ANUNȚ DE PARTICIPARE

privind achiziționarea: Licențe pentru produse software antivirus
(se indică obiectul achiziției)
prin procedura de achiziție: valoare mică
(tipul procedurii de achiziție)

1. **Denumirea autorității contractante:** Ministerul Muncii și Protecției Sociale
2. **IDNO:** 1021601000115
3. **Adresa:** MD-2009, mun.Chișinău, str.Vasile Alecsandri, 2
4. **Numărul de telefon/fax:** 022 268 809
5. **Adresa de e-mail și de internet a autorității contractante:** www.social.gov.md, diana.cucereanu@social.gov.md
6. **Adresa de e-mail sau de internet de la care se va putea obține accesul la documentația de atribuire:** *documentația de atribuire este anexată în cadrul procedurii în SIA RSAP*
7. **Tipul autorității contractante și obiectul principal de activitate (dacă este cazul, mențiunea că autoritatea contractantă este o autoritate centrală de achiziție sau că achiziția implică o altă formă de achiziție comună):** autoritate publică centrală
8. **Procedura a fost inclusă în planul de achiziții publice a autorității contractante (Da/Nu):** Da
Link-ul către planul de achiziții publice publicat: https://social.gov.md/informatie-de-interes-public/achizitii/achizitii-publice/
9. **Cumpărătorul invită operatorii economici interesați, care îi pot satisface necesitățile, să participe la procedura de achiziție privind livrarea următoarelor bunuri:**

Nr. d/o	Cod CPV	Denumirea bunurilor solicitate	Unitatea de măsură	Cantitatea	Specificarea tehnică deplină solicitată, Standarde de referință	Valoarea estimată (se va indica pentru fiecare lot în parte)
Lot 1. Licențe pentru produse software antivirus						**58000,00**
1.1	48761000-0	Prelungirea licențelor antivirus Bitfender GravityZone for Workstation	buc.	150	Prelungirea licențelor antivirus Bitdefender GravityZone for Worstation. Termen de valabilitate 12 luni. Specificația tehnică conform Anexei nr.1.	58000,00
1.2		Licențe CAL pentru utilizatori	buc.	8	License your RDS deployment with client access licenses (CALs). Termen de valabilitate 12 luni. Specificația tehnică conform Anexei nr.2.	
					Valoarea estimativă totală	**58000,00**

10. **În cazul în care contractul este împărțit pe loturi un operator economic poate depune oferta (se va selecta):**
    1) Pentru un singur lot ☑;
    2) Pentru mai multe loturi;
    3) Pentru toate loturile;
    4) Alte limitări privind numărul de loturi care pot fi atribuite aceluiași ofertant _____.
11. **Admiterea sau interzicerea ofertelor alternative:** nu se admite
(indicați se admite sau nu se admite)

12. **Termenii și condițiile de livrare solicitați:** Livrarea bunurilor va fi efectuată în decurs de 5 zile lucrătoare de la semnarea și înregistrarea contractului la Trezoreria de Stat.

13. **Termenul de valabilitate a contractului:** 31.12.2022

14. **Contract de achiziție rezervat atelierelor protejate sau că acesta poate fi executat numai în cadrul unor programe de angajare protejată (după caz):** nu
(indicați da sau nu)

15. **Prestarea serviciului este rezervată unei anumite profesii în temeiul unor acte cu putere de lege sau al unor acte administrative (după caz):** nu
(se menționează respectivele acte cu putere de lege și acte administrative)

16. **Scurta descriere a criteriilor privind eligibilitatea operatorilor economici care pot determina eliminarea acestora și a criteriilor de selecție; nivelul minim (nivelurile minime) al (ale) cerințelor eventual impuse; se menționează informațiile solicitate (DUAE, documentație):**

Nr. d/o	Descrierea criteriului/cerinței	Mod de demonstrare a îndeplinirii criteriului/cerinței:	Nivelul minim/ Obligativitatea
1	Informații generale despre participant	Să conțină obligatoriu numele, prenumele conducătorului, date de contact (telefon, e-mail) și coordonatele bancare, confirmat prin aplicarea semnăturii electronice	Obligatoriu
2	Oferta conform modelului atașat	Încărcată la procedură, confirmată prin aplicarea semnăturii electronice	Obligatoriu
3	Certificat/ Extras de înregistrare	Copie, emis de Agenția Servicii Publice, confirmată prin aplicarea semnăturii electronice	Obligatoriu
4	Autorizare de la producător	Copie, ce confirmă dreptul de a livra și/sau parteneriatul autorizat a operatorului economic cu produsul oferit, confirmată prin aplicarea semnăturii electronice	Obligatoriu
5	Specificații tehnice	Copie, confirmată prin aplicarea semnăturii electronice	Obligatoriu
6	Experiență similară în domeniul livrării produsului software antivirus	Prezentarea minim a 2 scrisori de recomandare de la clienți sau copiile a 2 contracte de livrare a produsului software oferit în ultimii 3 ani, confirmat prin aplicarea semnăturii electronice	Obligatoriu

17. **Motivul recurgerii la procedura accelerată (în cazul licitației deschise, restrânse și al procedurii negociate), după caz:** nu se aplică

18. **Tehnici și instrumente specifice de atribuire (dacă este cazul specificați dacă se va utiliza acordul-cadru, sistemul dinamic de achiziție sau licitația electronică):** licitație electronică. Numărul de runde – 3. Durata rundelor este stabilită de sistem. Pasul minim – 1% din suma totală a lotului fără TVA.

19. **Condiții speciale de care depinde îndeplinirea contractului** (indicați după caz)**:** nu se aplică

20. **Criteriul de evaluare aplicat pentru adjudecarea contractului:** cel mai mic preț fără TVA cu corespunderea cerințelor solicitate, pe lot.

21. **Factorii de evaluare a ofertei celei mai avantajoase din punct de vedere economic, precum și ponderile lor:** nu se aplică

Nr. d/o	Denumirea factorului de evaluare	Ponderea%

22. **Termenul limită de depunere/deschidere a ofertelor:**
    - **până la:** conform informației SIA RSAP (achizitii.md)
    - **pe:** conform informației SIA RSAP (achizitii.md)

23. **Adresa la care trebuie transmise ofertele sau cererile de participare:**

Ofertele sau cererile de participare vor fi depuse electronic prin intermediul SIA RSAP

24. **Termenul de valabilitate a ofertelor:** 30 zile

25. **Locul deschiderii ofertelor:** SIA RSAP
(SIA RSAP sau adresa deschiderii)
Ofertele întârziate vor fi respinse.

26. **Persoanele autorizate să asiste la deschiderea ofertelor:**
Ofertanții sau reprezentanții acestora au dreptul să participe la deschiderea ofertelor, cu excepția cazului când ofertele au fost depuse prin SIA "RSAP".

27. **Limba sau limbile în care trebuie redactate ofertele sau cererile de participare:** Limba de stat

28. **Respectivul contract se referă la un proiect și/sau program finanțat din fonduri ale Uniunii Europene:** nu se aplică
(se specifică denumirea proiectului și/sau programului)

29. **Denumirea și adresa organismului competent de soluționare a contestațiilor:**
Agenția Națională pentru Soluționarea Contestațiilor
Adresa: mun. Chișinău, bd. Ștefan cel Mare și Sfânt nr.124 (et.4), MD 2001;
Tel/Fax/email: 022-820 652, 022 820-651, contestatii@ansc.md

30. **Data (datele) și referința (referințele) publicărilor anterioare în Jurnalul Oficial al Uniunii Europene privind contractul (contractele) la care se referă anunțul respective (dacă este cazul):** nu se aplică

31. **În cazul achizițiilor periodice, calendarul estimat pentru publicarea anunțurilor viitoare:** nu se aplică

32. **Data publicării anunțului de intenție sau, după caz, precizarea că nu a fost publicat un astfel de anunț:** nu se aplică

33. **Data transmiterii spre publicare a anunțului de participare:** conform SIA RSAP

34. **În cadrul procedurii de achiziție publică se va utiliza/accepta:**

Denumirea instrumentului electronic	**Se va utiliza/accepta sau nu**
depunerea electronică a ofertelor sau a cererilor de participare	Se acceptă
sistemul de comenzi electronice	Se acceptă
facturarea electronică	Se acceptă
plățile electronice	Se acceptă

35. **Contractul intră sub incidența Acordului privind achizițiile guvernamentale al Organizației Mondiale a Comerțului (numai în cazul anunțurilor transmise spre publicare în Jurnalul Oficial al Uniunii Europene):** Nu
(se specifică da sau nu)

36. **Alte informații relevante:** nu sunt

Conducătorul grupului de lucru: _____ **Alexandru IACUB**

L.Ș.

SPECIFICAȚII TEHNICE

Caracteristicile generale pentru „Licențele antivirus Bitdefender GravityZone for Workstation"

Produsul reprezintă o platformă integrată pentru managementul securității, gândită ca o soluție modulară.

Produsul conține următoarele module de securitate:

A. O consola de management care asigura funcționalități de administrare;

B. Protecție pentru stații fizice / virtuale.

A. CONSOLA DE MANAGEMENT

1. Instalare și configurare:

1. Consola de management va fi livrată ca o mașină virtuală bazată pe sistem de operare Linux securizat care conține toate rolurile sau serviciile necesare. Consola nu va necesita o licență suplimentară pentru sistemul de operare. Imaginea de tip template se va putea importa în:

a. VMware vSphere, View, Horizon;

b. Citrix XenServer, XenApp, Xen Desktop;

c. Microsoft Hyper-V;

d. Red Hat Enterprise Virtualization;

e. KVM sau „Kernel-based Virtual Machine";

f. Oracle VM;

g. Nutanix;

h. Alte platforme de virtualizare, la cerere.

2. Consola de management se livrează cu o bază de date inclusă care este de tip non-relațională, pentru o funcționare cât mai rapidă, fără a fi nevoie de licențe adiționale.

3. Soluția va fi scalabilă, astfel că oricare dintre roluri sau servicii pot fi instalate separat pe mai multe mașini virtuale sau pe aceeași mașină virtuală.

4. Rolurile principale trebuie să fie cel puțin similare cu: Server cu baza de date, Server de comunicație, Server de actualizare, Server de Web.

5. Soluția va include adițional și un modul de balansare (load balancer) pentru cazurile în care mai multe mașini virtuale ale componentei de management sunt instalate cu același rol (pentru Load Balancing și performanță/redundantă).

6. Soluția va include un mecanism de configurare a disponibilității pentru Serverul cu baze de date (clustering pentru redundantă). Astfel, baza de date se va putea instala de mai multe ori, pe mai multe mașini virtuale.

7. Mașinile de scanare pentru mediile virtuale VMware și Citrix se instalează la distanță prin task din consola de management, iar pentru alte platforme se descarcă separat din interfața web a produsului.

2. Cerințe generale:

1. Interfața consolei de management va fi în limba română.

2. Interfața clientului de securitate, care se instalează pe stații și servere, va fi în limba română.

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

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

5. Produsul suporta licențierea per procesor fizic (socket). În felul acesta numărul mașinilor virtuale poate varia oricând, ele fiind protejate.

6. Soluția va include un modul de update server prin care se asigură actualizarea de produs și a semnăturilor.

7. Soluția va permite activarea/dezactivarea actualizărilor de produs/semnături.

8. Soluția permite stabilirea actualizării automate a consolei de management prin stabilirea recurenței zilnice, săptămânale sau lunare, dar și prin stabilirea intervalului orar în care acesta se va actualiza. De asemenea, permite și trimiterea unei alerte de nefuncționalitate, cu 30 de minute înainte de actualizare.

9. Pentru o mai buna urmărire a actualizărilor consolei de management, soluția permite vizualizarea unui jurnal de modificări în care sunt precizate istoric:

a. versiunea consolei de management;

b. data versiunii;

c. funcții noi și îmbunătățiri;

d. probleme rezolvate;

e. probleme cunoscute.

10. Notificările – prezente în interfață, notificările necitite sunt evidențiate, trimise către una sau mai multe adrese de email, alertează administratorul în cazul unor probleme majore: licențiere, detecție viruși, actualizări de produs disponibile).

11. Soluția va permite integrarea cu un server Syslog pentru raportarea evenimentelor antimalware.

12. Soluția va permite instalarea serviciului de SMNP prin care se pot raporta statusul mașinilor din cadrul componenței de management.

13. Soluția permite crearea unei copii de siguranță a bazei de date a consolei de administrare, la cerere sau programată, putând fi stocată local, pe un server FTP sau în rețea.

3. Panou de monitorizare și raportare (Dashboard):

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

2. Panoul central conține rapoarte pentru toate modulele suportate.

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

4. Inventarierea retelei – managementul securității:

1. Soluția se va integra cu domenii Active Directory multiple, VMware vCenter Server, Citrix Xen Server, Nutanix Prism și importa inventarul acestor platforme.

2. Se permite descoperirea stațiilor stații fizice neintegrate în Active Directory (Workgroup) cu ajutorul Network discovery.

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

4. Soluția va permite crearea unui pachet unic pentru toate sistemele de operare, de stații sau servere. Astfel, administratorul va putea descărca pachetele pentru protecția stațiilor și serverelor pe care rulează sistemul de operare Windows, Linux, Mac.

5. Soluția va permite instalarea la distanta sau manual a clienților antimalware pe mașini fizice/virtuale.

6. Soluția va permite selectarea modulelor componente atunci când se creează pachetul clientului care se instalează pe mașinile fizice/virtuale.

7. Soluția va permite lansarea de task-uri de scanare, actualizare, instalare, dezinstalarea la distanta pentru clientul antimalware.

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

9. Soluția va oferi informații detaliate despre fiecare task și se fixează dacă task-ul s-a finalizat sau nu cu succes.

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

11. Se vor oferi în consolă de management informații detaliate ale obiectelor din consola: Nume, IP, Sistem de operare, Grup, Politică atribuită, Ultimele actualizări, Versiunea produsului, Versiunea de semnături.

12. Pentru integrarea cu Active Directory, se va putea defini și intervalul (în ore) de sincronizare și forța sincronizarea.

13. Se permite descoperirea mașinilor din Microsoft Hyper-V, Red Hat VM, Oracle VM, KVM.

14. Soluția permite descoperirea tuturor aplicațiilor instalate pe toate stațiile și serverele din rețea, prin rularea unui task din consola de administrare.

5. Politici:

1. Soluția va permite configurarea setărilor clientului antimalware prin intermediul unei singure politici ce conține setări pentru toate modulele.

2. Politica va conține opțiuni specifice de activare/dezactivare și configurarea funcționalităților precum scanarea antimalware la cerere, firewall, controlul accesului la Internet, controlul aplicațiilor, scanarea traficului web, controlul dispozitivelor, power user.

3. Soluția permite aplicarea politicilor pe mașini client, grupuri de mașini, pool-uri de resurse (VMware), domeniu, unități organizaționale, grupuri de securitate, sau useri de active directoy.

4. Politica să poate fi schimbată automat în funcție de:

a. IP sau clasa de IP al stației;

b. Gateway-ul alocat;

c. DNS serverul alocat;

d. WINS serverul alocat;

e. Sufix DNS pentru conexiunea dhcp;

f. Clientul este/nu este în aceeași rețea cu infrastructura de management (stația de lucru poate soluționa implicit numele gazdei);

g. Tipul rețelei (lan, wireless);

h. User-ul logat pe stație;

i. Etichete definite pe mașini virtuale în cloud (disponibile doar prin integrare Amazon EC2 sau MS Azure).

6. Rapoarte:

1. Soluția va conține rapoarte care prezintă statutul mașinilor clienților din punct de vedere al actualizărilor, fișierelor malware detectate, aplicațiile blocate, site-urilor web blocate.

2. Rapoartele programate pot fi trimise către un număr nelimitat de adrese de email (nu este nevoie să aibă un cont în consola de management).

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

4. Soluția va permite exportarea rapoartelor în format .pdf și detaliile ca format .csv.

5. Soluția include un generator de rapoarte care oferă posibilitatea de a investiga o problemă de securitate pe baza mai multor criterii, menținând informațiile concise și ordonate corespunzător. Astfel, soluția include interogări precum: starea terminalului, evenimente terminal, evenimente Exchange.

6. Interogarea legată de starea terminalului include informații precum:

a. tip mașină;

b. infrastructura rețelei căreia îi aparține terminalul;

c. datele agentului de securitate;

d. starea modulelor de protecție;

e. rolurile terminalelor.

7. Interogarea legată de evenimente terminal include informații precum:

a. calculatorul țintă pe care a avut loc evenimentul;

b. tipul, starea si configurația agentului de securitate instalat;

c. starea modulelor și rolurilor de protecție instalate pe agentul de securitate;

d. denumirea și alocarea politicii;

e. utilizatorul autentificat în timpul evenimentului;

f. evenimente (site-uri blocate, aplicații blocate, detecțiile etc).

7. Carantina:

1. Soluția va permite restaurarea fișierelor carantinate în locația originală sau într-o cale configurabilă.

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

3. Permite descărcarea fișierelor carantinate doar pentru mașinile virtuale protejate prin modulul mediilor virtuale integrat cu VMware vShield.

8. Utilizatori:

1. Administrarea se va putea face pe bază de roluri.

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

a. Administrator companie: administrează arhitectura consolei de management;

b. Administrator rețea: administrează serviciile de securitate;

c. Reporter: monitorizează și generează rapoarte.

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

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

5. Se va permite deconectarea automată a oricărui tip de utilizator după un anumit timp pentru o protecție sporită a datelor afișate în consola de administrare. Acest interval se poate personaliza de administratorul soluției.

9. Log-uri:

1. Înregistrarea acțiunilor utilizatorilor.

2. Se vor oferi informații detaliate pentru fiecare acțiune a unui utilizator.

3. Se va permite filtrarea acțiunilor utilizatorului după numele utilizatorului, acțiune.

10. Actualizare:

1. Se permite definirea de locații de actualizare multiple.

2. Se permite activarea/dezactivarea actualizărilor de produs și semnături.

3. Se permite actualizarea produsului într-o rețea fără acces la Internet.

4. Orice client antivirus să poată fi configurat să livreze update-urile către alt client antivirus.

5. Soluția dispune un server de actualizare (update) care face posibilă stabilirea componentelor ce vor fi descărcate automat de pe internet, fără intervenția administratorului. Astfel, administratorul va putea descărca pachetele pentru protecția stațiilor și serverelor pe care rulează sistemul de operare Windows, Linux, Mac sau poate descărca pachetele pentru modul de scanare centralizată în mediile de virtualizare VMware, Hyper-V sau Citrix.

6. În cadrul serverului de actualizare, pentru o mai bună urmărire a actualizărilor pachetele pentru protecția stațiilor și serverelor sau a pachetelor pentru modul de scanare centralizată, se va putea vizualiza în jurnalul de modificări în care sunt precizate istoric:

a. versiunea pachetului;

b. data versiunii;

c. funcții noi și îmbunătățiri;

d. probleme rezolvate;

e. probleme cunoscute.

7. Soluția permite testarea noilor versiuni de pachete de instalare ale clientului antimalware, înainte de a fi instalate pe toate stațiile și serverele din rețea, evitând posibile probleme ce pot afecta serverele sau stațiile critice.

Astfel, serverul de actualizare include 2 tipuri de actualizări de produs:

a. Ciclu rapid, gândit pentru un mediu de test în cadrul rețelei;

b. Ciclu lent, gândit pentru restul rețelei (producție, servere critice etc).

8. Soluția permite stabilirea zonelor de test și critice din cadrul rețelei prin intermediul politicilor din consola de management.

11. Certificate:

1. Accesul la consolă de management să se facă doar prin HTTPS.

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

3. Soluția permite afișarea în consola de management informații despre certificate: nume, autoritatea emitentă, data eliberării și data expirării certificatelor eliberate.

B. PROTECȚIE STAȚII

1. Caracteristici generale minimale si eliminatorii:

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

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

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

4. Pentru o mai bună protecție a stațiilor și serverelor, soluția include protecție împotriva atacurilor zero-day de tip exploit (atacuri direcționate).

2. Cerințe de sistem:

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

2. 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.

3. 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 și instalare remote:

1. Înainte 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 în mai multe moduri:

a. prin descărcarea directă a pachetului pe stația pe care se va face instalarea;

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

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

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

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

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

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

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

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

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

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

4. Caracteristici și funcționalități principale ale modulului antimalware:

1. Soluția permite administratorului să stabilească acțiunea luată de produsul Antimalware la detectarea unei amenințări noi. Astfel administratorul va putea alege între următoarele acțiuni:

a. Acțiune implicită pentru fișiere infectate:

- interzice accesul;
- dezinfectează;
- ștergere;
- mută fișierele în carantină;
- nicio acțiune.

b. Acțiune alternativă pentru fișierele infectate:

- interzice accesul;
- dezinfectează;
- ștergere;
- mută fișierele în carantină.

c. Acțiune implicită pentru fișierele suspecte:

- interzice accesul;
- ștergere;
- mută fișierele în carantină;
- nicio acțiune.

d. Acțiune alternativă pentru fișierele suspecte:

- interzice accesul;
- ștergere;
- mută fișierele în carantină.

2. Scanarea automată în timp real va putea fi setată să nu scaneze arhive sau fișiere mai mari de « x » MB, mărimea fișierelor putând fi definită de administratorul soluției.

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

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

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

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

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

8. Clienții antimalware pentru workstation să permită definirea unor liste de excludere de la scanarea în timp real și la cerere a anumitor directoare, discuri, fișiere, extensii sau procese.

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

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

11. Produsul antimalware poate fi configurat să folosească scanarea în cloud, și parțial scanarea locală. Pentru stațiile ce nu au suficiente resurse hardware, scanarea se poate face cu o mașină de scanare instalată în rețea.

12. Administratorul poate personaliza și motoarele de scanare, având posibilitatea de a alege între mai multe tehnologii de scanare:

a. 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.

b. 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.

c. 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.

d. Scanare centralizată (Scanare în cloud privat cu server de securitate) cu fallback pe Scanare locală (motoare full).*

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

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

14. Pentru o protecție sporită, soluția antimalware trebuie să poată scana paginile HTTP și HTTPS.

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

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

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

18. Pentru o mai buna protecție a stațiilor și serverelor, soluția include protecție împotriva atacurilor zero-day de tip exploit avansate (atacuri direcționate) bazată pe tehnologii de învățare automată (machine learning).

19. Pentru o mai bună protecție a stațiilor și serverelor, soluția include un modul avansat de securitate – HyperDetect, bazat pe tehnologii de tip „machine learning tunabil" proiectat special pentru a detecta atacuri avansate și activități suspecte în faza pre-execuție.

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

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

22. Pentru a oferi un nivel adițional de protecție a stațiilor și serverelor, soluția include un sandbox în cloud-ul public al producătorului acesteia.

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

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

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

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

27. Modulul de Sandbox poate suporta „detonarea" următoarelor tipuri de fișiere: Batch, CHM, DLL, EML, Flash SWF, HTML, HTML/script, HTML (Unicode), JAR (archive), JS, LNK, MHTML (doc), MHTML (ppt), MHTML (xls), Microsoft Excel, Microsoft PowerPoint, Microsoft Word, MZ/PE files (executable), PDF, PEF (executable), PIF (executable), RTF, SCR, URL (binary), VBE, VBS, WSF, WSH, WSH-VBS, XHTML.

28. Fișierele menționate anterior, vor putea fi detectate corect chiar dacă sunt incluse în arhive de tipul: : 7z, ACE, ALZip, ARJ, BZip2, cpio, GZip, LHA, Linux TAR, LZMA Compressed Archive, MS Cabinet, MSI, PKZIP, RAR, Unix Z, ZIP, ZIP (multivolume), ZOO, XZ.

5. Anti-Exploit-Avansat:

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

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

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

6. Firewall:

1. Posibilitatea de a configura reguli de firewall pentru aplicații sau conectivitate.
2. Modulul poate fi instalat/dezinstalat în funcție de preferință administratorului.
3. Posibilitatea de a defini rețele de încredere pentru mașina destinație.
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 să permită trimiterea automată a fișierelor din carantină către laboratoarele antimalware ale producătorului.

2. Trimiterea conținutului carantinei va putea fi expediat în mod automat, la un interval definit de administrator.

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

4. Posibilitatea de a restaura un fișier din carantină în locația lui originală.

5. Modulul de carantină va permite rescanarea obiectelor după fiecare actualizare de semnături.

6. Modulul de carantină va permite salvarea unei copii a fișierului infectat respectiv transmiterea acestuia către carantina înainte de a efectua orice altă acțiune asupra acestuia.

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 particularități:

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 conțin anumite cuvinte cheie;

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

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

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

10. Controlul aplicațiilor:

1. Pentru o mai buna inventariere și administrare, soluția va include o secțiune în consola de administrare unde se vor regăsi toate aplicațiile descoperite în rețea, grupate după: nume, versiune, descoperit la, găsit pe.

2. Pentru o mai bună inventariere și administrare, soluția va include o secțiune în consola de administrare unde se vor regăsi toate procesele negrupate descoperite în rețea, grupate după: nume, versiune, nume produs, versiune produs, editor/autor, descoperit la, găsit pe.

3. Pentru prevenirea infectării stațiilor și serverelor dar și pentru a permite aplicațiilor descoperite în rețea să se poată actualiza, soluția permite definirea unor programe de actualizare (Updater) care vor fi lăsate să actualizeze diferite aplicații instalate pe stații sau servere.

4. Soluția include opțiunea de a permite sau a bloca rularea anumitor aplicații sau procese definite de administrator (inclusiv subprocese) după:

a. Cale fișier: local, CD-ROM, portabil sau rețea;

b. Hash;

c. Certificat.

11. Controlul dispozitivelor:

1. Modulul poate fi instalat/dezinstalat în funcție de preferință 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 mașina 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 mașina client cum ar fi: permis/blocat/custom respectiv poate limita accesul dispozitivelor externe la „read only" sau limita doar accesul la porturile USB ale endpoint-ului permițând orice alt tip de dispozitiv ce nu folosește acest tip de port/interfață.
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 și raporta prezența acestora în consola de management.

12. Power User:

1. Modulul poate fi instalat/dezinstalat în funcție de preferință administratorului.
2. Modulul permite posibilitatea de a acorda utilizatorilor drepturi de Power User. Utilizatorii vor putea accesa și modifica setările clientului antimalware dintr-o consolă disponibilă local pe mașina client.
3. Modificările efectuate din modulul Power User vor fi active local, pe mașina pe care s-au făcut respectivele modificări.
4. Administratorul va putea suprascrie din consola setările aplicate de utilizatorii Power User.

13. Actualizare:

1. Posibilitatea efectuării actualizării la nivel de stație în mod silențios (fără 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 și rol de server de actualizare.
4. Abilitatea de a împiedica punctele finale să iasă pe internet pentru a descărca actualizări.

SPECIFICAȚII TEHNICE

Caracteristicile generale pentru „Licențele CAL coorporativ pentru utiliatori"

License your RDS deployment with client access licenses (CALs)

Când un utilizator sau un dispozitiv se conectează la un server RD Session Host, serverul RD Session Host determină dacă este necesară o licență CAL RDS.

Serverul gazdă sesiune RD solicită apoi o licență CAL RDS de la serverul de licență Desktop la distanță. Dacă o licență CAL RDS adecvată este disponibilă de la un server de licență, licența CAL RDS este emisă clientului, iar clientul se poate conecta la serverul gazdă sesiunii RD și de acolo la desktopul sau la aplicațiile pe care încearcă să le folosească.

Licență perpetual.