CARACTERISTICI GENERALE ALE PRODUSULUI

Produsul este o platforma integrata pentru managementul securității, gândita ca o soluție modulara. Produsul conține următoarele module:

- **A.** O consola de management care asigura funcționalități de administrare;
- **B.** Protecție stații și servere fizice/virtuale;
- **C.** Protecție și securitate pentru telefoanele mobile de tip smartphone;
- **D.** Protecție și securitate pentru serverele email Microsoft Exchange.
- **E.** Integrare SIEM.

A. CONSOLA DE MANAGEMENT

1. Instalare și configurare:

1.1. Pachetul de instalare se poate instala pe mașina virtuala care sa opereze pe unul din hypervizori de mai jos :

- 1.1.1. VMware vSphere
- 1.1.2. Citrix XenServer
- 1.1.3. Microsoft Hyper-V
- 1.1.4. Oracle VM.

1.2. Soluția va fi scalabila, astfel ca oricare dintre roluri sau servicii pot fi instalate separat pe mai multe mașini virtuale sau pe aceeași mașina virtuala.

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

2. Cerințe generale:

2.1. Interfața consolei de management va fi în prezenta în limbile de circulație internațională

2.2. Interfața clientului de securitate, care se instalează pe stații și servere, va fi în prezenta în limbile de circulație internațională.

2.3. Manualul de instalare a produsului va fi în prezenta în limbile de circulație internațională .

2.4. Manualul de administrare a produsului va fi în prezenta în limbile de circulație internațională.

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

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

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

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

- 2.8.1. versiunea consolei de management
- 2.8.2. data versiunii
- 2.8.3. funcții noi și îmbunătățiri
- 2.8.4. probleme rezolvate
- 2.8.5. probleme cunoscute

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

2.10. Soluția va permite integrarea cu un server Syslog pentru raportarea evenimentelor anti malware.
2.11. Soluția va permite instalarea serviciului de SMNP prin care se pot raporta statusul mașinilor din cadrul componentei de management.
2.12. Soluția permite creare unei copii de siguranța a bazei de date a consolei de administrare, la cerere sau programata,.
2.13. Endpoint Risk Management și Analytics
2.14. Introduceți zero configurațiile greșite, aplicațiile vulnerabile, riscurile comportamentului utilizatorilor, dispozitivele și utilizatorii individuali și remediați configurările greșite sau vulnerabilitățile corecțiilor.

3. Panou de monitorizare și raportare (Dashboard):

3.1. 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 considerata neactualizata).
3.2. Panoul central conține rapoarte pentru toate modulele suportate.
3.3. Rapoartele din panoul central de comanda permit: adăugarea altor rapoarte, ștergerea lor și rearanjarea.
3.4. O platformă integrată de protecție a punctelor finale, gestionarea riscurilor și criminalistică pentru atacuri. Îmbunătățit cu analiza riscului comportamentului utilizatorului.
3.5. Modul include analiza cauzei rădăcină, vizualizarea lanțului de atac și acțiuni de remediere legate de amenințările detectate și blocate de tehnologiile de prevenire ca exemplu, Antimalware (Exploit Defense, PowerShell Defense, HyperDetect etc.), Sandbox și Network -Apărarea atacului.
3.6. Analiza securității traficului în rețea (NTSA) detectează atacurile avansate în timp real, oferă contextul amenințărilor și declanșează un răspuns autonom la incidente. NTSA folosește o combinație de învățare automată și analize de comportament cu informații de la Aanti Virus intelligence intelligence - format din cel puțin 400-500 de milioane de senzori la nivel global - pentru a detecta amenințările pentru toate entitățile, gestionate sau neadministrate, pentru traficul de rețea criptat sau necriptat.

4. Inventarierea rețelei – managementul securității:

4.1. Soluția se va integra cu domenii Active Directory multiple, VMware vCenter, Citrix Xen și importa inventarul acestor platforme.
4.2. Pentru integrarea cu Active Directory, se va putea defini și intervalul (în ore) de sincronizare și forța sincronizarea.
4.3. Se permite descoperirea mașinilor din Microsoft Hyper-V, Red Hat VM, Oracle VM, KVM.
4.4. Se permite descoperirea stațiilor stații fizice neintegrate în Active Directory (Workgroup) cu ajutorul Network discovery.
4.5. Soluția va oferi opțiuni de căutare, sortare și filtrare după numele sistemului, sistem de operare și adresa IP.
4.6. Soluția va permite instalarea la distanta sau manual a clienților anti malware pe mașini fizice/virtuale.
4.7. Soluția va permite selectarea modulelor componente atunci când se creează pachetul clientului care se instalează pe mașinile fizice/virtuale.
4.8. Soluția va permite lansarea de task-uri de scanare, actualizare, instalare, dezinstalarea la distanta pentru clientul anti malware.

4.9. Soluția va oferi posibilitatea de repornire a mașinilor fizice de la distanta.
4.10. Soluția va oferi informații detaliate despre fiecare task și va afișa daca task-ul s-a finalizat sau nu cu succes.
4.11. Soluția va permite configurarea centralizata a clienților anti malware prin intermediul politicilor
4.12. Se vor oferi în consola de management informații detaliate ale obiectelor din consola: Nume, IP, Sistem de operare, Grup, Politica atribuita, Ultimele actualizare, Versiunea produsului, Versiunea de semnături.
4.13. Soluția permite descoperirea tuturor aplicațiilor instalate pe toate stațiile și serverele din rețea, prin rularea unui task din consola de administrare.

5. Politici:

5.1. Soluția va permite configurarea setărilor clientului anti malware prin intermediul unei singure politici ce conține setări pentru toate module
5.2. Politica va conține opțiuni specifice de activare/dezactivare și configurarea funcționalităților precum scanarea anti malware la cerere, firewall, controlul accesului la Internet, controlul aplicațiilor, scanarea traficului web, controlul dispozitivelor, power user.
5.3. Solutia va permite crearea unei politici dedicate sau configurații care pot fi lansate în mod automat fara interventia administratorului în cazul în care numărul de incidente malware depășește un prag definit (de exemplu, in timpul unui " atac de virus ")Soluția permite aplicarea politicilor pe mașini client, grupuri de mașini, pool-uri de resurse (VMware), domeniu, unități organizaționale sau useri de active directory.

5.4. Politica să poate fi schimbata automat în funcție de:
5.4.1. User-ul logat pe stație
5.4.2. IP sau clasa de IP al stației
5.4.3. Gateway-ul alocat
5.4.4. DNS serverul alocat
5.4.5. Clientul este/nu este în aceeași rețea cu infrastructura de management
5.4.6. Tipul rețelei (lan, wireless)

6. Rapoarte:

6.1. Soluția va conține rapoarte care prezinta statutul mașinilor clienților din punct de vedere al actualizărilor, fișierelor malware detectate, aplicațiile blocate, site-urilor web blocate.
6.2. Rapoartele programate pot fi trimise către un număr nelimitat de adrese de email (nu este nevoie să aibă un cont în consola de management).
6.3. Soluția va permite vizualizarea rapoartelor curente programate de administrator.
6.4. Soluția va permite exportarea rapoartelor în format .pdf și detaliile ca format .csv.
6.5. Soluția include un generator de rapoarte care oferă posibilitatea de a investiga o problema de securitate pe baza mai multor criterii, menținând informațiile concise și ordonate corespunzător. Astfel, soluția include interogări precum: starea terminalului, evenimente terminal, evenimente Exchange.
6.6. Interogarea legata de starea terminalului include informații precum:
6.6.1. tip mașină
6.6.2. infrastructura rețelei căreia ii aparține terminalul
6.6.3. datele agentului de securitate
6.6.4. starea modulelor de protecție
6.6.5. rolurile terminalelor.
6.7. Interogarea legata de evenimente terminal include informații precum:

6.7.1. calculatorul ținta pe care a avut loc evenimentul
6.7.2. tipul starea și configurația agentului de securitate instalat
6.7.3. starea modulelor și rolurilor de protecție instalate pe agentul de securitate
6.7.4. denumirea și alocarea politicii
6.7.5. utilizatorul autentificat în timpul evenimentului
6.7.6. evenimente (site-uri blocate, aplicații blocate, detecțiile etc)

6.8. Interogarea legata de evenimente Exchange include informații precum:
6.8.1. Direcția traficului e-mail
6.8.2. Evenimente de securitate (detectarea programelor de tip malware sau a fișierelor atașate)
6.8.3. Masurile implementate în fiecare situație (curățarea, ștergerea, înlocuirea sau punerea în carantină a fișierului, ștergerea sau respingerea e-mail-ului)

7. Carantina:

7.1. Soluția va permite restaurarea fișierelor din carantină în locația originala sau într-o cale configurabila.
7.2. Carantina va fi locala, pe fiecare stația administrata și va fi administrata, fie local, fie din consola de management
7.3. Permite descărcarea fișierelor din carantină doar pentru mașinile virtuale protejate prin modulul mediilor virtuale integrat cu VMware vShield.

8. Utilizatori:

8.1. Administrarea se va putea face pe baza de roluri.
8.2. Roluri multiple predefinite: Administrator companie, Administrator rețea, Reporter sau rol personalizat.
8.3. Administrator companie: administrează arhitectura consolei de management;
8.4. Administrator rețea: administrează serviciile de securitate;
8.5. Reporter: monitorizează și generează rapoarte.
8.6. Utilizatorii pot fi importați din Microsoft Active Directory sau creați în consola de management.
8.7. Se va permite configurarea detaliata a drepturilor administrative, permițând selectarea serviciilor și obiectelor pentru care un utilizator poate face modificări.

9. Log-uri:

9.1. Înregistrarea acțiunilor utilizatorilor.
9.2. Se vor oferi informații detaliate pentru fiecare acțiune a unui utilizator.
9.3. Se va permite filtrarea acțiunilor utilizator după numele utilizatorului, acțiune.

10. Actualizare:

10.1. Se permite definirea de locații de actualizare multiple.
10.2. Se permite activarea/dezactivarea actualizărilor de produs și semnături.
10.3. Se permite actualizarea produsului într-o rețea fără acces la Internet.
10.4. Orice client antivirus să poată fi configurat să livreze update-urile către alt client antivirus
10.5. Soluția dispune un server de actualizare (update) care face posibila stabilirea componentelor ce vor fi descărcate automat de pe internet, fără intervenția administratorului. Astfel, administratorul va putea descarcă pachetele pentru protecția stațiilor și serverelor pe care rulează sistemul de operare Windows, Linux, Mac sau, poate descarcă pachetele pentru modul de scanare centralizata în mediile de virtualizare VMware, Hyper-V sau Citrix.
10.6. In cadrul serverului de actualizare, pentru o mai buna urmărire a actualizărilor pachetele pentru protecția stațiilor și serverelor sau a pachetelor pentru modul de

scanare centralizata, se va putea vizualiza un jurnal de modificări în care sunt precizate istoric:

10.6.1. versiunea pachetului
10.6.2. data versiunii
10.6.3. funcții noi și îmbunătățiri
10.6.4. probleme rezolvate
10.6.5. probleme cunoscute

10.7. Soluția permite testarea noilor versiuni de pachete de instalare ale clientului anti malware, 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:

11.Certificate:

11.1. Accesul la consola de management să se facă doar prin HTTPS.
11.2. Serverul web, din consola centrala de management trebuie să permită importarea de certificate digitale eliberate de o autoritate de certificare autorizata sau proprie organizației.
11.3. Soluția permite afișarea în consola de management informații despre certificate: nume, autoritatea emitenta, data eliberării și data expirării certificatelor eliberate.

B. PROTECȚIE STAȚII și SERVERE FIZICE/VIRTUALE

1. Caracteristici generale minimale și eliminatorii:

1.1. Pentru reducerea la minim a consumului de resurse, soluția anti malware trebuie să permită instalarea personalizata a modulelor deținute (de exemplu, să permită instalarea soluției anti malware fără modulul de control al accesului web, modul de control al dispozitivelor sau modulul firewall).
1.2. Pentru o mai buna protecție a stațiilor și serverelor, soluția include un vaccin anti-ransomware. Acest vaccin asigura protecția împotriva tuturor amenințărilor cunoscute de tip ransomware, prin imunizarea stațiilor și serverelor, chiar daca sunt infectate și prin blocarea procesului de criptare.
1.3. Pentru o mai buna protecție a stațiilor și serverelor, soluția include protecție împotriva atacurilor zero-day de tip exploit (atacuri direcționate).

2. Cerințe de sistem:

2.1. Sisteme de operare pentru stații de lucru: Windows 10, Windows 8, Windows 7, Mac OS X Sierra (10.12.x), Mac OS X El Capitan (10.11.x), Mac OS X Yosemite (10.10.5), Mac OS X Mavericks (10.9.5), Mac OS X Mountain Lion (10.8.5)
2.2. Sisteme de operare pentru servere: Windows Server 2012 R2, Windows Server 2012, Windows Small Business Server (SBS) 2011, Windows Small Business Server (SBS) 2008, Windows Server 2008 R2, Windows Server 2008, Windows Small Business Server (SBS) 2003, Windows Server 2003 R2, Windows Server 2003 with Service Pack 1,
2.3. Sisteme de operare Linux: Red Hat Enterprise Linux / CentOS 5.6 sau mai recent, Ubuntu 10.04 LTS sau mai recent, SUSE Linux Enterprise Server 11 sau mai recent, OpenSUSE 11 sau mai recent, Fedora 15 sau mai actual and Debian 5.0 sau mai recent.
2.4. Sisteme de operare MAC: Mac OS X El Capitan (10.11.x), Mac OS X Yosemite (10.10.5), Mac OS X Mavericks (10.9.5), Mac OS X Mountain Lion (10.8.5)

3. Administrare și instalare remote:

3.1. Înainte de instalare, administratorul va putea particulariza pachetele de instalare cu modulele dorite: firewall, content control, device control,

3.2. Instalarea se va putea face în mai multe moduri:
3.3. prin descărcarea directa a pachetului pe stația pe care se va face instalarea;
3.4. prin instalarea la distanta, direct din consola de management
3.5. Instalarea clienților la distanta în alte locații decât cele în care este instalata consola de management se va face prin intermediul unui alt client antivirus existent în locațiile respective pentru a minimiza traficul în WAN.
3.6. In consola vor fi disponibile informații despre fiecare stație: numele stației, IP, sistem de operare, module instalate, politica aplicata, informații despre actualizări etc.
3.7. Din consola se va putea trimite o singura politica pentru configurarea integrala a clientului de pe stații/servere.
3.8. 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.
3.9. Posibilitatea creării unui singur pachet de instalare, utilizabil atât pentru sistemele de operare pe 32 de biți cat și pentru cele pe 64 de biți.
3.10. Posibilitatea creării unui singur pachet de instalare, utilizabil pentru stații (fizice si/sau virtuale), servere (fizice si/sau virtuale),.
3.11. Administratorul va putea crea grupuri sau chiar subgrupuri, unde va putea muta stațiile/serverele din rețea pentru cele care nu sunt integrate domeniu.
3.12. Permite selectarea clientului care va realiza descoperirea stațiilor din rețea, altele decât cele integrate în domeniu.

4. Caracteristici și funcționalități principale ale modulului anti malware:

4.1. Soluția permite administratorului să stabilească acțiunea luata de produsul Anti malware la detectarea unei amenințări noi. Astfel administratorul va putea alege intre următoarele acțiuni:
  4.1.1. Acțiune implicită pentru fișiere infectate:
    4.1.1.1. interzice accesul
    4.1.1.2. dezinfectează
    4.1.1.3. ștergere
    4.1.1.4. muta fișierele în carantina
    4.1.1.5. nicio acțiune
  4.1.2. Acțiune alternativa pentru fișierele infectate:
    4.1.2.1. interzice accesul
    4.1.2.2. dezinfectează
    4.1.2.3. ștergere
    4.1.2.4. muta fișierele în carantina
  4.1.3. Acțiune implicită pentru fișierele suspecte:
    4.1.3.1. interzice accesul
    4.1.3.2. ștergere
    4.1.3.3. muta fișierele în carantina
    4.1.3.4. nicio acțiune
  4.1.4. Acțiune alternativa pentru fișierele suspecte:
    4.1.4.1. interzice accesul
    4.1.4.2. ștergere
    4.1.4.3. muta fișierele în carantina
4.2. Scanarea automata în timp real va putea fi setata să nu scaneze arhive sau fișiere mai mari de « x » MB, mărimea fișierelor putând fi definita de administratorul soluției,
4.3. Definirea pana la 16 nivele de profunzime pentru scanarea în arhive.
4.4. Scanarea euristica comportamentala 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 semnătură nu a fost lansata încă.

4.5. 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.

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

4.7. Configurarea cailor ce urmează a fi scanate la cerere.

4.8. Clienții anti malware pentru stațiile de lucru să permită definirea unor liste de excludere de la scanarea în timp real și la cerere a anumitor directoare, discuri, fișiere, extensii sau procese.

4.9. 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.

4.10. Posibilitatea de configura scanările programate să se execute cu prioritate redusa

4.11. Produsul anti malware poate fi configurat să folosească scanarea în cloud, și parțial scanarea locala. Pentru stațiile ce nu au suficiente resurse hardware, scanarea se poate face cu o mașina de scanare instalata în rețea.

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

4.12.1. 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.

4.12.2. 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.

4.13. Pentru o protecție sporita, soluția anti malware trebuie să aibă 3 tipuri de detecție: bazata pe semnături, bazata de comportamentul fișierelor și bazata pe monitorizarea proceselor.

4.14. Pentru o protecție sporita, soluția anti malware trebuie să poată scana paginile HTTP.

4.15. Pentru o mai buna gestionare a anti malware instalat pe stații, produsul va include opțiunea de setare a unei parole pentru protecția la dezinstalare.

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

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

4.18. Pe mașinile virtuale parte a unui pool instalarea clientului anti malware se face doar pe mașina de tip template, după care se recompune pool-ul de mașini virtuale.

5. Firewall:

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

5.2. Modulul poate fi instalat/dezinstalat în funcție de preferința administratorului.

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

6. Carantina:

6.1. Produsul anti malware să permită trimiterea automata a fișierelor din carantina către laboratoarele anti malware ale producătorului.

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

6.3. Produsul anti malware să permită ștergerea automata a fișierelor din carantină mai vechi de o anumita perioada, pentru a nu încărca inutil spațiul de stocare.

6.4. Posibilitatea de a restaura un fișier din carantina în locația lui originala.

6.5. Modulul de carantina va permite re-scanarea obiectelor după fiecare actualizare de semnături.

7. Controlul conținutului:

7.1. Consola va avea integrat un modul dedicat controlului accesului la Internet cu următoarele particularități:
   7.1.1. Permite blocarea accesului la Internet pentru anumite mașini client sau grupuri de mașini.
   7.1.2. Permite blocarea accesului la Internet pe intervale orare.
   7.1.3. Permite blocarea paginilor de internet care conțin anumite cuvinte cheie.
   7.1.4. Permite controlul accesului numai la anumite pagini de internet specificate de administrator;
   7.1.5. Permite blocarea accesului la anumite aplicații definite de administrator;
   7.1.6. Permite restricționarea accesului pe anumite pagini de internet după anumite categorii prestabilite (ex: online dating, violenta, pornografie etc).

8. Controlul aplicațiilor:

8.1. 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.

8.2. Produsul trebuie sa permită administratorului sa identifice toate încercările utilizatorului de pornire a aplicației si sa reglementeze lansarea aplicațiilor prin intermediul regulilor de control pentru pornirea aplicațiilor

8.3. produsul trebuie sa permită administratorului sa creeze reguli pentru pornirea aplicațiilor, stabilind multiple condiții cum ar fi:
- calea către florerul ce conține fișierul executabil al aplicației
- metadata (denumirea originala a fișierului executabil al unei aplicații, numele fișierului executabil al unei aplicații aflate pe un dispozitiv drive, versiunea fișierului executabil al aplicației, numele aplicației si producătorul aplicației)
- MD5 hash al fișierului executabil al aplicației.
- aplicația aparține unei categorii predefinite, care este actualizata constant de producător

8.4. Pentru o mai buna 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.

8.5. 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.

8.6. Produsul trebuie sa permită implementarea politicilor negare implicit pentru pornirea aplicațiilor

9. Controlul dispozitivelor:

9.1. Modulul poate fi instalat/dezinstalat în funcție de preferința administratorului.

9.2. Modulul va permite controlul următoarelor tipuri de dispozitive:
   9.2.1. Bluetooth Devices
   9.2.2. CDROM Devices
   9.2.3. USB
   9.2.4. Floppy Disk Drives
   9.2.5. Security Policies 153
   9.2.6. IEEE 1284.4
   9.2.7. IEEE 1394
   9.2.8. Imaging Devices
   9.2.9. Modems
   9.2.10. Tape Drives

9.2.11. Windows Portable
9.2.12. COM/LPT Ports
9.2.13. SCSI Raid
9.2.14. Printers
9.2.15. Network Adapters
9.2.16. Wireless Network Adapters
9.2.17. Internal and External Storage

9.3. Modulul va permite configurarea de reguli prin care se vor defini permisiunile pentru dispozitivele conectate la mașina client.

9.4. Modulul va permite configurarea de excluderi pentru diferite tipuri de dispozitive pentru care s-au configurat reguli.

10. Actualizare:

10.1. Posibilitatea efectuării actualizării la nivel de stație în mod silențios (fără avertizare).

10.2. Sistem de actualizare cascadat folosind unul sau mai multe servere de actualizare (cascadate).

10.3. Actualizarea pentru locațiile remote prin intermediul unui client anti malware care are și rol de server de actualizare.

C. PROTECȚIE și SECURITATE PENTRU TELEFOANELE MOBILE DE TIP SMARTPHONE

1. Cerințe minime de sistem:

1.1. Telefoane și tablete cu sistem de operare iOS 9+, iPadOS 13+: Apple iPhone și tablete iPad

1.2. Telefoane și tablet cu sistem de operare Android 4+

2. Caracteristici:

2.1. Permite asocierea unui dispozitiv cu un utilizator din Active Directory.

2.2. Instalarea se face prin trimiterea unui email către utilizator cu detaliile de instalare.

2.3. Activarea dispozitivului mobil în consola de management să se facă prin scanarea unui cod QR.

2.4. Pachetele de instalare se vor putea descarcă de pe Apple App Store și Google Play.

2.5. Se vor putea întreprinde următoarele acțiuni:
2.5.1. Blocarea dispozitivului;
2.5.2. Deblocarea dispozitivului;
2.5.3. Ștergerea datelor și revenirea la setările din fabrica;
2.5.4. Localizarea dispozitivului;
2.5.5. Scanarea dispozitivului(doar pentru cele cu sistem de operare Android);
2.5.6. Criptarea memoriei dispozitivului(doar pentru cele cu sistem de operare Android).

2.6. Consola va permite raportarea dispozitivelor: active, inactive, deconectate, cu sistemul de operare modificat astfel încât utilizatorul să aibă acces total asupra lui (rooted or jailbroken devices).

3. Setări de securitate:

3.1. In cazul în care un dispozitiv nu este conform cu setările dorite, se vor putea întreprinde automat acțiunile:
3.1.1. Ignorare;
3.1.2. Blocarea accesului;
3.1.3. Blocarea dispozitivului;

3.1.4. Ștergerea datelor și revenirea la setările din fabrica;
3.1.5. Ștergerea dispozitivului din consola.

3.2. Se va putea impune blocarea dispozitivelor cu ajutorul unei parole. Aceasta parola va putea fi configurata să conțină:
3.2.1. Parola simpla sau complexa (în funcție de cerințele sistemului de operare);
3.2.2. Numere și litere;
3.2.3. O lungime minima definita de administrator;
3.2.4. Un număr minim de caractere speciale, definit de administrator;
3.2.5. Perioada de expirare a parolei. Perioada va putea fi definita de administrator;
3.2.6. Configurarea restricției refolosirii parolei;
3.2.7. Numărul de introduceri incorecte a parolei, de către utilizator;
3.2.8. Perioada de autoblocare a dispozitivului după un număr de minute definite de administrator.

3.3. Se vor putea genera mai multe profiluri care vor stabili reguli de securitate pentru conectivitatea la Wi-Fi sau VPN (numai pentru sistemul de operare iOS) dar și unele legate de accesul la anumite pagini de internet.

3.4. Profilurile de Wi-Fi vor conține următoarele opțiuni:
3.4.1. Generale – se definește SSID precum și tipul securității rețelei;
3.4.2. Setări TCP/IP – atât pentru protocolul IPv4 dar și pentru IPv6;
3.4.3. Setări de proxy – dezactivat, automat sau configurat manual.

3.5. Profilurile acces pagini de internet pentru sistemul de operare Android includ opțiuni precum:
3.5.1. Permiterea, blocarea sau programarea pentru anumite zile și intervale orare a accesului la anumite pagini de internet;
3.5.2. Crearea unor excepții pentru blocarea sau permiterea accesului către anumite pagini de internet.

3.6. Profilurile acces pagini de internet pentru sistemul de operare iOS includ opțiuni de activare sau dezactivare a:
3.6.1. Utilizării browser-ului Safari;
3.6.2. Opțiunii de completare automata a informațiilor;
3.6.3. Alertării utilizatorului în cazul accesării unor pagini frauduloase;
3.6.4. Java script;
3.6.5. Pop-up-urilor;
3.6.6. Cookie-uri.

D. PROTECȚIE și SECURITATE PENTRU SERVERELE EMAIL MICROSOFT EXCHANGE

1.

1.1. Produsul va oferi protecție anti malware, anti spam (inclusiv anti phishing), precum și filtrare de atașamente și conținut, prin integrarea cu serverul Microsoft Exchange. De asemenea, va permite scanarea anti malware la cerere a bazelor de date Exchange.

1.2. Produsul va asigura scanarea atașamentelor și a conținutului mesajelor în timp real, fără a afecta vizibil performanta serverului de mail.

1.3. Actualizarea anti malware trebuie să poată fi făcută automat la un interval de maxim 1 ora, precum și la cerere.

1.4. In afara de detecția pe baza de semnături, modulul de protecție anti malware va trebui să includă și scanare euristica comportamentala, prin simularea unui calculator virtual în interiorul căruia sunt rulate și analizate aplicații cu potențial periculos, pentru a proteja sistemul de virușii necunoscuți prin detectarea codurilor periculoase a căror semnătură nu a fost lansata încă.

1.5. Produsul va oferi opțiuni multiple de acțiune la identificarea unui atașament virusat (dezinfectare, ștergere, mutare în carantina).
1.6. Cu ajutorul unei baze de date complete cu semnături de spyware și a euristicii de detecție a acestui tip de programe, produsul va oferi protecție anti-spyware pentru a preveni furtul de date confidențiale.
1.7. Produsul va oferi protecție anti spam, cu o baza de semnături actualizabila prin internet.
1.8. Modulul anti spam va trebui să includă un filtru URL cu o baza de adrese URL cunoscute a fi folosite în mesaje spam, precum și un filtru de caractere pentru detectarea automata a mesajelor scrise cu caractere chirilice sau asiatice.
1.9. Produsul va trebui să ofere filtru RBL care să identifice spam-ul prin sincronizarea cu anumite baze de date online care conțin liste de servere de mail cunoscute ca fiind la originea acestui tip de mesaje.
1.10. Produsul va trebui să ofere un serviciu/filtru online pentru îmbunătățirea protecției împotriva valurilor de spam nou apărute.
1.11. Produsul va oferi posibilitatea de a defini politici de filtrare anti malware, anti spam, a conținutului sau atașamentelor pentru diferite grupuri sau utilizatori.
1.12. Actualizarea produsului va fi configurabila și se va putea realiza de pe internet, direct sau printr-un proxy, sau din cadrul rețelei de pe un server de actualizare propriu.
1.13. Produsul va trebui să ofere statistici atât referitoare la scanarea antivirus cat și la scanarea anti spam.
1.14. Produsul se va integra în cadrul consolei de management unitar al soluției antivirus. Pentru ușurința accesului la setările produsului din diferite medii de operare, produsul va avea consola de administrare web.

E. CERINȚE FAȚĂ DE SERVICIILE DE IMPLEMENTARE și CONFIGURARE

1.

1.1. Ofertantul selectat va livra și instala licențele pentru soluția ofertată
1.2. Ofertantul selectat va efectua pregătirea mediului de instalare pentru soluția propusă, după care va asigura implementarea inițială a soluției aplicative în mediul de producție și mediul de testare.
1.3. Ofertantul selectat va efectua configurarea inițială a soluției, atât pentru mediul de producție, cât și mediul de testare. Prin configurare inițială se înțelege setarea tuturor parametrilor aplicabili în corespundere cu cerințele (clientului), inclusiv configurarea și instalarea soluției ofertate, setarea politicilor și testarea înainte de a fi pusa în producție.
1.4. În baza rezultatelor de la etapa de design, Ofertantul selectat va implementa toate configurările/customizările agreate darea în exploatare a soluției.
1.5. Ofertantul va asigura integrarea soluției cu cel puțin următoarele aplicații terțe:
    1.5.1. Integrarea cu Active Directory – pentru a asigura autentificarea utilizatorilor în cadrul soluției prin AD;
    1.5.2. Integrarea cu platforma mobila (telefoane, tablete) – pentru securizarea perimetrului mobile.
1.6. Ofertantul selectat va efectua instalarea soluției ofertate în întreaga infrastructură a Secretariatului Parlamentului inclusiv la toți utilizatorii finali (instalarea se va considera încheiată în momentul când toți utilizatorii vor avea instalat agentul și calculatorul va primi cel puțin o actualizare a bazelor și a agentului)
1.7. La sfârșitul etapei, Ofertantul va face o demonstrație a soluției și a modulelor care au fost acoperite, fapt care va servi drept unul din criteriile de acceptanță ale etapei de implementare.

1.8. După acceptanța finală a soluției, va fi activată în mod automat opțiunea de garanție post-implementare și suport. Perioada de garanție post-implementare și suport va fi de 1 an calendaristic de la data activării acestei opțiuni.
1.9. Serviciile de garanție post-implementare și suport se referă la serviciile oferite de către Ofertantul selectat adițional la serviciile de mentenanță și suport a licențelor, oferite direct de către producătorul licențelor.
1.10. Serviciile de garanție post-implementare și suport, vor include următoarele componente:
    1.10.1. Gestionarea serviciului de actualizare a serverelor la ultimele actualizări oferite de producător;
    1.10.2. Gestionarea incidentelor de securitate apărute pe perioada suportului activ;
    1.10.3. Solicitărilor de schimbare a politicilor de securitate;
    1.10.4. Solicitări de analiza și corecție a politicilor de securitate în cadrul companiei implementate.

F. Cerințele fata de serviciile de instruire

1.

1.1. În cadrul proiectului, Ofertantul va organiza sesiuni de instruire și transfer de cunoștințe pentru grupurile țintă în vederea formării setului de cunoștințe necesar pentru a permite echipei instruite să preia menținerea și configurarea ulterioară a soluției, în conformitate cu necesitățile utilizatorilor
1.2. Instruirea se va organiza pentru diferite grupuri țintă la sediul Cumpărătorului sau online.
    1.2.1. Analist - 1 persoană
    1.2.2. Administrator - 5 persoane,
1.3. În acest sens, ca parte a ofertei, Ofertantul va prezenta ca parte a ofertei, un plan de instruire, în care se va indica ce tipuri de instruiri va efectua Ofertantul, pentru ce categorie de utilizatori, precum și cuprinsul/agenda acestor instruiri.
1.4. În afara instruirilor ce țin de utilizarea soluției, Ofertantul trebuie să efectueze și sesiuni de instruire pentru echipa de menținere din partea Cumpărătorului, în scopul asigurării unui nivel adecvat de cunoștințe și competențe, pentru a putea utiliza eficient instrumentele de configurare și dezvoltare disponibile în cadrul soluției.
1.5. În cadrul serviciilor de implementare, pentru a asigura transferul necesar de cunoștințe către echipa Cumpărătorului, Ofertantul va fi de acord ca cel puțin o persoană să asiste la lucrările de parametrizare/configurare, stabilite de comun acord de către Părți.
1.6. Ofertantul selectat la etapa de încheiere a contractului, va trebui să elaboreze și să convină cu Cumpărătorul următoarele elemente ale componentei de instruire:
    1.6.1. Strategia Ofertantului cu privire la instruire și programul de formare;
    1.6.2. Structura și componența pachetului de cursuri pentru formare și a manualelor de studiu pentru fiecare categorie de utilizator;
    1.6.3. Metodologia și procedurile de evaluare și control al eficienței și suficienței sesiunilor de instruire.
1.7. În cadrul sesiunilor de instruire, Ofertantul va pune la dispoziția Cumpărătorului întreg setul de documentație al soluției, care să cuprindă cel puțin următoarele componente:

G. Licențe:

1.1. Desktopuri – 500
1.2. Căsuțe de email – 500
1.3. Mașini virtuale – 20
1.4. Servere – 10

H. Cerințe minime de calificare a ofertanților:

1.

1.1. Disponibilitatea interfeței administratorului și a agentului soluției ofertate în limbele circulație internaționala ;
1.2. Producătorul trebuie să ofere suport tehnic 24/7, inclusiv în limbele circulație internaționala prin e-mail sau telefon;
1.3. Suport tehnic local 24/7 în limbele circulație internaționala din partea partenerului local;
1.4. Autorizarea de la Producător a partenerului vis-a-vis de dreptul de vânzare a produselor pe teritoriul R. Moldova;
1.5. Autorizarea de la Producător a partenerului vis-a-vis de dreptul de a oferi suport tehnic pe teritoriul R. Moldova;
1.6. Prezentarea documentelor confirmative a minim 2 specialiști certificați pe soluția propusa.