Nr.1307AP/04.04.2023

Avizat,
DCDSI

SOLICITARE DE OFERTĂ

In vederea achiziţionării prin cumpărare directă vă solicităm ca până la data de 12.04.2023 **inclusiv**, să transmiteţi oferta de preţ (lei fără TVA), pentru următoarele produse:

Nr. crt	Denumire produs *Specificaţii tehnice minime*	UM	Cant.
1	**Software antivirus cu licenţă pentru minim 3 ani** de la prima instalare, 1 licenţă pentru minim 20 de staţii de lucru **CARACTERISTICI GENERALE ALE PRODUSULUI** Produsul reprezinta o platforma integrata pentru managementul securitatii, gandita ca o solutie modulara. Produsul contine urmatoarele module de securitate: **A.** O consola de management care asigura functionalitati de administrare. **B.** Protectie antimalware pentru statii fizice/virtuale **A. CONSOLA DE MANAGEMENT** **1. Instalare si configurare:** 1. Masinile de scanare (pentru tipul de scanare centralizata) pentru mediile virtuale se descarca din interfata web a produsului. **2. 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 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 (solutie de tip Cloud), 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). **3. 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.	buc	1

4. Inventarierea retelei – managementul securitatii:

1. Solutia se va integra cu domeniul Active Directory si va putea importa inventarul.
2. Se permite descoperirea statiilor 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 maşinile 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.

5. Politici:

1. Solutia va permite configurarea setarilor clientului antimalware prin intermediul unei singure politici ce contine setari pentru toate module
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)

6. Rapoarte:

1. Solutia va contine rapoarte care prezinta statusul masinilor clientilor 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

ADRESA: România, Iaşi, Bd.Carol I, nr.11, Corpul J EMAIL: stefania.plescan@uaic.ro
TEL: 0232201139 Cod fiscal: 4701126

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. sau arhiva.
5. Solutia include un generator de rapoarte care ofera posibilitatea de a investiga o problema de securitate pe baza mai multor criterii, mentinand informatiile concise si ordonate corespunzator. Astfel, solutia include interogari precum: starea terminalului, evenimente terminal, evenimente Exchange.
6. Interogarea legata de starea terminalului include informatii precum:
    a. tip masina
    b. infrastructura retelei careia ii apartine terminalul
    c. datele agentului de securitate
    d. starea modulelor de protectie
    e. rolurile terminalelor.
7. Interogarea legata de evenimente terminal include informatii precum:
    a. calculatorul tinta pe care a avut loc evenimentul
    b. tipul starea si configuratia agentului de securitate instalat
    c. starea modulelor si rolurilor de protectie instalate pe agentul de securitate
    d. denunmirea si alocarea politicii
    e. utilizatorul autentificat in timpul evenimentului
    f. evenimente (site-uri blocate, aplicatii blocate, detectiile etc)
8. Interogarea legata de evenimente Exchange include informatii precum:
    a. Directia traficului e-mail
    b. Evenimente de securitate (detectarea programelor de tip malware sau a fisierelor atasate)
    c. Masurile implementate in fiecare situatie (curatarea, stergerea, inlocuirea sau carantinarea fisierului, stergerea sau respingerea e-mail-ului)

7. Carantina:
1. Solutia va permite restaurarea fisierelor carantinate in locatia originala sau intr-o cale configurabila.
2. Carantina va fi locala, pe fiecare statie administrata si va fi administrata, fie local, fie din consola de management.

8. 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

ADRESA: România, Iaşi, Bd.Carol I, nr.11, Corpul J EMAIL: stefania.plescan@uaic.ro
TEL: 0232201139 Cod fiscal: 4701126

solutiei.

9. Log-uri:

1. Inregistrarea actiunilor utilizatorilor.
2. Se vor oferi informatii detaliate pentru fiecare actiune a unui utilizator.
3. Se va permite filtrarea actiunilor utilizator dupa numele utilizatorului, actiune.

10. 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 statiile si serverele din retea, evitand posibile probleme ce pot afecta serverele sau statiile critice. Astfel, serverul de actualizare 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 FIZICE/VIRTUALE

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
6. Pentru o mai buna protectie a statiilor si serverelor, solutia include un modul avansat de securitate – HyperDetect, bazat pe tehnologii de tip „machine learning tunabil" proiectat special pentru a detecta atacuri avansate si activitati suspecte in faza pre-executie.
7. Acest modul avansat de securitate va proteja impotriva: atacurilor directionate (Targeted Attack - APT), fisierelor suspecte si traficului

ADRESA: România, Iaşi, Bd.Carol I, nr.11, Corpul J EMAIL: stefania.plescan@uaic.ro
TEL: 0232201139 Cod fiscal: 4701126

la nivel de retea suspect, exploit-urilor, ransomware si grayware. Fiecarui tip de amenintare mentionat, i se vor putea stabili, independent, un nivel de protectie dorit: permisiv, normal, agresiv.

8. Modulul avansat de securitate are posibilitatea de a raporta, bloca accesul, dezinfecta, sterge sau muta in carantina pentru fiecare din categoriile descrise. Astfel, administratorul va putea decide daca doreste intai monitorizare sau doreste si blocarea amenintarilor. Aceste actiuni mentionate, vor putea fi stabilite independent, pentru fisiere sau pentru traficul din retea, cu posibilitatea extinderii nivelului de raportare pentru a include nivelurile superioare (vor putea fi raportate amenintarile care ar fi fost detectate daca nivelul de protectie era stabilit mai agresiv).
9. Pentru a oferi un nivel aditional de protectie a statiilor si serverelor, solutia include un sandbox in cloud-ul public al producatorului acesteia.
10. Modulul de Sandbox va putea trimite automat fisiere in Sandbox-ul din cloud-ul producatorului unde vor putea fi „detonate" pentru o analiza in profunzime.
11. Modulul de Sandbox include doua variante de analiza: doar monitorizare sau blocare. In modul monitorizare utilizatorul va putea accesa fisierul dorit, pe cand in modul blocare, utilizatorului i se va bloca rularea fisierului pana cand Sandbox-ul din cloud-ul producatorului va da verdictul.
12. Modulul de Sandbox include doua tipuri de actiuni remediere: implicita si de siguranta. Pentru actiunea implicita se va putea stabili: doar raportare, dezinfectie, stergere si carantinare. Pentru actiunea de siguranta se va putea stabili: stergere sau carantinare.
13. Modulul de Sandbox include si posibilitatea de trimitere manuala a fisierelor in Sandbox-ul din cloud-ul producatorului. Astfel, daca administratorul suspecteaza un fisier ca fiind malitios, il poate trimite manual in Sandbox pentru a fi „detonat" si a afla verdictul. Va putea trimite mai multe fisiere de odata, cu posibilitate de a specifica daca vor fi „detonate" individual sau toate in acelasi timp.
14. Modulul de Sandbox poate suporta „detonarea" urmatoarelor tipuri de fisiere: 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 (executable), RTF, SCR, URL (binary), VBE, VBS, WSF, WSH, WSH-VBS, XHTML.
15. Fisierele mentionate anterior, vor putea fi detectate corect chiar daca sunt incluse in 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.

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**

ADRESA: România, Iaşi, Bd.Carol I, nr.11, Corpul J EMAIL: stefania.plescan@uaic.ro
TEL: 0232201139 Cod fiscal: 4701126

	POS Ready 7 Windows Embedded POSReady 7, Windows Embedded Enterprise 7 **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 linkului cu pachetul de instalare pentru Windows, Linux, Mac. 3. Instalarea clientilor la distanta in alte locatii decat cele in care este instalata consola de management se va face prin intermediul unui alt client antivirus existent in locatiile respective pentru a minimiza traficul in WAN. 4. In consola vor fi disponibile informatii despre fiecare statie: 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 crearii 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), 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 statiile/serverele din retea pentru cele care nu sunt integrate domeniu. 11. Permite selectarea clientului care va realiza descoperirea statiilor din retea, altele decat 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: a. Actiune imiplicita pentru fisiere infectate: - interzice accesul - dezinfecteaza - stergere - muta fisierele in carantina - nicio actiune b. Actiune alternativa pentru fisierele infectate: - interzice accesul - dezinfecteaza - stergere - muta fisierele in carantina c. Actiune imiplicita pentru fisierele suspecte: - interzice accesul		

ADRESA: România, Iaşi, Bd.Carol I, nr.11, Corpul J EMAIL: stefania.plescan@uaic.ro
TEL: 0232201139 Cod fiscal: 4701126

- stergere
- muta fisierele in carantina
- nicio actiune

d. Actiune alternativa pentru fisierele suspecte:
- interzice accesul
- stergere
- 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 (incoming)/SMTP(outgoing).
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. Abilitatea de a detecta atacuri fără fişiere, inclusiv cele care folosesc instrumente legitime ale sistemului de operare, cum ar fi Powershell sau interpreţii de script. Soluţia nu va bloca global scripturile pentru a realiza acest lucru.
11. Ofera tehnologia Anti-Ransomware.
12. Posibilitatea de configura scanarile programate sa se execute cu prioritate redusa
13. Produsul antimalware poate fi configurat sa foloseasca scanarea in cloud, si partial scanarea locala. Pentru statiile ce nu au suficiente resurse hardware, scanarea se poate face cu o masina de scanare instalata in retea (scanare centralizata).
14. Administratorul poate personaliza şi motoarele de scanare, având posibilitatea de a alege între mai multe tehnologii de scanare:
    - Scanare locală, când scanarea se efectuează pe staţia de lucru locală. Modul de scanare locală este potrivit pentru maşinile puternice, având toate semnăturile şi motoarele stocate local.
    - Scanarea hibrid cu motoare light (Cloud public), cu o amprentă medie, folosind scanarea în cloud şi, parţial, 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)

ADRESA: România, Iaşi, Bd.Carol I, nr.11, Corpul J EMAIL: stefania.plescan@uaic.ro
TEL: 0232201139 Cod fiscal: 4701126

- Scanare centralizată (Scanare în cloud privat cu server de securitate) cu fallback* pe Scanare hibrid (cloud public cu motoare light)

15. 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.
16. Pentru o protectie sporita, solutia antimalware trebuie sa poata scana paginile HTTP.
17. Pentru o mai buna gestionare a antimalware instalat pe statii, produsul va include optiunea de setare a unei parole pentru protectia la dezinstalare.
18. Pentru siguranta utilizatorului, clientul va include un modul de antiphishing.
19. 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.
6. Modulul de carantina va permite salvarea unei copii a fisierului infectat respectiv transmiterea acestuia catre carantina inainte de a efectua orice alta actiune asupra acestuia.

8. Protectia datelor:

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

ADRESA: România, Iaşi, Bd.Carol I, nr.11, Corpul J EMAIL: stefania.plescan@uaic.ro
TEL: 0232201139 Cod fiscal: 4701126

9. Controlul continutului:

1. Consola va avea integrat un modul dedicat controlului accesului la Internet cu urmatoarele particularitati:
   a. Permite blocarea accesului la Internet pentru anumite masini client sau grupuri de masini.
   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 aplicatii definite de administrator;
   f. Permite restrictionarea accesului pe anumite pagini de internet dupa anumite categorii prestabilite (ex: online dating, violenta, pornografie etc).

11. Controlul dispozitivelor:

1. Modulul poate fi instalat/dezinstalat in functie de preferinta administratorului.
2. Modulul va permite controlul urmatoarelor 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.
5. Modulul va permite configurarea de reguli prin care se vor defini permisiunile pentru dispozitivele conectate la masina 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 permitand orice alt tip de dispozitiv ce nu foloseste acest tip de port/interfata.
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 poate „descoperi" noi dispozitive si raporta prezenta acestora in consola de management.

12. Power User:

1. Modulul poate fi instalat/dezinstalat in functie de preferinta administratorului.

ADRESA: România, Iaşi, Bd.Carol I, nr.11, Corpul J EMAIL: stefania.plescan@uaic.ro
TEL: 0232201139 Cod fiscal: 4701126

	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. Modificarile efectuate din modulul Power User vor fi active local, pe masina pe care s-au facut respectivele modificari. 4. Administratorul va putea suprascrie din consola setarile aplicate de utilizatorii Power User. **13. Actualizare:** 1. Posibilitatea efectuarii actualizarii la nivel de statie in mod silentios (fara avertizare). 2. Sistem de actualizare cascadat folosind unul sau mai multe servere de actualizare (cascadate). 3. Actualizarea pentru locatiile remote prin intermediul unui client antimalware care are si rol de server de actualizare. 4. Abilitatea de a împiedica punctele finale să iasă pe internet pentru a descărca actualizări.		
2	**Software antivirus cu licență pentru minim 3 ani** de la prima instalare, 1 licență pentru minim 30 de servere **CARACTERISTICI GENERALE ALE PRODUSULUI** Produsul reprezinta o platforma integrata pentru managementul securitatii, gandita ca o solutie modulara. Produsul contine urmatoarele module de securitate: **C.** O consola de management care asigura functionalitati de administrare. **D.** Protectie antimalware pentru servere fizice/virtuale **E.** Protectie si securitate pentru serverele email Microsoft Exchange **A. CONSOLA DE MANAGEMENT** **1. Instalare si configurare:** 1. Masinile de scanare (pentru tipul de scanare centralizata) pentru mediile virtuale se descarca din interfata web a produsului. **2. 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 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 (solutie de tip Cloud), 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). **3. 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	buc	1

ADRESA: România, Iaşi, Bd.Carol I, nr.11, Corpul J EMAIL: stefania.plescan@uaic.ro
TEL: 0232201139 Cod fiscal: 4701126

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.

4. Inventarierea retelei – managementul securitatii:

1. Solutia se va integra cu domeniul Active Directory si va putea importa inventarul.
2. Se permite descoperirea statiilor 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 maşinile 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.

5. Politici:

1. Solutia va permite configurarea setarilor clientului antimalware prin intermediul unei singure politici ce contine setari pentru toate module
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:
   h. IP sau clasa de IP al statiei
   i. Gateway-ul alocat
   j. DNS serverul alocat
   k. WINS serverul alocat
   l. Sufix DNS pentru conexiunea dhcp
   m. Clientul este/nu este in acceasi retea cu infrastructura de management (statia de lucru poate solutiona implicit numele gazdei)
   n. Tipul retelei (lan, wireless)

ADRESA: România, Iaşi, Bd.Carol I, nr.11, Corpul J EMAIL: stefania.plescan@uaic.ro
TEL: 0232201139 Cod fiscal: 4701126

6. Rapoarte:

1. Solutia va contine rapoarte care prezinta statusul masinilor clientilor 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. sau arhiva.
5. Solutia include un generator de rapoarte care ofera posibilitatea de a investiga o problema de securitate pe baza mai multor criterii, mentinand informatiile concise si ordonate corespunzator. Astfel, solutia include interogari precum: starea terminalului, evenimente terminal, evenimente Exchange.
6. Interogarea legata de starea terminalului include informatii precum:
    d. tip masina
    e. infrastructura retelei careia ii apartine terminalul
    f. datele agentului de securitate
    g. starea modulelor de protectie
    h. rolurile terminalelor.

    7. Interogarea legata de evenimente terminal include informatii precum:
    a. calculatorul tinta pe care a avut loc evenimentul
    b. tipul starea si configuratia agentului de securitate instalat
    c. starea modulelor si rolurilor de protectie instalate pe agentul de securitate
    d. denunmirea si alocarea politicii
    e. utilizatorul autentificat in timpul evenimentului
    f. evenimente (site-uri blocate, aplicatii blocate, detectiile etc)

    8.Interogarea legata de evenimente Exchange include informatii precum:
    i. Directia traficului e-mail
    j. Evenimente de securitate (detectarea programelor de tip malware sau a fisierelor atasate)
    k. Masurile implementate in fiecare situatie (curatarea, stergerea, inlocuirea sau carantinarea fisierului, stergerea sau respingerea e-mail-ului)

7. Carantina:

1. Solutia va permite restaurarea fisierelor carantinate in locatia originala sau intr-o cale configurabila.
2. Carantina va fi locala, pe fiecare statie administrata si va fi administrata, fie local, fie din consola de management.

8. 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

ADRESA: România, Iaşi, Bd.Carol I, nr.11, Corpul J EMAIL: stefania.plescan@uaic.ro
TEL: 0232201139 Cod fiscal: 4701126

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.

9. Log-uri:

1. Inregistrarea actiunilor utilizatorilor.
2. Se vor oferi informatii detaliate pentru fiecare actiune a unui utilizator.
3. Se va permite filtrarea actiunilor utilizator dupa numele utilizatorului, actiune.

10. 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 statiile si serverele din retea, evitand posibile probleme ce pot afecta serverele sau statiile critice. Astfel, serverul de actualizare 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 SERVERE FIZICE/VIRTUALE

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

ADRESA: România, Iaşi, Bd.Carol I, nr.11, Corpul J EMAIL: stefania.plescan@uaic.ro
TEL: 0232201139 Cod fiscal: 4701126

securizare al endpoint-ului

6. Pentru o mai buna protectie a statiilor si serverelor, solutia include un modul avansat de securitate – HyperDetect, bazat pe tehnologii de tip „machine learning tunabil" proiectat special pentru a detecta atacuri avansate si activitati suspecte in faza pre-executie.
7. Acest modul avansat de securitate va proteja impotriva: atacurilor directionate (Targeted Attack - APT), fisierelor suspecte si traficului la nivel de retea suspect, exploit-urilor, ransomware si grayware. Fiecarui tip de amenintare mentionat, i se vor putea stabili, independent, un nivel de protectie dorit: permisiv, normal, agresiv.
8. Modulul avansat de securitate are posibilitatea de a raporta, bloca accesul, dezinfecta, sterge sau muta in carantina pentru fiecare din categoriile descrise. Astfel, administratorul va putea decide daca doreste intai monitorizare sau doreste si blocarea amenintarilor. Aceste actiuni mentionate, vor putea fi stabilite independent, pentru fisiere sau pentru traficul din retea, cu posibilitatea extinderii nivelului de raportare pentru a include nivelurile superioare (vor putea fi raportate amenintarile care ar fi fost detectate daca nivelul de protectie era stabilit mai agresiv).
9. Pentru a oferi un nivel aditional de protectie a statiilor si serverelor, solutia include un sandbox in cloud-ul public al producatorului acesteia.
10. Modulul de Sandbox va putea trimite automat fisiere in Sandbox-ul din cloud-ul producatorului unde vor putea fi „detonate" pentru o analiza in profunzime.
11. Modulul de Sandbox include doua variante de analiza: doar monitorizare sau blocare. In modul monitorizare utilizatorul va putea accesa fisierul dorit, pe cand in modul blocare, utilizatorului i se va bloca rularea fisierului pana cand Sandbox-ul din cloud-ul producatorului va da verdictul.
12. Modulul de Sandbox include doua tipuri de actiuni remediere: implicita si de siguranta. Pentru actiunea implicita se va putea stabili: doar raportare, dezinfectie, stergere si carantinare. Pentru actiunea de siguranta se va putea stabili: stergere sau carantinare.
13. Modulul de Sandbox include si posibilitatea de trimitere manuala a fisierelor in Sandbox-ul din cloud-ul producatorului. Astfel, daca administratorul suspecteaza un fisier ca fiind malitios, il poate trimite manual in Sandbox pentru a fi „detonat" si a afla verdictul. Va putea trimite mai multe fisiere de odata, cu posibilitate de a specifica daca vor fi „detonate" individual sau toate in acelasi timp.
14. Modulul de Sandbox poate suporta „detonarea" urmatoarelor tipuri de fisiere: 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 (executable), RTF, SCR, URL (binary), VBE, VBS, WSF, WSH, WSH-VBS, XHTML.
15. Fisierele mentionate anterior, vor putea fi detectate corect chiar daca sunt incluse in 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.

2. Cerinte de sistem:

- Sisteme de operare pentru servere: **Windows Server 2022, Windows**

ADRESA: România, Iaşi, Bd.Carol I, nr.11, Corpul J EMAIL: stefania.plescan@uaic.ro
TEL: 0232201139 Cod fiscal: 4701126

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:
   d. prin descarcarea directa a pachetului pe statia pe care se va face instalarea;
   e. prin instalarea la distanta, direct din consola de management
   f. trimiterea pe email (oricate adrese) a linkului cu pachetul de instalare pentru Windows, Linux, Mac.
3. Instalarea clientilor la distanta in alte locatii decat cele in care este instalata consola de management se va face prin intermediul unui alt client antivirus existent in locatiile respective pentru a minimiza traficul in WAN.
4. In consola vor fi disponibile informatii despre fiecare statie: 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 crearii 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), 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 statiile/serverele din retea pentru cele care nu sunt integrate domeniu.
11. Permite selectarea clientului care va realiza descoperirea statiilor din retea, altele decat 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:
   a. Actiune imiplicita pentru fisiere infectate:
      - interzice accesul
      - dezinfecteaza

ADRESA: România, Iaşi, Bd.Carol I, nr.11, Corpul J EMAIL: stefania.plescan@uaic.ro
TEL: 0232201139 Cod fiscal: 4701126

- stergere
- muta fisierele in carantina
- nicio actiune

b. Actiune alternativa pentru fisierele infectate:
- interzice accesul
- dezinfecteaza
- stergere
- muta fisierele in carantina

c. Actiune imiplicita pentru fisierele suspecte:
- interzice accesul
- stergere
- muta fisierele in carantina
- nicio actiune

d. Actiune alternativa pentru fisierele suspecte:
- interzice accesul
- stergere
- 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 (incoming)/SMTP(outgoing).
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. Abilitatea de a detecta atacuri fără fişiere, inclusiv cele care folosesc instrumente legitime ale sistemului de operare, cum ar fi Powershell sau interpreţii de script. Soluţia nu va bloca global scripturile pentru a realiza acest lucru.
11. Ofera tehnologia Anti-Ransomware.
12. Posibilitatea de configura scanarile programate sa se execute cu prioritate redusa
13. Produsul antimalware poate fi configurat sa foloseasca scanarea in cloud, si partial scanarea locala. Pentru statiile ce nu au suficiente resurse hardware, scanarea se poate face cu o masina de scanare instalata in retea (scanare centralizata).
14. Administratorul poate personaliza şi motoarele de scanare, având posibilitatea de a alege între mai multe tehnologii de scanare:
    - Scanare locală, când scanarea se efectuează pe staţia de lucru

ADRESA: România, Iaşi, Bd.Carol I, nr.11, Corpul J EMAIL: stefania.plescan@uaic.ro
TEL: 0232201139 Cod fiscal: 4701126

locală. Modul de scanare locală este potrivit pentru maşinile puternice, având toate semnăturile şi motoarele stocate local.
- Scanarea hibrid cu motoare light (Cloud public), cu o amprentă medie, folosind scanarea în cloud şi, parţial, 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)

15. 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.
16. Pentru o protectie sporita, solutia antimalware trebuie sa poata scana paginile HTTP.
17. Pentru o mai buna gestionare a antimalware instalat pe statii, produsul va include optiunea de setare a unei parole pentru protectia la dezinstalare.
18. Pentru siguranta utilizatorului, clientul va include un modul de antiphishing.
19. 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.

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.
6. Modulul de carantina va permite salvarea unei copii a fisierului infectat respectiv transmiterea acestuia catre carantina inainte de a efectua orice alta actiune asupra acestuia.

8. Protectia datelor:

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

ADRESA: România, Iaşi, Bd.Carol I, nr.11, Corpul J EMAIL: stefania.plescan@uaic.ro
TEL: 0232201139 Cod fiscal: 4701126

9. Controlul continutului:

2. Consola va avea integrat un modul dedicat controlului accesului la Internet cu urmatoarele particularitati:
   g. Permite blocarea accesului la Internet pentru anumite masini client sau grupuri de masini.
   h. Permite blocarea accesului la Internet pe intervale orare.
   i. Permite blocarea paginilor de internet care contin anumite cuvinte cheie.
   j. Permite controlul accesului numai la anumite pagini de internet specificate de administrator;
   k. Permite blocarea accesului la anumite aplicatii definite de administrator;
   l. Permite restrictionarea accesului pe anumite pagini de internet dupa anumite categorii prestabilite (ex: online dating, violenta, pornografie etc).

11. Controlul dispozitivelor:

1. Modulul poate fi instalat/dezinstalat in functie de preferinta administratorului.
2. Modulul va permite controlul urmatoarelor 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.
5. Modulul va permite configurarea de reguli prin care se vor defini permisiunile pentru dispozitivele conectate la masina 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 permitand orice alt tip de dispozitiv ce nu foloseste acest tip de port/interfata.
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 poate „descoperi" noi dispozitive si raporta prezenta acestora in consola de management.

12. Power User:

1. Modulul poate fi instalat/dezinstalat in functie de preferinta administratorului.

ADRESA: România, Iaşi, Bd.Carol I, nr.11, Corpul J EMAIL: stefania.plescan@uaic.ro
TEL: 0232201139 Cod fiscal: 4701126

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. Modificarile efectuate din modulul Power User vor fi active local, pe masina pe care s-au facut respectivele modificari.
4. Administratorul va putea suprascrie din consola setarile aplicate de utilizatorii Power User.

13. Actualizare:

1. Posibilitatea efectuarii actualizarii la nivel de statie in mod silentios (fara avertizare).
2. Sistem de actualizare cascadat folosind unul sau mai multe servere de actualizare (cascadate).
3. Actualizarea pentru locatiile remote prin intermediul unui client antimalware care are si rol de server de actualizare.
4. Abilitatea de a împiedica punctele finale să iasă pe internet pentru a descărca actualizări.

D. PROTECTIE SI SECURITATE PENTRU SERVERELE EMAIL MICROSOFT EXCHANGE (SECURITY for Servers)

Cerinte minime de sistem:

- Exchange server 2019, 2016, 2013 cu rol de Edge Transport sau Mailbox
- Exchange server 2010 cu rold de Edge Transport, Hub Transport sau Mailbox

1. Produsul va oferi protectie antimalware, antispam (inclusiv antiphishing), precum si filtrare de atasamente si continut, prin integrarea cu serverul Microsoft Exchange. De asemenea, va permite scanarea antimalware la cerere a bazelor de date Exchange.

2. Produsul va asigura scanarea atasamentelor si a continutului mesajelor in timp real, fara a afecta vizibil performanta serverului de mail.

3. Actualizarea antimalware trebuie sa poata fi facuta automat la un interval de maxim 1 ora, precum si la cerere.

4. In afara de detectia pe baza de semnaturi, modulul de protectie antimalware va trebui sa includa si scanare euristica comportamentala, prin simularea unui calculator virtual in interiorul caruia sunt rulate si analizate aplicatii cu potential periculos, pentru a proteja sistemul de virusii necunoscuti prin detectarea codurilor periculoase a caror semnatura nu a fost lansata inca.

5. Produsul va oferi optiuni multiple de actiune la identificarea unui atasament virusat (dezinfectare, stergere, mutare in carantina).

6. Cu ajutorul unei baze de date complete cu semnaturi de spyware si a euristicii de detectie a acestui tip de programe, produsul va oferi protectie anti-spyware pentru a preveni furtul de date confidentiale.

7. Produsul va oferi protectie antispam, cu o baza de semnaturi

ADRESA: România, Iaşi, Bd.Carol I, nr.11, Corpul J EMAIL: stefania.plescan@uaic.ro
TEL: 0232201139 Cod fiscal: 4701126

	actualizabila prin internet. 8. Modulul antispam va trebui sa includa un filtru URL cu o baza de adrese URL cunoscute a fi folosite in mesaje spam, precum si un filtru de caractere pentru detectarea automata a mesajelor scrise cu caractere chirilice sau asiatice. 9. Produsul va trebui sa ofere filtru RBL care sa identifice spam-ul prin sincronizarea cu anumite baze de date online care contin liste de servere de mail cunoscute ca fiind la originea acestui tip de mesaje. 10. Produsul va trebui sa ofere un serviciu/filtru online pentru imbunatatirea protectiei impotriva valurilor de spam nou aparute. 11. Produsul va oferi posibilitatea de a defini politici de filtrare antimalware, antispam, a continutului sau atasamentelor pentru diferite grupuri sau utilizatori. 12. Actualizarea produsului va fi configurabila si se va putea realiza de pe internet, direct sau printr-un proxy, sau din cadrul retelei de pe un server de actualizare propriu. 13. Produsul va trebui sa ofere statistici atat referitoare la scanarea antivirus cat si la scanarea antispam. 14. Produsul se va integra in cadrul consolei de management unitar al solutiei antivirus. Pentru usurinta accesului la setarile produsului din diferite medii de operare, produsul va avea consola de administrare web.		

Nota1: Specificaţiile tehnice care indică o anumită origine, sursă, producţie, un procedeu special, sunt menţionate doar pentru identificarea cu uşurinţă a tipului de produs şi nu au ca efect favorizarea sau eliminarea anumitor operatori economici sau a anumitor produse. Aceste specificaţii vor fi considerate ca având menţiunea de ***„sau echivalent".***

Nota 2: Oferta va cuprinde un comentariu articol cu articol al cerintelor solicitate in tabelul de mai sus.

Nota 3: Se vor avea in vedere prevederile legii 354/2022 privind protectia sistemelor informatice ale autoritatilor si institutiilor publice in contextul invaziei declansate de Federatia Rusa impotriva Ucrainei

Nota 4: Toate componentele si produsele vor fi noi si nefolosite (chei de licență, seriale etc.).

Criteriul de atribuire: prețul cel mai scăzut, aplicabil la intreaga oferta, cuprinzand ambele pozitii din tabelul de mai sus. Nu se accepta oferte partiale.

Oferta de preț în lei fără TVA, trebuie să includă toate cheltuielile ocazionate de livrarea produselor si prestarea serviciilor conexe.

Ofertantul nu trebuie sa se afle sub incidenta legii 354/2022. Acesta va prezenta o declaratie pe propria raspundere privind neincadrarea in situatiile prevazute la art 1 alin 1 si 3 din legea 354/2022, conform modelului atasat.

Oferta trebuie sa fie valabilă minim 60 zile. Se va specifica obligatoriu valabilitatea ofertei.

ADRESA: România, Iași, Bd.Carol I, nr.11, Corpul J EMAIL: stefania.plescan@uaic.ro
TEL: 0232201139 Cod fiscal: 4701126

În conformitate cu prevederile Legii 139/2022, contractantul are obligația de a emite facturi electronice și de a le transmite Autorității Contractante prin sistemul national privind facture electronica RO e-factura.

Termenul de plată este:

a) 30 de zile calendaristice de la data la care factura electronica este disponibila spre descarcare de către Autoritatea Contractanta, din sistemul RO e-factura, daca receptia este anterioara acestei date;

a) 30 de zile calendaristice de la data receptiei daca factura electronica este disponibila spre descarcare de către Autoritatea Contractanta din sistemul RO e-factura, la data receptiei ori anterior acestei date.

Se va specifica obligatoriu termenul de livrare al produselor (maxim 7 zile). Cheia de licență se va livra în format tipărit/electronic; Kit-ul de instalare se va livra pe suport de date. La livrare produsele vor fi însoţite de factură fiscala.

Vă solicităm să transmiteți oferta, prin e-mail pe adresa: stefania.plescan@uaic.ro, fax 0232201148 sau la Registratura Universității Alexandru Ioan Cuza din Iași, B-dul Carol I nr. 11 (program de lucru de luni pînă vineri, între orele 08.00-16.00).

ŞEF SERVICIU ACHIZIŢII PUBLICE,
Ing. Gabriela ALEXOAEI

Întocmit,
Ec. Ştefania Pleşcan

ADRESA: România, Iaşi, Bd.Carol I, nr.11, Corpul J EMAIL: stefania.plescan@uaic.ro
TEL: 0232201139 Cod fiscal: 4701126

OPERATOR ECONOMIC

.....

(*denumirea/numele*)

DECLARAŢIEprivind neîncadrarea în situaţiile prevăzute la art. 1 alin 1 si 3 din din Legea 354/2022

Subsemnatul,....., reprezentant împuternicit al ..... (*denumirea/numele si sediul/adresa operatorului economic*), declar pe propria răspundere, sub sancţiunea excluderii din procedură şi a sancţiunilor aplicate faptei de fals în acte publice, că nu ne aflăm în situaţia prevazută la art. 1 alin 1 şi 3 din Legea 354/13.12.2022 privind protecţia sistemelor informatice ale autorităţilor şi instituţiilor publice în contextul invaziei declanşate de Federaţia Rusă împotriva Ucrainei, respectiv SC.....SRL *(denumirea operatorului economic)* nu se află în nici una din următoarele situaţii:

a) sub controlul direct sau indirect al unei persoane fizice sau juridice din Federaţia Rusă;

b) capitalul nu este constituit cu participaţie provenind în mod direct sau prin firme interpuse din Federaţia Rusă;

c) din cadrul organelor de administrare ale SC.....SRL *(denumirea operatorului economic)* nu fac parte persoane din Federaţia Rusă.

Este considerat *operator economic aflat sub controlul direct sau indirect al unei persoane fizice sau juridice din Federaţia Rusă* acela care se află în cel puţin una dintre următoarele situaţii:

a) una sau mai multe persoane fizice sau juridice din Federaţia Rusă deţin, individual sau împreună, în mod direct sau indirect, o participaţie calificată de cel puţin 25% din drepturile de vot ale respectivului operator;

b) una sau mai multe persoane fizice sau juridice din Federaţia Rusă deţin, în mod direct sau indirect, majoritatea drepturilor de vot în adunarea generală a operatorului respectiv;

c) în calitate de asociat sau acţionar al respectivului operator, o persoană fizică sau juridică din Federaţia Rusă dispune de puterea de a numi sau de a revoca majoritatea membrilor organelor de administraţie, conducere sau supraveghere;

d) una sau mai multe persoane fizice sau juridice din Federaţia Rusă îl finanţează, prin orice mod, direct sau indirect, pe operator;

e) una sau mai multe persoane fizice sau juridice din Federaţia Rusă promite, oferă sau dă bani sau alte foloase operatorului.

Subsemnatul declar că informaţiile furnizate sunt complete şi corecte în fiecare detaliu şi înţeleg că autoritatea contractantă are dreptul de a solicita, în scopul verificării şi confirmării declaraţiilor, orice documente doveditoare de care dispunem.

Înţeleg că în cazul în care această declaraţie nu este conformă cu realitatea sunt pasibil de încălcarea prevederilor legislaţiei penale privind falsul în declaraţii.

Data completării

.....

Operator economic,

.....

(*semnătura autorizată*)