Specificaţii tehnice

[Acest tabel va fi completat de către ofertant în coloanele 2, 3, 4, 6, 7, iar de către autoritatea contractantă – în coloanele 1, 5,]

Numărul procedurii de achiziţie:	**ocds-b3wdp1-MD-1650618355879 din 22.04.2022**
Denumirea procedurii de achiziţie:	**Licență antivirus**

Denumirea bunurilor/serviciilor	**Denumirea modelului bunului/serviciului**	**Ţara de origine**	**Producătorul**	**Specificarea tehnică deplină solicitată de către autoritatea contractantă**	**Specificarea tehnică deplină propusă de către ofertant**	**Standarde de referinţă**
1	2	3	4	5	6	7
Bunuri/servicii						
Lotul 1:						
Licență antivirus	**F-Secure Business Suite Premium License for 1 year Governmental**	**Finlanda**	**F-Secure**	Conform caietului de sarcini	Conform Anexei la formular. Matricea de conformitate	

Semnat:
Nume: **Irina Vicol**
În calitate de: **Administrator**
Ofertantul: **Xontech Systems SRL**
Adresa: str. Alexandru cel bun 85, MD-2012, mun Chisinau, Republica Moldova.
Data: 22.04.2022

Digitally signed by Vicol Irina
Date: 2022.04.29 12:50:34 EEST
Reason: MoldSign Signature
Location: Moldova

XONTECH

Anexa

Matricea de conformitate conform caietului de sarcini solicitate in SIA RSAP

<table>
<tr><th>Nr. d/o</th><th>Denumirea bunurilor solicitate</th><th>Specificarea tehnică deplină solicitată de către autoritatea contractantă</th><th>Specificarea tehnică deplină propusă de către ofertant</th></tr>
<tr><td>1.</td><td>Licență antivirus</td><td>

Cerințe generale solicitate:

<table>
<tr><th>Nr. lot</th><th>Denumirea bunurilor / serviciilor solicitate</th><th>Cantitatea (buc)</th><th>Specificația tehnică deplină solicitată, standarde de referință</th></tr>
<tr><td>1</td><td>Licență antivirus</td><td></td><td></td></tr>
<tr><td>1.1</td><td>Licențe antivirus (servere fizice)</td><td>5</td><td>Sistem de operare: Windows Server R2 2012, 2016, 2019;
Termen de valabilitate: 12 luni de la data instalării</td></tr>
<tr><td>1.2</td><td>Licențe antivirus (virtual machine’s)</td><td>5</td><td>Sistem de operare: Windows Server R2 2012,2016, 2019;
Termen de valabilitate: 12 luni de la data instalării</td></tr>
<tr><td>1.3</td><td>Licențe antivirus (stații de lucru)</td><td>Cel puțin 70</td><td>Sistem de operare: Windows 10;
Termen de valabilitate: 12 luni de la data instalării</td></tr>
</table>

</td><td>

Soluția ofertată: F-Secure Business Suite Premium License for 1 year Governmental – 80 licențe care vor acoperi serverele fizice, masinile virtuale și stațiile de lucru solicitate.

Specificații tehnice ofertate

<table>
<tr><th>Nr. lot</th><th>Denumirea bunurilor / serviciilor solicitate</th><th>Cantitatea (buc)</th><th>Specificația tehnică deplină solicitată, standarde de referință</th></tr>
<tr><td>1</td><td colspan="3">F-Secure Business Suite Premium License for 1 year Governmental – 80 licențe care vor acoperi cantitatea solicitată.</td></tr>
<tr><td>1.1</td><td>Licențe antivirus (servere fizice)</td><td rowspan="3">80</td><td>Sistem de operare: Windows Server R2 2012, 2016, 2019;
Termen de valabilitate: 12 luni de la data instalării</td></tr>
<tr><td>1.2</td><td>Licențe antivirus (virtual machine’s)</td><td>Sistem de operare: Windows Server R2 2012,2016, 2019;
Termen de valabilitate: 12 luni de la data instalării</td></tr>
<tr><td>1.3</td><td>Licențe antivirus (stații de lucru)</td><td>Sistem de operare: Windows 10;
Termen de valabilitate: 12 luni de la data instalării</td></tr>
</table>

</td></tr>
</table>

		1. Prezența unei interfețe / consolă de management web, care să asigure toate funcționalitățile de control și administrare; 2. Disponibilitatea unui instrument de management centralizat (server de management) al parametrilor și setărilor de protecție împotriva amenințărilor pe stațiile de lucru client. 3. Soluția achiziționată va oferi protecție împotriva malware (viruși, spyware, worms, tojans, rootkit, a mesajelor de tip spam, a tentativelor de fraudare de tip phishing și a altor coduri periculoase) pentru întreaga rețea. 4. Soluția trebuie sa fie bazata pe un agent unic pentru stațiile de lucru, servere fizice si virtuale; 5. Protecție pentru servere fizice și virtuale, stații de lucru; 6. Panou de monitorizare și raportate, cu opțiuni specifice pentru orice tip de raport; 7. Posibilitate de integrare cu domenii: Active Directory, VMware vCenter, Citrix Xen; 8. Soluția va permite instalarea la distanță sau manual a clienților anti malware pe mașini fizice și virtuale; 9. Soluția va permite lansarea de task-uri de scanare, actualizare, instalare, dezinstalarea la distanta pentru clientul anti malware; 10. Soluția va permite configurarea centralizata a clienților anti malware prin intermediul politicilor; 11. Soluția va permite diagnosticarea bazei de date a serverului de management; 12. Posibilitatea de a instala serverul de management în cadrul sistemului de operare Windows Server.	1. Soluția propusă oferă prezența unei console de management web, care asigura toate funcționalitățile de control și administrare; 2. Este disponibil instrumentul de management centralizat al parametrilor și setărilor de protecție împotriva amenințărilor pe stațiile de lucru client; 3. Soluția propusă oferă protecție împotriva malware (viruși, spyware, worms, trojans, rootkit, a mesajelor de tip spam, a tentativelor de fraudare de tip phishing și a altor coduri periculoase) pentru întreaga rețea; 4. Soluția propusă este bazata pe un agent unic pentru stațiile de lucru, servere fizice si virtuale; 5. Soluția propusă oferă protecția pentru servere fizice și virtuale, stații de lucru; 6. Este prezent panoul de monitorizare si raportare, cu opțiuni specific pentru orice tip de raport; 7. Este posibila integrare cu domenii: Active Directory, VMware, vCenter, Citrix Xen; 8. Soluția propusă permite instalarea la distanta sau manual a clienților anti malware pe mașini fizice si virtuale; 9. Soluția propusă permite lansarea de task-uri de scanare, actualizare, instalare, dezinstalarea la distanta pentru clientul anti malware; 10. Soluția propusă permite configurarea centralizata a clienților anti malware prin intermediul politicilor; 11. Soluția propusă permite diagnosticarea bazei de date a serverului de management; 12. Este posibil de instalat serverul de management in cadrul sistemului de operare Windows Server;

		13. Se vor oferi în consola de management informații detaliate ale obiectelor din consola: Nume, IP, Sistem de operare, Grup, Politica atribuita, Ultimele actualizare, Versiunea produsului, Versiunea de semnături; 14. Existența unui mecanism de detectare a conformității sau a neconformității cu criteriile specificate pentru prezența corecțiilor de securitate (patch-uri) în sistemul de securitate al sistemului de operare la stațiile de lucru; 15. Disponibilitatea propriei tehnologiei incorporate eficiente pentru instalarea forțată centralizată a actualizărilor de securitate (inclusiv patch-uri Windows Update) pe stații de lucru cu sistem de operare Windows; 16. Prezența unui mecanism încorporat (instrumente) pentru crearea și restaurarea copiilor de rezervă ale serverului de administrare (inclusiv baza de date pe care rulează serverul); 17. Capacitatea de a crea politici separate pentru fiecare tip de protecție (protecție antivirus, firewall, IPS etc.); 18. Abilitatea de a exporta / importa politici într-un fișier separat; 19. Prezența unui agent de protecție pentru stațiile de lucru 20. Soluția va permite descoperirea tuturor aplicațiilor instalate pe toate stațiile și serverele din rețea, prin rularea unui task din consola de administrare; 21. Soluția va permite configurarea setărilor clientului anti malware prin intermediul unei singure politici ce conține setări pentru toate modulele; 22. Soluția include un generator de rapoarte care oferă posibilitatea de a investiga o problema de securitate pe baza mai multor	13. Soluția propusă oferă în consola de management informații detaliate ale obiectelor din consola: Nume, IP, Sistem de operare, Grup, Politica atribuita, Ultimele actualizare, Versiunea produsului, Versiunea de semnături; 14. Este prezent mecanismul de detectare a conformității sau a neconformității cu criteriile specificate pentru prezența corecțiilor de securitate (patch-uri) în sistemul de securitate al sistemului de operare la stațiile de lucru; 15. Este prezenta propria tehnologie incorporata eficienta pentru instalarea forțată centralizată a actualizărilor de securitate (inclusiv patch-uri Windows Update) pe stații de lucru cu sistem de operare Windows; 16. Este prezent mecanismul încorporat (instrumente) pentru crearea și restaurarea copiilor de rezervă ale serverului de administrare (inclusiv baza de date pe care rulează serverul); 17. Este posibil de a crea politici separate pentru fiecare tip de protecție (protecție antivirus, firewall, IPS etc.); 18. Este posibil de a exporta/importa politici intr-un fișier separat; 19. Este prezent agentul de protecție pentru stațiile de lucru; 20. Soluția propusă permite descoperirea tuturor aplicațiilor instalate pe toate stațiile și serverele din rețea, prin rularea unui task din consola de administrare; 21. Soluția propusă permite configurarea setărilor clientului anti malware prin intermediul unei singure politici ce conține setări pentru toate modulele; 22. Soluția propusă include un generator de rapoarte care oferă posibilitatea de a investiga o problema de securitate pe baza mai

		criterii; 23. Soluția va permite restaurarea fișierelor din carantină în locația originala sau într-o cale configurabila; 24. Administrare pe bază de roluri; 25. Înregistrare tuturor acțiunilor utilizatorilor. Jurnalizare evenimente; 26. Posibilitatea de a configura reguli de firewall pentru aplicații sau conectivitate; 27. Consola va avea integrat un modul dedicat controlului accesului la Internet; 28. Soluția va dispune de funcțional de control a dispozitivelor; 29. Funcțional de alertă; 30. Ofertantul va asigura pregătirea mediului de instalare pentru soluția propusă, după care va asigura implementarea inițială a soluției aplicative în mediul de producție și mediul de testare. 31. Ofertantul va asigura integrarea soluției propuse cu Active Directory. Va seta politici de securitate. 32. Ofertantul trebuie sa asigure instruire și training departamentului IT din cadrul instituției.	multor criterii; 23. Soluția propusă permite restaurarea fișierelor din carantină în locația originala sau într-o cale configurabila; 24. Soluția propusă oferă Administrarea pe baza de roluri; 25. Soluția propusă oferă Înregistrarea tuturor acțiunilor utilizatorilor. Jurnalizare evenimente; 26. Soluția propusă oferă posibilitatea de a configura reguli de firewall pentru aplicații sau conectivitate; 27. Consola dispune de un modul dedicat controlului accesului la internet; 28. Soluția propusă dispune de funcțional de control a dispozitivelor; 29. Soluția propusă oferă funcțional pentru alertare; 30. Ofertantul va asigura pregătirea mediului de instalare pentru soluția propusă, după care va asigura implementarea inițială a soluției aplicative în mediul de producție și mediul de testare. 31. Ofertantul va asigura integrarea soluției propuse cu Active Directory si setarea politicilor de securitate. 32. Ofertantul va asigura instruire și training departamentului IT din cadrul instituției.