

**SA «Moldovagaz»**  
MD-2005, Republica Moldova, mun. Chişinău, str. Puşkin, 64  
**Comisia de achiziții**  
Tel. +373 22 578 014,  
E-mail: omts@moldovagaz.md, [www.moldovagaz.md](http://www.moldovagaz.md)

**ANUNȚ PRIVIND ÎNȚIEREA PROCEDURII DE ACHIZIȚII**  
**Licitația Nr. MG-03/20**

**1. Obiectul contractului de achiziție:** “Servicii de furnizare, instalare, configurare, punere în funcțiune și suport tehnic pentru software-ul licențiat pentru protecția și securitatea locurilor de muncă, a serverelor și a poștei corporative”. CPV:48761000-0, antivirus software.

Cerințe față de lucrările efectuate: în conformitate cu Caietul de sarcini (se anexează).

Data-limită pentru prezentarea ofertelor: 19 martie 2020, pînă la 12:00 (ora locală).

Termenul de valabilitate a ofertei: 30 de zile de la data deschiderii ofertelor.

Tipul procedurii de achiziții: licitație deschisă.

Data, ora și locul deschiderii ofertelor depuse: 19 martie 2020, 15:00 (ora locală), pe adresa Beneficiarului.

**2. Informații juridice, economice, financiare și tehnice:**

**2.1. Condiții de participare:**

- a) operatorul economic nu trebuie să fie inclus în listele neadmisibile la procedurile de achiziții a Beneficiarului sau Agenției pe achiziții publice;
- b) nu este în incapacitate de plată sau insolvabilitate, să nu se afle în proces de lichidare, bunurile nu trebuie să fie sechestrate, activitatea economică nu trebuie să fie suspendată;
- c) să-și îndeplinească obligațiile privind plata impozitelor la bugetele de toate nivelurile și plăți obligatorii la fondurile guvernamentale;
- d) să aibă actele necesare permise pentru practicarea acestui tip de activitate și personal calificat (licențele, de acreditare, de certificare, de atestare etc.).

**2.2. Oferta trebuie să fie pregătită conform cerințelor capitolului 4 “prezentarea ofertelor” compartimentul V Regulamentului privind procedurile de achiziții, aprobat de ANRE (plasat pe pagina web a SA “Modlovagaz” [www.moldovagaz.md](http://www.moldovagaz.md) - compartimentul «achiziții»), și exact:**

- a) să corespundă cerințelor, stabilite în documentația de atribuire;
- b) trebuie să fie pregătită clar, fără corectări, cu indicarea numărului de ieșire și data, cu semnătura persoanei responsabile;
- c) trebuie să fie tipărită sau scrisă cu cerneală. Dacă există modificări, este necesar să fie și semnătura persoanei împuternicite pe fiecare pagină, pe care au fost introduse modificări;
- d) trebuie să fie prezentată în termenul limită, stabilit în anunțul de achiziții;

e) plicul trebuie să fie opac, sigilat și etichetat cu adresa beneficiarului, adresa operatorului economic, numărul de telefon, cu indicarea denumirii și numărului licitației;

f) trebuie să conțină caracter ce nu permite discuții și obligatoriu din punct de vedere a conținutului pentru toată perioada de valabilitate, stabilit de beneficiar, și trebuie să fie semnată sub răspundere proprie de către operatorul economic sau persoanei, împuternicite în mod legal (cu procură).

### **2.3. Condiții referitor la contract (principalele condiții tehnice, financiare și modalității de plată);**

a) termeni de livrare, instalare, configurare și lansării în exploatare – în decurs de 5 zile lucrătoare de la data semnării contractului, suport tehnic și asistență – în decursul anului;

b) achitarea – după executarea lucrărilor în baza actului de predare-primire a lucrărilor executate și facturii fiscale eliberate și primite;

c) termenul încheierii contractului – nu mai mult de 10 de zile calendaristice de la data expedierii contractului câștigătorului sau a anunțului de atribuire a contractului.

### **3. Criteriile de calificare a ofertelor:**

a) respectarea de către operatorii economici a formalităților la prezentarea ofertelor (termenul depunerii, cerințele pentru pregătire, semnătura și integritatea plicului sigilat);

b) existența documentelor care trebuie să însoțească oferta în conformitate cu documentația pentru licitație.

### **4. Criteriile de evaluare a ofertelor:**

#### **4.1. Criteriile a Regulamentului intern.**

Operatorul economic poate fi exclus de la participarea în procesul de achiziții publice în cazul în care s-a constatat că acesta:

a) se află în situația de insolvență, lichidare, suspendare sau încetare a activității, de judecată, sau în orice altă situație similară.

b) comunică informații false în materialele prezentate.

#### **4.2. Pentru evaluarea ofertelor se adoptă un număr maxim total de puncte – 100, care se distribuie după criterii în următorul volum:**

4.2.1. Criteriul abilității profesionale (ponderea – 20 % din numărul total de puncte), și inclusiv:

a) disponibilitatea de angajați calificați (punctaj maxim – 15 % din numărul total de puncte);

b) experiența operatorului economic în domeniul îndeplinirii contractelor similare de achiziții (punctaj maxim - 5% din numărul total de puncte).

4.2.2. Criteriul celui mai mic preț a ofertei (punctaj – 80 %).

Calcularea valorii ofertelor se va efectua după formula:

$$V = C_{\min} / C_{1...n} \times 80$$

unde,

V – evaluarea prețului ofertei, puncte;  
C<sub>min</sub> – prețul cel mai mic a ofertei, lei;  
C<sub>1...n</sub> – valoarea ofertei a ofertantului respectiv, lei;  
80 – numărul maxim de puncte de evaluare a valorii ofertei.

## **5. Lista documentelor, prezentate în oferta.**

5.1. Oferta comercială (oferta, conform modelului anexa nr. 6 la Regulamentul privind procedurile de achiziții a bunurilor, lucrărilor și serviciilor **avînd în vedere caietul de sarcini**);

5.2. Informația generală (conform modelului anexa nr. 7 la Regulamentul cu privire la procedurile de achiziții);

5.3. Informații despre experiența similară în ultimii trei ani de activitate (conform modelului anexa nr. 8 la Regulamentul cu privire la procedurile de achiziții);

5.4. Declarație de conformitate cu criteriile de selecție (conform modelului din anexa nr. 9 la Regulamentul cu privire la procedurile de achiziții);

5.5. Extras din Registrul de stat a persoanelor juridice și a întreprinzătorilor individuali, care să reflecte situația la zi de depunere a ofertei, prezentată pe propria răspundere;

5.6. Copia certificatului a subiectului plătitor TVA;

5.7. Certificatul privind lipsa sau existența datoriilor față de buget, eliberat nu mai mult de 30 de zile înainte de depunerea ofertei.

5.8. Documente privind nivelul parteneriatului cu vânzătorul, certificatele de Standardizare ISO, calificările specialiștilor etc.

## **6. Ofertele alternative nu sunt acceptate.**

### **7. Persoane de contact:**

Secretarul comisiei de achiziții – Rtiscev Iurie, tel.: +373 22 578 014,  
e-mail: [iurie.rtiscev@moldovagaz.md](mailto:iurie.rtiscev@moldovagaz.md)

Șeful Direcției Tehnologii Informaționale – Burcovschi Vitalie, tel: +373 22 578 182, e-mail: [vitalie.burcovschi@moldovagaz.md](mailto:vitalie.burcovschi@moldovagaz.md)

Președintele comisiei de achiziții

Sîrbu Andrian

## **Soluție de protecție și securitate pentru locurile de muncă, servere și casute postale:**

Soluție de protecție și securitate pentru:

1. 240 locuri de muncă (PC/laptop/VDI), 116 servere virtualizate și 535 casute postale Exchange. Licențierea trebuie să fie de tip bundle pentru a se putea migra licențele între ele).
2. 240 locuri de munca Patch Management

Cantitate: Este responsabilitatea Ofertantului de a determina modelul de licențiere luând în calcul cantitatea de licențe necesare și tipul acestora.

## **Caracteristici generale ale produsului:**

Produsul va conține următoarele module, toate cu posibilitatea de a fi gestionate și administrate dintr-o singură consolă de management:

- Protecție stații și servere fizice și virtualizate:
  - Windows 10,8.1,7, Vista (SP1), Mac OS X 10.15.x - 10.8.x .
  - Windows Server 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.
- Protecție și securitate pentru telefoanele mobile de tip smartphone cu sistem de operare iOS și Android.
- Protecție și securitate pentru serverele email Microsoft Exchange.

## **Consola de management:**

Pachetul de instalare va fi oferit ca un appliance virtual. Aceasta din urmă nu va necesita o licență suplimentară pentru sistemul de operare, iar imaginea de tip template va fi posibil de a fi importată în următoarele platforme de virtualizare: VMware vSphere, Microsoft Hyper-V, Oracle VM.

Consola de management va fi oferită cu o bază de date inclusă, non-relațională.

Soluția trebuie să:

- fie scalabilă, astfel ca oricare dintre roluri sau servicii să poată fi instalate separat sau împreună pe aceeași sau mai multe VDI-uri.
- asigure următoarele roluri: server cu baza de date, server de comunicație, server de actualizare, server de web.
- asigure posibilitatea de a instala serviciile de scanare centralizată pentru mediile virtuale VMware prin task din consola de management.
- includă un modul load balancer pentru performanța și redundanță
- includă mecanisme de configurare a disponibilității pentru serverul cu baze de date (clustering).
- Includă posibilitatea de a fi accesată atât de pe stațiile de lucru cât și de pe dispozitivele mobile (tabletă, smartphone).
- Interfața consolei de management va fi în limba română, rusă sau engleză. Interfața agentului care se instalează pe stații de lucru și servere, va fi în limba română și rusă.

## **Cerințe generale produs:**

Soluția trebuie să:

1. includă unul sau mai multe module de update server prin care să asigure actualizarea componentelor și a semnăturilor.
2. permită activarea/dezactivarea actualizărilor automate de produs/semnături și a consolei de management.
3. transmite alerte de ne funcționalitate, cu 30 de minute înainte de actualizare.
4. permită vizualizarea unui jurnal de modificări în care sunt precizate istoric: versiunea consolei de management, data versiunii, funcții noi și îmbunătățiri, probleme rezolvate, probleme cunoscute
5. afișeze notificările și alertele existente, să alerteze administratorul în cazul unor probleme majore (configurabile): licențiere, detecție viruși, actualizări de produs disponibile).
6. permită integrarea cu un server Syslog pentru raportarea evenimentelor antivirus.

7. permită instalarea serviciului de SMNP pentru raportarea statusului mașinilor din cadrul componentei de management.
8. permită crearea unei copii de siguranță a bazei de date a consolei de administrare, la cerere sau programat, stocată local, pe un server FTP sau în rețea.

### **Inventarierea rețelei – managementul securității**

Produsul trebuie să:

- se integreze cu domenii Active Directory multiple, VMware vCenter și să importe inventarul acestor platforme.
- permită descoperirea mașinilor din Microsoft Hyper-V, Oracle VM.
- permită descoperirea stațiilor fizice neintegrate în Active Directory (Workgroup) cu ajutorul Network discovery.
- ofere opțiuni de căutare, sortare și filtrare după numele sistemului, sistem de operare și adresa IP.
- permită instalarea la distanță sau manual a clienților antivirus pe mașini fizice și virtuale.
- permită selectarea modulelor componente atunci când se creează pachetul clientului care se instalează pe mașinile fizice/virtuale.
- permită lansarea de task-uri de scanare, actualizare, instalare, dezinstalare la distanță pentru clientul antivirus.
- ofere posibilitatea de repornire a mașinilor fizice de la distanță.
- ofere informații detaliate despre fiecare task inițiat și afișarea statutului lui.
- permită configurarea centralizată a clienților antivirus prin intermediul politicilor.
- ofere în consola de management informații detaliate ale obiectelor din consola: Nume, IP, Sistem de operare, Grup, Politica atribuită, Ultimele actualizare, Versiunea produsului, Versiunea de semnături.
- permită descoperirea tuturor aplicațiilor instalate pe toate stațiile și serverele din rețea.
- Permită crearea unui pachet unic pentru toate sistemele de operare, de stații sau servere. Astfel, administratorul va putea descărca pachetele pentru protecția stațiilor și serverelor pe care rulează sistemul de operare Windows, Linux și Mac.

### **Politici:**

Produsul trebuie să:

- permită configurarea setărilor clientului antivirus prin intermediul unei singure politici ce conține setări pentru toate modulele.
- conțină opțiuni specifice de activare/dezactivare și configurare a funcționalităților precum scanarea antivirus la cerere, firewall, controlul accesului la Internet, controlul aplicațiilor, scanarea traficului web, controlul dispozitivelor, power user.
- permită aplicarea politicilor pe mașini client, grupuri de mașini, pool-uri de resurse (VMware), domenii, unități organizaționale sau useri de active directory.
- poată fi schimbată automat în funcție de: User-ul logat, IP sau clasa de IP, Gateway-ul alocat, DNS serverul alocat, Clientul este/nu este în aceeași rețea cu infrastructura de management, Tipul rețelei (lan, wireless).

### **Monitorizare și raportare:**

Produsul trebuie să:

- permită setarea de opțiuni specifice pentru afișarea rapoartelor existente.
- dețină un panou central care să afișeze statutul modulelor și rapoartelor pentru perioadele de timp specificate.
- conțină rapoarte care prezintă statusul mașinilor clienților, al actualizărilor, fișierelor malware detectate, aplicațiile blocate, site-urilor web blocate.
- trimită rapoarte către un număr nelimitat de adrese de email.
- permită vizualizarea rapoartelor curente programate de administrator.
- permită exportarea rapoartelor în format .pdf și detaliile ca format .csv.
- includă un generator de rapoarte care să ofere posibilitatea de a investiga o problemă de securitate pe baza mai multor criterii, menținând informațiile concise și ordonate corespunzător, să includă interogări precum: starea terminalului, evenimente terminal, evenimente Exchange.

- ofere interogări legate de starea terminalului precum: tip mașină, infrastructură rețelei căreia aparține, datele agentului de securitate, starea modulelor de protecție, rolurile terminalelor.
- ofere interogări legate de evenimente precum: calculatorul ținta pe care a avut loc evenimentul, tipul starea și configurația agentului de securitate instalat, starea modulelor și rolurilor de protecție instalate pe agentul de securitate, denumirea și alocarea politicii, utilizatorul autentificat în timpul evenimentului, evenimente (site-uri blocate, aplicații blocate, detecțiile etc)
- ofere interogări de evenimente Exchange precum: direcția traficului e-mail, evenimente de securitate (detectarea programelor de tip malware sau a fișierelor atașate), măsurile implementate în fiecare situație (curățarea, ștergerea, înlocuirea sau carantinarea fișierului, ștergerea sau respingerea e-mail-ului)

#### **Carantină:**

- Produsul trebuie să permită restaurarea fișierelor din carantină în locația originală sau într-o cale configurabilă.
- Locația, fișierele și administrarea Carantinei trebuie să fie efectuată central din consola de management.

#### **Utilizatori:**

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

#### **Log-uri:**

- Soluția trebuie să permită înregistrarea acțiunilor utilizatorilor și să ofere informații detaliate pentru fiecare acțiune a unui utilizator cu posibilitatea de filtrare.

#### **Actualizari:**

Soluția trebuie să:

- permite definirea de locatii de actualizare multiple.
- permite activarea/dezactivarea actualizarilor de produs si semnaturi.
- Ofere posibilitatea ca orice client antivirus să poată fi configurat să ofere update-urile catre alt client antivirus;
- permită testarea noilor versiuni de pachete de instalare ale clientului antimalware, înainte de a fi instalate pe toate statiile si serverele din retea, evitand posibile probleme ce pot afecta serverele sau statiile critice. Astfel, serverul de actualizare va include 2 tipuri de actualizari de produs:
  - a. Ciclu rapid, gândit pentru un mediu de test in cadrul rețelei;
  - b. Ciclu lent, gândit pentru restul rețelei (productie, servere critice etc);
- permită stabilirea zonelor de test si critice din cadrul rețelei prin intermediul politicilor din consola de management.

#### **Protecție stații și servere fizice si virtualizate – caracteristici minime:**

Soluția antivirus trebuie să:

- permită instalarea personalizată a modulelor,
- includă un vaccin anti-ransomware, cu actualizări de la producător, pentru protecția împotriva tuturor amenințărilor cunoscute de tip ransomware, prin imunizarea stațiilor și serverelor, chiar daca sunt infectate și blocarea procesului de criptare.
- includă protecție împotriva atacurilor zero-day de tip exploit (atacuri direcționate).
- includă module avansate de securitate, proiectate special pentru a detecta atacuri avansate și activități suspecte în faza pre-execuție, pentru protecție împotriva: atacurilor direcționate (Targeted Attack - APT), fișierelor suspecte și traficului la nivel de rețea suspect, exploit-urilor, ransomware și grayware cu posibilitatea de stabilire a nivelului de protecție dorit: permisiv, normal, agresiv cu posibilitatea extinderii nivelului de raportare pentru a include nivelurile superioare.

- includă un sandbox în cloud-ul producătorului, ce va putea trimite manual sau automat fișiere, unde vor putea fi „detonate” pentru o analiză în profunzime.
- includă două variante de analiza a sandbox-ului: doar monitorizare sau blocare cu două tipuri de acțiuni de remediere: implicită și de siguranță. Pentru acțiunea implicită: doar raportare, dezinfectie, ștergere și transmitere în carantină. Pentru acțiunea de siguranță: ștergere sau permutare în carantină;
- Modulul de Sandbox va include și posibilitatea de trimitere manuala a fișierelor în Sandbox-ul din cloud-ul producătorului. Astfel, dacă administratorul suspectează un fișier ca fiind malicios, 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. Acest 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, LHA, Linux TAR, LZMA Compressed Archive, MS Cabinet, MSI, PKZIP, RAR, Unix Z, ZIP, ZIP (multivolume), ZOO, XZ.

### **Administrare și instalare remote:**

- Pachetele de instalare trebuie să fie configurabile cu modulele necesare: firewall, content control, device control, power user.
- Să existe posibilitatea de instalare manuală, sau automată la distanță, direct din consola de management. Instalarea se va putea face în mai multe moduri:
  - a. prin descărcarea directă a pachetului pe stația pe care se va face instalarea;
  - b. prin instalarea la distanță, direct din consola de management
  - c. trimiterea pe email (oricâte adrese) a pachetului de instalare pentru Windows, Linux, Mac.
- Consola trebuie să includă o secțiune, „Audit”, unde se vor păstra toate acțiunile întreprinse de administratori și utilizatori ai consolei, cu informații detaliate: logare, editare, creare, delogare, permutare etc.
- Produsul trebuie să ofere posibilitatea de a crea pachetele de instalare de tip web installer sau kit full.
- Produsul trebuie să permită selectarea clientului care va realiza descoperirea stațiilor din rețea, altele decât cele integrate în domen.
- Produsul va oferi posibilitatea creării unui singur pachet de instalare, utilizabil pentru stații (fizice și/sau virtuale), servere (fizice și/sau virtuale), exchange;

### **Caracteristici și funcționalități principale ale modulului antivirus**

Produsul trebuie să permită:

- stabilirea acțiunilor întreprinse de modulul antivirus la detectarea unei amenințări noi. Astfel administratorul va putea alege între următoarele acțiuni:
  1. implicită pentru fișiere infectate: interzice accesul, dezinfectează, ștergere, mută fișierele în carantină, nici o acțiune.
  2. alternativă pentru fișierele infectate: interzice accesul, dezinfectează, ștergere, permutare fișiere în carantină.
  3. acțiune implicită pentru fișierele suspecte: interzice accesul, ștergere, mută fișierele în carantină, nici o acțiune.
  4. acțiune alternativă pentru fișierele suspecte: interzice accesul, ștergere, mută fișierele în carantină.
- scanarea automată în timp real cu setarea excepțiilor, definirea unor liste de excludere de la scanarea în timp real și la cerere a anumitor directoare, discuri, fișiere, extensii sau procese, să nu scaneze arhive sau fișiere mai mari de « x » MB, definirea nivelelor de profunzime pentru scanarea în arhive.
- scanarea euristică comportamentală prin simularea unui calculator virtual în interiorul căruia sunt rulate aplicații cu potențial periculos protejând sistemul de viruși 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.
- definirea până la 16 nivele de profunzime pentru scanarea în arhive.
- 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.

#### **Firewall:**

- să ofere posibilitatea de a configura reguli de firewall pentru aplicații sau conectivitate.
- modulul să poată fi instalat/dezinstalat la cerere.
- să permită definirea de rețele de încredere pentru mașina destinație.

#### **Protecția datelor:**

- Produsul trebuie să permită 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 aplicațiilor:**

Pentru administrare și inventariere eficientă produsul trebuie să dețină un modul care va oferi posibilitatea de a:

- efectua descoperirea aplicațiilor utilizate pe stațiile utilizatorilor grupate după: nume, versiune, descoperit la, găsit pe.
- regăsi toate procesele descoperite în rețea, grupate după: nume, versiune, nume produs, versiune produs, editor/autor, descoperit la, găsit pe.
- bloca rularea anumitor aplicații sau procese definite de administrator (inclusiv subproces) după: cale fișier: local, CD-ROM, portabil sau rețea, hash, certificat.

#### **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.

### **Patch management:**

Soluția trebuie să acopere următoarele funcționalități minime:

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

\*- (7-Zip, Adobe: Acrobat/Bridge/Creative Cloud/Distiller/Dreamweaver/Flash/Photoshop/Reader, Apache, Apache Tomcat, Apple: iCloud/iTunes/Mobile Device Support/QuickTime/Safari/Software Update, WebEx: Meeting Center/Productivity Tools, Citrix: Receiver/Single Sign-On/Delivery Controller/GoToMeeting/Online Plugin/Provisioning Services/Virtual Delivery Agent/XenApp/XenDesktop, FileZilla, Foxit: PhantomPDF/Reader, Gimp, TightVNC, Google: Chrome Browser for enterprise/Drive/Picasa, Greenshot, KeePass, LibreOffice, ImgBurn, Microsoft: .NET/Azure/DirectX/Dynamics/Exchange Server/Exchange System Manager/Forefront/Internet Explorer/Internet Information Server/Lync/Lync Server/Office/Outlook/Power BI Desktop/Report Viewer/Search/Services for Unix/Sharepoint/Skype/Silverlight/System Center Operations Manager/System Center Virtual Machine Manager/SQL Server/Systems Management Server/Virtual Machine/Virtual PC/Virtual Server/Visual Basic/Visual C++/Windows/Windows Defender/WSUS/Windows Mail/Kerberos, Firefox, Thunderbird, Notepad++, GeForce Experience, Opera, Oracle: OpenOffice/VM VirtualBox,

Recuva, Prezi Desktop, RealVNC, PuTTY, Java, TeamViewer, PDF-Xchange, UltraVNC, VLC, VMware: Horizon View Client/Player/Tools/Workstation, WinSCP, Wireshark, Xmind)

**Alte cerințe:**

Perioada de suport local și mentinere de la producător:

1. Pentru soluția oferită se solicită a fi 12 luni pentru perioada de suport local și mentinere de la producător.
2. Producătorul trebuie să ofere suport 24/24, prin e-mail sau conectare de la distanță, inclusiv suport local în limba română sau rusă din partea partenerului.
3. Se va oferi manual de instalare și administrare a produsului oferit în limba română și engleză.

**Cerințe de calificare:**

1. Partenerul va prezenta autorizarea de la producător pentru produsul livrat (diploma de partener autorizat).
2. Partenerul va prezenta minim 2 certificate tehnice a persoanelor certificate pe produsul oferit;
3. Partenerul va fi certificat cu standardele ISO 27001 și 9001 pentru care va prezenta dovadă;
4. Partenerul va prezenta dovezi că posedă experiență de vânzare și implementare a produsului propus (copia minim 2 contracte).

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.

**Termen de livrare:** maxim 5 zile lucrătoare de la data intrării în vigoare a contractului, care include și timpul lucrărilor de instalare, configurare și punerea în funcțiune a soluției