Matricea de conformitate

Subscriere anuală pentru soluția de protecție și securitate Bitdefender GravityZone for Workstation, pentru 200 entități (PC/laptop) pentru o perioada de 12 luni sau echivalentul.	**Subscriere anuală pentru soluția de protecție și securitate Bitdefender GravityZone for Workstation, pentru 200 entități (PC/laptop) pentru o perioada de 12 luni**
Caracteristici Generale Produsul reprezintă o platforma integrata pentru managementul securitatii, gandita ca o solutie modulara. Produsul conține următoarele module de securitate: **A.** O consola de management care asigura functionalitati de administrare. **B.** Protecție pentru stații fizice / virtuale.	**Caracteristici Generale** Produsul reprezintă o platforma integrata pentru managementul securitatii, gandita ca o solutie modulara. Produsul va conține următoarele module de securitate: **I.** O consola de management care asigura functionalitati de administrare. **II.** Protecție pentru stații fizice / virtuale.
A. CONSOLA DE MANAGEMENT	**I CONSOLA DE MANAGEMENT**
1. Instalare si configurare: 1. Consola de management va fi livrata ca o masina virtuala bazata pe sistem de operare Linux securizat care contine toate rolurile sau serviciile necesare. Consola nu va necesita o licenta suplimentara pentru sistemul de operare. Imaginea de tip template se va putea importa in: 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 livreaza cu o baza de date inclusa care este de tip non-relationala, pentru o functionare cat mai rapida, fara a fi nevoie de licente aditionale.	**1. Instalare si configurare:** 1. Pachetul de instalare este livrat ca o mașina virtuala preintalată care conține toate rolurile sau serviciile necesare. Consola nu va necesita o licenta suplimentara pentru sistemul de operare. Imaginea de tip template se va putea importa in: 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 livreaza cu o baza de date inclusa care este de tip non-relationala, pentru o functionare cat mai rapida, fara a fi nevoie de licente aditionale.

3. Solutia va fi scalabila, astfel ca oricare dintre roluri sau servicii pot fi instalate separat pe mai multe masini virtuale sau pe aceeasi masina virtuala. 4. Rolurile principale trebuie sa fie cel putin similare cu: Server cu baza de date, Server de comunicatie, Server de actualizare, Server de Web. 5. Solutia va include aditional si un modul de balansare (load balancer) pentru cazurile in care mai multe masini virtuale ale componentei de management sunt instalate cu acelasi rol (pentru Load Balancing si performanta/redundanta). 6. Solutia va include un mecanism de configurare a disponibilitatii pentru Serverul cu baze de date (clustering pentru redundanta). Astfel, baza de date se va putea instala de mai multe ori, pe mai multe masini virtuale. 7. Masinile de scanare pentru mediile virtuale VMware si Citrix se insteaza la distanta prin task din consola de management, iar pentru alte platforme se descarca separat din interfata web a produsului.	3. Solutia este scalabila, astfel ca oricare dintre roluri sau servicii pot fi instalate separat pe mai multe masini virtuale sau pe aceeasi masina virtuala. 4. Rolurile principale sunt similare cu: Server cu baza de date, Server de comunicatie, Server de actualizare, Server de Web. 5. Solutia include aditional si un modul de balansare (load balancer) pentru cazurile in care mai multe masini virtuale ale componentei de management sunt instalate cu acelasi rol (pentru Load Balancing si performanta/redundanta). 6. Solutia include un mecanism de configurare a disponibilitatii pentru Serverul cu baze de date (clustering pentru redundanta). Astfel, baza de date se va putea instala de mai multe ori, pe mai multe masini virtuale. 7. Masinile de scanare pentru mediile virtuale VMware si Citrix se insteaza la distanta prin task din consola de management, iar pentru alte platforme se descarca separat 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. Produsul suporta licentierea per procesor fizic (socket). In felul acesta numarul masinilor virtuale poate varia oricand, ele fiind protejate. 6. Solutia va include un modul de update server prin care se asigura actualizarea de produs si a semnaturilor. 7. Solutia va pemite activarea/dezactivarea actualizarilor de produs/semnaturi. 8. Solutia permite stabilirea actualizarii automate a consolei de management prin stabilirea recurentei zilnice, saptamanale	**2. Cerinte generale:** 1. Interfata consolei de management este in limba romana. 2. Interfata clientului de securitate, care se instaleaza pe statii si servere, este in limba romana. 3. Manualul de instalare a produsului este in limba romana. 4. Manualul de administrare a produsului este in limba romana. 5. Produsul suporta licentierea per procesor fizic (socket). In felul acesta numarul masinilor virtuale poate varia oricand, ele fiind protejate. 6. Solutia include un modul de update server prin care se asigura actualizarea de produs si a semnaturilor. 7. Solutia pemite activarea/dezactivarea actualizarilor de produs/semnaturi. 8. Solutia permite stabilirea actualizarii automate a consolei de management prin stabilirea recurentei zilnice, saptamanale

sau lunare, dar si prin stabilirea intervalului orar in care acesta se va actualiza. De asemenea, permite si trimiterea unei alerte de nefunctionalitate, cu 30 de minute inainte de actualizare. 9. Pentru o mai buna urmarire a actualizarilor consolei de management, solutia permite vizualizarea unui jurnal de modificari in care sunt precizate istoric: a. versiunea consolei de management b. data versiunii c. functii noi si imbunatatiri d. probleme rezolvate e. probleme cunoscute 10. 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). 11. Solutia va permite integrarea cu un server Syslog pentru raportarea evenimentelor antimalware. 12. Solutia va permite instalarea serviciului de SMNP prin care se pot raporta statusul masinilor din cadrul componentei de management. 13. Solutia permite creare unei copii de siguranta a bazei de date a consolei de administrare, la cerere sau programata, putand fi stocata local, pe un server FTP sau in retea. **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.	sau lunare, dar si prin stabilirea intervalului orar in care acesta se va actualiza. De asemenea, permite si trimiterea unei alerte de nefunctionalitate, cu 30 de minute inainte de actualizare. 9. Pentru o mai buna urmarire a actualizarilor consolei de management, solutia permite vizualizarea unui jurnal de modificari in care sunt precizate istoric: a) versiunea consolei de management b) data versiunii c) functii noi si imbunatatiri d) probleme rezolvate e) probleme cunoscute 10. 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). 11. Solutia permite integrarea cu un server Syslog pentru raportarea evenimentelor antimalware. 12. Solutia permite instalarea serviciului de SMNP prin care se pot raporta statusul masinilor din cadrul componentei de management. 13. Solutia permite crearea unei copii de siguranta a bazei de date a consolei de administrare, la cerere sau programata, putand fi stocata local, pe un server FTP sau in retea. **3. Panou de monitorizare si raportare (Dashboard):** 1. Rapoartele din panoul de monitorizare pot fi configurate specificand numele raportului, tipul raportului, tinta raportului, optiuni specifice pentru orice tip de raport (de exemplu pentru raportul de actualizare - care este intervalul dupa care o statie este considerata neactualizata). 2. Panoul central contine rapoarte pentru toate modulele suportate.

3. Rapoartele din panoul central de comanda permit: adaugarea altor rapoarte, stergerea lor si rearanjarea.	3. 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 domenii Active Directory multiple, VMware vCenter Server, Citrix Xen Server, Nutanix Prism si importa inventarul acestor platforme. 2. Se permite descoperirea statiilor statii fizice neintegrate in Active Directory (Workgroup) cu ajutorul Network discovery. 3. Solutia va oferi optiuni de cautare, sortare si filtrare dupa numele sistemului, sistem de operare, adresa IP, politica aplicata, ultima data cand s-a conectat (online si/sau offline) si FQDN. 4. Solutia va permite crearea unui pachet unic pentru toate sistemele de operare, de statii sau servere. Astfel, administratorul va putea descarca pachetele pentru protectia statiilor si serverelor pe care ruleaza sistemul de operare Windows, Linux, Mac. 5. Solutia va permite instalarea la distanta sau manual a clientilor antimalware pe masini fizice/virtuale. 6. Solutia va permite selectarea modulelor componente atunci cand se creaza pachetul clientului care se instalează pe mașinile fizice/virtuale. 7. Solutia va permite lansarea de task-uri de scanare, actualizare, instalare, dezinstalarea la distanta pentru clientul antimalware. 8. Solutia va oferi posibilitatea de repornire a masinilor fizice de la distanta. 9. Solutia va oferi informatii detaliate despre fiecare task si se fiseaza daca task-ul s-a finalizat sau nu cu succes. 10. Solutia va permite configurarea centralizata a clientilor antimalware prin intermediul politicilor 11. Se vor oferi in consola de management informatii detaliate ale obiectelor din consola: Nume, IP, Sistem de operare, Grup, Politica atribuita, Ultimele	**4. Inventarierea retelei – managementul securitatii:** 1. Solutia se integreaza cu domenii Active Directory multiple, VMware vCenter Server, Citrix Xen Server, Nutanix Prism si importa inventarul acestor platforme. 2. Se permite descoperirea statiilor statii fizice neintegrate in Active Directory (Workgroup) cu ajutorul Network discovery. 3. Solutia ofera 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 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 permite instalarea la distanta sau manual a clientilor antimalware pe masini fizice/virtuale. 6. Solutia permite selectarea modulelor componente atunci cand se creaza pachetul clientului care se instalează pe mașinile fizice/virtuale. 7. Solutia permite lansarea de task-uri de scanare, actualizare, instalare, dezinstalarea la distanta pentru clientul antimalware. 8. Solutia ofera posibilitatea de repornire a masinilor fizice de la distanta. 9. Solutia ofera informatii detaliate despre fiecare task si se fiseaza daca task-ul s-a finalizat sau nu cu succes. 10. Solutia permite configurarea centralizata a clientilor antimalware prin intermediul politicilor 11. Solutia ofera 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. 12. Pentru integrarea cu Active Directory, se va putea defini si intervalul (in ore) de sincronizare si forta sincronizarea. 13. Se permite descoperirea masinilor din Microsoft Hyper-V, Red Hat VM, Oracle VM, KVM. 14. Solutia permite descoperirea tuturor aplicatiilor instalate pe toate statiile si serverele din reatea, prin rularea unui task din consola de administrare.	actualizare, Versiunea produsului, Versiunea de semnaturi. 12. Pentru integrarea cu Active Directory, se poate defini si intervalul (in ore) de sincronizare si forta sincronizarea. 13. Se permite descoperirea masinilor din Microsoft Hyper-V, Red Hat VM, Oracle VM, KVM. 14. Solutia permite descoperirea tuturor aplicatiilor instalate pe toate statiile si serverele din reatea, prin rularea unui task din consola de administrare.
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, pool-uri de resourse (VMware), domeniu, unitati organizationale, grupuri de securitate, sau useri de active directoy. 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) h. User-ul logat pe statie i. Etichete definite pe masini virtuale in cloud (disponibile doar prin integrare Amazon EC2 sau MS Azure)	**5. Politici:** 1. Solutia permite configurarea setarilor clientului antimalware prin intermediul unei singure politici ce contine setari pentru toate module 2. Politicile contin 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, pool-uri de resourse (VMware), domeniu, unitati organizationale, grupuri de securitate, sau useri de active directoy. 4. Politica poate fi schimbata automat in functie de: j. IP sau clasa de IP al statiei k. Gateway-ul alocat l. DNS serverul alocat m. WINS serverul alocat n. Sufix DNS pentru conexiunea dhcp o. Clientul este/nu este in acceasi retea cu infrastructura de management (statia de lucru poate solutiona implicit numele gazdei) p. Tipul retelei (lan, wireless) q. User-ul logat pe statie r. Etichete definite pe masini virtuale in cloud (disponibile doar prin integrare Amazon EC2 sau MS Azure)
6. Rapoarte:	**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. 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) **7. Carantina:** 1. Solutia va permite restaurarea fisierelor carantinate in locatia originala sau intr-o cale configurabila.	1. Solutia 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 permite vizualizarea rapoartelor curente programate de administrator. 4. Solutia permite exportarea rapoartelor in format .pdf si detaliile ca format .csv. 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) **7. Carantina:** 1. Solutia permite restaurarea fisierelor carantinate in locatia originala sau intr-o cale configurabila.

2. Carantina va fi locala, pe fiecare statia administrata si va fi administrata, fie local, fie din consola de magement 3. Permite descarcarea fisierelor carantinate doar pentru masinile virtuale protejate prin modulul mediilor virtuale integrat cu VMware vShield.	2. Carantina va fi locala, pe fiecare statia administrata si va fi administrata, fie local, fie din consola de magement 3. Permite descarcarea fisierelor carantinate doar pentru masinile virtuale protejate prin modulul mediilor virtuale integrat cu VMware vShield.
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 solutiei.	**8. Utilizatori:** 1. Administrarea solutiei se 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 permite configurarea detaliata a drepturilor administrative, permitand selectarea serviciilor si obiectelor pentru care un utilizator poate face modificari. 5. Se 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.	**9. Log-uri:** 1. Inregistrarea actiunilor utilizatorilor. 2. Sunt oferite informatii detaliate pentru fiecare actiune a unui utilizator. 3. Se ofera posibilitatea de 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.	**10. Actualizare:** 1. Se permite definirea de locatii de actualizare multiple. 2. Se permite activarea/dezactivarea actualizarilor de produs si semnaturi.

3. Se permite actualizarea produsului intr-o retea fara acces la Internet. 4. Orice client antivirus sa poata fi configurat sa livreze update-urile catre alt client antivirus 5. Solutia dispune un server de actualizare (update) care face posibila stabilirea componentelor ce vor fi descarcate automat de pe internet, fara interventia administratorului. Astfel, administratorul va putea descarca pachetele pentru protectia statiilor si serverelor pe care ruleaza sistemul de operare Windows, Linux, Mac sau, poate descarca pachetele pentru modul de scanare centralizata in mediile de virtualizare VMware, Hyper-V sau Citrix. 6. In cadrul serverului de actualizare, pentru o mai buna urmarire a actualizarilor pachetele pentru protectia statiilor si serverelor sau a pachetelor pentru modul de scanare centralizata, se va putea vizualiza un jurnal de modificari in care sunt precizate istoric: a. versiunea pachetului b. data versiunii c. functii noi si imbunatatiri d. probleme rezolvate e. probleme cunoscute 7. 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) 8. Solutia permite stabilirea zonelor de test si critice din cadrul retelei prin intermediul politicilor din consola de management. **11. Certificate:**	3. Se permite actualizarea produsului intr-o retea fara acces la Internet. 4. Orice client antivirus sa poata fi configurat sa livreze update-urile catre alt client antivirus 5. Solutia dispune un server de actualizare (update) care face posibila stabilirea componentelor ce vor fi descarcate automat de pe internet, fara interventia administratorului. Astfel, administratorul va putea descarca pachetele pentru protectia statiilor si serverelor pe care ruleaza sistemul de operare Windows, Linux, Mac sau, poate descarca pachetele pentru modul de scanare centralizata in mediile de virtualizare VMware, Hyper-V sau Citrix. 6. In cadrul serverului de actualizare, pentru o mai buna urmarire a actualizarilor pachetele pentru protectia statiilor si serverelor sau a pachetelor pentru modul de scanare centralizata, se va putea vizualiza un jurnal de modificari in care sunt precizate istoric: a. versiunea pachetului b. data versiunii c. functii noi si imbunatatiri d. probleme rezolvate e. probleme cunoscute 7. 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: c. Ciclu rapid, gandit pentru un mediu de test in cadrul retelei d. Ciclu lent, gandit pentru restul retelei (productie, servere critice etc) 8. Solutia permite stabilirea zonelor de test si critice din cadrul retelei prin intermediul politicilor din consola de management. **11. Certificate:**

1. Accesul la consola de management sa se faca doar prin HTTPS. 2. Serverul web, din consola centrala de management trebuie sa permita importarea de certificate digitale eliberate de o autoritate de certificare autorizata sau proprie organizatiei. 3. Solutia permite afisarea in consola de management informatii despre certificate: nume, autoritatea emitenta, data eliberarii si data expirarii certificatelor eliberate.	1. Accesul la consola de management sa se faca doar prin HTTPS. 2. Serverul web, din consola centrala de management permite importarea de certificate digitale eliberate de o autoritate de certificare autorizata sau proprie organizatiei. 3. Solutia permite afisarea in consola de management informatii despre certificate: nume, autoritatea emitenta, data eliberarii si data expirarii certificatelor eliberate.
B. PROTECTIE STATII	**II. PROTECTIE STATII**
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 (atacuri directionate).	**1. Caracteristici generale minimale si eliminatorii:** 1. Pentru reducerea la minim a consumului de resurse, solutia antimalware permite instalarea personalizata a modulelor detinute (de exemplu, sa permite 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 (atacuri directionate).
2. Cerinte de sistem: • Sisteme de operare pentru statii de lucru: **Windows11**, **Windows 10, Windows 8/8.1, Windows 7**, **Mac OS Monterey**	**2. Cerinte de sistem mentiune:** • Sisteme de operare pentru statii de lucru: **Windows11**, **Windows 10, Windows 8/8.1, Windows 7**, **Mac OS Monterey**

12.x, macOS BIG SUR 11.x, macOS Catalina 10.15, **Mac OS X Mojave (10.14), Mac OS High Sierra (10.13), Mac OS Sierra (10.12),** • Sisteme de operare embedded: **Windows 10 IOT Enterprise**, **Windows Embedded 8.1 Industry, Windows Embedded 8 Standard, Windows Embedded Standard 7,Windows Embedded POS Ready 7 Windows Embedded POSReady 7, Windows Embedded Enterprise 7** • Sisteme de operare 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.	**12.x, macOS BIG SUR 11.x, macOS Catalina 10.15**, **Mac OS X Mojave (10.14), Mac OS High Sierra (10.13), Mac OS Sierra (10.12),** • Sisteme de operare embedded: **Windows 10 IOT Enterprise**, **Windows Embedded 8.1 Industry, Windows Embedded 8 Standard, Windows Embedded Standard 7,Windows Embedded POS Ready 7 Windows Embedded POSReady 7, Windows Embedded Enterprise 7** • Sisteme de operare Linux: Red Hat Enterprise Linux 7.x, 8.x,9.x, CentOS 7.x, 8.x, Ubuntu 16.04 sau mai recent, SUSE Linux Enterprise Server 12SP4,5, SUSE LINUX Exnterprise15 SP2,SP3, OpenSUSE LEAP 15-2-15.3., Fedora 31 sau mai recent, AWS Bottlerocket 2020.03, Amazon Linux v2, Google COS Milestones 77,81,85, Azure Mariner 2, AlmaLinux 8,9.x, Rocky Linux 8.x, Cloud Linux 7,8.x, Pardus 21, Linux Mint 20.3, Miracle 8.4.
3. Administrare si instalare remote: 1. Inainte de instalare, administratorul va putea particulariza pachetele de instalare cu modulele dorite: firewall, content control, device control, power user. 2. Instalarea se va putea face in mai multe moduri: a. prin descarcarea directa a pachetului pe statia pe care se va face instalarea; b. prin instalarea la distanta, direct din consola de management 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,	**3. Administrare si instalare remote:** 1. Inainte de instalare, administratorul poate particulariza pachetele de instalare cu modulele dorite: firewall, content control, device control, power user. 2. Instalarea se 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 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 sunt disponibile informatii despre fiecare statie: numele statiei, IP, sistem de operare, module instalate,

sistem de operare, module instalate, politica aplicata, informatii despre actualizari etc. 5. Din consola se va putea trimite o singura politica pentru configurarea integrala a clientului de pe statii/servere. 6. Consola va include o sectiune, „Audit", unde se vor mentiona toate actiunile intreprinse fie de administratori fie de reporteri, cu informatii detaliate: logare, editare, creare, delogare, mutare etc. 7. Posibilitatea creari unui singur pachet de instalare, utilizabil atat pentru sistemele de operare pe 32 de biti cat si pentru cele pe 64 de biti. 8. Posibilitatea creari unui singur pachet de instalare, utilizabil pentru statii (fizice si/sau virtuale), servere (fizice si/sau virtuale), 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.	politica aplicata, informatii despre actualizari etc. 5. Din consola se transmite o singura politica pentru configurarea integrala a clientului de pe statii/servere. 6. Consola 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 crearii unui singur pachet de instalare, utilizabil pentru statii (fizice si/sau virtuale), servere (fizice si/sau virtuale), exchange. 9. Posibilitatea crearii pachetelor de instalare de tip web installer sau kit full. 10. Administratorul poate 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	**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 poate alege intre urmatoarele actiuni: a. Actiune imiplicita pentru fisiere infectate: i. interzice accesul ii. dezinfecteaza iii. stergere iv. muta fisierele in carantina v. nicio actiune b. Actiune alternativa pentru fisierele infectate: i. interzice accesul ii. dezinfecteaza iii. stergere iv. muta fisierele in carantina

- 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/SMTP. 7. Configurarea cailor ce urmeaza a fi scanate la cerere. 8. Clientii antimalware pentru workstation sa permita definirea unor liste de excludere de la scanarea in timp real si la cerere a anumitor directoare, discuri, fisiere, extensii sau procese. 9. Cu ajutorul unei baze de date complete cu semnaturi de spyware si a euristicii de detectie a acestui tip de programe, produsul va trebui sa ofere protectie anti-spyware.	c. Actiune imiplicita pentru fisierele suspecte: i. interzice accesul ii. stergere iii. muta fisierele in carantina iv. nicio actiune d. Actiune alternativa pentru fisierele suspecte: i. interzice accesul ii. stergere iii. muta fisierele in carantina 2. Scanarea automata in timp real poate 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 poate anula scanarea in cazul in care sunt detectate unitati care au informatii stocate mai mult de « x » MB. 6. Scanarea automata a emailurilor la nivelul statiei de lucru pentru POP3/SMTP. 7. Configurarea cailor ce urmeaza a fi scanate la cerere. 8. Clientii antimalware pentru workstation sa permita definirea unor liste de excludere de la scanarea in timp real si la cerere a anumitor directoare, discuri, fisiere, extensii sau procese. 9. Cu ajutorul unei baze de date complete cu semnaturi de spyware si a euristicii de detectie a acestui tip de programe, produsul va trebui sa ofere protectie anti-spyware. 10. Posibilitatea de configura scanarile programate sa se execute cu prioritate redusa

10. Posibilitatea de configura scanarile programate sa se execute cu prioritate redusa 11. Produsul antimalware poate fi configurat sa foloseasca scanarea in cloud, si partial scanarea locala. Pentru statiile ce nu au suficiente resurse hardware, scanarea se poate face cu o masina de scanare instalata in retea. 12. Administratorul poate personaliza și motoarele de scanare, având posibilitatea de a alege între mai multe tehnologii de scanare: • Scanare locală, când scanarea se efectuează pe stația de lucru locală. Modul de scanare locală este potrivit pentru mașinile puternice, având toate semnăturile și motoarele stocate local. • Scanarea hibrid cu motoare light (Cloud public), cu o amprentă medie, folosind scanarea în cloud și, parțial, semnături locale. Acest mod de scanare oferă avantajul unui consum mai bun de resurse, fără să implice scanarea locală. • 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) 13. Pentru o protectie sporita, solutia antimalware trebuie sa aiba 3 tipuri de detectie: bazata pe semnaturi, bazata de	11. 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. 12. Administratorul poate personaliza și motoarele de scanare, având posibilitatea de a alege între mai multe tehnologii de scanare: • Scanare locală, când scanarea se efectuează pe stația de lucru locală. Modul de scanare locală este potrivit pentru mașinile puternice, având toate semnăturile și motoarele stocate local. • Scanarea hibrid cu motoare light (Cloud public), cu o amprentă medie, folosind scanarea în cloud și, parțial, semnături locale. Acest mod de scanare oferă avantajul unui consum mai bun de resurse, fără să implice scanarea locală. • 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) 13. Pentru o protectie sporita, solutia antimalware are 3 tipuri de detectie: bazata pe semnaturi, bazata de comportamentul fisierelor si bazata pe monitorizarea proceselor.

comportamentul fisierelor si bazata pe monitorizarea proceselor. 14. Pentru o protectie sporita, solutia antimalware trebuie sa poata scana paginile HTTP si HTTPS. 15. Pentru o mai buna gestionare a antimalware instalat pe statii, produsul va include optiunea de setare a unei parole pentru protectia la dezinstalare. 16. Pentru siguranta utilizatorului, clientul va include un modul de antiphishing. 17. Solutia ofera protectie in timp real pe masinile cu sistem de operare Linux in conformitate cu versiunea de kernel instalata. 18. 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). 19. 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. 20. 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. 21. 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	14. Pentru o protectie sporita, solutia antimalware poate scana paginile HTTP si HTTPS. 15. Pentru o mai buna gestionare a antimalware instalat pe statii, produsul include optiunea de setare a unei parole pentru protectia la dezinstalare. 16. Pentru siguranta utilizatorului, clientul va include un modul de antiphishing. 17. Solutia ofera protectie in timp real pe masinile cu sistem de operare Linux in conformitate cu versiunea de kernel instalata. 18. 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). 19. 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. 20. 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. 21. 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

fi raportate amenintarile care ar fi fost detectate daca nivelul de protectie era stabilit mai agresiv). 22. Pentru a oferi un nivel aditional de protectie a statiilor si serverelor, solutia include un sandbox in cloud-ul public al producatorului acesteia. 23. 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. 24. 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. 25. 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. 26. 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. 27. 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,	detectate daca nivelul de protectie era stabilit mai agresiv). 22. Pentru a oferi un nivel aditional de protectie a statiilor si serverelor, solutia include un sandbox in cloud-ul public al producatorului acesteia. 23. 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. 24. 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. 25. 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. 26. 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. 27. 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.

SCR, URL (binary), VBE, VBS, WSF, WSH, WSH-VBS, XHTML. 28. 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.	28. 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.
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.	**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	**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.	**7. Carantina:** 1. Produsul antimalware permite trimiterea automata a fisierelor din carantina catre laboratoarele antimalware ale producatorului. 2. Trimiterea continutului carantinei poate 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.	3. Produsul antimalware permite stergerea automata a fisierelor carantinate mai vechi de o anumita perioada, pentru a nu incarca inutil spatiul de stocare. 4. Posibilitatea ofera posibilitatea de a restaura un fisier din carantina in locatia lui originala. 5. Modulul de carantina permite rescanarea obiectelor dupa fiecare actualizare de semnaturi. 6. Modulul de carantina 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.	**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.
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).	**9. Controlul continutului:** 1. Consola are 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).
10. Controlul aplicatiilor:	**10. Controlul aplicatiilor:**

1. Pentru o mai buna inventariere si administrare, solutia va include o sectiune in consola de administrare unde se vor regasi toate aplicatiile descoperite in retea, grupate dupa: nume, versiune, descoperit la, gasit pe. 2. Pentru o mai buna inventariere si administrare, solutia va include o sectiune in consola de administrare unde se vor regasi toate procesele negrupate descoperite in retea, grupate dupa: nume, versiune, nume produs, versiune produs, editor/autor, descoperit la, gasit pe. 3. Pentru prevenirea infectarii statiilor si serverelor dar si pentru a permite aplicatiilor descoperite in retea sa se poata actualiza, solutia permite definirea unor programe de actualizare (Updater) care vor fi lasate sa actualizeze diferite aplicatii instalate pe statii sau servere. 4. Solutia include optiunea de a permite sau a bloca rularea anumitor aplicatii sau procese definite de administrator (inclusiv subprocese) dupa: a. Cale fisier: local, CD-ROM, portabil sau retea b. Hash c. Certificat	1. Pentru o mai buna inventariere si administrare, solutia include o sectiune in consola de administrare unde se vor regasi toate aplicatiile descoperite in retea, grupate dupa: nume, versiune, descoperit la, gasit pe. 2. Pentru o mai buna inventariere si administrare, solutia include o sectiune in consola de administrare unde se vor regasi toate procesele negrupate descoperite in retea, grupate dupa: nume, versiune, nume produs, versiune produs, editor/autor, descoperit la, gasit pe. 3. Pentru prevenirea infectarii statiilor si serverelor dar si pentru a permite aplicatiilor descoperite in retea sa se poata actualiza, solutia permite definirea unor programe de actualizare (Updater) care vor fi lasate sa actualizeze diferite aplicatii instalate pe statii sau servere. 4. Solutia include optiunea de a permite sau a bloca rularea anumitor aplicatii sau procese definite de administrator (inclusiv subprocese) dupa: a) Cale fisier: local, CD-ROM, portabil sau retea b) Hash c) Certificat
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	**12. Controlul dispozitivelor:** 1. Modulul poate fi instalat/dezinstalat in functie de preferinta administratorului. 2. Modulul 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. 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).	p) Internal and External Storage 3. Modulul permite configurarea de reguli prin care se vor defini permisiunile pentru dispozitivele conectate la masina client. 4. Modulul permite configurarea de excluderi pentru diferite tipuri de dispozitive pentru care s-au configurat reguli. 5. Modulul 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 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. 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 poate 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. 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