Specificații tehnice (F4.1)

[Acest tabel va fi completat de către ofertant în coloana 4, iar de către autoritatea contractantă - în coloanele 1,2,3,5]

Numărul procedurii de achiziție: **ocds-b3wdp1-MD-1567079532361**din 29.08.2019

Denumirea achiziției: ***Extinderea și menținerea licențelor McAfee***

Cod CPV	Denumirea seviciilor	Specificarea tehnică deplină solicitată de către autoritatea contractantă	Specificarea tehnică deplină propusă de către ofertant	Standarde de referinţă
1	2	3	4	5
Lotul 2: Extinderea și menținerea licențelor McAfee				
48732000-8	**1**. ***Licență pentru 50 utilizatori pentru soluția de prevenire a scurgerii de informație McAfee Total Protection For Data Loss Prevention Appliance Software, sau echivalentul, inclusiv 1 an de suport standard***	***Tip:*** *Soluție de prevenire în mod automatizat a scurgerii de informații clasificate ale BNM și sporirea controlului asupra datelor în cadrul BNM (DLP - Data Loss Prevention), care va include control pentru:* - *Stații de lucru (endpoint)* - *Serviciul proxy (iCap)* - *Serviciul de poștă electronica (SMTP)* - *Monitorizarea rețelei (Network monitor).* ***Cantitate:*** *licență pentru 50 utilizatori.* ***Condiții generale:*** *Se solicită extinderea numărului de licențe McAfee Total Protection For Data Loss Prevention Appliance Software, sau echivalentul, inclusiv un an de suport, pentru 50 utilizatori.* *Notă: Luând în considerație că în BNM sunt deja în exploatare licențe pentru 350 utilizatori, în caz de oferire a altui produs*	***Produsul ofertat:*** ***McAfee Total Protection for DLP with 1 year business support, pentru 50 utilizatori*** ***Tip:*** *Soluție de prevenire în mod automatizat a scurgerii de informații clasificate ale BNM și sporirea controlului asupra datelor în cadrul BNM (DLP - Data Loss Prevention), care va include control pentru:* - *Stații de lucru (endpoint)* - *Serviciul proxy (iCap)* - *Serviciul de poștă electronica (SMTP)* - *Monitorizarea rețelei (Network monitor).* ***Cantitate:*** *licență pentru 50 utilizatori.* ***Condiții generale:*** *Se oferă extinderea numărului de licențe McAfee Total Protection For Data Loss Prevention Appliance Software, inclusiv un an de suport, pentru 50 utilizatori.* *Notă: Nu este cazul, ca se oferă extinderea cu 50 de utilizatori la cei existenți pentru produsul deja existent în cadrul BNM.*	

Digitally signed by Cornei Andrian
Date: 2019.09.19 11:00:32 EEST
Reason: MoldSign Signature
Location: Moldova

		decât McAfee DLP, Ofertantul trebuie să acopere cu licență pentru toți 400 utilizatori (50 noi + 350 existente pentru care se solicită menținerea în poziția 2). Totodată, va fi responsabil pentru livrarea, instalarea, configurarea (inclusiv configurarea politicilor inițiale) şi punerea în funcțiune a soluției și pentru asigurarea suportului la definirea/configurarea și exploatarea soluției pentru primul an de exploatare a acesteia. ***<u>Caracteristici generale:</u>*** *<u>Protecție Endpoint:</u>* - *să suporte sistemele de operare: Microsoft Windows 7 (32/64-bit), Microsoft Windows 8.1 (32/64-bit), Microsoft Windows 10 (32/64-bit).* - *să identifice conținutul chiar dacă acesta este arhivat (minimum 10 niveluri de arhivare).* - *să poată aplica politici bazate pe conținut confidențial pentru cel putin 300 de tipuri de fișiere.* - *să poată detecta documentele ce au fost clasificate deja (fie prin intermeniul unui instrument de clasificare a documentelor prin înscrierea în Metadate și/sau prin aplicare de marcări vizuale, fie prin faptul că documentul dat conține careva marcaje vizuale cu privire la clasa căreia aparține (ex. mențiuni în header/footer pentru documente word) sau în funcție de sursa documentului - aplicația prin intermediul căreia a fost creat).* - *agentul soluției să poată proteja minim 100.000 de documente indiferent dacă stația este Online sau Offline;* - *analiza conținutului să nu fie limitată la limba utilizată;* - *soluția trebuie să permită parametrizarea nivelului de utilizare a resurselor utilizate (procesor, RAM);* - *să protejeze informația confidențială la:* - *scrierea pe suporturi de stocare mobile (memorii USB, optice etc.);* - *trimisă prin intermediul serviciilor de poștă electronică;* - *încărcată pe web;*	*Totodată, ofertantul va fi responsabil pentru livrarea, instalarea, configurarea (inclusiv configurarea politicilor inițiale) şi punerea în funcțiune a soluției și pentru asigurarea suportului la definirea/configurarea și exploatarea soluției pentru primul an de exploatare a acesteia.* ***<u>Caracteristici generale:</u>*** *<u>Protecție Endpoint:</u>* - *suportă sistemele de operare: Microsoft Windows 7 (32/64-bit), Microsoft Windows 8.1 (32/64-bit), Microsoft Windows 10 (32/64-bit).* - *va identifica conținutul chiar dacă acesta este arhivat (minimum 10 niveluri de arhivare).* - *va putea aplica politici bazate pe conținut confidențial pentru cel putin 300 de tipuri de fișiere.* - *va putea detecta documentele ce au fost clasificate deja (fie prin intermediul unui instrument de clasificare a documentelor prin înscrierea în Metadate și/sau prin aplicare de marcări vizuale, fie prin faptul că documentul dat conține careva marcaje vizuale cu privire la clasa căreia aparține (ex. mențiuni în header/footer pentru documente word) sau în funcție de sursa documentului - aplicația prin intermediul căreia a fost creat).* - *agentul soluției va putea proteja minim 100.000 de documente indiferent dacă stația este Online sau Offline;* - *analiza conținutului nu va fi limitată la limba utilizată;* - *soluția va permite parametrizarea nivelului de utilizare a resurselor utilizate (procesor, RAM);* - *va proteja informația confidențială la:* - *scrierea pe suporturi de stocare mobile (memorii USB, optice etc.);* - *trimisă prin intermediul serviciilor de poștă electronică;*	

		- *copiată cu ajutorul clipboard-ului;* - *printată în fișier sau pe imprimantă;* - *scrisă pe un share în rețea;* - *folosită în aplicațiile network–based;* - *la efectuarea screenshot–ului ecranului.* - *să mențină înregistrări de audit privind activitatea agentului de endpoint;* - *să mențină înregistrări de audit privind activitatea agentului de endpoint;* - *soluția trebuie să dispună de mecanisme proprii de instalare a agenților pe stațiile de lucru sau alte sisteme, sau să permită integrarea cu Directory Services;* - *agentul de endpoint trebuie să fie compatibil, determinat prin testări, cu soluții de antivirus, firewall, criptare, backup și antispyware third-party;* - *agentul de endpoint trebuie să permită aplicarea politicilor folosind conținut înregistrat/ amprentat;* - *agentul de endpoint trebuie să aibă opțiunea de blocare a activității pentru situațiile de încălcare a politicii de securitate prestabilită (ex. - se încearcă upload-area de documente considerate confidențiale; - copierea pe SD card, USB flash drive / memory stick; - crearea de noi documente pe baza celor originale; - crearea de arhive și upload-area ulterioară a acestora (sau copierea pe USB flash);* - *construirea regulilor de protecție trebuie să se poată face și în funcție de cuvinte-cheie, expresii regulate și amprente (hash-uri);* - *construcția regulilor trebuie să includă suport pentru logica booleana incluzând AND, OR, sau alte declarații logice;* - *soluția trebuie să aibă abilitatea de a identifica fișierele bazându-se pe conceptul de true file type și nu doar pe extensia fișierelor;*	- *încărcată pe web;* - *copiată cu ajutorul clipboard-ului;* - *printată în fișier sau pe imprimantă;* - *scrisă pe un share în rețea;* - *folosită în aplicațiile network–based;* - *la efectuarea screenshot–ului ecranului.* - *va menține înregistrări de audit privind activitatea agentului de endpoint;* - *va menține înregistrări de audit privind activitatea agentului de endpoint;* - *soluția va dispune de mecanisme proprii de instalare a agenților pe stațiile de lucru sau alte sisteme, sau să permită integrarea cu Directory Services;* - *agentul de endpoint va fi compatibil, determinat prin testări, cu soluții de antivirus, firewall, criptare, backup și antispyware third-party;* - *agentul de endpoint permite aplicarea politicilor folosind conținut înregistrat/ amprentat;* - *agentul de endpoint are opțiunea de blocare a activității pentru situațiile de încălcare a politicii de securitate prestabilită (ex. - se încearcă upload-area de documente considerate confidențiale; - copierea pe SD card, USB flash drive / memory stick; - crearea de noi documente pe baza celor originale; - crearea de arhive și upload-area ulterioară a acestora (sau copierea pe USB flash);* - *construirea regulilor de protecție se va putea face și în funcție de cuvinte-cheie, expresii regulate și amprente (hash-uri);* - *construcția regulilor include suport pentru logica booleana incluzând AND, OR, sau alte declarații logice;* - *soluția are abilitatea de a identifica fișierele bazându-se pe conceptul de true file type și nu doar pe extensia fișierelor;*	

		- *trebuie să poată scana stația și să identifice documentele ce conțin informații clasificate (funcții de tipul descoperă - discovery);* - *să permită efectuarea de notificări customizate;* - *trebuie să fie capabilă să identifice nivelul de clasificare a documentelor din marcajele vizuale și să aplice regulile de protectie pe aceste documente.;* - *trebuie să fie capabilă să protejeze documente nemarcate ce au conținut ce provine din documente clasificate cu marcaje vizuale.* - *soluția trebuie să permită creare de politici în mod granular de permitere / blocare a dispozitivelor periferice pe baza informațiilor despre:* *a. ID Producator* *b. ID Model Dispozitiv Periferic* *c. Tipul de dispozitiv* *d. Clasa dispozitivului detectat de sistemul de operare* *e. BUS Conectare (USB, S-ATA, ETC.)* *f. Numele Dispozitivului* *g. Tipul sistemului de fișiere (NTFS/FAT/FAT32)* *h. Numele Volumului / Partiției (în cazul dispozitivelor de stocare date)* - *soluția trebuie să poată lua urmatoarele acțiuni la conectarea unui dispozitiv periferic:* *a. blocare: să nu permită instalarea acestuia;* *b. monitorizare: să genereze un eveniment ce conține detalii despre dispozitiv;* *c. forțare mod utilizare ReadOnly: în cazul dispozitivelor de stocare date, acestea se vor utiliza doar pentru citirea datelor de pe ele.* *d. soluția trebuie sa poata prevenii executarea de cod si aplicatii direct de pe dispozitive externe. De asemenea, trebuie sa vina si cu un mecanism de macare a aplicatiilor permise.*	- *va putea scana stația și să identifice documentele ce conțin informații clasificate (funcții de tipul descoperă - discovery);* - *permite efectuarea de notificări customizate;* - *este capabilă să identifice nivelul de clasificare a documentelor din marcajele vizuale și să aplice regulile de protectie pe aceste documente.;* - *este capabilă să protejeze documente nemarcate ce au conținut ce provine din documente clasificate cu marcaje vizuale.* - *soluția permite creare de politici în mod granular de permitere / blocare a dispozitivelor periferice pe baza informațiilor despre:* *a. ID Producator* *b. ID Model Dispozitiv Periferic* *c. Tipul de dispozitiv* *d. Clasa dispozitivului detectat de sistemul de operare* *e. BUS Conectare (USB, S-ATA, ETC.)* *f. Numele Dispozitivului* *g. Tipul sistemului de fișiere (NTFS/FAT/FAT32)* *h. Numele Volumului / Partiției (în cazul dispozitivelor de stocare date)* - *soluția poate lua următoarele acțiuni la conectarea unui dispozitiv periferic:* *a. blocare: nu va permite instalarea acestuia;* *b. monitorizare: generează un eveniment ce conține detalii despre dispozitiv;* *c. forțare mod utilizare ReadOnly: în cazul dispozitivelor de stocare date, acestea se vor utiliza doar pentru citirea datelor de pe ele.* *d. soluția poate prevenii executarea de cod si aplicații direct de pe dispozitive externe. De asemenea, vine si cu un mecanism de macare a aplicatiilor permise.*	

		- *soluția trebuie să permită aplicarea de politici diferite în funcție de locația utilizatorlui (ex: să nu poată conecta imprimante atunci când nu se află în perimetrul rețelei).* - *soluția trebuie să ofere un mecanism de dezactivare a restricțiilor pentru utilizatorii ce nu au conectivitate cu severul de administrare.* - *soluția trebuie să permită construirea unei liste de dispozitive permise și corelarea acestei liste la utilizatori / grupuri de utilizatori din Directory Services, astfel încât aceștia să poată utiliza dispozitivele indiferent de calculatorul la care se afla.* - *soluția trebuie să permită alertarea administratorului atunci când sunt copiate informații pe dispozitive externe de stocare date. Pentru situații în care stația de lucru este offline, soluția va stoca informația respectivă local, iar la prima conectare on-line, va asigura alertarea administratorului.* - *soluția trebuie să permită filtrarea fișierelor ce sunt copiate pe dispozitive externe de stocare date după extensie și /sau tip de fișier. Tipul de fișier trebuie identificat indiferent de extensia acestuia. (ex: blocarea copierii fișierelor Microsoft Office Word, Adobe Reader PDF).* - *soluția trebuie să nu poată fi oprită (stopată activitatea) de utilizator chiar dacă acesta are dreptul de administrator local.* - *soluția trebuie sa permita creare unei reguli de shadowing(duplicare) a fisierelor copiate pe dispozitive externe atunci cand anumite criteria sunt indeplinite (Ex: un anumit utilizator, grup de utilizatori, tipul fisierului, extensia fisierului). Duplicatul fisierului trebuie sa poata fi accesat numai de cei ce au acest drept in consola de administrare.*	- *soluția permite aplicarea de politici diferite în funcție de locația utilizatorului (ex: să nu poată conecta imprimante atunci când nu se află în perimetrul rețelei).* - *soluția oferă un mecanism de dezactivare a restricțiilor pentru utilizatorii ce nu au conectivitate cu severul de administrare.* - *soluția permite construirea unei liste de dispozitive permise și corelarea acestei liste la utilizatori / grupuri de utilizatori din Directory Services, astfel încât aceștia să poată utiliza dispozitivele indiferent de calculatorul la care se afla.* - *soluția permite alertarea administratorului atunci când sunt copiate informații pe dispozitive externe de stocare date. Pentru situații în care stația de lucru este offline, soluția va stoca informația respectivă local, iar la prima conectare on-line, va asigura alertarea administratorului.* - *soluția permite filtrarea fișierelor ce sunt copiate pe dispozitive externe de stocare date după extensie și /sau tip de fișier. Tipul de fișier trebuie identificat indiferent de extensia acestuia. (ex: blocarea copierii fișierelor Microsoft Office Word, Adobe Reader PDF).* - *soluția are posibilitatea de a nu fi oprită (stopată activitatea) de utilizator chiar dacă acesta are dreptul de administrator local.* - *soluția trebuie permite creare unei reguli de shadowing(duplicare) a fisierelor copiate pe dispozitive externe atunci cand anumite criterii sunt îndeplinite (Ex: un anumit utilizator, grup de utilizatori, tipul fișierului, extensia fișierului). Duplicatul fișierului va putea fi accesat numai de cei ce au acest drept in consola de administrare.*	

		Protecția resurselor de rețea: - *să poată efectua descoperirea, indexarea și înregistrarea datelor din baze de date de tipul MySQL, Oracle.* - *pentru fișierele ce trebuiesc protejate să poată preveni upload-ul efectuat direct din consolă.* - *poluția trebuie asigure accesul la interfața de administrare prin intermediul unui portal web securizat SSL.* - *să permită aplicarea de filtre în procesul de descoperire a datelor (spre exemplu, excluderea fișierelor mai mari de X MB).* - *să poată efectua extragerea de informații din arhive cu peste 10 niveluri.* - *să permită setarea nivelului de resurse pe care în consumă (ex. lățimea de bandă la scanare).* - *soluția trebuie să scaneze incremental în CIFS, NFS, FTP.* *Protecție Proxy: soluția trebuie să fie capabilă să se integreze cu serviciul de proxy al BNM (McAfee WebGateway) și trebuie să protejeze împotriva transmiterii neautorizate de date și informații prin protocoalele de rețea HTTP , HTTP/S și FTP.* *Protecție Email: soluția trebuie să fie capabilă să se integreze cu serviciul de email al BNM (Microsoft Exchange 2013/2016, Outlook 2016).* *Network monitor:* - *soluția trebuie să fie capabilă să scaneze, analizeze și să clasifice în timp real traficul de ieșire din/în rețeaua Internet/BNM pentru majoritatea protocoalelor de rețea (HTTP, SMTP, IMAP, POP3, FTP,Telnet, Rlogin, SSH, webmail, Yahoo! Chat, AOL Chat, MSN Chat, ICY, TSP, SOCKS, PCAnywhere, RDP, VNC, SMB, Citrix, Skype, IRC, LDAP, DASL, NTLM, Kazaa, BitTorrent, eDonkey, Gnutella, DirectConnect, MP2P, WinMX, Sherlock, eMule, and more);*	*Protecția resurselor de rețea:* - *poate efectua descoperirea, indexarea și înregistrarea datelor din baze de date de tipul MySQL, Oracle.* - *pentru fișierele ce necesită protejate să poată preveni upload-ul efectuat direct din consolă.* - *poluția trebuie asigure accesul la interfața de administrare prin intermediul unui portal web securizat SSL.* - *să permită aplicarea de filtre în procesul de descoperire a datelor (spre exemplu, excluderea fișierelor mai mari de X MB).* - *să poată efectua extragerea de informații din arhive cu peste 10 niveluri.* - *să permită setarea nivelului de resurse pe care în consumă (ex. lățimea de bandă la scanare).* - *soluția trebuie să scaneze incremental în CIFS, NFS, FTP.* *Protecție Proxy: soluția trebuie este capabilă să se integreze cu serviciul de proxy al BNM (Mcafee WebGateway) și să protejeze împotriva transmiterii neautorizate de date și informații prin protocoalele de rețea HTTP , HTTP/S și FTP.* *Protecție Email: soluția este capabilă să se integreze cu serviciul de email al BNM (Microsoft Exchange 2013/2016, Outlook 2016).* *Network monitor:* - *soluția este capabilă să scaneze, analizeze și să clasifice în timp real traficul de ieșire din/în rețeaua Internet/BNM pentru majoritatea protocoalelor de rețea (HTTP, SMTP, IMAP, POP3, FTP,Telnet, Rlogin, SSH, webmail, Yahoo! Chat, AOL Chat, MSN Chat, ICY, TSP, SOCKS, PCAnywhere, RDP, VNC, SMB, Citrix, Skype, IRC, LDAP, DASL, NTLM, Kazaa, BitTorrent, eDonkey, Gnutella, DirectConnect, MP2P, WinMX, Sherlock, eMule, and more);*	

		- *soluția trebuie să fie capabilă să se integreze pasiv cu echipamentul de rețea utilizând SPAN port sau "physically inline network tap" (optional);* - *soluția trebuie să asigure vizualizarea rapoartelor de incident.* ***Cerințe privind administrarea:*** - *consola trebuie să permită atribuirea automată a politicilor pe stații și servere în funcție de specificațiile sistemului. (Ex: Platforma desktop/server, Subnet, tip procesor, sistem de operare).* - *sincronizarea dintre server și client trebuie să se facă dinspre client către server.* - *administrarea componentelor de data loss prevention și de control al dispozitivelor externe trebuie să se poată face dintr-o singura consola.* - *consola de administrare trebuie să poată fi instalată într-un mediu virtual.* - *soluția trebuie să poată filtra evenimentele ce sunt generate de componentele aflate pe stațiile de lucru astfel încât baza de date sa nu se încarce cu informații considerate inutile.* - *soluția trebuie să permită configurarea de mesaje în funcție de tipul evenimentului.* - *accestul în consola de administrare să poată fi făcut pe baza credențialelor din Directory Services.* - *consola de administrare trebuie să permită creare de roluri în mod granular pentru cei ce o administrează.* - *soluția trebuie să ducă loguri (înregistrări de audit) cu privire la acțiunile utilizatorilor în consolă.* - *consola trebuie să permită construirea unei liste de contacte în vederea folosirii acestora pentru notificări prin mesagerie electronică (E-mail).* - *consola de administrare trebuie să poată fi accesată de pe orice computer din rețea în mod securizat, fără necesitatea instalării de software adițional.*	- *soluția este capabilă să se integreze pasiv cu echipamentul de rețea utilizând SPAN port sau "physically inline network tap" (optional);* - *soluția asigură vizualizarea rapoartelor de incident.* ***Cerințe privind administrarea:*** - *consola permite atribuirea automată a politicilor pe stații și servere în funcție de specificațiile sistemului. (Ex: Platforma desktop/server, Subnet, tip procesor, sistem de operare).* - *sincronizarea dintre server și client se face dinspre client către server.* - *administrarea componentelor de data loss prevention și de control al dispozitivelor externe poate fi făcută dintr-o singura consola.* - *consola de administrare poate fi instalată într-un mediu virtual.* - *soluția poate filtra evenimentele ce sunt generate de componentele aflate pe stațiile de lucru astfel încât baza de date sa nu se încarce cu informații considerate inutile.* - *soluția permite configurarea de mesaje în funcție de tipul evenimentului.* - *accesul în consola de administrare poate fi făcută pe baza credențialelor din Directory Services.* - *consola de administrare permite creare de roluri în mod granular pentru cei ce o administrează.* - *soluția duce loguri (înregistrări de audit) cu privire la acțiunile utilizatorilor în consolă.* - *consola permite construirea unei liste de contacte în vederea folosirii acestora pentru notificări prin mesagerie electronică (E-mail).* - *consola de administrare poate fi accesată de pe orice computer din rețea în mod securizat, fără necesitatea instalării de software adițional.*	

		- *daca serverul de administrare este accesat prin intermediul unei interfețe web, trebuie să fie posibil importul unui certificat ssl generat de o autoritate locala, înlocuindu-l astfel pe cel auto-generat.* - *sistemul trebuie să permită setarea periodicității de sincronizare dintre server și componente.* - *sistemul trebuie să permită setarea periodicității de transmitere a evenimentelor de pe client pe server.* - *sistemul trebuie să poată / permită automatizarea de sarcini de instalare / dezinstalare a componentelor pe stațiile de lucru, de rulare a rapoartelor și de transmiterea de notificări de prin mesagerie electronică.* - *sistemul (serverul) trebuie să fie capabil să declanșeze acțiuni automate atunci când anumite condiții sunt îndeplinite (ex: generarea unui eveniment pe server, pe o stație de lucru, detectarea unui nou sistem pe rețea).* - *soluția trebuie să permită aplicarea de politici diferite pentru sisteme pe: a. sisteme individuale; b. grupuri de sisteme; c. sisteme din Directory Services ce aparțin aceleiași OU.* - *soluția trebuie să permită accesarea logurilor componentei de sincronizare de pe sisteme în timp real prin intermediul unui serviciu web.* ***<u>Cerințe privind subsistemul de raportare:</u>*** - *soluția trebuie să asigure generarea de rapoarte despre nodurile administrate (endpoint-uri sau de rețea) și despre evenimentele generate de ele.* - *soluția trebuie să permită crearea de noi rapoarte în mod granular cu informații extrase din evenimente, sau despre sistemele administrate.* - *rapoartele pot fi generate sub formă de tabel, pie chart, buble chart, listă, sumar, sau grafic istoric.* - *soluția trebuie să poată exporta rapoartele în cel puțin următoarele formate: pdf, csv, html.*	- *daca serverul de administrare este accesat prin intermediul unei interfețe web posibil importul unui certificat ssl generat de o autoritate locala, înlocuindu-l astfel pe cel auto-generat.* - *sistemul permite setarea periodicității de sincronizare dintre server și componente.* - *sistemul permite setarea periodicității de transmitere a evenimentelor de pe client pe server.* - *sistemul poate / permite automatizarea de sarcini de instalare / dezinstalare a componentelor pe stațiile de lucru, de rulare a rapoartelor și de transmiterea de notificări de prin mesagerie electronică.* - *sistemul (serverul) este capabil să declanșeze acțiuni automate atunci când anumite condiții sunt îndeplinite (ex: generarea unui eveniment pe server, pe o stație de lucru, detectarea unui nou sistem pe rețea).* - *soluția permite aplicarea de politici diferite pentru sisteme pe: a. sisteme individuale; b. grupuri de sisteme; c. sisteme din Directory Services ce aparțin aceleiași OU.* - *soluția permite accesarea logurilor componentei de sincronizare de pe sisteme în timp real prin intermediul unui serviciu web.* ***<u>Cerințe privind subsistemul de raportare:</u>*** - *soluția asigură generarea de rapoarte despre nodurile administrate (endpoint-uri sau de rețea) și despre evenimentele generate de ele.* - *soluția permite crearea de noi rapoarte în mod granular cu informații extrase din evenimente, sau despre sistemele administrate.* - *rapoartele pot fi generate sub formă de tabel, pie chart, buble chart, listă, sumar, sau grafic istoric.* - *soluția poate exporta rapoartele în cel puțin următoarele formate: pdf, csv, html.*	

		- soluția trebuie să permită personalizarea rapoartelor (ex. aplicarea logo-ului BNM). *- soluția trebuie să permită atât salvarea sub formă de fișiere a rapoartelor cât și expedierea acestora prin e-mail.* *- soluția trebuie să permită aplicarea de filtre pe evenimente la generarea rapoartelor.* *- soluția trebuie să poată genera rapoarte privind (dar nelimitându-se la):* ✓ *log-urile de audit administrative;* ✓ *detalii despre sistemele administrate (detalii de configurare, hardware, utilizator);* ✓ *evenimente de la sistem;* ✓ *Informații despre politicile și sarcinile aplicate sistemelor;* ✓ *Informații furnizate de agenți.* ***Alte cerințe obligatorii:*** *Perioada de suport standard de la producător trebuie să fie egalată cu perioada licențelor DLP exploatate în cadrul Sistemului Informațional al BNM, până la 13.12.2020* ***Termen de livrare:*** *până la 13.12.2019 inclusiv.*	*- soluția permite personalizarea rapoartelor (ex. aplicarea logo-ului BNM).* *- soluția trebuie permite atât salvarea sub formă de fișiere a rapoartelor cât și expedierea acestora prin e-mail.* *- soluția permite aplicarea de filtre pe evenimente la generarea rapoartelor.* *- soluția poate genera rapoarte privind (dar nelimitându-se la):* ✓ *log-urile de audit administrative;* ✓ *detalii despre sistemele administrate (detalii de configurare, hardware, utilizator);* ✓ *evenimente de la sistem;* ✓ *Informații despre politicile și sarcinile aplicate sistemelor;* ✓ *Informații furnizate de agenți.* ***Alte cerințe obligatorii:*** *Perioada de suport standard de la producător va fi egalată cu perioada licențelor DLP exploatate în cadrul Sistemului Informațional al BNM, până la 13.12.2020* ***Termen de livrare:*** *până la 13.12.2019 inclusiv.*	
72268000-1	**2.** Servicii de asigurare a accesului la suport anual Business Support, sau echivalentul, pentru licența McAfee Total Protection for Data Loss Prevention Software pentru 350 utilizatori	**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 14.12.2019-13.12.2020 pentru licențele McAfee Total Protection for Data Loss Prevention Software exploatate în cadrul Sistemului Informațional al BNM pentru 350 utilizatori și vor include:* *- prezentarea de către Prestator a unui document confirmativ parvenit de la compania producător, sau*	***Produsul ofertat: Servicii suport anual pentru licența McAfee Total Protection for DLP - 1 year business support, pentru 350 utilizatori*** **Tip:** *Servicii de asigurare a accesului la suport anual Business Support, de la producătorul licențelor McAfee, se vor oferi în baza prelungirii termenului de prestare a serviciilor respective pentru perioada 14.12.2019-13.12.2020 pentru licențele McAfee Total Protection for Data Loss Prevention Software exploatate în cadrul Sistemului Informațional al BNM pentru 350 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.*	

		- publicarea informației confirmative pe site-ul producătorului. ***Cerinţe faţă 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:** până la 13.12.2019 inclusiv*	***Cerinţe faţă 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:** până la 13.12.2019 inclusiv*	
48219100-7	**3.** Subscriere anuală pentru licența McAfee Web Protection, inclusiv 1 an de suport anual Business Support, sau echivalentul, pentru 400 utilizatori	***Tip: S**ubscriere anuală pentru perioada 07.11.2019 - 06.11.2020 a licenței McAfee Web Protection exploatată în cadrul Sistemului Informațional al BNM, cu un an de suport de tipul Business Support inclus, sau echivalentul, cu extindere până la 400 utilizatori.* ***Cerinţe faţă 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*	***<u>Produsul ofertat:</u> Subscriere anuală pentru licența McAfee Web Protection Suite - 1 year business support, pentru 400 utilizatori*** ***Tip: S**ubscriere anuală pentru perioada 07.11.2019 - 06.11.2020 a licenței McAfee Web Protection exploatată în cadrul Sistemului Informațional al BNM, cu un an de suport de tipul Business Support inclus, cu extindere până la 400 utilizatori.* ***Cerinţe faţă 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:*** *până la 07.11.2019 inclusiv*	- *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:*** *până la 07.11.2019 inclusiv*	

Semnat:_____
Numele, Prenumele: **Andrian Cornei**
În calitate de: **Director**
Ofertantul:Reliable Solutions Distributor
Adresa: str. Alexandru cel bun 85, MD-2012, mun Chisinau, Republica Moldova.