Anexă
la Anunţul de participare

CERINȚE TEHNICE
Licențe produs program antivirus
pentru asigurarea protecției infrastructurii TIC a ASP - reînnoirea subscripției licențelor programului antivirus Bitdefender GravityZone Business Security Enterprise pentru asigurarea protecției infrastructurii TIC a ASP

CERINȚELE GENERALE

Soluția de protecție și securitate din gestiunea ASP - Bitdefender GravityZone Business Security Enterprise (ID: 621b49e0de202a473d64c662) (în continuare Soluție) trebuie să acopere volumul de 3001 unități (stații de lucru, laptop-uri, servere fizice, servere virtuale), începând cu 16.04.2024 pentru 36 luni consecutive.

CONSOLA DE MANAGEMENT

1. Cerințe generale:

1. Interfața consolei de management să fie în limba română.
2. Interfața clientului de securitate, care se instalează pe stații și servere, să fie în limba română.
3. Manualul de instalare a soluției să fie în limba română.
4. Manualul de administrare a soluției să fie în limba română.
5. Soluția trebuie să includă un modul de update server prin care să asigure actualizarea de soluție și a semnăturilor/signatures.
6. Soluția trebuie să permite activarea/dezactivarea actualizărilor de soluție semnături.
7. Soluția trebuie să permite stabilirea actualizării automate a consolei de management prin stabilirea recurenței zilnice, săptămânale sau lunare, dar și prin stabilirea intervalului orar în care acesta se va actualiza.
8. Pentru o mai buna urmărire a actualizărilor consolei de management, soluția trebuie să permită vizualizarea unui jurnal de modificări în care sunt precizate istoric:
   a. versiunea consolei de management;
   b. data versiunii;
   c. funcții noi și îmbunătățiri;
   d. probleme rezolvate;
   e. probleme cunoscute.
9. Notificările – prezente în interfața, notificările necitite sunt evidențiate, trimise către una sau mai multe adrese de email, alertează administratorul în cazul unor probleme majore: licențiere, detecție viruși, actualizări de soluție disponibile).
10. Soluția trebuie să permită integrarea cu un server Syslog pentru raportarea evenimentelor antimalware.
11. Soluția trebuie să permită integrarea cu produsele IBM QRadar Security Information and Event Management (SIEM) pentru raportarea evenimentelor antimalware.
12. Soluția trebuie să permită în mod preferabil instalarea serviciului de SMNP prin care se pot raporta statusul mașinilor din cadrul componentei de management.
13. Soluția trebuie să permită creare unei copii de siguranța a bazei de date a consolei de administrare, la cerere sau programata, putând fi stocata local, pe un server FTP sau in rețea.

2. Cerințe de instalare și configurare:

1. Instalarea și configurarea trebuie să fie asigurată prin o mașina virtuală. Consola nu trebuie să necesită o licența suplimentară pentru sistemul de operare. Imaginea de tip template se va putea importa in:
   a. VMware vSphere : 6.5, 6.0, 5.5, 5.1, 5.0, ESXi 5.0

b. Microsoft Hyper-V Server 2012, sau mai nou.

c. Alte platforme de virtualizare, la cerere.

2. Soluția trebuie să fie scalabilă, astfel ca oricare dintre roluri sau servicii pot fi instalate separat pe mai multe mașini virtuale sau pe aceeași mașină virtuală.

3. Rolurile principale trebuie sa fie cel puțin similare cu: Server cu baza de date, Server de comunicație, Server de actualizare, Server Web, etc.).

4. Mașinile de scanare pentru mediile virtuale trebuie să inițializeze la distanta prin task-ri din consola de management.

3. Panou de monitorizare și raportare (Dashboard):

1. Rapoartele din panoul de monitorizare trebuie să fie configurate specificând numele raportului, tipul raportului, opțiuni specifice pentru orice tip de raport.

2. Panoul central trebuie să conțină rapoarte pentru toate modulele suportate.

3. Rapoartele din panoul central de comandă trebuie să permită: adăugarea altor rapoarte, ștergerea lor și rearanjarea.

4. Inventarierea rețelei – managementul securității:

1. Soluția necesită a fi integrată cu serviciile de directoare Microsoft Active Directory, LDAP VMware vCenter Server.

2. Trebuie să permită descoperirea stațiilor stații fizice neintegrate în Active Directory (Workgroup) cu ajutorul Network discovery. Pentru integrarea cu Active Directory, necesită a fi definit intervalul (in ore) pentru sincronizare și posibilitatea sincronizării forțate.

3. Soluția trebuie să ofere opțiuni de căutare, sortare și filtrare după numele sistemului, sistem de operare, adresa IP, politica aplicata, ultima data când s-a conectat (online și/sau offline) și FQDN.

4. Soluția trebuie să 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, Mac.

5. Soluția trebuie să permită instalarea la distanță sau manual a clienților antimalware pe mașini fizice/virtuale.

6. Soluția trebuie să permită selectarea modulelor componente atunci când se creează pachetul clientului care se instalează pe mașinile fizice/virtuale.

7. Soluția trebuie să permită lansarea de task-uri de scanare, actualizare, instalare, dezinstalarea la distanta pentru clientul antimalware.

8. Soluția trebuie să ofere posibilitatea de repornire a mașinilor fizice de la distanță.

9. Soluția trebuie să dispună informații detaliate despre fiecare task și să afișeze dacă task-ul s-a finalizat sau nu cu succes.

10. Soluția trebuie să permită configurarea centralizată a clienților antimalware prin intermediul politicilor.

11. Soluția va oferi în consola de management informații detaliate ale obiectelor din consola: Nume, IP, Sistem de operare, grup, politica atribuită, ultimele actualizări, versiunea soluției, versiunea de semnături.

12. Soluția trebuie să permită descoperirea mașinilor virtuale din Microsoft Hyper-V.

13. Soluția trebuie să permită descoperirea tuturor aplicațiilor instalate pe toate stațiile și serverele din rețea, prin rularea unui task din consola de administrare.

5. Politici:

1. Soluția trebuie să permită configurarea setărilor clientului antimalware prin intermediul unei singure politici ce conține setări pentru toate modulele.

2. Politica trebuie să conțină opțiuni specifice de activare/dezactivare și configurarea funcționalităților precum scanarea antimalware la cerere, firewall, controlul accesului la Internet, scanarea traficului web, controlul dispozitivelor, power user, sandbox în cloud, modul avansat bazat pe tehnologii de tip machine-learning tunabil, modul de tip Endpoint-Detection and Response (EDR).

3. Soluția trebuie să permită aplicarea politicilor pe mașini client, grupuri de mașini, domeniu, unități organizaționale.

4. Politica trebuie să fi schimbată automat in funcție de:

- IP sau clasa de IP a stației;
- Gateway-ul alocat;
- DNS serverul alocat;
- WINS serverul alocat;

5. Este necesar că clientul să fie/sau nu în aceeași rețea a Cumpărătorului cu infrastructura de management (stația de lucru poate soluționa implicit numele gazdei).

6. Rapoarte:

1. Soluția trebuie să conțină rapoarte care prezintă statusul mașinilor clienților din punct de vedere al actualizărilor, fișierelor malware detectate, aplicațiile blocate, site-urilor web blocate.
2. Rapoartele trebuie să fie programate și trimise către un număr nelimitat de adrese de email (nu este nevoie sa aibă un cont in consola de management).
3. Soluția trebuie să permită vizualizarea rapoartelor curente programate de administrator.
4. Soluția trebuie să permite exportarea rapoartelor in format .pdf și detaliile ca format .csv.
5. Soluția trebuie să permită filtrarea conținutul informației în rapoartele trimise pe email astfel încât doar informațiile relevante cerute de către administrator.
6. Soluția trebuie să permite arhivarea rapoartelor care se trimit pe email.
7. Soluția trebuie să includă un generator de rapoarte care oferă posibilitatea de a investiga o problema de securitate pe baza mai multor criterii, menținând informațiile concise și ordonate corespunzător.
8. Interogările legate de starea terminalului trebuie să include informații precum:
   a. tip mașina;
   b. infrastructura rețelei căreia îi aparține terminalul;
   c. datele agentului de securitate;
   d. starea modulelor de protecție;
   e. rolurile terminalelor.
9. Interogarea legată de evenimentele terminalului trebuie să includă informații precum:
   a. calculatorul țintă pe care a avut loc evenimentul;
   b. tipul starea și configurația agentului de securitate instalat;
   c. starea modulelor și rolurilor de protecție instalate pe agentul de securitate;
   d. denumirea și aplicarea politicii;
   e. utilizatorul autentificat în timpul evenimentului;
   f. evenimente (site-uri blocate, aplicații blocate, detecțiile etc).

7. Carantina:

1. Soluția trebuie să permită restaurarea fișierelor din carantina în locația originală sau într-o cale configurabilă.
2. Carantina trebuie să fie locală, pe fiecare stație administrată și va fi administrată, fie local, fie din consola de management.

8. Utilizatori:

1. Administrarea se va putea face pe baza de roluri.
2. Roluri multiple predefinite: Administrator Cumpărătorului Administrator rețea, Reporter sau rol personalizat:
   a. Administrator Cumpărătorului: administrează arhitectura consolei de management;
   b. Administrator rețea a Cumpărătorului: administrează serviciile de securitate;
   c. Reporter: monitorizează și generează rapoarte.

3. Utilizatorii ale Cumpărătorului vor fi importați din Microsoft Active Directory sau creați în consola de management.

4. Trebuie să permite configurarea detaliată a drepturilor administrative, permițând selectarea serviciilor și obiectelor pentru care un utilizator poate face modificări.

5. Trebuie să permită deconectarea automata a oricărui tip de utilizator după un anumit timp pentru o protecție sporită a datelor afișate în consola de administrare.

9. Log-uri:

1. Înregistrarea acțiunilor utilizatorilor.
2. Se vor oferi informații detaliate pentru fiecare acțiune a unui utilizator.
3. Se va permite filtrarea acțiunilor utilizatorilor după: nume, acțiune.

10. Actualizări:

1. Trebuie să permite definirea de locații de actualizare multiple.
2. Trebuie să permită activarea/dezactivarea actualizărilor de soluție și semnături.
3. Trebuie să permită actualizarea soluției într-o rețea fără acces la Internet.
4. Orice client antivirus trebuie să fie configurat sa livreze update-urile către alt client antivirus.
5. Soluția trebuie să dispună un server de actualizare (update) care face posibilă stabilirea componentelor ce vor fi descărcate automat de pe internet, fără intervenția administratorului.
6. Soluția trebuie să permită testarea noilor versiuni de pachete de instalare ale clientului antimalware, înainte de a fi instalate pe toate stațiile și serverele din rețea, evitând posibile probleme ce pot afecta serverele sau stațiile critice. Astfel, serverul de actualizare va include 2 tipuri de actualizări:
   a. Ciclu rapid, gândit pentru un mediu de test în cadrul rețelei.
   b. Ciclu lent, gândit pentru restul rețelei (producție, servere critice etc).
7. Soluția trebuie să permită stabilirea zonelor de test și critice din cadrul rețelei prin intermediul politicilor din consola de management.

11. Certificate:

1. Accesul la consola de management trebuie să fie doar prin HTTPS.

2. Serverul web, din consola centrala de management trebuie să permită importarea de certificate digitale eliberate de o autoritate de certificare autorizată sau proprie organizației.

3. Soluția trebuie să permită afișarea în consola de management informații despre certificate: nume, autoritatea emitenta, data eliberării și data expirării certificatelor eliberate.

12. API

1. Soluția trebuie să permită administratorului sa efectueze „call-uri" API.

2. Soluția trebuie să includă metode de management a conturilor de utilizator, a notificărilor, grupurilor de endpoint-uri, a politicilor respectiv a generării de rapoarte prin intermediul cheilor API.

PROTECȚIA STAȚIILOR ȘI SERVERELOR FIZICE/VIRTUALE

1. Cerințe generale minimale:

1. Soluția anti-malware va utiliza un singur motor de scanare și va include toate tehnologiile descrise mai jos intr-un singur client software.

2. Pentru reducerea la minim a consumului de resurse, soluția antimalware trebuie să permită instalarea personalizată a modulelor deținute (de exemplu, sa permită instalarea soluției antimalware fără modulul de control al accesului web, modul de control al dispozitivelor sau modulul firewall).

3. Pentru o mai bună protecție a stațiilor și serverelor, soluția trebuie să includă un vaccin anti-ransomware. Acest vaccin va asigura protecția împotriva tuturor amenințărilor cunoscute de

tip ransomware, prin imunizarea stațiilor și serverelor, chiar dacă sunt infectate și prin blocarea procesului de criptare.

4. Vaccinul anti-ransomware va primi actualizări de la producător, odată cu actualizarea semnăturilor soluției Antimalware.

5. Pentru o buna protecție a stațiilor și serverelor, soluția trebuie să include protecție împotriva atacurilor zero-day de tip exploit avansate (atacuri direcționate) bazată pe tehnologii de invitare automata (machine learning).

6. Pentru o buna protecție a stațiilor și serverelor, soluția trebuie să includă un modul avansat de securitate – HyperDetect, bazat pe tehnologii de tip „machine learning tunabil" proiectat special pentru a detecta atacuri avansate și activități suspecte in faza pre-executie.

7. Modul de securitate va proteja împotriva: atacurilor direcționate (Targeted Attack - APT), fișierelor suspecte și traficului la nivel de rețea suspect, exploit-urilor, ransomware și grayware. Fiecărui tip de amenințare menționat, i se va putea stabili, independent, un nivel de protecție dorit: permisiv, normal, agresiv.

8. Modulul de securitate va avea posibilitatea de a raporta, bloca accesul, dezinfecta, șterge sau muta în carantina pentru fiecare din categoriile descrise. Astfel, administratorul va putea decide dacă dorește întâi monitorizare sau dorește și blocarea amenințărilor. Aceste acțiuni menționate, vor putea fi stabilite independent, pentru fișiere sau pentru traficul din rețea, cu posibilitatea extinderii nivelului de raportare pentru a include nivelurile superioare (vor putea fi raportate amenințările care ar fi fost detectate dacă nivelul de protecție a fost stabilit mai agresiv).

9. Pentru a oferi un nivel adițional de protecție a stațiilor și serverelor, soluția trebuie să includă un sandbox în cloud-ul public al producătorului acesteia.

10. Modulul de Sandbox va putea trimite automat fișiere în Sandbox-ul din cloud-ul producătorului, unde vor putea fi „detonate" pentru o analiza în profunzime.

11. Modulul de Sandbox va include două variante de analiză: doar monitorizare sau blocare. În modul monitorizare utilizatorul va putea accesa fișierul dorit, pe când în modul blocare, utilizatorului i se va bloca rularea fișierului pană când Sandbox-ul din cloud-ul producătorului va da verdictul.

12. Modulul de Sandbox va include doua tipuri de acțiuni remediere: implicită și de siguranță. Pentru acțiunea implicită se va putea stabili: doar raportare, dezinfecție, ștergere și carantinare. Pentru acțiunea de siguranță se va putea stabili: ștergere sau carantinare.

13. Modulul de Sandbox va include și posibilitatea de trimitere manuală a fișierelor în Sandbox-ul din cloud-ul producătorului. Astfel, dacă administratorul suspectează un fișier ca fiind malițios, îl poate trimite manual în Sandbox pentru a fi „detonat" și a afla verdictul. Va putea trimite mai multe fișiere o odată, cu posibilitatea de a specifica dacă vor fi „detonate" individual sau toate în același timp.

14. Modulul de Sandbox trebuie să suporte „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 (executabile), RTF, SCR, URL (binary), VBE, VBS, WSF, WSH, WSH-VBS, XHTML.

15. Fișierele 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.

16. Modul de detectare, corelare și răspuns la evenimente de tip EDR („endpoint detection and response") trebuie să fie capabil să identifice amenințări avansate sau atacuri în curs de desfășurare. Acest modul va cuprinde colectarea de date și evenimente despre hardware și software aferent fiecărei stații de lucru aducând informații detaliate referitoare la incidentele detectate, o harta detaliata a acestora, precum și acțiuni de remediere automate și integrare cu modulele de Sandbox și modulul avansat de securitate – HyperDetect.

17. Modulul EDR va avea capacitatea de a evalua activitatea tipică a unui endpoint din perspectiva securității acestuia conform tehnicilor de atac MITRE („baselining") și poate raporta orice deviație de la acest comportament sub forma unui incident.

18. Modulul EDR va permite filtrarea incidentelor din interfața grafica în funcție intervalul de timp, pe baza unui scor de încredere („confidence score"), indicatori de atac, tehnici de atac (ATT&CK) respectiv sistem de operare afectat cat și după IP, nume fișier, nume stație.

19. Modulul EDR va permite vizualizarea detaliată a incidentelor incluzând detalii specifice fiecărui nod afectat după cum urmează: tabul „rezumat" generează o harta de principiu a incidentului, tabul „timeline" detaliază incidentul în funcție de amprenta de timp a fiecărei acțiuni aferente incidentului, respectiv butonul „acționează" care poate genera un set de măsuri specifice fiecărui element din harta incidentului (kill, carantina – la nivel de nod, investigați – virus total, sandbox, google – la nivel de fișier, adăugare în lista de blocare – la nivel de rețea sau instalare patch – la nivel de nod).

20. Modulul EDR va putea bloca fișiere și/sau procese folosind valori hash de tip MD5/SHA256 direct din pagina aferenta incidentului sau importate folosind un fișier CSV.

21. Modulul EDR va putea excepta fișiere non-malițioase de la acțiunea de investigare sau poate genera/adăuga un set de fișiere malițioase într-o lista neagra pentru a preveni mișcarea laterala a fișierelor/proceselor malițioase.

22. Modulul EDR va permite deschiderea unei conexiuni remote către un endpoint potențial infectat pentru a permite o investigare rapida a gazdei, colecta date despre atac respectiv remedia în timp real a breșelor de securitate eliminând astfel posibile incertitudini privitoare la comportamentul potențial malițios al unor fișiere/procese, reducând timpul de remediere (downtime) în cazul în care un atac a avut succes și stația țintă trebuie reconfigurată/reinstalată, permite executarea unor comenzi în linia de comanda care se execută cu privilegii de kernel ce permit eliminarea în timp real a unor amenințări sau colectarea de date privitoare la atacul în desfășurare.

23. Modulul EDR să permită creare regulilor de detecție personalizate bazate pe procese, fișiere, registre și conexiuni de rețea.

24. Modulul EDR să permită creare regulilor de excludere personalizate bazate pe procese, fișiere, registre si conexiuni de rețea.

25. Modulul EDR să permită căutarea proactivă pe stațiile de lucru protejate a indicatorilor de compromitere precum hash-uri, nume de fișiere, nume de procese, chei de registre, valori de registre.

26. Soluția să includă un modul de tip host IPS capabil să blocheze atacuri la nivel de rețea incluzând mișcarea laterală a unor categorii de malware.

27. Modulul de tip host IPS va reprezenta o sursa de telemetrie / date despre atac pentru modulul de tip EDR, acesta din urma având abilitatea de a integra informații despre acțiunile luate de către o potențiala amenințare la nivel de rețea.

2. Cerințe de sistem:

- **Sisteme de operare pentru stații de lucru:** Windows XP, Windows 7, Windows 8/8.1, Windows 10//11, MAC OS X Catalina (10.15.x), Mac OS X Mojave (10.14.x), Mac OS X High Sierra (10.13.x), Mac OS X Sierra (10.12.x), Mac OS X El Capitan (10.11.x).
- **Sisteme de operare embedded:** Windows 10 IoT Enterprise, Windows Embedded 8.1 Industry, Windows Embedded 8 Standard, Windows Embedded Standard 7, Windows Embedded POSReady 7, Windows Embedded Enterprise 7.
- **Sisteme de operare pentru servere:** Windows Server 2003 32bit/64bit, Windows Server 2008 32bit/64bit/R2, Windows Server 2012/R2, Windows Server 2016, Windows Server 2019, Windows Small Business Server (SBS) 2011, Windows Server 2022.
- **Sisteme de operare Linux:** Red Hat Enterprise Linux / CentOS 6 sau mai recent, Ubuntu 14.04 LTS sau mai recent, Fedora 25 sau mai recent, Debian 8.0 sau mai recent.

3. Administrare și instalare remote trebuie să asigure:

1. Înainte de instalare, administratorul va putea particulariza pachetele de instalare cu modulele dorite: advanced threat control, anti-exploit, firewall, network protection respectiv content control, device control, power user, patch management, full disk encryption, EDR sensor, exchange protection respectiv „relay" (cu sau fără „patch caching server").

2. Instalarea se va putea efectua prin mai multe metode:

a. prin descărcarea directă a pachetului pe stația pe care va fi instalat;

b. prin instalarea la distanță, direct din consola de management;

c. trimiterea pe email (oricare adrese) a pachetului de instalare pentru Windows, Linux, Mac.

3. Instalarea clienților la distanță în alte locații decât cele în care este instalata consola de management se va efectua prin intermediul unui alt client antivirus existent în locațiile respectiv pentru a minimiza traficul în WAN.

4. In consola vor fi disponibile informații despre fiecare stație: numele stației, IP, sistem de operare, module instalate, politica aplicata, informații despre actualizări etc.

5. Din consola se va putea trimite o singura politica pentru configurarea integrală a clientului de pe stații/servere.

6. Consola va include o secțiune, „Acțiuni Utilizator", unde se vor menționa toate acțiunile întreprinse fie de administratori, fie de reporteri, cu informații detaliate: logare, editare, creare, delogare, mutare etc.

7. Posibilitatea creări unui singur pachet de instalare, utilizabil atât pentru sistemele de operare pe 32 de biți cât și pentru cele pe 64 de biți.

8. Posibilitatea creări unui singur pachet de instalare, utilizabil pentru stații (fizice și/sau virtuale), servere (fizice și/sau virtuale), Microsoft Exchange.

9. Posibilitatea de a crea pachetele de instalare de tip web installer sau kit full.

10. Administratorul va putea crea grupuri sau chiar subgrupuri, unde va putea muta stațiile/serverele din rețea pentru cele care nu sunt integrate domeniu.

11. Permite selectarea clientului care va realiza descoperirea stațiilor din rețea, altele decât cele integrate în domeniu.

12. Permite raportarea stațiilor care sunt protejate respectiv neprotejate de către soluție.

13. Permite definirea de portlet-uri (reprezentări grafice) configurabile.

4. Cerințele obligatorii cu referire la caracteristicile și funcționalitățile principale ale modulului antimalware și antispyware

1. Soluția va permite administratorului sa stabilească acțiunea luata de soluție Antimalware la detectarea unei amenințări noi. Astfel administratorul va putea alege între următoarele acțiuni:

a. Acțiune implicită pentru fișiere infectate:
- interzice accesul;
- dezinfectează;
- ștergere;
- mută fișierele în carantină;
- nicio acțiune.

b. Acțiune alternativa pentru fișierele infectate:
- interzice accesul;
- dezinfectează;
- ștergere;
- mută fișierele în carantină.

c. Acțiune implicită pentru fișierele suspecte:
- interzice accesul;
- ștergere;
- mută fișierele în carantină;
- nicio acțiune.

d. Acțiune alternativa pentru fișierele suspecte:
- interzice accesul;

- ștergere;
- muta fișierele in carantina;

2. Scanarea automata in timp real va putea fi setata sa nu scaneze arhive sau fișiere mai mari de un volum (MB), mărimea fișierelor putând fi definită de administrator.

3. Definirea până la 16 nivele de profunzime pentru scanarea in arhive.

4. Scanarea euristica comportamentala prin simularea unui calculator virtual in interiorul căruia sunt rulate aplicații cu potențial periculos protejând sistemul de virușii necunoscuți prin detectarea codurilor periculoase a căror semnătura nu a fost lansată.

5. Scanarea oricărui suport de stocare a informației (CD-uri, harduri externe, unități partajate etc). De asemenea, se va putea anula scanarea in cazul in care sunt detectate unități care au informații stocate mai mult de un volum (MB).

6. Scanarea automata a emailurilor la nivelul stației de lucru pentru POP3/SMTP.

7. Configurarea directoriilor ce urmează a fi scanate la cerere.

8. Clienții antimalware pentru stațiile de lucru să permită definirea unor liste de excludere la scanarea în timp real și la cerere a anumitor directoare, discuri, fișiere, certificate, extensii sau procese, incluzând amprenta (hash) în cazul fișierelor sau certificatelor.

9. Cu ajutorul unei baze de date complete cu semnături de spyware și a euristicii de detecție a acestui tip de programe, soluția va trebui să ofere protecție anti-spyware.

10. Posibilitatea de a configura scanările programate să se execute cu prioritate redusă.

11. Soluție antimalware poate fi configurat sa folosească scanarea în cloud, și parțial scanarea locală. Pentru stațiile ce nu au suficiente resurse hardware, scanarea se poate face cu o mașina de scanare instalata în rețea.

12. Administratorul al Cumpărătorului va putea personaliza și motoarele de scanare, având posibilitatea de a alege între mai multe tehnologii de scanare:

- Scanare locală, când scanarea se efectuează pe stația de lucru locală. Modul de scanare locală este potrivit pentru mașinile puternice, având toate semnăturile și motoarele stocate local.
- Scanarea hibrid cu motoare light (Cloud public), cu o amprentă medie, folosind scanarea în cloud și, parțial, semnături locale. Acest mod de scanare oferă avantajul unui consum mai bun de resurse, fără să implice scanarea locală.
- Scanarea centralizată în Cloud-ul privat, cu o amprentă redusă, necesitând un server de securitate pentru scanare. În acest caz, nu se stochează local nicio semnătură, iar scanarea este transferată către serverul de securitate.
- Scanare centralizată (Scanare în cloud privat cu server de securitate) cu fallback* pe Scanare locală (motoare full).
- Scanare centralizată (Scanare în cloud privat cu server de securitate) cu fallback* pe Scanare hibrid (cloud public cu motoare light).

13. Pentru o protecție sporita, soluția antimalware trebuie sa permită 3 tipuri de detecție: bazata pe semnături, bazata de comportamentul fișierelor si bazata pe monitorizarea proceselor.

14. Pentru o protecție sporita, soluția antimalware trebuie sa poată scana paginile HTTP (incluzând SSL).

15. Pentru o mai buna gestionare a antimalware instalat pe stații, soluție va include opțiunea de setare a unei parole pentru protecția la dezinstalare.

16. Pentru siguranța utilizatorului, clientul va include un modul de antiphishing (acesta va putea verifica linkurile indexate si prezentate utilizatorului in urma unei căutări – „search advisor”).

17. Soluția va oferi protecție in timp real pe mașinile cu sistem de operare Linux in conformitate cu versiunea de kernel instalata.

18. Soluția va oferi o tehnologie de tip „preventiv / vaccin” ce va acționa împotriva potențialelor atacuri de tip ransomware.

19. Soluția va oferi un set de excluderi predefinite pentru Roluri de tip „server” Microsoft (DNS, DHCP, AD, Exchange, Sharepoint).

20. Soluția va putea detecta atacuri de tip „file-less” incluzând pe cele ce folosesc utilitare aferente sistemelor de operare de tip interpretor de script (powershell). Soluția nu va bloca in mod uzual scripturi pentru a proteja împotriva acestor tipuri de atacuri.

21. Soluția va oferi un modul adițional de securitate bazat pe algoritmi turnabili de machine learning respectiv algoritmi euristici agresivi capabili sa detecteze si blocheze atacuri de tip persistent sau targetat precum si alte categorii de malware sofisticat înainte de faza de executie. Acest modul oferă următoarele funcționalități:

a. Clasificarea tipului de atac;

b. Abilitatea de a raporta amenințările detectate fără a le bloca;

c. Abilitate de a ajusta agresivitatea detecției pe cel puțin 3 nivele (incluzând posibilitatea de a raporta atacuri ce ar fi fost blocate pe un nivel de agresivitate a detecției „mai ridicat” decât cel setat in mod curent in modul);

d. Abilitatea de a acționa in mod diferit in funcție de tipul amenințării (fișier sau atac prin rețea).

22. Soluția oferă posibilitatea de restaurare a fișierelor modificate de un proces suspicios/necunoscut cu comportament de ransmoware, odată ce soluția determina ca procesul este malițios.

23. Soluția oferă protecție împotriva atacurilor ransomware inițiate la distanta, de pe alte stații de lucru (de exemplu: încercarea de atac ransomware pe un repozitoriu share de pe o stație de lucru care are acces la share).

5. Anti-Exploit-Avansat

1. Posibilitatea de a opri atacurile avansate de tip „zero-day” efectuate prin intermediul unor exploit-uri evazive.

2. Depistarea in timp real a celor mai recente exploit-uri ce pot vulnerabiliza un sistem de operare.

3. Protejarea aplicațiilor utilizate frecvent și a celor de tip „sistem” cum ar fi browser-e, aplicațiile de tip office sau reader, procesele critice aferente sistemelor de operare.

6. Firewall

1. Posibilitatea de a configura reguli de firewall pentru aplicații sau conectivitate.
2. Modulul poate fi instalat/dezinstalat in funcție de preferința administratorului.
3. Posibilitatea de a defini rețele de încredere pentru mașina destinație.

7. Carantina

1. Soluție antimalware va permite trimiterea automata a fișierelor din carantina către laboratoarele antimalware ale producătorului.
2. Trimiterea conținutului carantinei va putea fi expediat in mod automat, la un interval definit de administrator.
3. Soluție antimalware va permite ștergerea automata a fișierelor carantinate mai vechi de o anumita perioada, pentru a nu încarcă inutil spațiul de stocare.
4. Posibilitatea de a restaura un fișier din carantina în locația lui originală.
5. Modulul de carantină va permite re-scanarea obiectelor după fiecare actualizare de semnături.
6. Modulul de carantina va permite salvarea unei copii a fișierului infectat respectiv transmiterea acestuia către carantina înainte de a efectua orice alta acțiune asupra acestuia.

8. Protecția datelor

1. Soluție va permite blocarea datelor confidențiale (pin-ul cardului, cont bancar etc) transmise prin HTTP sau SMTP prin crearea unor reguli specifice.

9. Controlul conținutului

1. Consola va avea integrat un modul dedicat controlului accesului la Internet cu următoarele particularități:

a. Permite blocarea accesului la Internet pentru anumite mașini client sau grupuri de mașini;

b. Permite blocarea accesului la Internet pe intervale de timp (orar);

c. Permite blocarea paginilor de internet care conțin anumite cuvinte cheie;

d. Permite controlul accesului numai la anumite pagini de internet specificate de administrator;

e. Permite blocarea accesului la anumite aplicații definite de administrator;

f. Permite restricționarea accesului pe anumite pagini de internet după anumite categorii prestabilite (ex: online dating, violenta, pornografie etc).

10. Controlul dispozitivelor

1. Modulul va permite prevenirea scurgerea accidentală sau intenționată de date respectiv potențiale infecții cu malware prin atașarea de dispozitive externe.
2. Modulul poate fi instalat/dezinstalat în funcție de preferința administratorului.
3. Modulul va permite controlul următoarelor tipuri de dispozitive:

a. Bluetooth Devices;
b. CDROM Devices;
c. Floppy Disk Drives;
d. Security Policies 153;
e. IEEE 1284.4;
f. IEEE 1394;
g. Imaging Devices;
h. Modems;
i. Tape Drives;
j. Windows Portable;
k. COM/LPT Ports;
l. SCSI Raid;
m. Printers;
n. Network Adapters;
o. Wireless Network Adapters;
p. Internal and External Storage

4. Modului va permite capturarea unor informații specifice legate de dispozitivele externe cum ar fi: nume, class ID, momentul în timp când a fost conectat.
5. Modulul va permite configurarea de reguli prin care se vor defini permisiunile pentru dispozitivele conectate la mașina client cum ar fi: permis/blocat/custom respectiv poate limita accesul dispozitivelor externe la „read only” sau limita doar accesul la porturile USB ale endpoint-ului permițând orice alt tip de dispozitiv ce nu folosește acest tip de port/interfața.
6. Modulul va permite configurarea de excluderi pentru diferite tipuri de dispozitive pentru care s-au configurat reguli pe baza a Product/Device/Hardware ID.
7. Modului va putea „descoperi” noi dispozitive si raporta prezenta acestora in consola de management.

11. Power User

1. Modulul va fi instalat/dezinstalat in funcție de preferința administratorului.
2. Modulul va permite posibilitatea de a acorda utilizatorilor drepturi de Power User. Utilizatorii vor putea accesa si modifica setările clientului antimalware dintr-o consola disponibila local pe mașina client.
3. Administratorul va putea suprascrie din consola setările aplicate de utilizatorii Power User.

12. Actualizare

1. Posibilitatea efectuării actualizării la nivel de stație în mod silentios (fara avertizare).
2. Sistem de actualizare va putea folosi unul sau mai multe servere de actualizare (cascad).

3. Actualizarea pentru locațiile remote prin intermediul unui client antimalware care are și rol de server de actualizare.

13. Protecție pentru Dispozitive de Stocare Externe

1. Soluția va oferi protecția dispozitivelor de stocare externe ce suport ICAP (Internet Content Adaptation protocol, așa cum a fost definit acesta in RFC 3507).
2. Soluția va oferi protecție antimalware pentru fișiere stocate pe orice dispozitiv de stocare extern compatibil ICAP.
3. Soluția va oferi mai multe nivele de protecție împotriva amenințărilor bazate pe algoritmi de tip machine learning, euristici, semnături precum și informații obținute din cloud-ul de tip „threat intel" al producătorului.
4. Soluția va oferi protecția dispozitivele de stocare externe împotriva amenințărilor necunoscute (pentru care nu există o semnătura).
5. Soluția va oferi scanare la acces pentru dispozitivele de stocare externe.
6. Soluția va oferi scanare la acces pentru arhive stocate pe dispozitive de stocare externe cu opțiuni configurabile cum ar fi mărimea maxima a arhivei sau nivelul de adâncime a acesteia (cel puțin 64 de nivele de adâncime vor fi permise).
7. Soluția va pune la dispoziția administratorului cel puțin 2 metode prin care să reducă supra-încărcarea serverului de scanare respectiv cel puțin 2 acțiuni ce pot fi luate in momentul in care a fost identificat un fișier infectat pe un dispozitiv de stocare extern.

16. Controlul aplicațiilor:

1. Pentru o mai bună inventariere și administrare, soluția va include o secțiune în consola de administrare unde se vor regăsi toate aplicațiile descoperite in rețea, grupate după: nume, versiune, descoperit la, găsit pe.
2. Pentru o mai buna inventariere și administrare, soluția va include o secțiune in consola de administrare unde se vor regăsi toate procesele negrupate descoperite in rețea, grupate după: nume, versiune, nume soluției, versiune soluției, editor/autor, descoperit la, găsit pe.
3. Pentru prevenirea infectării stațiilor si serverelor, dar și pentru a permite aplicațiilor descoperite in rețea sa se poată actualiza, soluția va permite definirea unor programe de actualizare (Updater) care vor fi lăsate sa actualizeze diferite aplicații instalate pe stații sau servere.
4. Soluția va include opțiunea de a permite, sau a bloca rularea anumitor aplicații sau procese definite de administrator (inclusiv sub-procese) după:
   a. Cale fisier: local, CD-ROM, portabil sau rețea;
   b. Hash;
   c. Certificat.

ALTE CERINȚE OBLIGATORII

1. Pentru soluția ofertată se solicită suport local de la Furnizor și de la producătorul produsului program antivirus pentru 36 luni consecutive din data reînnoirii subscripției.
2. Furnizorul trebuie să asigure suport 24/7, prin e-mail și/sau conectare de la distanță(după caz), inclusiv suport local.

Termeni de reacție:

În cazul în care vor parveni solicitări privind oferirea suportului, în special cu referire la cazurile de asigurare a funcţionării produsului program antivirus, este necesară aplicarea timpului de reacţie/de restabilire a funcţionalităţii conform tabelului:

Neconcor-danță	**Descriere**	**Timpul maxim de reacție**	**Timp maxim de restabilire a funcționalității sau soluționare a problemei (ore de lucru, zile)**

Critică	Problemă care afectează funcționalitatea întregului produs program antivirus inclusiv modulele	Timp maxim de reacție – 2 ore	Timp maxim de restabilire a funcționalității – 4 ore
Înaltă	Probleme care au o influență înaltă asupra funcționalității produsului program antivirus, care pot conduce la limitarea utilizării produsului program antivirus	Timp maxim de reacție – 4 ore	Timp maxim de restabilire a funcționalității – 8 ore
Medie	Probleme ce țin de dereglările funcționalității produsului program antivirus, care pot fi soluționate fără riscul pierderii de date sau prejudicierea funcționalității produsului program antivirus	Timp maxim de reacție – 8 ore	Timp maxim de restabilire a funcționalității – 2 zile
Redusă	Probleme cu impact redus sau foarte redus asupra funcționalității produsului program antivirus	Timp maxim de reacție – 8 ore	Timp maxim de restabilire a funcționalității – 5 zile