Conform Anexei nr.21 la Documentația Standard,
aprobată prin ordinul Ministrului Finanțelor
al RM nr.115 din 15.09.2021

CAIET DE SARCINI
Bunuri

1. **DESCRIERE GENERALĂ. INFORMAȚII**
Autoritatea contractantă: Procuratura Generală a Republicii Moldova
Obiectul achiziției: Pachete software antivirus
Codul CPV: 48761000-0

2. **CERINȚE FAȚĂ DE BUNURI:**

Nr. d/o	Cod CPV	Denumirea bunurilor	Unit. de măs.	Cant-tea	Specificarea tehnică deplină solicitată, Standarde de referință	Valoarea estimată, fără TVA, MDL (se va indica pentru fiecare lot în parte)
Lotul 1: Pachete software antivirus						
1	48761000-0	Pachete software antivirus (inclusiv Disk Encryption management)	buc	1150	*Conform Caietului de sarcini*	
Valoarea estimată totală, lei fără TVA						**900 000,00**

Tip: Subscriere anuală pentru soluția de protecție și securitate pentru 1150 entități (PC/ laptop/ VDI/ Server) pentru perioada de 3 ani.
Cantitate: Este responsabilitatea Ofertantului de a determina modelul de licențiere luând în calcul:
- 1150 entități (PC/laptop/VDI/Server)
- Disk Encryption management pentru 250 entități.

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").

Specificații tehnice:
Soluția va acoperi **minim** următoarele cerințe și specificații tehnice:
Caracteristici generale ale produsului:
Soluția trebuie să reprezinte o platformă integrată pentru managementul securității, gândita ca o soluție modulară.
Produsul va conține următoarele module, toate cu posibilitatea de a fi gestionate și administrate dintr-o singură consolă de management:
- Protecție stații și servere fizice și virtualizate;
- Serviciu de corelare și răspuns la evenimente de tip EDR („endpoint detection and response").

Consola de management:
Accesibilitate atât de pe browser desktop cât și tip mobile.
Să ofere opțiune configurabilă de actualizare automată a consolei de management.
Soluția de scanare centralizată:
Soluția de scanare (pentru VDI/scanare centralizată) disponibilă de tip template și compatibilă cu următoarele hipervizoare:
1. VMware vSphere;
2. Citrix XenServer;
3. Microsoft Hyper-V.

Cerințe generale produs:
Soluția trebuie să:

- permită activarea/dezactivarea actualizărilor automate de produs/semnături şi a consolei de management;
- ofere vizualizarea unui jurnal de modificări în care sunt precizate istoric: versiunea consolei de management, data versiunii, funcţii noi si îmbunătăţiri, probleme rezolvate, probleme cunoscute;
- afişeze notificările şi alertele existente, să alerteze administratorul în cazul unor probleme majore (configurabile): licenţiere, detecţie virusi, actualizări de produs disponibile);

Panou de monitorizare si raportare (Dashboard):

- să ofere posibilitatea creării rapoartelor configurabile după tip, ţintă şi scop cu opţiuni specifice pentru orice tip de raport cu posibilităţi de adăugare/eliminare şi rearanjare.
- să prezinte rapoarte pentru toate modulele suportate(stare/statut/actualizare).

Inventarierea reţelei – managementul securităţii:

Produsul trebuie să:

- se integreze cu domenii Active Directory multiple, să poată importa inventarul.
- permită descoperirea PC neintegrate în Active Directory (Workgroup);
- ofere opţiuni de căutare, sortare şi filtrare după numele sistemului, sistem de operare si adresa IP, politica aplicată, online şi/sau offline şi FQDN;
- permită instalarea la distanţă sau manual a clienţilor antivirus pe maşini fizice şi virtuale;
- permită selectarea modulelor componente atunci când se creează pachetul clientului care se instalează pe maşinile fizice/virtuale;
- permită lansarea de task-uri de scanare, actualizare, instalare, dezinstalare la distanţă pentru clientul antivirus;
- ofere posibilitatea de repornire a maşinilor fizice de la distanţă;
- ofere informaţii detaliate despre fiecare task iniţiat şi afişarea statutului lui;
- permită configurarea centralizată a clienţilor antivirus prin intermediul politicilor;
- ofere în consola de management informaţii detaliate ale obiectelor din consola: Nume, IP, Sistem de operare, Grup, Politica atribuită, Ultimele actualizare, Versiunea produsului, Versiunea de semnături;
- permită descoperirea tuturor aplicaţiilor instalate pe toate staţiile şi serverele din reţea.

Politici:

Produsul trebuie să:

- permită configurarea setărilor clientului antivirus prin intermediul unei singure politici ce conţine setări pentru toate module;
- conţină opţiuni specifice de activare/dezactivare şi configurare a funcţionalităţilor precum scanarea antivirus la cerere, firewall, controlul accesului la Internet, controlul aplicaţiilor, scanarea traficului web, controlul dispozitivelor, power user;
- permită aplicarea politicilor pe maşini client, grupuri de maşini, pool-uri de resurse (VMware), domeniu, unităţi organizaţionale sau useri de active directoy;
- poată fi schimbată automat în funcţie de: User-ul logat, IP sau clasa de IP, Gateway-ul alocat, DNS serverul alocat, Clientul este/nu este în accesai reţea cu infrastructura de management, Tipul reţelei (lan, wireless).

Monitorizare şi raportare:

Produsul trebuie să:

- permită setarea de opţiuni specifice pentru afişarea rapoartelor existente;
- deţină un panou central care să afişeze statutul modulelor şi rapoartele lor pentru perioadele de timp specificate;
- conţină rapoarte care prezinta statusul maşinilor clienţilor, al actualizărilor, fişierelor malware detectate, aplicaţiile 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, menţinând informaţiile concise si ordonate corespunzător, să includă interogări precum: starea terminalului, evenimente terminal;

- ofere interogări legate de starea terminalului precum: tip maşină, infrastructură reţelei căreia aparţine, datele agentului de securitate, starea modulelor de protecţie, rolurile terminalelor;
- ofere interogări legate de evenimente precum: calculatorul ţinta pe care a avut loc evenimentul, tipul starea şi configuraţia agentului de securitate instalat, starea modulelor şi rolurilor de protecţie instalate pe agentul de securitate, denumirea şi alocarea politicii, utilizatorul autentificat în timpul evenimentului, evenimente (site-uri blocate, aplicaţii blocate, detecţiile etc);

Carantină:

- Produsul trebuie să permită restaurarea fişierelor din carantină în locaţia originală sau într-o cale configurabilă;
- Administrarea Carantinei să fie posibilă atât pe terminalul administrat cât şi din consola de management;

Utilizatori:

- Administrarea este necesar să fie efectuată pe bază de roluri multiple predefinite: Administrator companie, Administrator reţea, Reporter şi alte roluri configurabile detaliat cu posibilitatea de selectare a serviciilor şi obiectelor pentru care un utilizator poate face modificări;
- Utilizatorii să poată fi importaţi din Microsoft Active Directory sau creaţi în consola de management;
- Să fie posibilă deconectarea automată a oricărui tip de utilizator după un anumit timp - configurabil.

Log-uri:

- Soluţia trebuie să permită înregistrarea acţiunilor utilizatorilor şi să ofere informaţii detaliate pentru fiecare acţiune a unui utilizator cu posibilitatea de filtrare.

Actualizare:

Soluţia va permite:

- definirea de locaţii de actualizare multiple
- activarea/dezactivarea actualizărilor
- testarea noilor versiuni înainte de a fi instalate pe toţi clienţii (posibilitate de actualizare în mai multe cicluri – 1 mediu de test, 2 – mediu de producţie)
- definirea zonelor de test şi zonelor critice de producţie

Protecţie staţii şi servere fizice si virtualizate – caracteristici minime:

Soluţia trebuie să:

- permită instalarea personalizată a modulelor;
- includă un „vaccin" anti-ransomware, cu actualizări de la producător, pentru protecţia împotriva tuturor ameninţărilor cunoscute de tip ransomware, prin imunizarea staţiilor şi serverelor, chiar daca sunt infectate şi blocarea procesului de criptare;
- includă protecţie împotriva atacurilor zero-day de tip exploit (atacuri direcţionate);
- includă modul de analiză la risc capabil să identifice şi să remedieze riscurile identificate la nivel de reţea sau sistem de operare, cu posibilitate de configurare şi automatizare;
- includă modul avansat de securitate bazat pe tehnologii de tip „machine learning tunabil" proiectat special pentru a detecta atacuri avansate şi activităţi suspecte în faza pre-execuţie;
- includă modul avansat de securitate pentru protecţie împotriva: atacurilor direcţionate (Targeted Attack), fişierelor suspecte si traficului la nivel de reţea suspect, exploit-urilor, ransomware şi grayware. Fiecărui tip de ameninţare menţionat, i se vor putea stabili, independent, un nivel de protecţie dorit: permisiv, normal, agresiv cu posibilitate de extindere a nivelului de raportare;
- includă modul de sandbox, unde se vor putea trimite manual sau automat fişiere pentru a putea fi „detonate" pentru o analiză în profunzime;
- includă variante de analiză a sandbox-ului tip: doar monitorizare sau blocare cu acţiuni de remediere: implicită şi de siguranţa. Pentru acţiunea implicită: doar raportare, dezinfecţie, ştergere şi transmitere în carantină. Pentru acţiunea de siguranţa: ştergere sau permutare în carantină;
- suporte "detonarea" în modulul sandbox, minim, tipurile de fişiere: 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. Acestea vor fi detectate corect chiar dacă vor fi în arhive de tipul : 7z, ACE, ALZip, ARJ, BZip2, cpio, GZip, LHA, Linux TAR, LZMA Compressed Archive, MS Cabinet, MSI, PKZIP, RAR, Unix Z, ZIP, ZIP (multivolume), ZOO, XZ ;

- ofere posibilitate de filtrare a incidentelor din interfața grafică în funcție intervalul de timp, pe baza unui scor de încredere, indicatori de atac, tehnici de atac, sistem de operare afectat cît și după IP, nume fișier, nume stație;
- permită vizualizarea detaliată a incidentelor incluzând detalii specifice fiecărui nod: să generează o hartă de principiu a incidentului, să detalieze incidentul în funcție de amprenta de timp a fiecărei acțiuni aferente incidentului, să poată genera un set de măsuri specifice fiecărui element din harta incidentului (kill, carantina – la nivel de nod, investigare – virus total, sandbox, google – la nivel de fișier, adăugare în lista de blocare – la nivel de rețea sau instalare patch – la nivel de nod);
- poată bloca fișiere și/sau procese folosind valori hash de tip MD5/SHA256 direct din pagina aferentă incidentului sau importate folosind un fișier CSV;
- poată excepta fișiere non-malițioase de la acțiunea de investigare sau poate genera/adaugă un set de fișiere malițioase într-o listă neagră pentru a preveni mișcarea laterală a fișierelor/proceselor malițioase;
- permită deschiderea unei conexiuni remote către un endpoint potențial infectat pentru a permite o investigare rapidă a gazdei/ colectare date despre atacul respectiv/ remediere în timp real a breșelor de securitate/ permită executarea unor comenzi în linia de comandă care se execută cu privilegii de kernel pentru eliminarea în timp real a unor amenințări sau colectarea de date privitoare la atacul în desfășurare;
- permită crearea regulilor de detecție customizabilă bazată pe procese, fișiere, registre și conexiuni de rețea;
- permită creare regulilor de excludere customizabilă bazată pe procese, fișiere, registre si conexiuni de rețea;
- permită căutarea pro activă pe endpoint-urile protejate a indicatorilor de compromitere precum hash-uri, nume de fișiere, nume de procese, chei de registre, valori de registre;
- permită deschiderea unei conexiuni remote către un endpoint potențial infectat pentru investigare rapidă, colectare date și remedierea în timp real a breșei de securitate, reducând timpul de remediere (downtime) în cazul unui atac, executarea comenzilor în linia de comandă cu privilegii de kernel ce permit eliminarea în timp real a unor amenințări sau colectarea de date privitoare la atacul în desfășurare
- includă modul de detectare, corelare și răspuns la evenimente de tip EDR („endpoint detection and response") capabil să identifice amenințări avansate sau atacuri în curs de desfășurare. Acest modul va fi capabil să :

a. cuprindă colectarea de date și evenimente despre hardware și software aferent fiecărei stații de lucru aducând informații detaliate referitoare la incidentele detectate, o hartă detaliata a acestora precum și acțiuni de remediere automate și integrare cu modulele de Sandbox și modulul avansat de securitate;
b. ofere senzori de colectare a datelor și componente de procesare și interpretare a acestora;
c. posede capacitarăți de evaluare a activității tipice a unui endpoint din perspectiva securității acestuia conform tehnicilor de atac MITRE („baselining") și va raporta orice deviație de la acest comportament sub forma unui incident;
d. ofere vizualizarea detaliată a incidentelor incluzând detalii specifice fiecărui nod afectat generînd o hartă de principiu a incidentului, detaliind incidentul în funcție de amprenta de timp a fiecărei actiuni aferente incidentului, respectiv butonul „acționează" care poate genera un set de masuri specifice fiecărui element din harta incidentului (kill, carantina – la nivel de nod, investigați – virus total, sandbox, google – la nivel de fișier, adăugare în lista de blocare – la nivel de rețea sau instalare patch – la nivel de nod);
e. poate bloca fișiere si/sau procese folosind valori hash de tip MD5/SHA256 direct din pagina aferentă incidentului sau importate folosind un fișier CSV;
f. poată excepta fișiere non-malițioase de la acțiunea de investigare sau poate genera/adaugă un set de fișiere malițioase într-o listă pentru a preveni mișcarea laterală a fișierelor/proceselor malițioase

g. permită vizualizarea incidentelor extinse corelate de pe mai multe endpoint-uri.

Cerințe de sistem:

- Sisteme de operare pentru stații de lucru: Windows 10/11 (inclusiv Embebed și IoT), Mac OS X de la 10.12 și mai recent, Red Hat Enterprise Linux / CentOS 7 și mai recent, Oracle Linux 6.3 și mai recent, Ubuntu 16 și mai recent, SUSE Linux Enterprise Server 12 și mai recent, OpenSUSE 15 și mai recent, Fedora 31 și mai recent;
- Sisteme de operare Windows pentru servere: Windows Server 2012/2012 R2/2016/2019/2022.

Administrare și instalare remote:

- Pachetele de instalare trebuie să fie configurabile cu modulele necesare cu domenii tip firewall, device control, power user, content control, disk encryption, EDR sensor, „relay" (update server");
- Să existe posibilitatea de instalare manuală, sau automată la distanță, direct din consola de management;
- Din consola să fie disponibile informații despre fiecare endpoint: numele, IP, sistem de operare, module instalate, politica aplicată, informații despre actualizări;
- Posibilități de creare kit pentru endpoint – tip: universar – 32/64bit, fizic/VDI, web installe/full.
- Gestionare, creare și configurare grupuri pentru endpoint ce nu sunt în AD;
- Posibilitate de atribuire a funcționalității de descoperire a endpointurilor și în afara AD, pentru oricare endpoint.

Caracteristici și funcționalități principale ale modulului antivirus:

Produsul trebuie sa permită:

- stabilirea acțiunilor întreprinse de modulul antivirus la detectarea unei amenințări noi. Astfel administratorul va putea alege între următoarele acțiuni:

a. implicită pentru fișiere infectate: interzice accesul, dezinfectează, ștergere, mută fișierele în carantină, nici o acțiune;
b. alternativă pentru fișierele infectate: interzice accesul, dezinfectează, ștergere, permutare fișiere în carantină;
c. acțiune implicită pentru fișierele suspecte: interzice accesul, ștergere, mută fișierele în carantină, nici o acțiune;
d. 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 lansată 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 bazate 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 în 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;
- utilizarea uni modul adițional de securitate bazat pe algoritmi tunabili de machine learning respectiv algoritmi euristici agresivi capabili să detecteze și blocheze atacuri de tip persistent sau targetat precum și alte categorii de malware sofisticat înainte de faza de execuție. Acest modul oferă următoarele funcționalități:

a. clasificarea tipului de atac;
b. abilitatea de a raporta amenințările detectate fără a le bloca;
c. abilitate de a ajusta agresivitatea detecției pe cel puțin 3 nivele (incluzând posibilitatea de a raporta atacuri ce ar fi fost blocate pe un nivel de agresivitate a detecției „mai ridicat" decât cel setat în mod curent în modul);
d. abilitatea de a acționa în mod diferit în funcție de tipul amenințării (fișier sau atac prin rețea);

- posibilitatea de restaurare a fișierelor modificate de un proces suspicios/necunoscut cu comportament de ransomware, cînd determină că procesul este malițios;
- oprirea atacurile avansate de tip „zero-day" efectuate prin intermediul unor exploit-uri evazive;
- depistarea în timp real a celor mai recente exploit-uri ce pot vulnerabiliza un sistem de operare;
- protejarea aplicațiilor utilizate frecvent și a celor de tip „sistem" cum ar fi browserele, aplicațiile de tip office sau reader, procesele critice aferente sistemelor de operare.

Firewall:

- sa ofere posibilitatea de a configura reguli de firewall pentru aplicații sau conectivitate;
- modulul să poată fi instalat/ activat/ dezactivat/ 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).

Controlul dispozitivelor:

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.
- gestionabil – doar local sau și servere online.

Protecție Anti-Tampering:

- va permite detecția driverelor vulnerabile pe dispozitivele conectate (endpointuri) și când sunt efectuate încercări avansate de atac pentru a dezactiva agentul de securitate, ceea ce poate duce la compromiterea integrității produsului;
- va permite detectarea de drivere vulnerabile pe dispozitivele conectate care pot fi exploatate de atacatori, reprezentând amenințări la adresa integrității produsului. Tehnologia este compatibilă cu sistemele de operare Windows și Linux;
- va fi capabilă să protejeze împotriva amenințărilor noi sau erorilor umane neintenționate ce ar putea fi proiectate pentru a permite acces neautorizat la kernel, ducând la compromiterea integrității poate detecta când funcțiile de tip callback ale agentului de securitate au fost eliminate sau dezactivate în mod malițios.

Disk Encryption:

Soluție pentru managementul criptării discurilor pentru 250 entități.

Soluția va oferi următoarele funcționalități minime:

- Administrarea produsului trebuie să fie realizată din aceeași consolă de management ca și soluția de protecție antivirus;
- produsul va utiliza mecanismul nativ de criptare al sistemului de operare: BitLocker pentru Windows și FileVault pentru Mac OSX;
- va asigura vizibilitatea completă 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 10/11 Pro/Enterprise (with TPM); WindowsServer 2012/2012 R2, 2016, 2019, 2022 (with TPM), OSX de la 10.12.

Alte cerințe:

Perioada de suport și menținere de la producător:

1.Pentru soluția ofertată se solicită a fi 36 luni;

2.Producătorul trebuie să ofere suport 24/24, prin e-mail sau conectare de la distanță.

Notă: Lucrările de instalare, configurare, punerea în funcțiune a soluției trebuie să fie executate de Ofertant, iar costul acestora trebuie să fie incluse în ofertă (după caz).

Președinte grup de lucru **Iuri LEALIN**