SPITALUL CLINIC JUDEȚEAN DE URGENȚĂ „PIUS BRÎNZEU" TIMIȘOARA

• Bulevardul Liviu Rebreanu, Nr. 156 Timișoara, jud. Timiș, Cod Postal 300723
• Cod fiscal 4663448 • Telefon +4 0356 433111 • Fax +4 0256 486956
• e-mail: judeteana@hosptm.ro • www.hosptm.ro

ANMCS unitate aflată în SUPRAVEGHEREA

Nr. 6807/10.02.2025

CAIET DE SARCINI PENTRU

ACHIZIȚIE PACHET LICENȚĂ ANTIVIRUS PENTRU 1100 DISPOZITIVE

AUTORITATEA CONTRACTANTĂ

Spitalul Clinic Județean de Urgență Pius Brînzeu Timișoara

Cap.1 Informatii generale

1.1. Introducere

Prezenta documentație cuprinde condițiile generale pentru îndeplinirea contractului ce are ca obiect **"Achiziție pachet licență antivirus pentru 1100 de dispozitive "** la Spitalul Clinc Județean de Urgență "Pius Brînzeu" Timișoara.

CONTEXT

Autoritatea contractantă consideră că prezentul caiet de sarcini oferă informații detaliate privind echipamentul ce se doreste a fi achiziționat, respectiv **"Achiziție licență antivirus pentru 1100 de dispozitive "**
Cerințele impuse vor fi considerate ca fiind minimale.

Caietul de sarcini conține specificații tehnice și indicații privind regulile de bază catre trebuiesc respectate astfel încât operatorii economici să elaboreze propunerea tehnică și propunerea financiară corespunzător cu necesitățile autorității contractante.
Cerințele impuse prin caietul de sarcini vor fi considerate ca fiind minimale și obligatorii.În acest sens, prezentata, care se abate de la prevederile caietului de sarcini, va fi luată în considerare, dar numai în

măsura în care propunerea tehnicăpresupune asigurarea unei nivel calitativ superior cerințelor minimale din caoetul de sarcini.
Orice oferta care se abate de la prevederile caietului de sarcini sau prezintă caracteristici tehnice inferioare celor prevăzute în acesta sau care nu satisfac cerințele impuse în acesta, va fi respinsă ca fiind neconformă.

1.2. Autoritatea contractantă:

Spitalul Clinic Judetean de Urgenta Pius Brînzeu Timișoara

Adresă poșală - Timisoara, Bv.Liviu Rebreanu, nr.156, jud.Timis, cod Fiscal 4663448
Tel.0356/433.127, fax. 0356/433.114

Cod CPV: 48900000-7 Diverse pachete software și sisteme informatice

1.3. Obiectul procedurii de achiziție

Obiectul caietului de sarcini îl constituie achiziția unei licențe antivirus pentru **1100 dispozitive.**

Cap.2 Definiția antivirusului

Un antivirus este un software specializat care detectează, previne și elimină programele malicioase, cunoscute sub denumirea de viruși, precum și alte amenințări cibernetice, cum ar fi spyware, ransomware sau troieni. Scopul principal al unui antivirus este de a proteja calculatorul și datele personale de potențiale daune cauzate de aceste programe nocive.

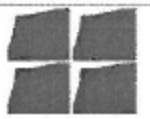
Antivirusurile funcționează pe baza unor algoritmi avansați care scanează fișierele și datele din calculator pentru a identifica semne ale unor programe maligne. Dacă software-ul detectează un fișier sau o aplicație suspectă, aceasta va fi fie blocată, fie pusă în carantină, pentru a preveni răspândirea virusului în sistem. Astfel, antivirusul devine un scut esențial în fața amenințărilor cibernetice, oferindu-ți liniștea de care ai nevoie atunci când utilizezi computerul.

Cap.3 Caracteristici generale ale produsului

Produsul („soluția") reprezintă o platformă integrată pentru gestionarea securității, concepută ca o soluție modulară. Produsul conține următoarele module:

A. O consolă de gestionare care oferă funcționalități de administrare.

B. Protecție antimalware pentru stații de lucru fizice, laptopuri și servere.



• Bulevardul Liviu Rebreanu, Nr. 156 Timișoara, jud. Timiș, Cod Poștal 300723
• Cod fiscal 4663448 • Telefon +4 0356 433111 • Fax +4 0256 486056
• e-mail: judetean@hosptm.ro • www.hosptm.ro

A. CONSOLA DE ADMINISTRARE

1. Cerințe generale:

1. Interfața consolei de gestionare va fi în limba engleză.

2. Interfața clientului de securitate, care este instalată pe stații și servere, va fi în limba engleză.

3. Manualul de instalare a produsului va fi în limba engleză.

4. Manualul de administrare a produsului va fi în limba engleză.

5. Soluția trebuie să permită să activarea/dezactivarea actualizările/semnăturile produsului.

6. Actualizări automate ale consolei de administrare realizate de producătorul soluției, fără a fi necesară intervenția utilizatorului.

7. Notificări - prezente în interfață, notificările necitite sunt evidențiate, sunt trimise la una sau mai multe adrese de email, alertează administratorul în cazul unor probleme majore: licențiere, detectare viruși, actualizări produse disponibile).

8. Consola de administrare este accesibilă de oriunde din lume (se bazează pe un serviciu de cloud Software-as-a-Service), fără a fi nevoie de setări suplimentare din partea utilizatorului.

9. Consola de gestionare este accesibilă atât de pe stațiile de lucru, cât și de pe dispozitivele mobile (smartphone, tabletă).

2. Panou de monitorizare și raportare (tablou de bord):

1. Rapoartele din panoul de monitorizare vor putea fi configurate specificând numele raportului, tipul raportului, ținta raportului, opțiuni specifice pentru orice tip de raport (de exemplu pentru raportul de actualizare - care este intervalul după care o stație este considerată neactualizată).

2. Panoul central conține rapoarte pentru toate modulele acceptate.

3. Rapoartele din panoul central permit: adăugarea altor rapoarte, ștergerea lor și rearanjarea lor.

3. Inventarul rețelei - gestionarea securității:

1. Soluția se va integra cu domeniul Active Directory și va fi capabilă să importe inventarul.

2. Este permisă descoperirea stațiilor fizice neintegrate în Active Directory (Workgroup) cu ajutorul Network discovery.

3. Soluția va oferi opțiuni de căutare, sortare și filtrare după numele sistemului, sistemul de operare, adresa IP, politica aplicată, ultima dată când a fost conectat (online și/sau offline) și FQDN.

4. Soluția va permite crearea de un pachet unic pentru toate sistemele de operare, stațiile de lucru sau serverele. Astfel, administratorul va putea descărca pachetele pentru protecția stațiilor și serverelor care rulează sistemul de operare Windows, Linux, Mac.

5. Soluția permite instalarea de la distanță sau manuală a clienților antimalware pe mașini fizice/virtuale.

6. Soluția va permite selectarea modulelor componente în momentul creării pachetului de client ce urmează a fi instalat pe mașini fizice/virtuale.

7. Soluția va permite lansarea la distanță a sarcinilor de scanare, actualizare, instalare, dezinstalare pentru clientul antimalware.

8. Soluția va oferi posibilitatea repornirii de la distanță a mașinilor fizice.

9. Soluția va oferi informații detaliate despre fiecare sarcină și va înregistra dacă sarcina a fost finalizată cu succes sau nu.

10. Soluția va permite configurarea centralizată a clienților antimalware prin intermediul politicilor

11. Informațiile detaliate ale obiectelor din consolă vor fi furnizate în consola de administrare: Nume, IP, Sistem de operare, Grup, Politică atribuită, Ultimele actualizări, Versiunea produsului, Versiunea semnăturii.

4. Politici:

1. Soluția trebuie să permită configurarea setărilor antimalware prin intermediul politicilor din consola de administrare.

2. Politica trebuie să conțină opțiuni specifice de activare/dezactivare și configurarea unor funcționalități precum scanarea antimalware la cerere, firewall, controlul accesului la internet, controlul aplicațiilor, scanarea traficului web, controlul dispozitivelor, power user.

3. Soluția va permite aplicarea de politici pe mașini client, grupuri de mașini, domeniu, unități organizaționale.

4. Politica sa poate fi modificată automat în funcție de:

a. IP-ul sau clasa IP a stației

b. Gateway-ul atribuit

c. Serverul DNS atribuit

d. Serverul WINS atribuit

e. Sufix DNS pentru conexiunea dhcp

f. Clientul este/nu este în aceeași rețea cu infrastructura de gestionare (stația de lucru poate rezolva implicit numele de gazdă)

g. Tipul rețelei (lan, wireless)

5. Rapoarte:

1. Soluția va conține rapoarte care arată starea echipamentelor clienților în ceea ce privește actualizările, fișierele malware detectate, aplicațiile blocate, site-urile web blocate.

2. Rapoartele programate pot fi trimise la un număr nelimitat de adrese de e-mail (nu este necesar să aveți un cont în consola de administrare).

3. Soluția va permite vizualizarea rapoartelor curente programate de administrator.

4. Soluția va permite exportarea de rapoarte în format .pdf și detalii în format .csv.

6. Carantină:

1. Soluția va permite restaurarea fișierelor aflate în carantină în locația lor originală sau într-o cale configurabilă, cu opțiunea de a exclude automat fișierul restaurat.

2. Carantina va fi locală, pe fiecare stație administrată și va fi administrată local sau din consola de administrare.

7. Utilizatori:

1. Administrarea va fi posibilă pe baza rolurilor.

2. Roluri predefinite multiple: Administrator companie, Administrator rețea, Reporter sau rol personalizat.

a. Administrator al unității gestionează arhitectura consolei de administrare;

b. Administrator de rețea: administrează serviciile de securitate;

c. Reporter: monitorizează și generează rapoarte.

3. Utilizatorii pot fi importați din Microsoft Active Directory sau creați în consola de administrare.

4. Va fi permisă configurarea detaliată a drepturilor administrative, permițând selectarea serviciilor și obiectelor pentru care un utilizator poate face modificări.

5. Va fi permisă deconectarea automată a oricărui tip de utilizator după un anumit interval de timp pentru o protecție sporită a datelor afișate în consola de administrare. Acest interval poate fi personalizat de către administratorul soluției.

8. Log-uri:

1. Înregistrarea acțiunilor utilizatorului.
2. Vor fi furnizate informații detaliate pentru ficcare acțiune a utilizatorului.
3. Va fi permisă filtrarea acțiunilor utilizatorului după numele utilizatorului, acțiune.

9. Actualizari:

1. Este permisă definirea mai multor locații de actualizare.
2. Este permisă activarea/dezactivarea actualizărilor și semnăturilor produselor.
3. Orice client antivirus poate fi configurat să livreze actualizări către un alt client antivirus
4. Soluția permite testarea noilor versiuni ale pachetelor de instalare ale clienților antimalware, înainte ca acestea să fie instalate pe toate stațiile și serverele din rețea, evitând eventualele probleme care pot afecta serverele sau stațiile critice. Astfel, soluția include 2 tipuri de actualizări ale produsului:
   a. Ciclu rapid, conceput pentru un mediu de testare a rețelei
   b. Ciclu lent, gândit pentru restul rețelei (producție, servere critice, etc.)
5. Soluția permite stabilirea zonelor de testare și a zonelor critice în cadrul rețelei prin intermediul politicilor din consola de administrare

B. PROTECȚIA STAȚIILOR FIZICE ȘI A SERVERELOR

1. Caracteristici generale minime și eliminatorii:

1.1 Pentru a minimiza consumul de resurse, soluția antimalware trebuie să permită instalarea personalizată a modulelor proprietare (de exemplu, să permită instalarea soluției antimalware fără modulul de control al accesului web, modulul de control al dispozitivelor sau modulul firewall).

1.2 Pentru o mai bună protecție a stațiilor și a serverelor, soluția vainclude un vaccin anti-ransomware. Acest vaccin asigură protecția împotriva tuturor amenințărilor ransomware cunoscute, prin imunizarea stațiilor și serverelor, chiar dacă sunt infectate, și prin blocarea procesului de criptare.

1.3 Vaccinul anti-ransomware primește actualizări de la producător, odată cu actualizarea semnăturilor produsului Antimalware.

1.4 Pentru o mai bună protecție a stațiilor și serverelor, soluția va include protecție împotriva atacurilor avansate de tip exploit zero-day (atacuri direcționate) bazate pe tehnologii de învățare automată.

1.5 Pentru o mai bună protecție a stațiilor și serverelor, soluția va include un modul integrat ERA (Endpoint Risk Analytics) capabil să identifice și să remedieze automat sau manual un număr mare de riscuri existente la nivel de rețea sau sistem de operare care pot afecta funcționalitatea și nivelul de securitate al punctului final

2. Cerințe de sistem:

2.1 Sistem de operare pentru stații de lucru: Windows11, Windows 10, Windows 8/8.1, Windows 7, Mac OS Monterey 12.x, macOS BIG SUR 11.x, macOS Catalina 10.15, Mac OS X Mojave (10.14), Mac OS High Sierra (10.13),Mac OS Sierra (10.12),

2.2 Sisteme de operare integrate: Windows 10 IOT Enterprise, Windows Embedded 8.1 Industry, Windows Embedded 8 Standard, Windows Embedded Standard 7, Windows Embedded POS Ready 7 Windows Embedded POSReady 7, Windows Embedded Enterprise 7

2.3 Sisteme de operare pentru servere: Windows Server 2022, Windows Server 2019, Windows Server 2019 CORE, Windows Server 2016, Windows Server 2016 (Core),Windows Server 2012 R2,Windows Server 2012, Windows Small Business Server (SBS) 2011,, Windows Server 2008 R2,

2.4 Sisteme de operare Linux: Red Hat Enterprise Linux 7.x, 8.x,9.x, CentOS 7.x, 8.x, Ubuntu 16.04 sau ulterior, SUSE Linux Enterprise Server 12SP4,5, SUSE LINUX Exnterprise15 SP2,SP3, OpenSUSE LEAP 15- 2-15.3. , Fedora 31 sau ulterior, AWS Bottlerocket 2020.03, Amazon Linux v2, Google COS Milestones 77,81,85, Azure Mariner 2, AlmaLinux 8,9.x, Rocky Linux 8.x, Cloud Linux 7,8 .x, Pardus 21, Linux Mint 20.3, Miracle 8.4.

3. Administrare și instalare la distanță:

3.1 Înainte de instalare, administratorul va putea să personalizeze pachetele de instalare cu modulele dorite: firewall, controlul conținutului, controlul dispozitivelor, power user.

3.2 Instalarea se poate face în mai multe moduri:

a. prin descărcarea directă a pachetului pe stația unde se va face instalarea;
b. prin instalare de la distanță, direct din consola de administrare
c. prin trimiterea prin e-mail (orice adrese) a pachetului de instalare pentru Windows, Linux, Mac.

3.3 Instalarea clienților la distanță în alte locații decât cele în care este instalată consola de management se va face prin intermediul unui client existent în locațiile respective de tip releu pentru a minimiza traficul în WAN.

3.4 Informațiile despre fiecare stație vor fi disponibile în consolă: numele stației, IP, sistemul de operare, modulele instalate, politica aplicată, informații despre actualizări etc.

3.5 Din consolă va fi posibilă trimiterea unei singure politici pentru configurarea completă a clientului pe stații/servere.

• Bulevardul Liviu Rebreanu, Nr. 156Timișoara, jud. Timiș, Cod Poștal 300723
• Cod fiscal 4663448 • Telefon +4 0356 433111 • Fax +4 0256 486956
• e-mail: judetean@hosptm.ro • www.hosptm.ro

3.6 Consola va include o secțiune, „Audit", unde vor fi menționate toate acțiunile întreprinse fie de administratori, fie de reporteri, cu informații detaliate: logare, editare, creare, logout, mutare etc.

3.7 Posibilitatea de a crea un singur pachet de instalare, utilizabil atât pentru sistemele de operare pe 32 de biți, cât și pentru cele pe 64 de biți.

3.8 Posibilitatea de a crea un singur pachet de instalare, utilizabil pentru stații (fizice și/sau virtuale), servere (fizice și/sau virtuale).

3.9 Posibilitatea de a crea pachete de instalare web sau kit complet de instalare.

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

3.11 Permite selectarea clientului care va descoperi stațiile din rețea, altele decât cele integrate în domeniu.

4. Caracteristicile și principalele funcționalități ale modulului antimalware:

1. Solutia permite administratorului sa stabileasca actiunea luata de produsul Antimalware la detectarea unei amenintari noi. Astfel administratorul va putea alege intre urmatoarele actiuni:

a. <u>Actiune imiplicita pentru fisiere infectate:</u>

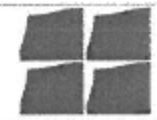
- interzice accesul
- dezinfecteaza
- stergere
- muta fisierele in carantina
- nicio actiune

b. <u>Actiune alternativa pentru fisierele infectate:</u>

- interzice accesul
- dezinfecteaza
- stergere
- muta fisierele in carantina

c. <u>Actiune imiplicita pentru fisierele suspecte:</u>

- interzice accesul
- stergere



• Bulevardul Liviu Rebreanu, Nr. 156Timișoara, jud. Timiș, Cod Postal 300723
• Cod fiscal 4663448 • Telefon +4 0356 433111 • Fax +4 0256 486956
• e-mail: judetean@hosptm.ro • www.hosptm.ro

ANMCS
unitate aflată în
SUPRAVEGHEREA

- muta fisierele in carantina
- nicio actiune

d. <u>Actiune alternativa pentru fisierele suspecte:</u>

- interzice accesul
- stergere
- muta fisierele in carantina

2. Scanarea automată în timp real poate fi setată să nu scaneze arhive sau fișiere mai mari de un anumit numar de MB, dimensiunea fișierelor poate fi definită de administratorul soluției,

3. Definirea a până la 16 niveluri de adâncime pentru scanarea în arhive.

4. Scanarea euristică comportamentală prin simularea unui calculator virtual în interiorul căruia sunt rulate aplicații potențial periculoase, protejând sistemul de viruși necunoscuți prin detectarea codurilor periculoase a căror semnătură nu a fost încă publicată.

5. Scanarea oricăror medii de stocare a informațiilor (CD-uri, hard disk-uri externe, unități partajate etc.). De asemenea, va fi posibilă anularea scanării dacă sunt detectate unități care au mai mult de un anumit număr de MB de informații stocate.

6. Scanarea automată a e-mailurilor la nivelul stației de lucru pentru POP3/SMTP.

7. Configurarea cailor care urmează să fie scanați la cerere.

8. Clienții antimalware pentru stațiile de lucru permit definirea de liste de excludere de la scanarea în timp real și la cerere a anumitor directoare, discuri, fișiere, extensii sau procese.

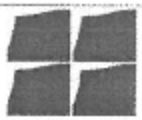
9. Cu ajutorul unei baze de date complete cu semnături spyware și euristica de detecție a acestui tip de programe, produsul va trebui să ofere protecție anti-spyware.

10. Posibilitatea de a configura scanările programate pentru a fi executate cu prioritate redusă

11. Produsul antimalware poate fi configurat pentru a utiliza scanarea în cloud și parțial scanarea locală.

12. De asemenea, administratorul poate personaliza motoarele de scanare, având posibilitatea de a alege între mai multe tehnologii de scanare:

- Scanare locală, când scanarea este efectuată pe stația de lucru locală. Modul de scanare locală este potrivit pentru mașinile puternice, având toate semnăturile și motoarele stocate local.



• Bulevardul Liviu Rebreanu, Nr. 156 Timișoara, jud. Timiș, Cod Poștal 300723
• Cod fiscal 4663448 • Telefon +4 0356 433111 • Fax +4 0256 436056
• e-mail: judetean@hosptim.ro • www.hosptim.ro

- Scanare hibridă cu motoare ușoare (Public Cloud), cu o amprentă medie, utilizând scanarea în cloud și semnături parțial locale. Acest mod de scanare oferă avantajul unui consum mai bun de resurse, fără a implica scanarea locală.

13. Pentru o protecție sporită, soluția antimalware trebuie să aibă 3 tipuri de detecție: bazată pe semnături, bazată pe comportamentul fișierelor și bazată pe monitorizarca proceselor.

14. Pentru o protecție sporită, soluția antimalware trebuie să fie capabilă să scaneze paginile HTTP.

15. Pentru o mai bună gestionare a antimalware-ului instalat pe stații, produsul va include opțiunea de setare a unei parole pentru protecția dezinstalării.

16. Pentru siguranța utilizatorului, clientul va include un modul antiphishing.

17. Soluția oferă protecție în timp real pe mașinile cu sistem de operare Linux, în funcție de versiunea de kernel instalată.

5. Advanced Anti-Exploit:

1. Abilitatea de a opri atacurile avansate de tip zero-day prin exploatări evazive

2. Detectarea în timp real a celor mai recente exploatări care pot face vulnerabil un sistem de operare.

3. 4. Protecția aplicațiilor utilizate frecvent și a celor de tip „sistem", cum ar fi browserele, aplicațiile de tip office sau reader, procesele critice legate de sistemele de operare.

6. Firewall:

1. Posibilitatea de a configura reguli firewall pentru aplicații sau conectivitate.

2. Modulul poate fi instalat/dezinstalat în funcție de preferințele administratorului.

3. Posibilitatea de a defini rețele de încredere pentru mașina de destinație.

4. Posibilitatea de a detecta scanarea porturilor.

5. Posibilitatea de a defini diferite profiluri de rețea ((Acasă/Oficiu, De încredere, Publice, Neîncrezătoare sau Lăsați Windows-ul să decidă)

6. Abilitatea de a crea reguli personalizate bazate pe aplicație și/sau conexiune

7. Carantină:

1. Produsul antimalware permite trimiterea automată a fișierelor din carantină către laboratoarele antimalware ale producătorului.

2. Trimiterea conținutului din carantină poate fi trimisă automat, la un interval definit de administrator.

3. Produsul antimalware trebuie să permită ștergerea automată a fișierelor din carantină mai vechi de o anumită perioadă, pentru a nu încărca inutil spațiul de stocare.

4. Posibilitatea de a restaura un fișier aflat în carantină în locația sa inițială.

5. Modulul de carantină vă va permite să reanalizați obiectele după fiecare actualizare a semnăturii.

8. Protecția datelor:

1. Produsul permite blocarea datelor confidențiale (pin de card, cont bancar etc.) transmise prin HTTP sau SMTP prin crearea de reguli specifice.

9. Controlul conținutului:

1. Consola va avea un modul integrat dedicat controlului accesului la internet cu următoarele caracteristici:

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

b. Permite blocarea accesului la Internet pe intervale de timp.

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

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

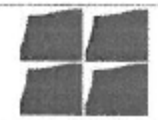
e. Permite blocarea accesului la anumite aplicații definite de administrator;

f. Permite restricționarea accesului la anumite pagini de internet în funcție de anumite categorii predefinite (de exemplu: întâlniri online, violență, pornografie etc.).

10. Controlul dispozitivelor:

1. Modulul poate fi instalat / dezinstalat în funcție de preferințele administratorului.

2. Modulul vă va permite să controlați următoarele tipuri de dispozitive:



• Bulevardul Liviu Rebreanu, Nr. 156Timișoara, jud. Timiș, Cod Postal 300723
• Cod fiscal 4663448 • Telefon +4 0356 433111 • Fax +4 0256 486056
• e-mail: judeteanz@hosptm.ro • www.hosptm.ro

a. Dispozitive Bluetooth

b. Dispozitive CDROM

c. Unități de dischetă

d. Politici de securitate 153

e. IEEE 1284.4

f. IEEE 1394

g. Dispozitive de imagistică

h. Modemuri

i. Unități de bandă

j. Windows portabil

k. Porturi COM/LPT

l. SCSI Raid

m. Imprimante

n. Adaptoare de rețea

o. Adaptoare de rețea fără fir

p. Stocare internă și externă

3. Modulul va permite configurarea de reguli care vor defini permisiunile pentru dispozitivele conectate la computerul client.

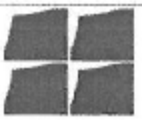
4. Modulul va permite configurarea de excluderi pentru diferite tipuri de dispozitive pentru care au fost configurate reguli.

11. Power user:

1. Modulul poate fi instalat/dezinstalat în funcție de preferințele administratorului.

2. Modulul permite utilizatorilor să primească drepturi Power User. Utilizatorii vor putea să acceseze și să modifice setările clientului antimalware de la o consolă disponibilă local pe computerul client.

3. Modificările efectuate din modulul Power User vor fi active local, pe mașina pe care au fost efectuate modificările respective.



• Bulevardul Liviu Rebreanu, Nr. 156 Timișoara, jud. Timiș, Cod Poștal 300723
• Cod Fiscal 4663448 • Telefon +4 0356 433111 • Fax +4 0256 486956
• e-mail: judetean@hosptm.ro • www.hosptm.ro

4. Administratorul va putea să anuleze setările aplicate de Power Users din consolă.

12. **Actualizari**:

1. Posibilitatea de a efectua actualizarea la nivelul stației în modul silențios (fără avertizare).

2. Sistem de actualizare în cascadă utilizând unul sau mai multe servere de actualizare (în cascadă).

3. Actualizare pentru locații la distanță prin intermediul unui client antimalware care acționează, de asemenea, ca un server de actualizare.

13. EDR

1.Utilizează funcționalitatea EPP și colecteaza date de la toate punctele finale.

2. Identifică automat incidentele care reușesc să ocolească tehnologiile de prevenire și protecție, adesea provenind de la dispozitive negestionate.

3. Mișcarea laterală în rețea este detectată fie direct prin observarea tehnicilor comune (de exemplu, utilizarea WMI/PsExec), fie indirect prin corelarea diferitelor evenimente

4. Utilizează modele probabilistice, monitorizând și analizând constant situația pentru a descoperi atacuri evazive.

Cap.4 Obligațiile Furnizorului

Licențele furnizate trebuie să îndeplinească normativele și strandardele europene specifice, aplicabile, aflate în vigoare;

Plata se va face pe baza facturii emise de furnizor, în urma efectuării recepției licențelor și a semnării procesului verbal de recepție de către ambele părți;

Achizitiorul are dreptul de a notifica imediat furnizorul, orice plângere sau reclamație ce apare în conformitate cu garanția acordată produselor.

Cap. 5 Reguli și standardele de referință

- ISO 9001: 2015 pentru certificare conformitatii sistemului de management al calitatii pentru executant
- ISO 27001:2018 pentru certificarea conformitatii sistemului de management al securitatii informatiei pentru executant
- ISO 14001:2015 pentru certificarea conformitatii sistemului de management al mediului pentru executant
- ISO 45001: 2018 pentru certificarea conformitatii sistemului de management al sanatatii si securitatii in munca pentru executant.

• Bulevardul Liviu Rebreanu, Nr. 156Timișoara, jud. Timiș, Cod Postal 300723
• Cod fiscal 4663448 • Telefon +4 0356 433111 • Fax +4 0256 486956
• e-mail: judetean@hosptm.ro • www.hosptm.ro

Instalarea si configurarea solutiei sa va face de către tehnician/tehnicieni autorizați de producatorul aplicației anti-virus.
Furnizorul va pune la dispozitia Beneficiarului autorizația de comercializare din partea producatorului a aplicatiei anti-virus

Valabilitate licențe: pe o perioadă de 12 luni .

ANEXA NR.1 la caiet de sarcini

Nr.crt.	Denumire produs	Cantitate	U.M.
1	Antivirus 1100 dispozitive	1	pachet