ROMÂNIA
JUDEŢUL BACĂU
MUNICIPIUL ONEŞTI
B-dul Oituz, nr.17, Cod 601032, Tel: 0234.324.243, 0234.312.340, Fax: 0234.313.911, 0234.321.869

Nr. 5876/28.01.2025

In atenţia operatorilor economici interesaţi,

SCRISOARE DE INTENTIE ACHIZITIE DIRECTA

I. Autoritatea contractantă: MUNICIPIUL ONEŞTI, cu sediul în Oneşti, B-dul Oituz, nr. 17, jud.Bacău, Cod 601032, telefon 0234.324243, fax 0234.313911/0234.312502, intenţionează sa achizitioneze servicii ce constau in **Servicii de actualizare ANTIVIRUS pentru echipament FortiGate 100F si clienti**, în conformitate cu prevederile art. 7, alineat 5 din Legea 98/2016 - privind achiziţiile publice, cu modificarile si completarile ulterioare si Anexa la H.G. nr. 395/2016 pentru aprobarea Normelor metodologice de aplicare a prevederilor referitoare la atribuirea contractului de achiziţie publică/acordului-cadru din Legea nr. 98/2016 privind achiziţiile publice, cu modificarile si completarile ulterioare.

II. Obiectul achiziţiei:

„Servicii de actualizare antivirus pentru echipament FortiGate 100F si clienti ",
Cod de clasificare CPV: 72540000-2 Servicii de actualizare informatica (Rev.2)

III. Valoarea estimată:

Valoarea estimata a achizitiei publice este de 16.900 lei fără TVAcare se compune din:

Nr. crt	Denumire produs	Cantitate	Valoare estimata fara TVA
1	Actualizare software firewall FortiGate, subscriptie 12 luni; suport tehnic	1	9.100,00
2	Actualizare software antivirus, subscriptie 12 luni; suport tehnic	- minim 200 clienti - 10 clienti pentru servere/masini virtuale	7.800,00

IV. Achiziţia se finalizează prin: comanda ferma**.**

V. Durata de prestare a serviciilor:

Durata de prestare a serviciilor este de 12 luni.

VI. Informatii juridice, economice, financiare si tehnice

Cadrul Legal:

- Legea privind achizitiile nr 98/2016, cu modificarile si completarile ulterioare;
- Hotărârea nr. 395/2016 pentru aprobarea Normelor metodologice de aplicare a prevederilor referitoare la atribuirea contractului de achiziţie publică/acordului-cadru din Legea nr. 98/2016 privind achiziţiile publice, cu modificarile si completarile ulterioare;
- www.anap.gov.ro;

Prezenta enumerare nu are caracter limitativ.

VII.Locul şi condiţii de prestare a serviciilor: Primăria Municipiului Oneşti situata in Bulevardul Oituz, Nr.17, Judetul Bacau.

VIII. Descrierea achizitiei publice:

Autoritatea contractanta - Municipiul Oneşti intenţionează sa achiziţioneze:

- actualizare software firewall, subscriptie 12 luni; suport tehnic pentru actualizare software antivirus, subscriptie 12 luni; suport tehnic pentru **FortiGate 100F**
- actualizare software antivirus, subscriptie 12 luni; suport tehnic pentru - minim 200 clienti si 10 clienti pentru servere/masini virtuale

Finanţarea achizitiei publice se va realiza din bugetul local.

Cerintele din prezenta sunt minimale.

Ofertantul este pe deplin responsabil pentru prestarea serviciilor in conformitate cu necesitatea autoritatii contractante, stabilita in documentatia achizitiei publice si va respecta cerintele prevazute in caietul de sarcini nr. 1875/14.01.2025.

IX. Modul de elaborare şi de prezentare a ofertei, formalităţi care trebuie îndeplinite în legătură cu transmiterea ofertei

A) DOCUMENTE CE INSOTESC OFERTA*:*

Cerinta nr. 1 **-** Ofertantii/fiecare membru al asocierii vor prezenta **Împuternicire scrisa, Formular 1** din sectiunea *modele de formulare*, prin care semnatarul ofertei este autorizat sa angajeze ofertantul/asocierea în procesul achizitiei publice - semnata (in cazul in care este altul decat reprezentantul legal al ofertantului/asociatului).

Cerinta nr. 2 **-** Ofertantii/fiecare membru al asocierii/subcontractantii vor prezenta **Formularul 2** din sectiunea *modele de formulare* - DECLARATIE privind denumirea şi datele de identificare ale ofertantului/ ofertantului asociat/ subcontractantului prin care se vor comunica datele de identificare ale societăţii (număr de înmatriculare, CUI, cont Banca/Trezorerie si banca la

care este deschis acesta), precum şi datele de contact (adresă, telefon, email, etc) ale persoanei desemnate să implice societatea în relaţiile cu Primaria Municipiului Oneşti.
Cerinta nr. 3 **-** Ofertantii/fiecare membru al asocierii/subcontractantii vor prezenta **Formularul GDPR** – **Formularul 3** din sectiunea *modele de formulare* – semnat.

B) DOCUMENTE DE CALIFICARE:
B.1) Criterii de calificare privind situaţia personală
Se solicita îndeplinirea următoarelor cerinţe minime de calificare:
Cerinţa nr.1- Ofertantii/fiecare membru al asocierii/subcontractantii vor prezenta o declaraţie privind neîncadrarea în prevederile art. 58 - 63 din Legea nr.98/2016. Se vor prezenta **Formularul 4** cu Anexa din Secţiunea Modele de Formulare, semnate.
Cerinta nr.2 - Ofertantii/fiecare membru al asocierii /subcontractantii vor prezenta o declaratie privind neîncadrarea în prevederile art. 164 - 167 din Legea nr. 98/2016. Se va prezenta **Formularul 5** din sectiunea *modele de formulare* semnat.

B.2) Criterii de calificare privind capacitatea de exercitare a activităţii profesionale
Se solicita îndeplinirea urmatoarei cerinţe minime de calificare:
Cerinţa nr.1 – Ofertantii/fiecare membru al asocierii subcontractantii vor prezenta Certificat Constatator emis de Oficiul Registrului Comerţului. Obiectul achiziţiei publice trebuie sa aiba corespondent în codul CAEN din Certificatul constatator emis de ONRC. Informaţiile cuprinse în certificatul constatator trebuie sa fie reale / actuale la data limita de depunere a ofertelor. Persoanele juridice /fizice străine vor prezenta documente care dovedesc o forma de înregistrare / atestare ori apartenenţa din punct de vedere profesional în conformitate cu prevederile legale din tara în care ofertantul este stabilit.

C.) Propunerea Tehnica
Propunerea tehnica va contine:
Cerinta nr.1:
Document intitulat „***Propunere tehnica"*** **- model propriu**, semnat. Propunerea tehnica va fi întocmita într-o manieră organizată astfel încât, în procesul de evaluare, informatiile din aceasta sa permita identificarea facila a corespondentei cu specificatiile tehnice din caietul de sarcini si documentatia tehnica. Din acest document trebuie să rezulte că ofertantul respectă, în totalitate, cerinţele solicitate de autoritatea contractanta, inclusiv Caietul de Sarcini nr. 1875 din data de 14.01.2025 intocmit de Serviciul IT&C.
Cerinta nr. 2:
Formularul nr.9 din Sectiunea Formulare - ""Declaratie privind respectarea reglementarilor obligatorii din domeniul mediului, social, al relatiilor de munca si privind respectarea legislatiei de securitate si sanatate in munca". Informatii suplimentare pot fi obtinute de la institutiile abilitate, respectiv: Ministerul Mediului, Apelor si Padurilor, Bvd. Libertatii nr. 12, Sector 5, Bucuresti, Romania, Tel. +40 21 408 9605, Fax: +40 21 408 9615, Adresa internet (URL): http://www.mmediu.ro. Ministerul Muncii si Solidaritatii Sociale , str. Dem.I.Dobrescu nr.2-4 sectorul 1, Sistemul Electronic de Achizitii Publice Sistemul Electronic de Achizitii Publice, 23.10.2018 07:40 Pagina 8 Bucuresti, Romania, Tel. +40 213136267, Fax: +40 213136267, Adresa internet (URL): www.mmuncii.ro Acest formular se va prezenta si de ofertantii asociati sau/si de catre subcontractantii declarati, daca este cazul.

D.) Propunere Financiara
Cerinta 1
Formularul nr.10-**FORMULAR DE OFERTĂ + Anexa** din Sectiunea Formulare semnat de catre reprezentantul legal al ofertantului. Preţul reprezintă preţul total al ofertei, fiind exprimat în lei fara TVA.. Pretul ofertei include Serviciile de suport tehnic aferente implementarii, configurarii si bunei functionari a echipamentului timp de 12 luni de la data activarii licentei software.

Evaluarea financiara, respectiv incadrarea in art. 137 din Anexa la Hotararea Guvernului nr.395/2016 pentru aprobarea Normelor metodologice de aplicare a prevederilor referitoare la atribuirea contractului de achizitie publica/acordului-cadru din Legea nr.98/2016 privind achizitiile publice actualizate, se va realiza prin aplicarea criteriului de atribuire. Documentele propunerii financiare se vor prezenta intr-o modalitate in care sa furnizeze toate informatiile cu privire la preturile si tarifele respective (exprimate în Lei, fara TVA) precum si la alte conditii financiare si comerciale, astfel încât aceasta sa asigure realizarea tuturor categoriilor de servicii solicitate prin documentatia de atribuire.
Propunerea financiara are caracter ferm si obligatoriu, din punctul de vedere al continutului pe toata perioada de valabilitate. Modul de prezentare a propunerii financiare este obligatoriu si trebuie sa contina toate documentele solicitate si in forma solicitata.

Ofertele ce cuprind: documentele de calificare, propunerea tehnica si propunerea financiara se vor transmite pana la data de **31.01.2025, inclusiv** prin e-mail la adresa oferte@onesti.ro.

X. Criteriul de atribuire: ***Pretul cel mai scazut.***
Criteriul utilizat pentru desemnarea ofertei câştigătoare este *Preţul cel mai scăzut* in conformitate cu prevederile art. 187 alin.(3) lit.d) din Legea nr.98/2016. Dintre ofertele admisibile, va fi declarată câştigătoare oferta care are cel mai scăzut pret in urma aplicării criteriului ***Preţul cel mai scăzut****.*
In cazul în care două sau mai multe oferte conţin, în cadrul propunerii financiare, acelaşi pret minim, atunci, în vederea desemnării ofertantului câştigător, se va solicita în scris, respectivilor ofertanţi, pentru departajare, intr-un termen rezonabil o nouă ofertă de preţ.

Informaţii suplimentare:

Locul si termenul de solicitare a clarificarilor la documentele achizitiei: prin email cumpararidirecte@onesti.ro , cu cel putin 24 de ore înainte de termen limita primire oferte. Raspunsurile la eventualele solicitari de clarificari privind documentele achizitiei publice se vor publica si vor putea fi accesate, pe site-ul oficial al institutiei publice, la adresa www.onesti.ro, Sectiunea Actualitate - Achizitii Publice(se va accesa https://onesti.ro/primarie_onesti/noutati/achizitii-publice).

Toti operatorii economici interesati vor transmite ofertele pe e-mail la adresa oferte@onesti.ro pana la termenul limita de primire oferte stabilit si precizat anterior.

Limbile in care pot fi depuse ofertele sau cererile de participare: **limba romana.**

Ofertele financiare trebuie sa fie intocmite in moneda nationala si sa fie valabile 60 de zile de la termenul limita primire oferte.

Caietul de sarcini si formularele pentru achizitia serviciilor ce fac obiectul solicitarii pot fi consultate pe site-ul www.onesti.ro la sectiunea Actualitate - Achizitii Publice(se va accesa https://onesti.ro/primarie_onesti/noutati/achizitii-publice).

Propunerile, tehnica si financiara, vor fi intocmite respectand caietul de sarcini.

In cazul in care ofertantul declarat castigator are cont in SEAP, autoritatea contractanta va finaliza achizitia in Catalogul electronic de produse/servicii/lucrari existent in SEAP.

Se vor comunica datele de identificare ale societăţii (adresă, număr de înmatriculare, CUI, cont Trezorerie), precum şi datele de contact (adresă, telefon, email, etc) ale persoanei desemnate să implice societatea în relaţiile cu Municipiul Oneşti.

Cu stimă,

Municipiul ONEŞTI
DIRECTIA URBANISM
***Serviciul** Tehnologia Informației și Comunicațiilor*
Nr.inreg: 1875/14.01.2025

CAIET de SARCINI
Actualizare software sistem ANTIVIRUS Echipament FortiGate pentru Rețea–LAN

1. INTRODUCERE

Caietul de Sarcini face parte integrantă din documentația de atribuire și conține specificațiile tehnice, respectiv, ansamblul cerințelor minimale obligatoriu de îndeplinit, pe baza cărora se elaborează, de către fiecare ofertant, propunerea tehnică în acord cu necesitățile autorității contractante.

Scopul întocmirii caietului de sarcini este de a asigura ***Actualizarea*** **ANTIVIRUS-ului** pentru ***Rețea Locală*** de ***Calculatoare*** (**LAN**) din Primăria Municipiului Onești, în baza unei comenzi de servicii de actualizare corespunzătoare dotării și funcționalităților existente în prezent.

Achizitia se va efectua pentru o perioadă de **1** (***un***) an de zile prin actualizări zilnice ale bazei de date cu semnăturile virușilor nou apăruți, sub forma de abonament anual.

2. SCURTĂ DESCRIERE

Serviciile de ***actualizare ANTIVIRUS*** **solicitate** în prezentul Caiet de Sarcini, sunt destinate asigurării bunei funcționări a Rețelei locale de calculatoare și a întregului Sistem informatic integrat pentru managementul activităților specifice departamentelor de specialitate din cadrul Primăriei Municipiului Onesti.

Primăria Municipiului Onesti are în exploatare, încă din anul 2006, Servere și Echipamente de Rețea Locală de Calculatoare (**LAN**), în dezvoltare permanentă, cu noi programe și aplicații informatice, noi echipamente IT&C, care acoperă cele trei modalități standard de funcționare (**LAN**), specifice:

- **INTRANET** > pe rețeaua locală de calculatoare din sediul central, servicii, birouri și compartimente de specialitate interconectate pe o ***Infrastructură*** pe ***Fibră Optică*** + ***UTP***;
- **EXTRANET** > rețea locală prelungită pe ***Fibră Optică*** în locațiile la distanta, vechiul sediu al primăriei (***DGAS***), Biblioteca Municipală Onești și Piața agroalimentară;
- **INTERNET** > furnizare servicii de WebBrowsing, e-Mail și Comunicații de date pentru toți clienții din Intranet si Extranet asigurând și conexiuni ***VPN***–Virtual Private Network - conexiune privată între două sau mai multe rețele sau calculatoare pentru Comunicații de date distribuite, protejate peste o rețea publică de date sau prin Internet.

Măsurile minimale de ***protecție*** și ***securitate cibernetică*** pentru o rețea locală de calculatoare ***obligă*** la existența a două componente principale, specifice: **Firewall** hardware și **Firewall** software – pachete software dedicate, generic denumite programe **Antivirus**.

În anul 2021 s-a achiziționat echipamentul ***hardware*** **Firewall FortiGate 100F** care conține și un **abonament** anual la ***pachetul software*** **specific** pentru antivirus, administrare, filtrare și securitate comunicații pentru a asigura securitate informatică, protecție antivirus și împotriva atacurilor cibernetice.

Cerințele din caietul de sarcini vor fi considerate ca fiind minimale. În acest sens vor fi luate în considerație toate ofertele care, prin propunerea tehnică, asigură un nivel egal sau superior cerințelor minimale din caietul de sarcini; ofertele de servicii cu caracteristici tehnice inferioare celor prevăzute în caietul de sarcini vor fi declarate neconforme în temeiul Legii 98/2016 și HG 395/2016.

Specificațiile tehnice care indică o anumită origine, sursă, producție, un produs special, o marcă de fabricație sau de comerț, un brevet de invenție, o licență de fabricație sau o autorizație sunt menționate doar pentru identificarea cu ușurință a tipului de produs/serviciu si nu au ca efect favorizarea sau

eliminarea anumitor operatori economici sau anumitor produse. **Aceste specificații vor fi considerate ca având mențiunea: "*sau echivalent*".**

3. OBIECTUL ACHIZITIEI

Actualizare software sistem ANTIVIRUS si firewall Echipament FortiGate pentru ***Rețeaua Locală*** de ***Calculatoare*** (LAN), programe și aplicați informatice în exploatare, existente în dotarea Primăriei Municipiului Onești.

Cod de clasificare CPV: **72540000-2** Servicii de actualizare informatică (antivirus);

Infrastructura **IT&C**, bazată pe **7 Servere**, ***interconectează*** peste 200 **PC-*uri*** și peste 60 de ***Imprimante,*** asigură ***accesul securizat,*** *partajat,* a peste **200** de ***utilizatori*** la ***Bazele*** de ***Date*** cu programele și sistemele informatice aflate în exploatare.

Deasemenea asigura interconectarea bibliotecii, DGAS, piata, Protectie Civila si Baza Sportiva la serverele primariei si a colaboratorilor la reteaua primariei.

A. **Autoritatea contractantă**: Municipiul ONEȘTI, B-dul Oituz, nr. 17, județul Bacău

B. **Sursa de finanțare**: Buget local

C. **Informații achiziție**: ***Actualizarea*** **ANTIVIRUS** pentru ***Rețeaua*–LAN** din dotarea Primăriei Municipiului Onești, se vor achiziționa conform legislației privind achizițiile publice, respectiv, Legea 98/2016 și HG 395/2016 prin cumpărare/furnizare/prestare servicii în baza unei comenzi ferme conform specificațiilor din prezentul caiet de sarcini.

D. ***Obiectul*** achizitiei constă în ***efectuarea*** *următoarelor activitati* ***principale de*** strictă specialitate pentru ***Actualizare*** **ANTIVIRUS** pentru ***Rețea*–LAN:**

III. ***Actualizare zilnică*** a bazei de date cu ***semnăturile*** virușilor identificați și
IV. ***Servicii suport tehnic de specialitate*** prin ***e-Mail*** și/sau ***telefon***/fax;

E. ***DETALIERE*** ***Actualizare*** software a sistemului de **ANTIVIRUS si Firewall** pentru ***Rețea*–LAN** pentru echipamentul **Firewall FortiGate**, din Primăria Municipiului Onești, pentru un an de zile:

I. Actualizările pentru firewal-ul **FortiGate 100F,** pentru 1 an, harware plus, 24x7, Forticare si FortiGuard Unified Threat Protection (UTP) si conține și un **abonament *software* specific** pentru antivirus, administrare, filtrare și securitate comunicații, având următoarele ***componente dedicate***, așa cum sunt ele detaliate în oferta producatorului (*atașată*) :

1. **FortiCare** - servicii suport prin telefon, web, mail – 24x7
2. **FortiGuard App Control Service** – filtrare aplicatii si servicii web
3. **FortiGuard IPS Service** - pentru protectia retelei la tentative de acces neautorizat
4. **FortiGuard Advanced Malware Protection (AMP)** — componenta de antivirus
5. **Mobile Malware, Botnet, CDR, Virus Outbreak Protection and FortiSandbox Cloud Service** – componenta de malware, virus, scanare fisiere
6. **FortiGuard Web and Video Filtering Service (doar de la versiunea 7.0)** – componenta de filtrare web si video
7. **FortiGuard Antispam Service** – pentru filtrare spam-uri

II. Pentru a asigura protectia statiilor de lucru este necesara instalarea clienților de antivirus pe stațiile de lucru si servere/mașini virtuale. Avem nevoie de 200 de clienți pentru stațiile de lucru si 10 clienți pentru servere/mașini virtuale.

CARACTERISTICI GENERALE ALE PRODUSULUI

Produsul („soluția") reprezintă o platforma integrata pentru managementul securității, gândita ca o solutie modulara. Produsul conține următoarele module:

A. O consola de management care asigura functionalitati de administrare.
B. Protectie antimalware pentru statii fizice, laptop-uri si servere.

A. CONSOLA DE MANAGEMENT

1. Cerinte generale:

1. Interfata consolei de management va fi in limba romana.
2. Interfata clientului de securitate, care se instaleaza pe statii si servere, va fi in limba romana.
3. Manualul de instalare a produsului va fi in limba romana.
4. Manualul de administrare a produsului va fi in limba romana.
5. Solutia va pemite activarea/dezactivarea actualizarilor de produs/semnaturi.
6. Actualizari automate a consolei de management facute de catre producatorul solutiei, fara a fi necesara interventia utilizatorului.
7. Notificarile – prezente in interfata, notificarile necitite sunt evidentiate, trimise catre una sau mai multe adrese de email, alerteaza administratorul in cazul unor probleme majore: licentiere, detectie virusi, actualizari de produs disponibile).
8. Consola de management este accesibila de oriunde in lume (este bazata pe un serviciu cloud de tip Software-as-a-Service), fara a fi nevoie de setari suplimentare din partea utilizatorului.
9. Consola de management este accesibila atat de pe statii de lucru cat si de pe dispozitive mobile (smartphone, tableta).

2. Panou de monitorizare si raportare (Dashboard):

1. Rapoartele din panoul de monitorizare vor putea fi configurate specificand numele raportului, tipul raportului, tinta raportului, optiuni specifice pentru orice tip de raport (de exemplu pentru raportul de actualizare - care este intervalul dupa care o statie este considerata neactualizata).
2. Panoul central contine rapoarte pentru toate modulele suportate.
3. Rapoartele din panoul central de comanda permit: adaugarea altor rapoarte, stergerea lor si rearanjarea.

3. Inventarierea retelei – managementul securitatii:

1. Solutia se va integra cu domeniul Active Directory si va putea importa inventarul.
2. Se permite descoperirea statiilor statii fizice neintegrate in Active Directory (Workgroup) cu ajutorul Network discovery.
3. Solutia va oferi optiuni de cautare, sortare si filtrare dupa numele sistemului, sistem de operare, adresa IP, politica aplicata, ultima data cand s-a conectat (online si/sau offline) si FQDN.
4. Solutia va permite crearea unui pachet unic pentru toate sistemele de operare, de statii sau servere. Astfel, administratorul va putea descarca pachetele pentru protectia statiilor si serverelor pe care ruleaza sistemul de operare Windows, Linux, Mac.
5. Solutia va permite instalarea la distanta sau manual a clientilor antimalware pe masini fizice/virtuale.
6. Solutia va permite selectarea modulelor componente atunci cand se creaza pachetul clientului care se instalează pe mașinile fizice/virtuale.
7. Solutia va permite lansarea de task-uri de scanare, actualizare, instalare, dezinstalarea la distanta pentru clientul antimalware.
8. Solutia va oferi posibilitatea de repornire a masinilor fizice de la distanta.
9. Solutia va oferi informatii detaliate despre fiecare task si se fiseaza daca task-ul s-a finalizat sau nu cu succes.
10. Solutia va permite configurarea centralizata a clientilor antimalware prin intermediul politicilor
11. Se vor oferi in consola de management informatii detaliate ale obiectelor din consola: Nume, IP, Sistem de operare, Grup, Politica atribuita, Ultimele actualizare, Versiunea produsului, Versiunea de semnaturi.

4. Politici:

1. Solutia va permite configurarea setarilor antimalware prin intermediul politicilor din consola de magement.
2. Politica va contine optiuni specifice de activare/dezactivare si configurarea functionalitatilor precum scanarea antimalware la cerere, firewall, controlul accesului la Internet, controlul aplicatiilor, scanarea traficului web,controlul dispozitivelor, power user.
3. Solutia permite aplicarea politicilor pe masini client, grupuri de masini, domeniu, unitati organizationale.
4. Politica sa poate fi schimbata automat in functie de:

a. IP sau clasa de IP al statiei
b. Gateway-ul alocat
c. DNS serverul alocat
d. WINS serverul alocat
e. Sufix DNS pentru conexiunea dhcp
f. Clientul este/nu este in acceasi retea cu infrastructura de management (statia de lucru poate solutiona implicit numele gazdei)
g. Tipul retelei (lan, wireless)

5. Rapoarte:

1. Solutia va contine rapoarte care prezinta statusul masinilor clientil din punct de vedere al actualizarilor, fisierelor malware detectate, aplicatiile blocate, site-urilor web blocate.
2. Rapoartele programate pot fi trimise catre un numar nelimitat de adrese de email (nu este nevoie sa aiba un cont in consola de management).
3. Solutia va permite vizualizarea rapoartelor curente programate de administrator.
4. Solutia va permite exportarea rapoartelor in format .pdf si detaliile ca format .csv.

6. Carantina:

1. Solutia va permite restaurarea fisierelor carantinate in locatia originala sau intr-o cale configurabila cu optiunea de excludere automata a fisierului restaurat.
2. Carantina va fi locala, pe fiecare statia administrata si va fi administrata, fie local, fie din consola de management.

7. Utilizatori:

1. Administrarea se va putea face pe baza de roluri.
2. Roluri multiple predefinite: Administrator companie, Administrator retea, Reporter sau rol personalizat.
   a. Administrator companie: administreaza arhitectura consolei de management;
   b. Administrator retea: administreaza serviciile de securitate;
   c. Reporter: monitorizeaza si genereaza rapoarte.
3. Utilizatorii pot fi importati din Microsoft Active Directory sau creati in consola de management.
4. Se va permite configurarea detaliata a drepturilor administrative, permitand selectarea serviciilor si obiectelor pentru care un utilizator poate face modificari.
5. Se va permite deconectarea automata a oricarui tip de utilizator dupa un anumit timp pentru o protectie sporita a datelor afisate in consola de administrare. Acest interval se poate personaliza de administratorul solutiei.

8. Log-uri:

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

9. Actualizare:

1. Se permite definirea de locatii de actualizare multiple.
2. Se permite activarea/dezactivarea actualizarilor de produs si semnaturi.
3. Orice client antivirus sa poata fi configurat sa livreze update-urile catre alt client antivirus
4. Solutia permite testarea noilor versiuni de pachete de instalare ale clientului antimalware, inainte de a fi instalate pe toate stațiile si serverele din retea, evitand posibile probleme ce pot afecta serverele sau statiile critice. Astfel, solutia include 2 tipuri de actualizari de produs:
   a. Ciclu rapid, gandit pentru un mediu de test in cadrul retelei
   b. Ciclu lent, gandit pentru restul retelei (productie, servere critice etc)
5. Solutia permite stabilirea zonelor de test si critice din cadrul retelei prin intermediul politicilor din consola de management

B. PROTECTIE STATII SI SERVERE FIZICE

1. Caracteristici generale minimale si eliminatorii:

1. Pentru reducerea la minim a consumului de resurse, solutia antimalware trebuie sa permita instalarea personalizata a modulelor detinute (de exemplu, sa permita instalarea solutiei antimalware fara modulul de control al accesului web, modul de control al dispozitivilelor sau modulul firewall).
2. Pentru o mai buna protectie a statiilor si serverelor, solutia include un vaccin anti-ransomware. Acest vaccin asigura protectia impotriva tuturor amenintarilor cunoscute de tip ransomware, prin imunizarea statiilor si serverelor, chiar daca sunt infectate si prin blocarea procesului de criptare.
3. Vaccinul anti-ransomware primeste actualizari de la producator, odata cu actualizarea semnaturilor produsului Antimalware.
4. Pentru o mai buna protectie a statiilor si serverelor, solutia include protectie impotriva atacurilor zero-day de tip exploit avansate (atacuri directionate) bazata pe tehnologii de invatare automata (machine learning).
5. Pentru o mai buna protectie a a statiilor si serverelor, solutia include un modul integrat de tip ERA (Endpoint Risk Analytics – Analiza de risc a endpoint-ului) capabil sa identifice si remedieze in mod automatizat sau manual un numar mare de riscuri existente la nivel de retea sau sistem de operare ce pot afecta functionalitatea si nivelul de securizare al endpoint-ului

2. Cerinte de sistem:

- Sisteme de operare pentru statii 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),**
- Sisteme de operare embedded: **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**
- 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,**
- Sisteme de operare Linux: Red Hat Enterprise Linux 7.x, 8.x,9.x, CentOS 7.x, 8.x, Ubuntu 16.04 sau mai recent, SUSE Linux Enterprise Server 12SP4,5, SUSE LINUX Exnterprise15 SP2,SP3, OpenSUSE LEAP 15-2-15.3., Fedora 31 sau mai recent, 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 si instalare remote:

1. Inainte de instalare, administratorul va putea particulariza pachetele de instalare cu modulele dorite: firewall, content control, device control, power user.
2. Instalarea se va putea face in mai multe moduri:
   a. prin descarcarea directa a pachetului pe statia pe care se va face instalarea;
   b. prin instalarea la distanta, direct din consola de management
   c. trimiterea pe email (oricate adrese) a pachetului de instalare pentru Windows, Linux, Mac.
3. Instalarea clienților la distanta in alte locatii decat cele in care este instalata consola de management se va face prin intermediul unui client existent in locatiile respective de tip relay pentru a minimiza traficul in WAN.
4. In consola vor fi disponibile informații despre fiecare stație: numele statiei, IP, sistem de operare, module instalate, politica aplicata, informatii despre actualizari etc.
5. Din consola se va putea trimite o singura politica pentru configurarea integrala a clientului de pe statii/servere.
6. Consola va include o sectiune, „Audit", unde se vor mentiona toate actiunile intreprinse fie de administratori fie de reporteri, cu informatii detaliate: logare, editare, creare, delogare, mutare etc.

7. Posibilitatea creari unui singur pachet de instalare, utilizabil atat pentru sistemele de operare pe 32 de biti cat si pentru cele pe 64 de biti.
8. Posibilitatea creari unui singur pachet de instalare, utilizabil pentru statii (fizice si/sau virtuale), servere (fizice si/sau virtuale).
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 statiile/serverele din retea pentru cele care nu sunt integrate domeniu.
11. Permite selectarea clientului care va realiza descoperirea stațiilor din rețea, altele decât cele integrate in domeniu.

4. Caracteristici si functionalitati principale 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:
    1. Actiune imiplicita pentru fisiere infectate:
        i. interzice accesul
        ii. dezinfecteaza
        iii. stergere
        iv. muta fisierele in carantina
        v. nicio actiune
    2. Actiune alternativa pentru fisierele infectate:
        i. interzice accesul
        ii. dezinfecteaza
        iii. stergere
        iv. muta fisierele in carantina
    3. Actiune imiplicita pentru fisierele suspecte:
        i. interzice accesul
        ii. stergere
        iii. muta fisierele in carantina
        iv. nicio actiune
    4. Actiune alternativa pentru fisierele suspecte:
        i. interzice accesul
        ii. stergere
        iii. muta fisierele in carantina
2. Scanarea automata in timp real va putea fi setata sa nu scaneze arhive sau fisiere mai mari de « x » MB, marimea fisierelor putand fi definita de administratorul solutiei,
3. Definirea pana la 16 nivele de profunzime pentru scanarea in arhive.
4. Scanarea euristica comportamentala prin simularea unui calculator virtual in interiorul caruia sunt rulate aplicatii cu potential periculos protejand sistemul de virusii necunoscuti prin detectarea codurilor periculoase a caror semnatura nu a fost lansata inca.
5. Scanarea oricarui suport de stocare a informatiei (CD-uri, harduri externe, unitati partajate etc). De asemenea, se va putea anula scanarea in cazul in care sunt detectate unitati care au informatii stocate mai mult de « x » MB.
6. Scanarea automata a emailurilor la nivelul statiei de lucru pentru POP3/SMTP.
7. Configurarea cailor ce urmeaza a fi scanate la cerere.
8. Clientii antimalware pentru workstation sa permita definirea unor liste de excludere de la scanarea in timp real si la cerere a anumitor directoare, discuri, fisiere, extensii sau procese.
9. Cu ajutorul unei baze de date complete cu semnaturi de spyware si a euristicii de detectie a acestui tip de programe, produsul va trebui sa ofere protectie anti-spyware.
10. Posibilitatea de configura scanarile programate sa se execute cu prioritate redusa
11. Produsul antimalware poate fi configurat sa foloseasca scanarea in cloud, si partial scanarea locala.
12. Administratorul poate 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.

13. Pentru o protectie sporita, solutia antimalware trebuie sa aiba 3 tipuri de detectie: bazata pe semnaturi, bazata de comportamentul fisierelor si bazata pe monitorizarea proceselor.
14. Pentru o protectie sporita, solutia antimalware trebuie sa poata scana paginile HTTP.
15. Pentru o mai buna gestionare a antimalware instalat pe statii, produsul va include optiunea de setare a unei parole pentru protectia la dezinstalare.
16. Pentru siguranta utilizatorului, clientul va include un modul de antiphishing.
17. Solutia ofera protectie in timp real pe masinile cu sistem de operare Linux in conformitate cu versiunea de kernel instalata.

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 aplicatiilor utilizate frecvent si a celor de tip „sistem" cum ar fi browserele, aplicatiile de tip office sau reader, procesele critice aferente sistemelor de operare.

6. Firewall:

1. Posibilitatea de a configura reguli de firewall pentru aplicatii sau conectivitate.
2. Modulul poate fi instalat/dezinstalat in functie de preferinta administratorului.
3. Posibilitatea de a defini retele de incredere pentru masina destinatie.
4. Abilitatea de a detecta scanarea de porturi.
5. Posibilitatea de a seta diferite profiluri de rețea ((Home/Office, Trusted, Public, Untrusted sau Let the Windows decide)
6. Abilitatea de a crea reguli personalizate bazate pe aplicație și/sau conexiune

7. Carantina:

1. Produsul antimalware sa permita trimiterea automata a fisierelor din carantina catre laboratoarele antimalware ale producatorului.
2. Trimiterea continutului carantinei va putea fi expediat in mod automat, la un interval definit de administrator.
3. Produsul antimalware sa permita stergerea automata a fisierelor carantinate mai vechi de o anumita perioada, pentru a nu incarca inutil spatiul de stocare.
4. Posibilitatea de a restaura un fisier din carantina in locatia lui originala.
5. Modulul de carantina va permite rescanarea obiectelor dupa fiecare actualizare de semnaturi.

8. Protecția datelor:

1. Produsul 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 particularitati:
   a. Permite blocarea accesului la Internet pentru anumite mașini client sau grupuri de mașini.
   b. Permite blocarea accesului la Internet pe intervale orare.
   c. Permite blocarea paginilor de internet care contin 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 dupa anumite categorii prestabilite (ex: online dating, violenta, pornografie etc).

10. Controlul dispozitivelor:

1. Modulul poate fi instalat/dezinstalat in funcție de preferința administratorului.
2. 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
3. Modulul va permite configurarea de reguli prin care se vor defini permisiunile pentru dispozitivele conectate la masina client.
4. Modulul va permite configurarea de excluderi pentru diferite tipuri de dispozitive pentru care s-au configurat reguli.

11. Power User:

1. Modulul poate fi instalat/dezinstalat in functie de preferinta administratorului.
2. Modulul permite posibilitatea de a acorda utilizatorilor drepturi de Power User. Utilizatorii vor putea accesa si modifica setarile clientului antimalware dintr-o consola dispobibila local pe masina client.
3. Modificările efectuate din modulul Power User vor fi active local, pe masina pe care s-au facut respectivele modificări.
4. Administratorul va putea suprascrie din consola setarile aplicate de utilizatorii Power User.

12. Actualizare:

1. Posibilitatea efectuării actualizării la nivel de statie in mod silențios (fara avertizare).
2. Sistem de actualizare cascadat folosind unul sau mai multe servere de actualizare (cascadate).
3. Actualizarea pentru locațiile remote prin intermediul unui client antimalware care are si rol de server de actualizare.

4. CERINȚE SPECIFICE pentru ofertant/prestator:

Orice operator economic interesat să depună ofertă va trebui să respecte termenii, condițiile tehnice și cerințele specificate prin prezentul caiet de sarcini, mai sus detaliate.

Operatorul economic **ofertant/prestator** al serviciilor solicitate trebuie să se regăsească între partenerii producătorului echipamentului **FortiNet** prin care se oferă soluții de securitate specifice, respectiv și pentru echipamentul existent în dotarea Primăriei Municipiului Onești.

5. MODUL de ÎNTOCMIRE a OFERTEI:

Oferta ***transmisă*** va trebui să conțină, ***detaliat***, ***caracteristicile*** și ***specificațiile*** tehnice ale serviciilor **ofertate** și elementele de identificare/descriere specifice în vederea analizei îndeplinirii condițiilor cerute prin caietul de sarcini.

Valoarea totală a ofertei privind *asigurarea* serviciilor de ***Actualizare*** **ANTIVIRUS** pentru ***Rețea-LAN*** și suport tehnic de specialitate, în acord cu caracteristicele detaliate în caietul de sarcini, ***va trebui*** să acopere furnizarea acestora pentru un an de zile și este echivalentă cu valoarea abonamentului anual.

Criteriul de adjudecare al ofertei este "**prețul cel mai scăzut**" conform art. 187 alin. (3) lit. a) din Legea 98/2016, dacă sunt respectate condițiile minimale solicitate prin prezentul caiet de sarcini.

Termenul de finalizare și activare electronică a funcționalităților abonamentului pentru serviciile de actualizare Antivirus, obiectul prezentei achiziții este de maxim **7** zile de la emiterea comenzii ferme.