, pentru a proteja sistemul de virușii necunoscuți prin detectarea codurilor periculoase a căror semnătură nu a fost lansată încă.</p> <p>1.5. Produsul va oferi opțiuni multiple de acțiune la identificarea unui atașament virusat (dezinfectare, ștergere, mutare în carantină).</p> <p>1.6. Produsul va oferi protecție anti-spyware pentru a preveni furtul de date confidențiale.</p> <p>1.7. Produsul va oferi protecție anti spam, cu o bază de semnături actualizată prin internet.</p> <p>1.8. Modulul antispam va trebui să includă un filtru URL cu o bază de adrese URL cunoscute a fi folosite în mesaje spam, precum și un filtru de caractere pentru</p>
--	--	--	--	---

				<p>detectarea automată a mesajelor scrise cu caractere chirilice sau asiatice.</p> <p>1.9. Produsul va trebui să 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.</p> <p>1.10. Produsul va trebui să ofere un serviciu/filtru online pentru îmbunătățirea protecției împotriva valurilor de spam nou apărute.</p> <p>1.11. Produsul va oferi posibilitatea de a defini politici de filtrare anti malware, anti spam, a conținutului sau atașamentelor pentru diferite grupuri sau utilizatori.</p> <p>1.12. 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.</p> <p>1.13. Produsul va trebui să ofere statistici atât referitoare la scanarea antivirus cat și la scanarea anti spam.</p> <p>1.14. Produsul se va integra în cadrul consolei de management unitar al soluției antivirus. Pentru ușurința accesului la setările produsului din diferite medii de operare, produsul va avea consola de administrare web.</p> <p>E. CERINȚE FAȚĂ DE PATCH MANAGEMENT:</p> <p>1. Soluția pentru managementul actualizării aplicațiilor exploatare* pentru 200 stații de lucru: Full Patch Managemnt.</p> <p>Soluția trebuie să acopere următoarele funcționalități minime:</p> <p>1.1. Integrarea clientului de patch management cu clientul Antivirus, ca un modul separat.</p> <p>1.2. 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 și servere virtuale), căsuțe de email Exchange și dispozitive mobile (Android si iOS).</p> <p>1.3. Abilitatea de a funcționa în mod automat cu următoarele presetări:</p> <p>1.3.1. Programarea evaluării pentru patch-ul lipsă.</p> <p>1.3.2. Programarea instalării automate, în baza categoriei de patch-uri (securitate / non-securitate).</p> <p>1.3.3. Posibilitatea de a amâna repornirea, dacă instalarea patch-ului o cere.</p> <p>1.4. Opțiunea de a iniția scanarea, descoperirea și instalarea de patch-uri la cerere.</p> <p>1.5. Posibilitatea de a vedea toate patch-urile care lipsesc din infrastructură și agregarea lor într-un inventar de patch-uri.</p> <p>1.6. Vizibilitatea de patch-uri instalate și a celor lipsă pe stațiile de lucru.</p> <p>1.7. Informații despre patch-uri instalate și motivul sau cauza instalării nereușite.</p> <p>1.8. Posibilități de a instala rapid patch-uri lipsă.</p> <p>1.9. Posibilitatea de a stopa instalarea unuia sau a mai multor patch-uri/update-uri.</p> <p>1.10. Notificarea periodică privind statutul infrastructurii, patch-uri instalate, patch-uri lipsă</p> <p>1.11. Stocarea locală a patch-urilor primite.</p> <p><i>*(7-Zip, Adobe: Acrobat / Bridge / Creative Cloud / Distiller / Dreamweaver / Flash / Photoshop / Reader, Apache, Apache Tomcat, Apple: iCloud / iTunes /</i></p>
--	--	--	--	--

				<p><i>Mobile Device Support / QuickTime / Safari / Software Update, WebEx: Meeting Center / Productivity Tools, Citrix Receiver / Single Sign-On / Delivery Controller / GoToMeeting / Online Plugin / Provisioning Services / Virtual Delivery Agent / XenApp / XenDesktop, FileZilla, Foxit: Phantom PDF / 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)</i></p> <p>F. CERINȚE FAȚĂ DE DISK ENCRYPTION</p> <p>1. Soluție pentru managementul criptării discurilor pentru 100 calculatoare portabile: Full Disk Encryption. Soluția trebuie să acopere următoarele funcționalități minime:</p> <p>1.1. 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 și servere virtuale), căsuțe de email Exchange și dispozitive mobile (Android și iOS).</p> <p>1.2. Clientul pentru disk encryption nu trebuie să fie ca un modul separat în cadrul clientului Antivirus.</p> <p>1.3. Produsul trebuie să folosească mecanismul nativ de criptare al sistemului de operare: BitLocker pentru Windows și FileVault pentru Mac OSX.</p> <p>1.4. Produsul trebuie să creeze hard diskurile stațiilor de lucru integral.</p> <p>1.5. Produsul trebuie să impună autentificarea utilizatorului înainte de startarea sistemului de operare (pre-boot authentication).</p> <p>1.6. 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.</p> <p>1.7. 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.</p> <p>1.8. 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</p>
--	--	--	--	--

G. CERINȚE FAȚĂ DE SERVICIILE DE IMPLEMENTARE ȘI CONFIGURARE

1.

1.1. Limba de comunicare și documentare va fi limba română

1.2. Ofertantul selectat va livra și instala licențele pentru soluția oferită.

1.3. Ofertantul selectat va efectua pregătirea mediului de instalare pentru soluția propusă, după care va asigura implementarea inițială a soluției aplicative în mediul de producție și mediul de testare al clientului.

1.4. Ofertantul selectat va efectua configurarea inițială a soluției, atât pentru mediul de producție, cât și mediul de testare. Prin configurare inițială (Furnizorul) înțelege setarea tuturor parametrilor aplicabili în corespundere cu cerințele (clientului), inclusiv configurarea și instalarea soluției oferite, setarea politicilor și testarea înainte de a fi pusă în producție.

1.5. În baza rezultatelor de la etapa de design, Ofertantul selectat va implementa toate configurările/personalizările agreate darea în exploatare a soluției.

1.6. Ofertantul va asigura integrarea soluției cu cel puțin următoarele aplicații terțe:

1.6.1. Integrarea cu Active Directory – pentru a asigura autentificarea utilizatorilor în cadrul soluției prin AD;

1.6.2. Integrarea cu platforma mobilă (telefoane, tablete) – pentru securizarea perimetrului de dispozitive mobile.

1.7. Ofertantul selectat va efectua instalarea soluției oferite în întreaga infrastructură a Ministerului Apărării inclusiv la toți utilizatorii finali (instalarea se va considera încheiată în momentul când toți utilizatorii vor avea instalat agentul și calculatorul va primi cel puțin o actualizare a bazelor și a agentului)

1.8. La sfârșitul etapei, Ofertantul va face o demonstrație a soluției și a modulelor care au fost acoperite, fapt care va servi drept unul din criteriile de acceptanță ale etapei de implementare.

1.9. După acceptanța finală a soluției, va fi activată în mod automat opțiunea de garanție post-implementare și suport. Perioada de garanție post-implementare și suport va fi de 36 luni de la data activării acestei opțiuni.

1.10. Serviciile de garanție post-implementare și suport se referă la serviciile oferite de către Ofertantul selectat adițional la serviciile de mentenanță și suport a licențelor, oferite direct de către producătorul licențelor.

1.11. Serviciile de garanție post-implementare și suport, vor include următoarele componente:

1.11.1. Gestionarea serviciului de actualizare a serverelor la ultimele actualizări oferite de producător;

1.11.2. Gestionarea incidentelor de securitate apărute pe perioada suportului activ;

1.11.3. Solicitărilor de schimbare a politicilor de securitate;

1.11.4. Solicități de analiza și corecție a politicilor de securitate în cadrul companiei implementate.

H. CERINȚELE FATA DE SERVICIILE DE INSTRUIRE

1.

				<p>1.1. Limba de comunicare și documentare va fi limba română</p> <p>1.2. În cadrul proiectului, Ofertantul va organiza sesiuni de instruire și transfer de cunoștințe pentru grupurile țintă în vederea formării setului de cunoștințe necesar pentru a permite echipei instruite să preia menținerea și configurarea ulterioară a soluției, în conformitate cu necesitățile companiei.</p> <p>1.3. Instruirea se va organiza pentru diferite grupuri țintă la sediul Cumpărătorului.</p> <p>1.3.1. Analist – nr. persoane stabilite de către client</p> <p>1.3.2. Administrator - nr. persoane stabilite de către client</p> <p>1.4. În acest sens, ca parte a ofertei, Ofertantul va prezenta ca parte a ofertei, un plan de instruire, în care se va indica ce tipuri de instruire va efectua Ofertantul, pentru ce categorie de utilizatori, precum și cuprinsul/agenda acestor instruirii.</p> <p>1.5. În afara instruirilor ce țin de utilizarea soluției, Ofertantul trebuie să efectueze și sesiuni de instruire pentru echipa de menținere din partea Cumpărătorului, în scopul asigurării unui nivel adecvat de cunoștințe și competențe, pentru a putea utiliza eficient instrumentele de configurare și dezvoltare disponibile în cadrul soluției.</p> <p>1.6. În cadrul serviciilor de implementare, pentru a asigura transferul necesar de cunoștințe către echipa Cumpărătorului, Ofertantul va fi de acord ca cel puțin o persoană să asiste la lucrările de parametrizare/configurare, stabilite de comun acord de către Părți.</p> <p>1.7. Ofertantul selectat la etapa de încheiere a contractului, va trebui să elaboreze și să convină cu Cumpărătorul următoarele elemente ale componentei de instruire:</p> <p>1.7.1. Strategia Ofertantului cu privire la instruire și programul de formare;</p> <p>1.7.2. Structura și componența pachetului de cursuri pentru formare și a manualelor de studiu pentru fiecare categorie de utilizator;</p> <p>1.7.3. Metodologia și procedurile de evaluare și control al eficienței și suficienței sesiunilor de instruire.</p> <p>1.8. În cadrul sesiunilor de instruire, Ofertantul va pune la dispoziția Cumpărătorului întreg setul de documentație al soluției, care să cuprindă cel puțin următoarele componente:</p> <p>1.8.1. Ghidurile administratorilor</p> <p>1.8.2. Ghidurile de instalare și configurare.</p> <p>1.8.3. Fișierele surse pentru toate configurările și personalizările realizate pe parcursul proiectului.</p> <p>II. Cerințe minime de calificare a ofertanților:</p> <p>1.7. Producătorul trebuie să ofere suport 24/7, prin e-mail sau conectare de la distanță, inclusiv suport local din partea partenerului.</p> <p>1.8. Prezentare a minim 2 certificate tehnice al ofertantului;</p> <p>1.9. Lucrările de instalare, configurare, punerea în funcțiune a soluției trebuie să fie executate de Ofertant, iar costul acestora trebuie să fie incluse în ofertă.</p> <p>1.10. Ofertantul trebuie să fie certificat ISO 9001 și 27001. Prezentarea documentelor justificate este obligatorie.</p> <p>1.11. Prezentarea autorizării de la Producător (MAF);</p>	
--	--	--	--	--	--

					<p>1.12. <i>Autorizarea de la Producător a partenerului vis-a-vis de dreptul de a oferi suport tehnic pe teritoriul R. Moldova;</i></p> <p><i>Termen livrare: pînă la 30 zile de la data intrării în vigoare a contractului, care include și timpul lucrărilor de instalare, configurare și punerea în funcțiune a soluției.</i></p>	
						833350,00

3. Pregătirea ofertelor

3.1.	Oferte alternative:	Nu vor fi acceptate
3.2.	Garanția pentru ofertă:	<p>a) Oferta va fi însoțită de o Garanție pentru ofertă (emisă de o bancă comercială) conform formularului F3.2 din secțiunea a 3-a – Formulare pentru depunerea ofertei sau</p> <p>b) Garanția pentru ofertă prin transfer la contul autorității contractante, conform următoarelor date bancare: Beneficiarul plății: AGENȚIA ASIGURARE RESURSE ȘI ADMINISTRARE PATRIMONIU A MINISTERULUI APĂRĂRII Denumirea Băncii: Ministerul Finanțelor - Trezoreria de Stat Codul fiscal: 1006601001229 IBAN: MD28TRPCAA518410A00572AA cu nota “Pentru garanția pentru ofertă” Termenul de valabilitate a garanției sa fie exact ca si termenul de valabilitate a ofertei.</p>
3.3.	Garanția pentru ofertă va fi în valoare de:	1% din valoarea ofertei fără TVA.
3.4.	Ediția aplicabilă a Incoterms și termenii comerciali acceptați vor fi:	Nu se aplică
3.5.	Termenul de livrare:	30 de zile de la înregistrarea contractului la Trezoreria regională Chișinău
3.6.	Locul livrării bunurilor:	Livrarea și instalarea se va efectua la adresa: Centru comunicații și informatică - or. Chișinău, șos. Hîncești 84.
3.7.	Metoda și condițiile de plată vor fi:	Achitarea va fi efectuată utilizând sistemul de e-facturare. Prin virament, în termen de 30 de zile bancare după prezentarea facturii fiscale
3.8.	Perioada valabilității ofertei va fi de:	45 zile
3.9.	Ofertele în valută străină:	Nu se acceptă

4. Depunerea și deschiderea ofertelor

4.1.	Locul/Modalitatea de depunerea ofertelor , este:	Ofertele vor fi prezentate în forma electronică prin SIA „RSAP”
4.2.	Termenul limită de depunere a ofertelor este:	Data: conform platformei SIA”RSAP”
4.3.	Persoanele autorizate să asiste la deschiderea ofertelor (cu excepția cazului când ofertele au fost depuse prin SIA “RSAP”).	Ofertanții sau reprezentanții acestora au dreptul să participe la deschiderea ofertelor, cu excepția cazului când ofertele au fost depuse prin SIA “RSAP”

5. Evaluarea și compararea ofertelor

5.1.	Prețurile ofertelor depuse în diferite valute vor fi convertite în:	lei MD
	Sursa ratei de schimb în scopul convertirii:	
	Data pentru rata de schimb aplicabilă va fi:	
5.2.	Modalitatea de efectuare a evaluării:	Prețul cel mai scăzut fără TVA, pentru fiecare lot în parte. Pentru ofertele cu același preț, suplimentar se va utiliza criteriu de selecție conform capacității economice și financiare.
5.3.	Factorii de evaluare vor fi următorii:	-

6. Adjudecarea contractului

6.1.	Criteriul de evaluare aplicat pentru adjudecarea contractului va fi:	Prețul cel mai scăzut fără TVA, pentru fiecare lot și prezentarea documentelor obligatorii solicitate (art. 20, alin. 8, Legea nr. 131 din 03.07.2015).
6.2.	Suma Garanției de bună execuție (se stabilește procentual din prețul contractului adjudecat):	5% din valoarea contractului, inclusiv TVA.
6.3.	Garanția de bună execuție a contractului:	a) Garanția de buna execuție (emisă de o bancă comercială) conform formularului F3.3 sau b) Garanția de buna execuție prin transfer la contul autorității contractante, conform următoarelor date bancare: Beneficiarul plății: AGENȚIA ASIGURARE RESURSE ȘI ADMINISTRARE PATRIMONIU A MINISTERULUI APĂRĂRII Denumirea Băncii: Ministerul Finanțelor - Trezoreria de Stat Codul fiscal: 1006601001229 IBAN: MD28TRPCAA518410A00572AA cu nota "Pentru garanția de bună execuție a contractului"
6.4.	Forma de organizare juridică pe care trebuie să o ia asocierea grupului de operatori economici cărora li s-a atribuit contractul	Nu se cere
6.5.	Numărul maxim de zile pentru semnarea și prezentarea contractului către autoritatea contractantă, de la remiterea acestuia spre semnare:	3 zile lucrătoare

Conținutul prezentei Fișe de date a achiziției este identic cu datele procedurii din cadrul Sistemului Informațional Automatizat "REGISTRUL DE STAT AL ACHIZIȚIILOR PUBLICE". Grupul de lucru pentru achiziții confirmă corectitudinea conținutului Fișei de date a achiziției, fapt pentru care poartă răspundere conform prevederilor legale în vigoare.

Conducătorul grupului de lucru: _____