Caracteristici tehnice ale produsului care asigură îndeplinirea serviciilor de protecție ofertate

Caracteristici generale:

* să asigurare protecţie avansată în timp real antivirus, anti-malware, anti-spam, anti-spyware, anti-phishing, anti-ransomware, firewall

Modulul antivirus şi anti-spyware:

* să asigurare diferite niveluri de detecţie bazată pe semnături, bazată de comportamentul fişierelor, pe monitorizarea proceselor.
* să aibă un singur motor de scanare bazat pe scanare automată în timp real, scanare în profunzime a arhivelor, euristică comportamentală, scanare bazată pe semnături, scanarea la cerere și la acces a oricărui mediu de stocare al informaţiei, scanare automată a emailurilor atât la primire cât şi la trimitere, scanare în reţea.
* să permită funcţionarea şi în modul standalone (cu sau fără suport de reţea)

Modulul anti-malware:

* să asigurare protecţie în timp real și filtrare contra website-uri maliţioase
* să ofere protecţie completă contra vulnerabilităţiilor de sistem şi software, astfel încât să nu fie exploatate de către un program maliţios
* să asigurare straturi multiple de protecţie anti-ransomware cu rol de prevenire, detecţie şi remediere
* să monitorizeze procesele în timp real.

Modulul anti-spam:

* să permită funcţia de filtrare a mesajelor de tip spam
* să permită funcţia de scanare avansată anti-spam
* să se adapteze la noile tehnici de lansare a spam-ului

Modulul anti-phishing:

* să blocheze automat accesul la pagini web de tip phishing
* să detecteze trafic web şi de reţea suspecte

Modulul actualizare:

* Actualizări de semnături de antivirus şi antispyware periodice în mod automat şi manual, protecţie continuă împotriva celor mai noi ameninţări informatice şi upgrade la noile versiuni ale produsului pe perioada derulării contractului.

Modulul carantină:

* să trimită în carantină fişierele suspecte sau infectate printr-un mediu securizat care să nu afecteze funcţionalitatea şi disponibilitatea aplicaţiilor care rulează în timp real pe staţia de lucru şi servere
* să șteargă automat fişierele carantinate mai vechi de o anumită perioadă
* să permită posibilitatea de restaurare şi mutare a fişierelor din carantină în locaţiile lor originale

Modulul administrare pentru stații de lucru și servere

* Consolele centrale de management vor facilita administrarea și instalarea agenților. După caz, soluția de virtualizare poate necesita una sau mai multe console pentru instalarea, configurarea, monitorizarea și raportarea stării de securitate a stațiilor de lucru și a serverelor.
* Consola de management trebuie să îndeplinească următoarele funcții minimale:

1. identificarea echipamentelor accesibile în rețea gruparea și gestionarea grupărilor de clienți antivirus pentru echipamentele din rețea;
2. identificarea stării echipamentelor din punctul de vedere al instalării soluției antivirus;
3. identificarea stării de activare globală și individuală a funcțiilor (activ/inactiv) și schimbarea acesteia în funcție de necesități;
4. identificarea stării de actualizare și forțarea actualizării la nevoie;
5. gestionarea licențelor;

* Consola trebuie să aibă integrat un modul dedicat controlului activității utilizatorilor, cu următoarele funcții minimale:

1. restricționarea accesului la internet pentru anumiți clienți sau grupuri de clienți;
2. restricționarea accesului la internet pentru anumite aplicații;
3. restricționarea accesului la internet pentru anumite perioade de timp;
4. blocarea paginilor web care conțin anumite cuvinte cheie.

* Accesul la consola de management în urma introducerii credențialelor de acces (username și parolă).

Modulul rapoarte, grafice și alerte trebuie să asigure îndeplinirea următoarelor funcții:

* Crearea de rapoarte pe baza șabloanelor definite în consola de management.
* Generarea de rapoarte complete privind rezultatele scanării și infecțiilor detectate dar și a tuturor obiectelor scanate, inclusiv la nivelul clienților.
* Generarea în mod automat, în cazul detecției unui eveniment, a unui mesaj de alertă către una sau mai multe adrese de e-mail prin intermediul componentei centralizate.
* Generarea rapoartelor în mod programat și expedierea lor în mod automat prin e-mail către administrator.
* Generarea rapoartelor într-un format standardizat (ex.: html, pdf, etc.).

Capabilităţi:

* protecţia mediilor de stocare de tipul USB/HDD, SSD, NVME, USB flash, CD/CD RW, DVD/DVD RW
* posibilitate blocare acces porturi citire/scriere a mediilor de stocare a stațiilor de lucru şi servere
* posibilitatea de a oferi și de a utiliza o consolă centralizată de administrare, instalată local sau la distanță.
* Posibilitate detectare sandboxing

Compatibilitate:

* Prestatorul trebuie să asigure compatibilitatea cu sistemele de operare Windows 11, Windows 10 Professional, Windows 7 pentru stațiile de lucru și Windows Server Standard 2019 și Windows 2003 Server Enterprise Edition pentru servere, Mac, IPhone, IPad, Android.

În situația în care soluția generală nu poate acoperi un produs end-of-life solicităm o soluție compatibilă pentru Windows 2003 Server.

* Prestatorul trebuie să asigure compatibilitatea și integrabilitatea soluției de management centralizat cu Microsoft®Active Directory sistemele de operare Windows Server suportate.

Certificări:

* Să deţină cel puțin o certificare de specialitate emisă de organizaţii internaţionale de profil (ex. Virus Bulletin, ICSA Labs, Checkmark)