

ANUNȚ DE PARTICIPARE

privind achiziționarea, prin procedura de COP: prelungirea licențelor la sistemul de protecție și securitate cibernetică, de tip Antivirus

1. Denumirea autorității contractante: *Instituția Publică „Centrul de Tehnologii Informaționale în Finanțe”*
2. IDNO: 1005600036924
3. Adresa: mun. Chișinău, str. C. Tănase 7
4. Numărul de telefon/fax: 022-822-021; 069691917
5. Adresa de e-mail și de internet a autorității contractante: ctif@ctif.gov.md; www.ctif.gov.md
6. Adresa de e-mail sau de internet de la care se va putea obține accesul la documentația de atribuire: *documentația de atribuire este anexată în cadrul procedurii în SIA RSAP.*
7. Tipul autorității contractante și obiectul principal de activitate (dacă este cazul, mențiunea că autoritatea contractantă este o autoritate centrală de achiziție sau că achiziția implică o altă formă de achiziție comună): *Instituție Publică, Servicii informaționale.*
8. Cumpărătorul invită operatorii economici interesați, care îi pot satisface necesitățile, să participe la procedura de achiziție privind livrarea/prestarea/executarea următoarelor bunuri /servicii/lucrări:

Nr. lot	Cod CPV	Denumirea serviciilor	UM	Cantitatea	Specificarea tehnică deplină solicitată, standarde de referință	Valoarea estimată (fără TVA)
1	48761000-0	Prelungirea licențelor la sistemul de protecție și securitate cibernetică, de tip Antivirus	licențe	600	Conform anexei la Anunțul de participare	162 600,00
Valoarea totală estimată, lei (fără TVA)						162 600,00

9. În cazul în care contractul este împărțit pe loturi un operator economic poate depune oferta (se va selecta): *Pentru toate loturile.*
10. Admiterea sau interzicerea ofertelor alternative: *nu se vor admite.*
11. Termenii și condițiile de livrare/prestare/executare solicitați: *Vânzătorul va preda licențele, începând cu data de 10.05.2021, pe un termen de 12 luni.*
12. Termenul de valabilitate a contractului: *12 luni.*
13. Contract de achiziție rezervat atelierelor protejate sau că acesta poate fi executat numai în cadrul unor programe de angajare protejată (după caz): *nu.*
14. Prestarea serviciului este rezervată unei anumite profesii în temeiul unor acte cu putere de lege sau al unor acte administrative (după caz): *nu.*
15. Scurta descriere a criteriilor privind eligibilitatea operatorilor economici care pot determina eliminarea acestora și a criteriilor de selecție; nivelul minim (nivelurile minime) al (ale) cerințelor eventual impuse; se menționează informațiile solicitate (DUAE, documentație):

Nr. d/o	Descrierea criteriului/cerinței	Mod de demonstrare a îndeplinirii criteriului/cerinței:	Nivelul minim/ Obligatorietatea
1	Demonstrarea eligibilității (în conformitate cu art. 18 din Legea nr. 131 din 03.07.2015 privind achizițiile publice)	Formularul DUAЕ, confirmat prin semnătura electronică	Obligatoriu
2	Formularul ofertei	Formularul 3.1, confirmat prin semnătura electronică	Obligatoriu
3	Oferta tehnică	Formularul 4.1, confirmat prin semnătura electronică	Obligatoriu
4	Oferta financiară	Formularul 4.2, confirmat prin semnătura electronică	Obligatoriu
5	Garanția la oferta în mărime de 1% din valoarea ofertei fără TVA	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; semnată electronic de operatorul economic Sau, prin transfer la contul autorității contractante, conform datelor bancare descrise în documentația standard, confirmată prin Ordin de plată semnat electronic de operatorul economic	Obligatoriu
6	Garanție de bună execuție a contractului în mărime de 3% din suma totală a contractului	Garanția de bună execuție (emisă de o bancă comercială) conform formularului F3.3 din secțiunea a 3-a – Formulare pentru depunerea ofertei; Sau, prin transfer la contul autorității contractante, conform datelor bancare descrise în documentația standard, cu prezentarea în Ordinului de plată în original	Obligatoriu (pentru ofertantul declarat câștigător)
7	Document care dovedește că operatorul economic este distribuitor oficial sau partener autorizat de producător pentru produsul solicitat (MAF)	Copia certificatului (MAF), ce atestă că operatorul economic este partener autorizat pentru produsele de antivirus ca dovadă a dreptului de a vinde produsele pe piața RM, confirmată prin semnătura electronică a operatorului economic	Obligatoriu
8	Minim doi specialiști tehnici, certificați în administrarea produsului oferit.	Copie certificat, confirmată prin semnătura electronică a operatorului economic	Obligatoriu
9	Experiența similară în domeniul livrării produsului software antivirus	Prezentarea minim 2 scrisori de recomandare de la clienți, confirmate prin semnătura electronică a operatorului economic	Obligatoriu

16. Motivul recurgerii la procedura accelerată (în cazul licitației deschise, restrânse și al procedurii negociate), după caz: *nu e cazul*.

17. Tehnici și instrumente specifice de atribuire (dacă este cazul specificați dacă se va utiliza acordul-cadru, sistemul dinamic de achiziție sau licitația electronică): *se va utiliza licitație electronică din trei runde, pasul minim fiind de 1%.*

18. Condiții speciale de care depinde îndeplinirea contractului (după caz): *nu sunt.*
19. Criteriul de evaluare aplicat pentru adjudecarea contractului: *prețul cel mai scăzut.*
20. Termenul limită de depunere/deschidere a ofertelor:
- până la: *conform datelor SIA RSAP.*
 - pe: *conform datelor SIA RSAP.*
21. Adresa la care trebuie transmise ofertele sau cererile de participare:
- Ofertele sau cererile de participare vor fi depuse electronic prin intermediul SIA RSAP.*
22. Termenul de valabilitate a ofertelor: *45 zile.*
23. Locul deschiderii ofertelor: *SIA RSAP.*
- Ofertele întârziate vor fi respinse.*
24. Persoanele autorizate să asiste la deschiderea ofertelor:
- Ofertanții sau reprezentanții acestora au dreptul să participe la deschiderea ofertelor, cu excepția cazului când ofertele au fost depuse prin SIA „RSAP”.*
25. Limba sau limbile în care trebuie redactate ofertele sau cererile de participare: *limba de stat.*
26. Respectivul contract se referă la un proiect și/sau program finanțat din fonduri ale Uniunii Europene: *nu.*
27. Denumirea și adresa organismului competent de soluționare a contestațiilor:
- Agencia Națională pentru Soluționarea Contestațiilor.*
- Adresa: mun. Chișinău, bd. Ștefan cel Mare și Sfânt nr.124 (et.4), MD 2001;*
- Tel/Fax/email: 022-820 652, 022 820-651, contestatii@ansc.md*
28. Data (datele) și referința (referințele) publicărilor anterioare în Jurnalul Oficial al Uniunii Europene privind contractul (contractele) la care se referă anunțul respective (dacă este cazul): *nu.*
29. În cazul achizițiilor periodice, calendarul estimat pentru publicarea anunțurilor viitoare:--.
30. Data publicării anunțului de intenție sau, după caz, precizarea că nu a fost publicat un astfel de anunț: --.
31. Data transmiterii spre publicare a anunțului de participare: *conform datelor din SIA RSAP.*
32. În cadrul procedurii de achiziție publică se va utiliza/accepta:
- | Denumirea instrumentului electronic | Se va utiliza/accepta sau nu |
|------------------------------------------------------------------|------------------------------|
| Depunerea electronică a ofertelor sau a cererilor de participare | Da |
| Sistemul de comenzi electronice | Nu |
| Facturarea electronică | Da |
| Plățile electronice | Da |
33. Contractul intră sub incidența Acordului privind achizițiile guvernamentale al Organizației Mondiale a Comerțului (numai în cazul anunțurilor transmise spre publicare în Jurnalul Oficial al Uniunii Europene): *nu.*
34. Alte informații relevante: --

Conducătorul grupului
de lucru pentru achiziții



Vadim MUNTEAN

la Anunțul de participare _____,
privind achiziționarea: prelungirea
licențelor la sistemul de protecție și
securitate cibernetică, de tip Antivirus

Specificațiile tehnice minime pentru sistemul de protecție și securitate cibernetică, de tip Antivirus

Produsul antivirus oferit trebuie să ocupe locurile de top în testele internaționale independente cu renume mondial în domeniu (certificări AV-TEST) și să fie prezent în mențiunile Gartner. Satisfacerea necesităților minime va constitui: **500 licențe** (workstation PC, mailboxes) și **100 licențe** (VDI/VS/Server), în scopul managementului centralizat pentru dispozitive.

Licențele oferite trebuie să fie capabile să prelungească pe un termen de 12 luni, licențele existente compatibile sau echivalente pentru Bitdefender Gravity Zone Elite.

Caracteristici generale ale produsului:

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

1. Protecție stații și servere fizice și virtualizate:
 - 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 2003/2008/2008/2012 R2/2012/2012 R2/2016.
 - 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.
2. Protecție și securitate pentru telefoanele mobile de tip smartphone cu sistem de operare iOS și Android.
3. Protecție și securitate de tip „sandboxing” pentru serverele și stațiile de lucru;
4. Controlul dispozitivelor, controlul accesului la Internet, filtrarea traficului prin modul de tip firewall pentru mașinile fizice și virtuale
5. 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, Citrix XenServe, Microsoft Hyper-V, Red Hat Enterprise Virtualization, KVM, Oracle VM.

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

Soluția trebuie să:

1. Fie scalabilă, astfel ca oricare dintre roluri sau servicii să poată fi instalate separat sau împreună pe aceeași sau mai multe VDI-uri.
2. Asigure următoarele roluri: server cu baza de date, server de comunicație, server de actualizare, server de web.

3. Asigure posibilitatea de a instala serviciile de scanare centralizată pentru mediile virtuale VMware și Citrix prin task din consola de management.
4. Includă un modul load balancer pentru performanța și redundanță
5. Includă mecanisme de configurare a disponibilității pentru serverul cu baze de date (clustering).
6. 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. Interfața agentului care se instalează pe stații de lucru și servere, va fi în limba română.

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 SNMP 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:

1. Se integreze cu domenii Active Directory multiple, VMware vCenter, Citrix Xen și să importe inventarul acestor platforme.
2. Permită descoperirea mașinilor din Microsoft Hyper-V, Red Hat VM, Oracle VM, KVM.
3. Permită descoperirea stațiilor fizice neintegrate în Active Directory (Workgroup) cu ajutorul Network discovery.
4. Ofere opțiuni de căutare, sortare și filtrare după numele sistemului, sistem de operare și adresa IP.
5. Permită instalarea la distanță sau manual a clienților antivirus pe mașini fizice și virtuale.
6. Permită selectarea modulelor componente atunci când se creează pachetul clientului care se instalează pe mașinile fizice/virtuale.
7. Permită lansarea de task-uri de scanare, actualizare, instalare, dezinstalare la distanță pentru clientul antivirus.
8. Ofere posibilitatea de repornire a mașinilor fizice de la distanță.
9. Ofere informații detaliate despre fiecare task inițiat și afișarea statutului lui.
10. Permită configurarea centralizată a clienților antivirus prin intermediul politicilor.
11. 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.
12. Permită descoperirea tuturor aplicațiilor instalate pe toate stațiile și serverele din rețea.

13. Permite 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:

1. Permite configurarea setărilor clientului antivirus prin intermediul unei singure politici ce conține setări pentru toate module
2. 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.
3. Permite aplicarea politicilor pe mașini client, grupuri de mașini, pool-uri de resurse (VMware), domeniu, unități organizaționale sau useri de active directoy.
4. 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:

1. Permite setarea de opțiuni specifice pentru afișarea rapoartelor existente.
2. Dețină un panou central care să afișeze statutul modulelor și rapoartele lor pentru perioadele de timp specificate.
3. Conțină rapoarte care prezintă statusul mașinilor clienților, al actualizărilor, fișierelor malware detectate, aplicațiile blocate, site-urilor web blocate.
4. Trimite rapoarte către un număr nelimitat de adrese de email.
5. Permite vizualizarea rapoartelor curente programate de administrator.
6. Permite exportarea rapoartelor în format .pdf și detaliile ca format .csv.
7. Include 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.
8. Ofere interogări legate de starea terminalului precum: tip mașină, infrastructură rețelei căreia aparține, datele agentului de securitate, starea modulelor de protecție, rolurile terminalelor.
9. 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)
10. 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 plasarea în carantină a fișierului, ștergerea sau respingerea e-mail-ului)

Carantină:

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

Utilizatori:

1. 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.
2. Utilizatorii să poată fi importați din Microsoft Active Directory sau creați în consola de management.
3. Să fie posibilă deconectarea automată a oricărui tip de utilizator după un anumit timp.

Log-uri:

1. 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:

1. Permită definirea de locații de actualizare multiple.
2. Permită activarea/dezactivarea actualizărilor de produs si semnături.
3. Ofere posibilitatea ca orice client antivirus să poată fi configurat să ofere update-urile către alt client antivirus;
4. Permită testarea noilor versiuni de pachete de instalare ale clientului antimalware, înainte de a fi instalate pe toate stațiile si serverele din rețea, evitând posibile probleme ce pot afecta serverele sau stațiile critice. Astfel, serverul de actualizare va include 2 tipuri de actualizări de produs:
5. Ciclu rapid, gândit pentru un mediu de test în cadrul rețelei;
6. Ciclu lent, gândit pentru restul rețelei (producție, servere critice etc);
7. 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:

1. Permită instalarea personalizată a modulelor,
2. 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 dacă sunt infectate și blocarea procesului de criptare.
3. Includă protecție împotriva atacurilor zero-day de tip exploit (atacuri direcționate).
4. 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.
5. 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.
6. 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, dezinfecție, ștergere și transmitere în carantină. Pentru acțiunea de siguranță: ștergere sau permutare în carantină;

7. Modulul de Sandbox va include si posibilitatea de trimitere manuala a fișierelor in Sandbox-ul din cloud-ul producătorului. Astfel, daca administratorul suspectează un fișier ca fiind malițios, îl poate trimite manual in Sandbox pentru a fi „detonat” si a afla verdictul. Va putea trimite mai multe fișiere de odată, cu posibilitate de a specifica daca vor fi „detonate” individual sau toate in același timp. Acest modul va poate 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 daca sunt incluse in 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:

1. Pachetele de instalare trebuie să fie configurabile cu modulele necesare: firewall, content control, device control, power user.
2. Să existe posibilitatea de instalare manuală, sau automată la distanță, direct din consola de management. Instalarea se va putea face in mai multe moduri:
 - prin descărcarea directa a pachetului pe stația pe care se va face instalarea;
 - prin instalarea la distanta, direct din consola de management
 - remiterea pe email (oricâte adrese) a pachetului de instalare pentru Windows, Linux, Mac.
3. 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.
4. Produsul trebuie să ofere posibilitatea de a crea pachetele de instalare de tip web installer sau kit full.
5. Produsul trebuie să permită selectarea clientului care va realiza descoperirea stațiilor din rețea, altele decât cele integrate în domen.
6. Produsul va oferi posibilitatea creării unui singur pachet de instalare, utilizabil pentru stații (fizice si/sau virtuale), servere (fizice si/sau virtuale), exchange;

Caracteristici și funcționalități principale ale modulului antivirus

Produsul trebuie sa permită:

1. Stabilirea acțiunilor întreprinse de modulul antivirus la detectarea unei amenințări noi. Astfel administratorul va putea alege între următoarele acțiuni:
2. Implicită pentru fișiere infectate: interzice accesul, dezinfectează, ștergere, mută fișierele în carantină, nici o acțiune.
3. Alternativă pentru fișierele infectate: interzice accesul, dezinfectează, ștergere, permutare fișiere în carantină.
4. Acțiune implicită pentru fișierele suspecte: interzice accesul, ștergere, mută fișierele în carantină, nici o acțiune.
5. Acțiune alternativă pentru fișierele suspecte: interzice accesul, ștergere, mută fișierele în carantină.
6. 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.

7. 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.
8. Scanarea oricărui suport de stocare a informației (CD-uri, harduri externe, unități partajate etc).
9. Scanarea automată a emailurilor la nivelul stației de lucru pentru POP3/SMTP.
10. Definirea până la 16 nivele de profunzime pentru scanarea în arhive.
11. Configurarea căilor ce urmează a fi scanate la cerere.
12. 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.
13. Setarea priorităților scanărilor programate.
14. Configurarea scanării în cloud sau pe mașina de scanare instalată în rețea și parțial scanarea locală pentru stațiile ce nu au suficiente resurse hardware
15. 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.
16. Setarea a tipurilor de detecție: bazate pe semnături, bazate de comportamentul fișierelor și bazate pe monitorizarea proceselor.
17. Scanarea paginilor web.
18. Setarea a unei parole pentru protecția la dezinstalare.
19. Modul de antiphishing.
20. Protecție în timp real pe mașinile cu sistem de operare Linux în conformitate cu versiunea de kernel instalată.
21. Instalarea clientului pe mașinile virtuale parte a unui pool doar pe mașina de tip template, după care se recompilează pool-ul de mașini virtuale.

Firewall:

1. Să ofere posibilitatea de a configura reguli de firewall pentru aplicații sau conectivitate.
2. Modulul să poată fi instalat/dezinstalat la cerere.
3. Să permită definirea de rețele de încredere pentru mașina destinație.

Protecția datelor:

1. 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, violența, pornografie etc).

Controlul aplicațiilor:

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

1. Efectua descoperirea aplicațiilor utilizate pe stațiile utilizatorilor grupate după: nume, versiune, descoperit la, găsit pe.
2. Regăsi toate procesele descoperite în rețea, grupate după: nume, versiune, nume produs, versiune produs, editor/autor, descoperit la, găsit pe.
3. 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:

4. Poate fi instalat/dezinstalat conform setărilor stabilite.
5. 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.
6. Permite configurarea de reguli prin care se vor defini permisiunile pentru dispozitivele conectate la mașina client.
7. 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:

1. Poată fi instalat/dezinstalat în funcție de preferința administratorului.
2. 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.
3. Permită administratorului soluției să suprascrie din consola setările aplicate de utilizatorii Power User.

Actualizare:

Produsul trebuie să ofere posibilitatea de efectuare a actualizărilor:

1. La nivel de stație în mod silențios (fără avertizări).
2. Folosind unul sau mai multe servere de actualizare.
3. Pentru locațiile la distanță prin intermediul unui client antivirus care are și rol de server de actualizare.

Protecție și securitate pentru telefoane mobile de tip smartphone:

Produsul trebuie să ofere client de protecție pentru dispozitive mobile cu platforma Android (de la v. 2.2) și iOS (de la v 5.)

Clientul mobil trebuie să:

1. Permită asocierea unui dispozitiv cu un utilizator din Active Directory.
2. Ofere posibilitatea instalării prin trimiterea unui email către utilizator cu detaliile de instalare.
3. Permită activarea dispozitivului mobil în consola de management prin scanarea unui cod QR.
4. Asigure disponibilitatea pachetele de instalare pe Apple App Store si Google Play.
5. Să poată întreprinde următoarele acțiuni: blocarea dispozitivului; deblocarea dispozitivului; ștergerea datelor si revenirea la setările din fabrica; localizarea dispozitivului; scanarea dispozitivului(doar pentru cele cu sistem de operare Android); criptarea memoriei dispozitivului(doar pentru cele cu sistem de operare Android).

6. Consola va permite raportarea dispozitivelor: active, inactive, deconectate, cu sistemul de operare modificat astfel încât utilizatorul să aibă acces total asupra lui (rooted or jailbroken devices).
7. Întreprindă automat acțiuni în cazul în care un dispozitiv nu este conform cu setările dorite: Ignorare; Blocarea accesului; Blocarea dispozitivului; Ștergerea datelor și revenirea la setările din fabrică; Ștergerea dispozitivului din consola.
8. Ofere posibilitatea de a impune blocarea dispozitivelor cu ajutorul unei parole cu complexitate și perioada de expirare configurabilă, posibilitate de autoblocare a dispozitivului după un număr de minute definite de administrator.
9. Ofere posibilitate de a genera mai multe profiluri care vor stabili reguli de securitate pentru conectivitatea la Wi-Fi sau VPN (numai pentru sistemul de operare iOS) dar și unele legate de accesul la anumite pagini de internet, precum: permiterea, blocarea sau programarea pentru anumite zile și intervale orare a accesului la anumite pagini de internet; crearea unor excepții pentru blocarea sau permiterea accesului către anumite pagini de internet.
10. Include posibilitatea de configurare profilurile acces pagini de internet pentru sistemul de operare iOS cu opțiuni de activare sau dezactivare a: utilizării browser-ului Safari; opțiunii de completare automată a informațiilor; alertării utilizatorului în cazul accesării unor pagini frauduloase; Javascript; Pop-up-urilor; Cookie-uri.

Protecție și securitate pentru serverele de mail Microsoft Exchange

Soluția de protecție a serverelor de Exchange trebuie să:

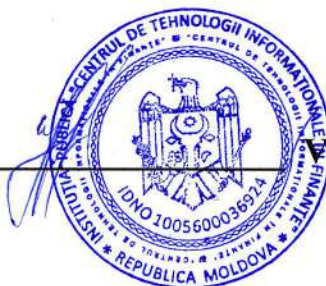
1. Ofere protecție antivirus, antispam (inclusiv antiphishing), precum și filtrare de atașamente și conținut, prin integrarea cu serverul Microsoft Exchange cu posibilitatea de scanarea antivirus la cerere a bazelor de date Exchange.
2. Asigure scanarea atașamentelor și a conținutului mesajelor în timp real, fără a afecta vizibil performanța serverului de mail.
3. Asigure actualizarea antivirus automat la un interval de maxim 1 ora, precum și la cerere.
4. Include, pe lângă detecția pe baza de semnături, scanarea euristică comportamentală pentru a proteja sistemul de viruși necunoscuți prin detectarea codurilor.
5. Ofere opțiuni multiple de acțiune la identificarea unui atașament virusat (dezinfectare, ștergere, mutare în carantină).
6. Ofere protecție anti-spyware (cu bază de semnături actualizabilă) pentru a preveni furtul de date confidențiale.
7. Ofere protecție antispam (cu o bază de semnături actualizabilă). 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 detectarea automată a mesajelor scrise cu caractere chirilice sau asiatice.
8. 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.
9. Ofere un serviciu/filtru online pentru îmbunătățirea protecției împotriva valurilor de spam nou apărute.
10. Ofere posibilitatea de a defini politici de filtrare antivirus, antispam, a conținutului sau atașamentelor pentru diferite grupuri sau utilizatori.
11. Asigure actualizarea produsului să fie 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.
12. Ofere statistici atât referitoare la scanarea antivirus cât și la scanarea antispam.
13. Să integreze în cadrul consolei de management unitar al soluției antivirus în consola centrală unică.

Alte cerințe:

Perioada de suport local și menținere de la producător:

1. Pentru soluția ofertată se solicită a fi 12 luni pentru perioada de suport local și menținere 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. Ofertantul va prezenta autorizarea de la producător pentru produsul și suportul livrat;
4. Ofertantul trebuie să aibă minim 2 persoane tehnice calificate pe produsul oferit;
5. Se va oferi manual de instalare și administrare a produsului oferit în limba română și engleză.
6. Compania învingătoare trebuie să prezinte până la semnarea contractului pachetul antivirus (consolă de management, etc) pentru a verifica în practică dacă produsul dat corespunde cerințelor cerute;
7. Lucrările de instalare, configurare, punerea în funcțiune a soluției trebuie să fie executate de Ofertant, iar costul acestora trebuie să fie incluse în ofertă;
8. Termen de livrare: din data de 10.05.2020, pe un termen de 12 luni.

**Conducătorul grupului
de lucru pentru achiziții:**



Vadim MUNTEAN