Cerințe generale

Soluția oferită trebuie să satisfacă următoarele cerințe:

1. Prezența unei interfață / 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 v Center, 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.
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 module;
22. Soluția include un generator de rapoarte care oferă posibilitatea de a investiga o problema de securitate pe baza mai multor 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 controlul 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. Seta politici de securitate;
32. Ofertantul trebuie sa asigure instruire și training departamentului IT din cadrul instituției.

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

Președinta
Comisiei Electorale Centrale
Conducătorul grupului de lucru _____ **/ Angelica CARAMAN**

L.Ș.